

UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE TECNOLOGÍA

CARRERA ELECTRÓNICA Y TELECOMUNICACIONES



**DISEÑO FÍSICO Y LÓGICO PARA UNA RED DE
INTRANET EN LA FACULTAD DE TECNOLOGÍA**

Proyecto de Grado presentado para obtener el Grado de Licenciatura UMSA.

POR: MARCO ANTONIO USCAMAYTA SUCAZACA

TUTOR: LIC. JULIA TORREZ

La Paz - Bolivia

Agosto 2022

DEDICATORIA

*A Dios por darme fuerza y aliento en la adversidad.
A mis padres francisco Uscamayta. Y Dominga
Sucazaca. Por ser mi fuerza y aliento de superación.*

AGRADECIMIENTO

*Dar gracias a nuestro director de carrera
Lic. Luis Richard Márquez Gonzales por sus
consejos como amigo y como docente.*

*A mi Tutor Lic. Julia Torrez, por su tiempo y
dedicación.*

*A los Docentes de la carrera por
transmitirnos sus valiosos conocimientos.*

Que Dios los proteja y bendiga siempre

Índice

Índice.....	I
Índice De Figuras	IV
Índice De Tablas	VII
Resumen.....	IX
CAPITULO 1.....	1
1.1 Antecedentes	1
1.2 Planteamiento Del Problema	2
1.3 Objetivos	3
1.3.1 Objetivo general	3
1.3.2 Objetivos específicos	3
1.4 Justificaciones.	4
1.4.1 Justificación académica.....	4
1.4.2 Justificación tecnológica.....	4
1.4.3 Justificación económica.	4
1.4.4 Justificación social.	4
1.5 Delimitación De La Investigación.....	4
1.5.1 Delimitación temática	4
1.5.2 Delimitación temporal.....	5
1.5.3 Delimitación espacial.	5
1.6 Metodología De La Investigación Aplicativo	5
CAPITULO 2.....	6
Fundamento Teórico	6
2.1 la Internet.....	6
2.2 La Intranet	7
2.3 Capa de Aplicación (TCP/IP).....	8
2.3.1 Protocolos de la capa de aplicación.	8

2.3.2	Navegadores web.....	9
2.3.3	Servidores Web.....	9
2.3.4	Sitios web.....	11
2.3.5	Diseño web.....	12
2.4	Transporte (Tcp/Ip).....	17
2.4.1	Segmentación y reensamblaje.....	17
2.4.2	TCP (Protocolo de Control de Transmisión).....	17
2.4.3	UDP (Protocolo de Datagramas de Usuario).....	18
2.5	Internet (Tcp/Ip).....	19
2.5.1	Protocolos de capa de red.....	19
2.5.2	Protocolo de Internet versión 4 (IPv4).....	20
2.5.3	División de redes.....	20
2.5.4	Ventajas de la división de redes en grupos.....	21
2.5.5	Direccionamiento IP.....	21
2.5.6	Cálculo de direcciones - división en subredes.....	22
2.6	Enlace De Datos.....	24
2.6.1	Topologías.....	24
2.6.2	Control de enlace lógico (LLC).....	24
2.6.3	Control de acceso al medio (MAC).....	24
2.6.4	Técnicas de control de acceso al medio.....	25
2.6.5	Protocolos de la capa de enlace de datos.....	25
2.6.6	Protocolo de resolución de direcciones (ARP).....	25
2.6.7	Medios.....	26
2.7	Firewall.....	26
2.7.1	Firewall Mangle.....	27

2.8	Control De Ancho De Banda.....	32
2.8.1	Cola simple (Simple Queues).	32
2.8.2	Árbol de cola (Simple Queues).	33
2.9	Red Privada Virtual (VPN)	35
2.9.1	Protocolo de Tunelización de Punto a Punto (PPTP).....	36
CAPITULO 3.....		37
Ingeniería Del Proyecto.....		37
3.1	Capa De Aplicación.....	37
3.1.1	XAMPP	38
3.1.2	Servidor HTTP	43
3.1.3	Servidor DNS	43
3.1.4	Base De Datos	45
3.1.5	Seguridad	49
3.1.6	Sitios Web	56
3.2	Capa De Transporte.....	72
3.2.1	Redireccionamiento de puertos	73
3.2.2	Nat	78
3.3	Capa De Red.....	80
3.3.1	Direccionamiento ip	80
3.3.2	Enrutamiento	85
3.3.3	Enlace de redundancia.....	87
3.4	Capa De Acceso A La Red.....	88
3.4.1	Topología.	88
3.4.2	Bridge.....	89
3.4.3	Control de ancho de banda.....	92

3.4.4	Equipos.....	100
3.4.5	Normas de instalación y cableado estructurado	106
3.5	VPN	108
3.5.1	Protocolo de Tunelización de Punto a Punto (PPTP).....	108
3.5.2	VPN en Mikrotik.....	108
CAPITULO 4.....		112
4.1	Cronograma de implementación	112
4.2	Estructura De Costos	113
4.3	Conclusiones	115
4.4	Recomendaciones	117
Referencias Bibliográficas		119

Índice De Figuras

Figura 1.	Capas Del Modelo Y TCP/IP	6
Figura 2.	Intranet	7
Figura 3.	Página Web	11
Figura 4.	Estructura de una página web	13
Figura 5.	Paquete De Red	19
Figura 6.	Enlace PTP de dos host.....	21
Figura 7.	Apertura de Firewall en Equipos Mikrotik	27
Figura 8.	Reglas de Mangle.....	28
Figura 9.	Acciones de firewall.....	29
Figura 10.	Marca de conexión	30
Figura 11.	Marcado de una nueva conexión.....	31
Figura 12.	Marcado de paquete	31
Figura 13.	Configuración general Simple Queue	32
Figura 14.	Configuración general Simple Queue avanzado	33
Figura 15.	Diagrama de un árbol de cola	33
Figura 16.	Distribución de anchos de banda.....	34

Figura 17.	VPN.....	35
Figura 18.	Aplicaciones Web	37
Figura 19.	Comunicación con Redes Privadas	38
Figura 20.	Acceso de dispositivos móviles al servidor.	39
Figura 21.	Desactivación de XAMPP	41
Figura 22.	Ingreso a la Configuración de Apache	41
Figura 23.	Modificación de capacidad de subida en el Servidor.....	42
Figura 24.	Tamaño máximo de archivos post.....	42
Figura 25.	Modificación de capacidad de memoria para el código.....	42
Figura 26.	Interfaz de noIp	44
Figura 27.	Bases de Datos de la Intranet	45
Figura 28.	Tablas de la Base de Datos Principal	45
Figura 29.	Entrada y salida de anuncios	46
Figura 30.	Estructura BD Principal.	46
Figura 31.	Almacenamiento en B.D. Principal.....	46
Figura 32.	Estructura de Tabla de Logeo	47
Figura 33.	Cifrado de Clave	47
Figura 34.	Tabla Matricula	48
Figura 35.	Base de Datos Para Recursos Audiovisuales	48
Figura 36.	Estructura de la B.D. YouTec	49
Figura 37.	B.D. WikiTec	49
Figura 38.	Sistema encriptado.	50
Figura 39.	Registro HTML.....	50
Figura 40.	Registro PHP.....	52
Figura 41.	Sistemas de Ingreso HTML.	54
Figura 42.	Página Principal de la Intranet	56
Figura 43.	páginas Principales Responsivas.....	57
Figura 44.	Página de Administración Audiovisual.....	60
Figura 45.	Página de Administración Audiovisual Responsiva	61
Figura 46.	Página de administración de archivos	64

Figura 47.	Página de Administración de Archivos Responsiva	65
Figura 48.	Modelo General De Intranet.....	72
Figura 49.	Redireccionamiento de puertos en router de borde.....	73
Figura 50.	Habilitación de puerto 80	74
Figura 51.	Ingreso al NAT de Mikrotik.....	74
Figura 52.	Redireccionamiento de puertos en router de administración	75
Figura 53.	Diagrama de habilitación de puerto 80:	76
Figura 54.	Creación de regla para puerto 80	76
Figura 55.	Especificación de puerto 80 en servidor.	77
Figura 56.	Permisos de conexión.....	77
Figura 57.	Colocamos un nombre a la regla creada	78
Figura 58.	Ingreso a regla de NAT en mikrotik	78
Figura 59.	Configuración de regla de NAT en mikrotik	79
Figura 60.	Enmascaramiento de Dirección IP	79
Figura 61.	Direccionamiento general de la intranet	83
Figura 62.	Asignación de Direcciones ip en Router Mikrotik.....	84
Figura 63.	diagrama de red con direcciones de red	84
Figura 64.	Distribución De Gateway	85
Figura 65.	Creación de rutas Estáticas.....	86
Figura 66.	Topología de red	88
Figura 67.	Puentes en los Enlaces de Enrutamiento.....	89
Figura 68.	Creación de Bridge en Mikrotik.....	90
Figura 69.	Asignación de Interfaces al Bridge	90
Figura 70.	Estructura de la Intranet de la av. Arce	91
Figura 71.	Distribución de Ancho de Banda por Carrera.....	92
Figura 72.	Preroutin En Mangle de Mikrotik	93
Figura 73.	Asociamos mangle con una lista.....	93
Figura 74.	Realizamos la marca de conexión.....	94
Figura 75.	Relación de marca de paquete con la marca de conexión.....	94
Figura 76.	Creamos una marca de paquete.....	95

Figura 77.	Reglas de marcado de conexión y de paquetes	95
Figura 78.	Creación De Un Tipo De Cola Para Control De Ancho De Banda	96
Figura 79.	Queue List	97
Figura 80.	Queue de Bajada y Subida	98
Figura 81.	Configuración De Ancho De Banda Por Carrera	99
Figura 82.	Árbol de colas final	99
Figura 83.	Lista de direcciones.....	100
Figura 84.	servidor DL380p Gen8 Management Server	100
Figura 85.	RB760iGS	101
Figura 86.	RB941-2nd	104
Figura 87.	TPLINK TL-WR941HP.....	104
Figura 88.	Cable Utp CAT 6	105
Figura 89.	Conexión RJ45 normas T568A y T568B.....	106
Figura 90.	diseño de cableado estructurado.....	107
Figura 91.	Habilitación del servicio en router De servicio.....	108
Figura 92.	Creamos un pool de direcciones	108
Figura 93.	Se crea un perfil VPN	109
Figura 94.	Se habilita la compresión y la encriptación.....	109
Figura 95.	Claves secretas	109
Figura 96.	Configuración de VPN en celulares	110
Figura 97.	Configuración de VPN en PC	110
Figura 98.	Activación de las VPN	111

Índice De Tablas

Tabla 1.	Población Universitaria de la Facultad de Tecnología U.M.S.A.	1
Tabla 2.	Diferencia entre Internet e intranet	8
Tabla 3.	Tecnologías Web.....	12
Tabla 4.	Estructura HTML	14
Tabla 5.	estilos CSS más sobresalientes.....	15
Tabla 6.	Encabezado IP	20

Tabla 7.	Dirección ip Binaria	21
Tabla 8.	Dirección ip Decimal	21
Tabla 9.	Trama ethernet.	25
Tabla 10.	Población Universitaria De La Facultad De Tecnología.....	80
Tabla 11.	Cálculo De Numero De Host Por Carrera.....	81
Tabla 12.	VLSM para cada carrera	82

Resumen

Una intranet tiene las mismas funciones que la internet que conocemos hoy en día, con la diferencia de este, solo puede ser accedido por personal autorizado de dicha empresa o corporación, que en nuestro caso será para nuestra facultad.

En el presente proyecto desarrollara una red intranet siguiendo modelo funcional de internet (TCP/IP) paso a paso.

El proyecto comenzara por la capa de aplicación montando un servidor HTTP y un servidor de bases de datos, en el cual estarán alojados un sistema de login encriptado, y los sitios web que nos darán acceso a los recursos del servidor, los cuales serán recursos visuales y audiovisuales. También implementaremos un servidor DNS que nos proporcionara un nombre de dominio.

Se prosigue con la capa de transporte, para habilitar los puertos con los que trabajan los servidores, así de esta manera los usuarios podrán acceder al el, también realizaremos un redireccionaremos los puertos, punto muy importante si queremos que usuarios de otras redes quieran conectarse.

La capa de red proporcionara el direccionamiento de las subredes que tendremos en cada carrera, las cuales calcularemos según la cantidad de estudiantes utilizando VLSM. Por otra parte, realizaremos enrutamientos estáticos con enlaces redundantes para proteger nuestra red de fallos de enlace.

Por último, en la capa de acceso a la red implementa una topología híbrida anillo estrella con enlaces trónceles gigabit, en esta parte realizaremos el control del ancho de banda realizando marcas de conexión, paquetes y árbol de colas, en esta parte también especificaremos las características de los equipos adecuados para nuestra intranet

CAPÍTULO I.

1.1 Antecedentes

La facultad de tecnología de universidad mayor de san Andrés según datos estadísticos proporcionados por DSIE, se tuvo una cantidad de 7278 estudiantes matriculados en la gestión 2020, si bien la red con la que actualmente contamos integra principalmente a las direcciones de carrera y oficinas administrativas de manera general, no se cuenta con un sistema integrado específico a nivel estudiantil la cual nos facilite recursos nuestra población.

Tabla 1. *Población Universitaria de la Facultad de Tecnología U.M.S.A.*

POBLACION UNIVERSITARIA DE LA U.M.S.A.						
FACULTAD TECNOLOGÍA						
	Carrera	2016	2017	2018	2019	2020
1	Electrónica y Telec.	1917	1882	1841	1793	1721
2	Química Industrial	988	1023	1028	1040	1020
3	Mecánica Automotriz	912	957	970	918	897
4	Electromecánica	894	904	900	859	861
5	Aeronáutica	461	542	599	688	743
6	Construcciones Civiles	723	733	726	704	667
7	Topografía y Geodesia	604	616	617	614	602
8	Mecánica Industrial	321	305	303	369	393
9	Electricidad	329	336	332	356	374
Total		7149	7298	7316	7341	7278

Fuente: Departamento de tecnologías de Información y Comunicación-UMSA

Las universidades de hoy en día están en constantes actualizaciones con el fin de poder sacar profesionales competentes y con sólidos conocimientos en su área, por lo que se tienen que implementar nuevas tecnologías para poder impartir una educación adecuada al entorno laboral actual.

El internet y los recursos académicos digitales se han vuelto un pilar fundamental en la educación de hoy en día, el poder acceder a páginas web, clases virtuales, videos educativos en alta velocidad juega un papel muy importante.

Para ello es necesario una red física y lógica acorde con las necesidades de una universidad, mucho más si es tecnológica

La gran competitividad de las universidades de hoy en día hace que elevemos nuestros conocimientos con el fin de presentar a la sociedad grados profesionales, para ello debemos implementar nuevos sistemas de enseñanza y acceso a la información de manera segura, veloz y gratuita en ciertas condiciones que es lo que nos ofrece una intranet.

1.2 Planteamiento Del Problema

En la facultad hay mucho material de excelentes docentes y auxiliares que pueden ser de mucha ayuda al estudiante, pero que lastimosamente no contamos con un lugar de almacenamiento digital donde podamos almacenar, y muchas veces todo este material se queda en el olvido.

Si bien los estudiantes de la facultad de tecnología, y toda la universidad cuentan con el repositorio de la U.M.S.A. no cuenta con material académico de apoyo por semestre y por materia, material que sería de mucha ayuda en el aprendizaje del estudiante.

Debido a que todo el material tecnológico como libros, formularios, solucionarios, revistas, etc. Están en formato digital, así también los recursos audiovisuales como tutoriales, seminarios o clases virtuales están en formato digital, el estudiante tiene la necesidad de una biblioteca digital que ofrece la intranet, donde se almacene todos estos recursos.

Con la llegada de la pandemia se implementó el modelo de enseñanza a distancia, modelo que existía hace años atrás, pero que no era muy popular en nuestro país, este modelo vino para quedarse ya que en cierta manera es más versátil y cómodo. Debido a esto surgió y seguirá surgiendo muchos recursos audiovisuales, en cual deberá ser almacenada, y de uso exclusivo de alumnos de la facultad, servicio que nos brindará la intranet.

Otro problema que se nos presentara es el manejo de la información clasificada y/o comunicados, en la que solo deseamos que sea de conocimiento de cierta unidad académica, estos pueden ser reuniones, asambleas, seminarios, fechas de inscripciones, postulaciones, suspensión de actividades, etc.

A todo lo expuesto en los anteriores párrafos. **¿Cómo la intranet puede mejorar la gestión de los recursos visuales, audiovisuales y programas de computadora, necesarios para el mejor desenvolvimiento de nuestros estudios, sin restricción de ancho de banda o almacenamiento limitantes que nos ofrece la internet?**

1.3 Objetivos

1.3.1 Objetivo general

Diseño físico y lógico para una red de intranet, encargada de gestionar recursos académicos para toda la población universitaria de la facultad de tecnología de forma fácil, segura y veloz.

1.3.2 Objetivos específicos

- Implementar un servidor HTTP de alta velocidad.
- Desarrollar aplicaciones web que puedan gestionar los recursos de las bases de datos del servidor
- Calcular y diseñar un árbol de cola que gestionara el ancho de banda de cada carrera
- Implementar una VPN en la tecnología mikrotik para usuarios remotos

1.4 Justificaciones.

1.4.1 Justificación académica

Con los conocimientos que se recabaron sobre sistemas digitales 1 y 2; en áreas de (diseño de redes lan, y wan) e informática superior 1 y 2 en áreas de (programación web y bases de datos) facilita a la realización de dicho proyecto.

1.4.2 Justificación tecnológica

El acceso a la información de forma segura se lo puede realizar mediante la implementación de nuevas tecnologías como son las VPN`s, y la INTRANET, así como la implementación de lenguajes de programación para la creación de páginas web y bases de datos que almacenen toda la información de la intranet.

1.4.3 Justificación económica.

Montar un intranet para alrededor de 8000 estudiantes no conlleva un fuerte gasto económico, debido a que los equipos para esta cantidad de usuarios no consumen demasiados recursos.

1.4.4 Justificación social.

El proyecto ayudará a toda la población estudiantil de la facultad de tecnología a centralizar todo el material académico de una forma fácil segura y veloz, y esto a su vez ayudará al estudiante a elevar sus conocimientos de una manera más eficiente, por que tendrá toda esta información al alcance de sus manos.

1.5 Delimitación De La Investigación

1.5.1 Delimitación temática

La intranet estará enfocado al manejo de datos de alta velocidad y de forma fácil y segura, para ello debemos de dimensionar muy bien la parte de física y lógica,

En la parte de física los equipos que se usarán en el presente proyecto serán de la tecnología MikroTik, HP y líneas de transmisión gigabit.

En la parte de lógica se hará la implementación de servidores, bases de datos, algoritmos de encriptación de datos y tecnologías de diseño web como HTML, CSS, JS, Y PHP.

1.5.2 Delimitación temporal

El proyecto se lo implementará alrededor de 1 mes, y se pondrá en etapa de prueba durante 3 meses para diagnosticar el rendimiento y capacidad de ancho de banda, posterior a ello, se determinará si es que se tiene que realizar alguna modificación o no.

1.5.3 Delimitación espacial.

La red de intranet estará alojada en las bases de datos de un servidor ubicado el cuarto piso de la facultad de tecnología, carrera que este hará gestión de la intranet.

1.6 Metodología De La Investigación Aplicativo

La investigación aplicada o práctica tiene este nombre debido a que busca aplicar nuestros conocimientos en un proyecto, y a su vez genera más conocimientos por la aplicación real que se realiza.

El concepto de investigación aplicada se basa en el orden del conocimiento humano, al responder a los retos que demanda entender la compleja y cambiante realidad social, el cual se base de distinciones tales como saber y hacer.

En base a este método se podrá explicar el funcionamiento y arquitectura del diseño de la intranet y sus principales características y recomendaciones

Tipo de Estudio Exploratorio: el tipo de estudio que presentará el presente proyecto será el exploratorio, es to debido a que integraremos varias tecnologías tanto de hardware como de software.

Métodos y técnicas de investigación: los fundamentos para el desarrollo de nuestro estudio comenzaran con la previa investigación de las tecnologías ya existentes para luego aplicar el que se adecue más a la orientación del proyecto

CAPÍTULO II.

Fundamento Teórico

2.1 la Internet

La internet es un conjunto de redes de comunicación que están interconectadas entre sí de manera que varias entidades ejerzan el control sobre él. Y está basada en el Modelo TCP/IP

El modelo OSI define los parámetros necesarios para la transferencia de información entre redes. TCP/IP es la arquitectura funcional de Internet el cual solo cuenta de 4 capas, pero su desarrollo fue en base al modelo OSI.

Figura 1. Capas Del Modelo Y TCP/IP



Fuente: Elaboración propia

Con el pasar del tiempo esta tecnología se fue mejorando y popularizándose debido a que ofrecía muchos servicios y beneficios, entre ellos podemos mencionar.

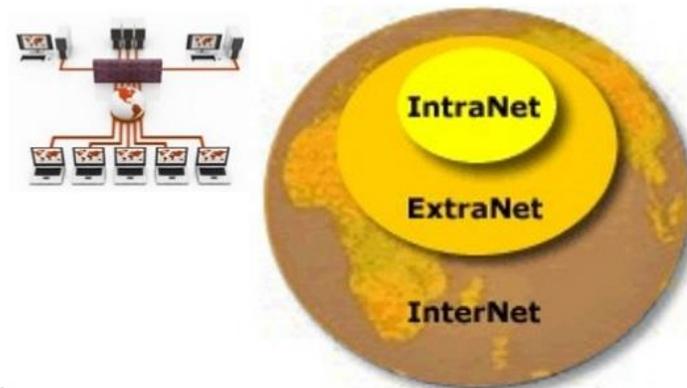
- Acceso remoto de información,

- Transferencia de datos de forma segura,
- Transferencia de audio y video,
- Mensajería instantánea, etc.

2.2 La Intranet

Una intranet es una red interna similar a la internet, solo que, a diferencia de este, solo puede ser accedido por personal autorizado de dicha empresa o corporación.

Figura 2. *Intranet*



Fuente: tecnologia-informatica.com

Una intranet no necesariamente tiene que hacer uso de una nueva infraestructura de red, puede utilizar la infraestructura de red existente.

Para la implementación de una intranet se deberá de hacer algunas modificaciones e implementar dispositivos de red o softwares que sean necesarios.

La intranet es útil para poder difundir cierta información de forma interna u confidencial, interconecta a empleados por medios de host de manera más veloz y eficiente.

Una intranet hace uso de uno o varios servidores que contengan la información, por lo general un pc sería suficiente para funcionar como un servidor. Una intranet al ser del tipo privado es bastante accesible tanto por las personas que carguen y realicen dicha información, así como los consumidores de este medio.

Una intranet no es más que una internet, pero en menor dimensión para ello se debe tomar en cuenta todas las propiedades y características que tiene la internet.

Tabla 2.
Diferencia entre Internet e intranet

Intranet	Internet
Información privada	Información Pública
Solo personal autorizado	No requiere autorización
Internet no es prescindible	El internet es imprescindible

Fuente: Elaboración propia

El proyecto estará en base al sistema funcional de internet TCP/IP.

2.3 Capa de Aplicación (TCP/IP)

Como antes ya se mencionó con anterioridad, la intranet utiliza los mismos protocolos y servicios de la internet. La capa superior de los modelos OSI y TCP/IP proporciona una interfaz entre las aplicaciones con las que interactúa el usuario y las capas inferiores.

Esta capa engloba la capa de presentación y sesión encargadas de codificar, comprimir y encriptar los datos, también es responsable de crear iniciar y finalizar diálogos entre aplicaciones.

2.3.1 Protocolos de la capa de aplicación.

- **DNS:** El protocolo Servicio de nombres de dominio usada para resolver nombres de Internet en direcciones IP.
- **HTTP:** El protocolo de transferencia de hipertexto usada para transferir archivos que forman las páginas Web.
- **SMTP:** El Protocolo simple de transferencia de correo se utiliza para la transferencia de mensajes de correos.
- **Telnet:** usada para proporcionar acceso remoto a dispositivos de red.
- **FTP:** El Protocolo de transferencia de archivos se utiliza para la transferencia interactiva de archivos entre sistemas.

2.3.2 Navegadores web.

El navegador es el encargado de interpretar el código, HTML, CSS, JS, etc. De una página web y lo presenta al usuario de manera que este puede interactuar con la página web.

Google Chrome: Compatible con plataformas como (Windows, MacOS, Android, iOS, Linux.), y es totalmente compatible con los estándares HTML5 y CSS3.

Safari: Navegador de código cerrado compatible con plataformas como Mac OS X, iOS y Microsoft Windows. y los estándares HTML5 y CSS3.

Microsoft Internet Explorer: Compatible con (equipos con Windows) y con los estándares HTML5 y CSS3

Mozilla Firefox: Navegador web libre y de código abierto compatible con (Windows, MacOS, Android, iOS, Linux.) soporta los estándares HTML5 y CSS3.

Opera: Navegador web libre y de código abierto compatible Windows, MacOS, Android, iOS, Linux y FreeBSD. soporta los estándares HTML5 y CSS3

2.3.3 Servidores Web

El servidor web es un componente de un servidor. El servidor es el equipo en que se alojan los sitios web, mientras que el servidor web es un software perteneciente al servidor, encargado de enviar el código HTML a través el protocolo HTTP a los usuarios.

2.3.3.1 Servidor Nginx:

Es un software de código abierto y multiplataforma compatible con Window, IOS, y Linux, se caracteriza por su rapidez en el cargado de páginas Web. En la actualidad es el software para servidores web más usado en el mundo.

2.3.3.2 Servidor Apache:

Apache es un software de código abierto y multiplataforma compatible con sistemas operativos como Linux, Window, IOS entre otros.

2.3.3.3 XAMPP

Es un conjunto de servicios necesarios para que funcione un servidor, por ello su nombre no es más que el acrónimo de: (X) que indica que puede funcionar en cualquier sistema operativo ósea que es multiplataforma, (A) hace referencia al servidor web Apache, (M) referencia a la base de datos MySQL que se utiliza, y por último (PP) que no es más que los intérpretes de lenguaje PHP y Perl

Sistemas operativos: Un sistema operativo es un conjunto de programas que controlan los recursos básicos de un computador, como ser, discos de almacenamiento, periféricos de entradas y salidas como monitor teclado y ratón o también dispositivos externos como impresoras, etc. Ósea un sistema operativo es aquel que controla todo el hardware de cualquier computador.

En la actualidad los sistemas operativos más conocidos son:

- Windows
- Linux
- Mac OS
- Android (teléfonos móviles)

Cabe señalar que solo estamos haciendo referencia de los sistemas operativos de computadores, otros equipos como routers, switch, antenas, etc. también poseen sistemas operativos distintos.

La intranet usara XAMMP que puede ejecutarse en cualquiera de los sistemas operativos mencionados

Apache: Es un servidor web que utiliza protocolo HTTP para transferir páginas web a través de la World Wide Web, esto se logra colocando los archivos web en la raíz de documentos apache que en nuestro caso la carpeta tiene el nombre de htdocs.

Mysql: Es un sistema de bases de datos de código abierto desarrollado por Oracle, la cual presenta una licencia publica y otra comercial.

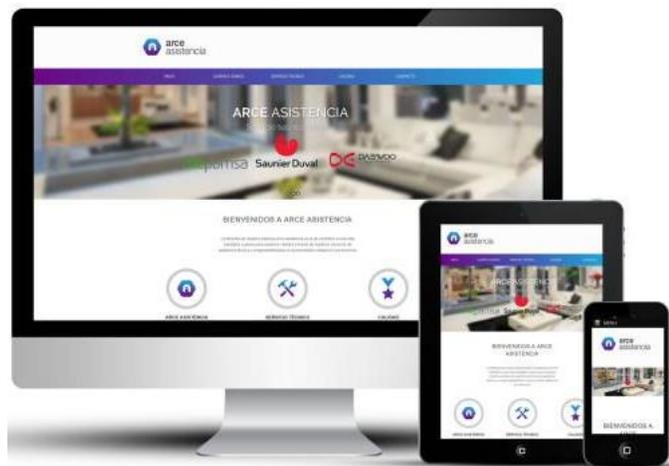
php y perl: Son lenguajes de programación que se ejecutan en servidores web y que se ejecuta en este.

2.3.4 Sitios web.

Para la creación de una intranet necesitamos de la creación de sitios WEB encargadas de interactuar con los usuarios. Para crear painas web se hace uso de lenguajes que programación.

Un sitio web es una página digital, solo que en vez de escribirlo con un bolígrafo se usa un lenguaje de marcado de hipertexto conocido como HTML. Estas páginas son documentos electrónicos que pueden ser almacenados en cualquier computador, desde un simple pc hasta sofisticados servidores.

Figura 3. *Página Web*



Fuente: conceptodefinicion.de

Estas páginas son del tipo cliente servidor, que un servidor proporciona alguna información que pueda interesarle a un cliente. El servidor comparte esta información mediante un servidor Web que como ya dijimos puede ser un simple pc o un potente servidor. Las páginas web pueden ser de dos tipos, estáticos y dinámicos.

Las paginas estáticas solo son capaces de compartir información con el cliente mas no interactuar con él.

Las paginas dinámicas no solo comparten información, también son capaces de interactuar con el cliente.

2.3.5 *Diseño web*

La web está estructurada básicamente con tres tecnologías HTML que nos define la estructura y el contenido de la página, CSS es la que nos define la apariencia y JAVA SCRIPT que define el comportamiento de la página web.

Tabla 3. *Tecnologías Web*

Diseño de página web		Tecnología web
Estructura	Encabezados Párrafos Listas tablas Etc.	HTML
Contenido	Textos Formularios Imágenes Enlaces Etc.	
Apariencia	Fondos Colores Tamaños Bordes Etc.	CSS
Comportamiento	Automatización Validación Etc.	JAVASCRIPT

Fuente: Elaboración propia

2.3.5.1 **Lenguaje de Marcado de Hiper Texto (HTML)**

Lenguaje de Marcado de Hiper texto; Es el código nativo de las páginas web, y en sus inicios era el único lenguaje que se podía utilizar para la creación de páginas

web. Su forma de codificación es bastante simple ya que se lo puede realizar en un editor de texto.

Estructura de una página web

Para la creación de páginas web no existe reglas para crear páginas web, solo existen formatos, uno de los más usados es el formato siguiente:

Este lenguaje puede ser escrito en simple editor de texto, o también se puede hacer uso de un editor de texto como Visual Studio Code, El cual nos ofrece más facilidad al momento de escribir código html.

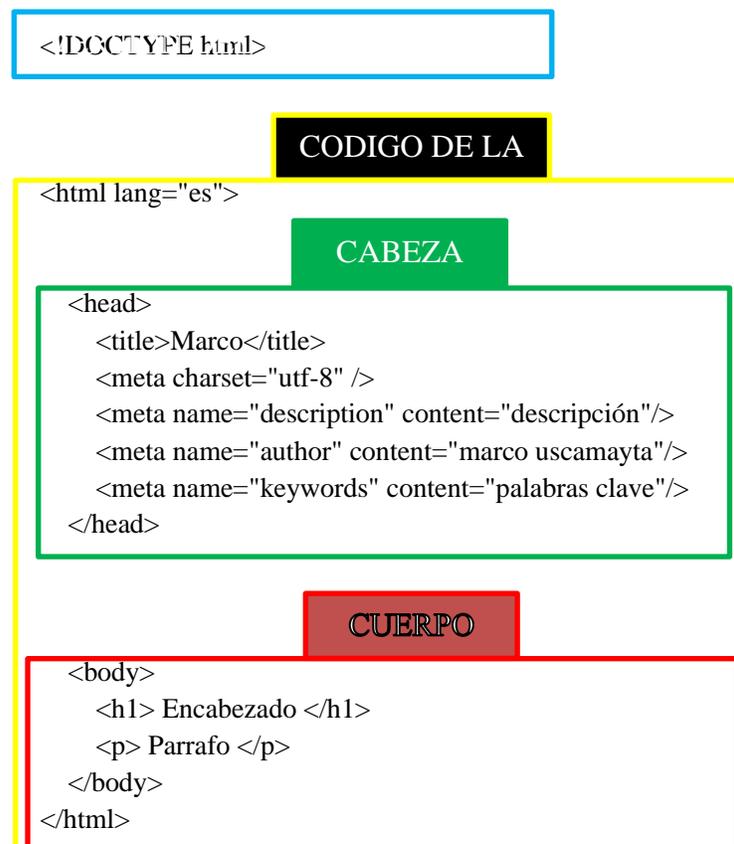
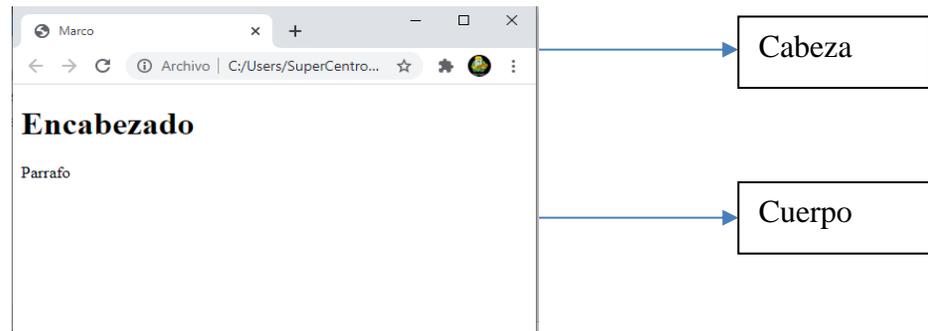


Figura 4. Estructura de una página web



Fuente: Elaboración propia

Tabla 4. Estructura HTML

Código De La Pagina	Etiqueta	Explicación
<code><!DOCTYPE html></code>	<code><!DOCTYPE html></code>	Versión del html
<code><html></code>	<code><html></html></code>	Lenguaje de la pagina
<code><head></code>	<code><title></title></code>	Establece el nombre del documento. Dentro de <head>
<code><title></title></code>		
<code><meta></code>		
<code></head></code>	<code><body></body></code>	Cuerpo del documento
<code><body></code>	<code><header> </header></code>	Cabecera
<code><header></header></code>	<code><nav> </nav></code>	Barra de Navegación
<code><nav> </nav></code>	<code><section></section></code>	contenido principal.
<code><section></section></code>	<code><article></article></code>	detalla un contenido común y repetitivo
<code><article></article></code>	<code><aside></aside></code>	Hace referencia al contenido lateral
<code><aside></aside></code>		
<code><footer></footer></code>	<code><footer></footer></code>	Hace referencia al pie de pagina
<code></body></code>		
<code></html></code>		

Fuente: Elaboración Propia

2.3.5.2 Hojas de Estilo en Cascada CSS

Esta tecnología nos permite dar estilos a nuestro código html, en simples palabras nos ayuda a definir el aspecto de nuestra página web.

Y algunas de sus características son:

Estilos en línea: se coloca estilos como atributo de una etiqueta es poco óptimo ya que nuestro código HTML se haría muy extenso.

```
<header style="background-color: red;">ELECTRONICA</header>
```

Estilos en Selectores

- **Con etiquetas**

```
<style></style>
```

- **Con identificadores: selector** óptimo para trabajar con JS

```
<header id="cabecera"></header>
```

- **Con clases:** reutilizable

```
<header class="cabecera"></header>
```

Archivo CSS. La sintaxis no cambia solo se escribe en un archivo separado y el nombre del archivo para el código siguiente es archivo.css, cabe resaltar que es muy importante crear el archivo con extensión .css.

```
<link rel="stylesheet" href="archivo.css">
```

Tabla 5. *estilos CSS más sobresalientes*

Descripción		Atributo	Propiedad	
Tamaño de letra		Font-size:	25px;	
Estilo de letra		Font-family:	sans-serif;	
Ancho de letra		Font-weight:	initial;	
Posición de la letra		text-align:	Center, left, Right, etc	
Color de fondo		background-color:	lightblue;	
Bordes		border:	5px solid;	
Márgenes	Superior	margin-top:	20px;	
	Inferior	margin-bottom:	20px;	
	Izquierda	margin-left:	20px;	
	Derecha	margin-right:	20px;	
	Centrado	margin:	auto;	
Margen interno		padding:	20px	15;

Fuente: Elaboración propia

2.3.5.3 Java Script JS

Esta tecnología proporciona dinamismo a nuestra página web. El lenguaje HTML tiene restricciones en cuanto a dinamismo se refiere, lo cual es poco práctico para los usuarios de las páginas web.

Los sistemas CMS ofrecen factibilidad a los programadores de páginas web al momento de realizar páginas web, debido a que les ahorra toda la parte de codificación al desarrollar dichas páginas.

La creación de páginas se facilita debido a estos presentan una forma de programación visual, entre estos podemos resaltar a WordPress y Joomla

Tipos de datos

Numéricos

- `var numero = 42.22+10;`

Cadenas de texto

- `texto.length;` // devuelve la longitud de la cadena de texto
- `texto.substring(4);` // elimina los primeros 4 textos de la cadena

Arreglos

- `var arreglo=["marco _____ ","antonio ",12];` //creación
- `document.write(num[2]);` //acceso a valores
- `document.write(num.length);` //longitud del arreglo

Booleanos

- `var val=true;`

Creación de elementos

crear un elemento

- `var elemento=document.createElement("h2");`

crear el contenido

- `var contenido=document.createTextNode("titularrrr");`

Añadir el contenido al elemento

- `elemento.appendChild(contenido);`

2.4 Transporte (Tcp/Ip)

Se encarga de la segmentación de datos y el control necesario reensamblar la información segmentada.

2.4.1 Segmentación y reensamblaje

La segmentación de datos se la realiza debido a que algunas aplicaciones transmiten grandes cantidades de información y estas tienen que fluir a través de un solo medio el cual debe ser accedido por otras aplicaciones.

TCP: contiene un número de secuencia. Este número permite reensamblar los segmentos en el mismo orden en el que fueron enviados.

UDP: no tiene número de secuencia en el encabezado los datos pueden llegar en un orden distinto al que fue enviado, ya que los paquetes pueden tomar diversas rutas a través de la red.

2.4.2 TCP (Protocolo de Control de Transmisión)

Este protocolo es ideal para aplicaciones como base de datos, páginas web y los e-mails, debido a que los datos lleguen tal como han sido enviados

TCP es un protocolo orientado a la conexión, sus funciones son:

- Mismo orden de entrega
- Entrega confiable
- Control de flujo

El protocolo TCP posee 20 bytes de carga en el encabezado, debido a la seguridad de entrega las aplicaciones que usa este protocolo son Exploradores Web, Mensajería y transferencia de archivos.

2.4.2.1 Establecimiento y finalización de la conexión TCP

Establecimiento de la conexión TCP:

- El cliente envía un segmento que contiene un valor de secuencia inicial, que es la solicitud para la conexión.
- El servidor responde con un segmento con un valor igual al valor de secuencia recibido más 1, y además de su propio valor de secuencia de sincronización.
- El cliente que inicia la conexión responde con un valor de reconocimiento igual al valor de secuencia que recibió más uno. Esto completa el proceso de establecimiento de la conexión.

Finalización de la conexión TCP

- El cliente envía un segmento de finalización.
- El servidor recibe el segmento de finalización y envía un acuse de recibido.
- El servidor envía un segmento de finalización.
- El cliente recibe el segmento de finalización, y envía un acuse de recibido.

2.4.2.2 Control del flujo

TCP utiliza tamaños dinámicos de ventana para controlar el flujo de los datos, el receptor puede enviar un valor de ventana conforme a la calidad de la red. Si es que se pierden datos las ventanas serán mas pequeñas, si es una red altamente eficiente los tamaños de ventana serán más grandes.

2.4.3 UDP (*Protocolo de Datagramas de Usuario*)

Este protocolo es utilizado por aplicaciones como sistema de nombres de dominios (DNS), transmisiones de voz.

UDP es un protocolo no orientado a la conexión sus funciones son:

- El orden de entrega no siempre es tal como fue enviado.
- Si un datagrama se pierde no es retransmitido.
- Sin control de flujo

El protocolo UDP posee 8 bytes de carga en el encabezado, debido a su baja sobrecarga es usado por aplicaciones que requieren velocidad de transmisión.

2.5 Internet (Tcp/Ip)

La capa de red es la responsable de entrega de paquetes a través de una o múltiples redes asegura que los paquetes fluyan de forma segura a nivel de red, para realizar este proceso la capa de red utiliza cuatro procesos básicos

- **Direccionamiento:** esta se encarga de proporcionar una dirección de origen y destino a nivel de red a todos los dispositivos finales.
- **Encapsulamiento:** es el proceso de agregar un encabezado de capa 3 a la PDU de la capa de transporte.

Figura 5. *Paquete De Red*



Fuente: Elaboración propia

- **Enrutamiento:** es el proceso de seleccionar rutas y dirigir paquetes hacia su destino.
- **Desencapsulamiento.** Es el proceso en el cual el host extrae el encabezado de capa de red.

2.5.1 Protocolos de capa de red

Los protocolos de capa de red actualmente usados son:

- AppleTalk.

- Protocolo de Internet versión 4 (IPv4).
- Protocolo de Internet versión 6 (IPv6).
- Servicio de red sin conexión (CLNS/DECNet).
- intercambio Novell de paquetes de internetwork (IPX).

2.5.2 Protocolo de Internet versión 4 (IPv4).

Es el protocolo de red más utilizada, provee las funciones necesarias para la transmisión de paquetes a través de la red.

Algunas características de este protocolo es la independencia de los medios, ofrece servicios de mejor intento y sin conexión. Este tipo de protocolo contiene los siguientes campos en su encabezado.

Tabla 6. Encabezado IP

1 byte		1 byte	2 byte	
VERSIÓN	IHL	TIPO DE SERVICIO	LONGITUD TOTAL	
IDENTIFICACIÓN			SEÑALIZADOR	DESPLAZAMIENTO DE FRAGMENTOS
TTL		PROTOCOLO	CHECKSUM DEL ENCABEZADO	
DIRECCIÓN DE ORIGEN				
DIRECCIÓN DE DESTINO				
OPCIONES				

Fuente: Cisco Certified Network Associate (CCNA)

2.5.3 División de redes

Las redes pueden agruparse basadas en factores que incluyen:

- Ubicación geográfica
- Propósito
- Propiedad

2.5.4 Ventajas de la división de redes en grupos

- Mejoramiento del rendimiento
- Seguridad
- Administración de direcciones

2.5.5 Direccionamiento IP

Todo host en la capa de red está identificado por una dirección IP de 32 bits

Figura 6. Enlace PTP de dos host



Fuente: Elaboración propia

Tabla 7. Dirección ip Binaria

Dirección de origen		Dirección de destino	
IP	10101100000100000000010000010100	IP	10101100000100000000010000010000
MASK	11111111111111111111111100000000	MASK	11111111111111111111111100000000

Fuente: Elaboración propia

Pero para las personas es más fácil recordar un numero decimal que uno binario

Tabla 8. Dirección ip Decimal

Dirección de origen		Dirección de destino	
IP	172.16.4.20	IP	172.16.4.16
MASK	255.255.255.0	MASK	255.255.0.0

Fuente: Elaboración propia

2.5.5.1 Tipos de direcciones en una red IPv4

- **Dirección de red:** la dirección en la que se hace referencia a la red, se le asigna la primera dirección de una red.

- **Dirección de broadcast:** una dirección especial utilizada para enviar datos a todos los hosts de la red, se le asigna la última dirección de una red.
- **Direcciones host:** las direcciones asignadas a los dispositivos finales de la red. se le asigna direcciones entre la primera después de la dirección de red y la última antes de la dirección de broadcast.

2.5.5.2 Prefijo de una red o mascara de red

Es el número binario de 32 bits que acompaña a la dirección IP, este nos ayuda a identificar porción de red y porción de host.

/24 → 11111111 11111111 11111111 00000000 → 255.255.255.0

Longitud de prefijo: Es la cantidad de bits en la dirección que conforma la porción de red.

2.5.5.3 Cálculo de direcciones de host, de red y de broadcast

- **Cálculo de la dirección de red:** Se lo calcula realizando un AND con la dirección ip del host y la máscara de red.
- **Cálculo de dirección de broadcast:** Se lo calcula realizando un OR con la dirección de red y la máscara negada.
- **1ra IP utilizable:** Dirección ip después de la dirección de red.
- **Ultima IP utilizable:** Dirección ip antes de la dirección de Broadcast.

2.5.6 Cálculo de direcciones - división en subredes

$$NR = 2^n \quad \text{Donde: } \begin{array}{l} \#R = \text{cantidad de redes requeridas} \\ n = \text{cantidad de bits prestados} \end{array}$$

$$NH = 2^n - 2 \quad \text{Donde: } \begin{array}{l} NH = \text{cantidad de hosts por subred} \\ n = \text{bits de la porcion de red} \end{array}$$

2.5.6.1 FLSM (Máscara de Subred de Longitud Fija)

Se caracteriza por utilizar una máscara de subred de tamaño fijo para todas las subredes, una de las ventajas que tiene esta forma de calcular subredes es su simplicidad, y la desventaja es que al tener una longitud fija puede desperdiciar direcciones, ya que el cálculo de su prefijo está en función a la potencia cuadrada superior de la subred que tenga más demanda de host.

2.5.6.2 VLSM (Máscara de Subred de Longitud Variable)

- VLSM permite dividir un espacio de red en partes desiguales
- La red se divide en subredes y a continuación las subredes se vuelven a dividir en subredes
- Se recomienda iniciar con subredes que tengan mayor demanda de host

una red cuando se convierte muy grande conviene dividirla para reducir los dominios de broadcast.

2.6 Enlace De Datos

La capa de enlace de datos es la responsable de entrega de tramas en una red local común.

2.6.1 Topologías

Son configuraciones de conexiones físicas y nodos, las más sobresalientes son:

- **Topología punto a punto:** Configuración punto a punto que conecta dos nodos de forma directa, sea física o lógicamente.
- **Topología en anillo:** Configuración multipunto Interconecta varios nodos mediante una línea de conexión de forma punto a punto solo con los nodos de sus lados.
- **Topología bus:** Configuración multipunto interconecta varios nodos mediante una línea troncal.

2.6.2 Control de enlace lógico (LLC)

Estándar:

- Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC.

Funciones:

- Entrama el paquete de la capa de red.
- Se encarga de la comunicación entre las capas superiores (**software**) y las capas inferiores (**hardware**).
- Identifica qué protocolo de capa de red está siendo utilizado por la trama.
- Cumple funciones de corrección de errores

2.6.3 Control de acceso al medio (MAC)

Estándar:

- Para Ethernet, el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física.

Funciones:

- Proporciona direcciones a los distintos nodos para que puedan ser identificados a nivel enlace.
- Delimita los datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

2.6.4 Técnicas de control de acceso al medio

- **Acceso controlado:** los nodos deberán turnarse para acceder al medio.
- **Acceso contención:** permiten que cualquier dispositivo intente acceder al medio. Para evitar colisiones en los medios, estos métodos usan un proceso de Acceso múltiple por detección de portadora con detección de colisión (CSMA/CD) y Prevención de colisión (CSMA/CA).

2.6.5 Protocolos de la capa de enlace de datos

En esta capa se pueden encontrar diversos protocolos debido a la gran variedad de medios de transmisión que existen. Se podría decir que existe un protocolo distinto para cada medio de transmisión.

Tabla 9. Trama ethernet.

Encabezado			Paquete	Tráiler	
Iniciar trama	Dirección	Tipo/ longitud	Datos	FCS	Detener trama

Fuente: Cisco Certified Network Associate (CCNA)

2.6.6 Protocolo de resolución de direcciones (ARP)

- Una trama necesita direcciones MAC de origen y destino para ser colocado en una red LAN.

- Cuando se envía un paquete a la capa de Enlace de datos, el nodo (PC) consulta la tabla ARP. Esta tabla se denomina tabla ARP o caché ARP y esta tabla se almacena en la RAM del dispositivo.
- Cada entrada o fila de la tabla ARP tiene un par de valores: una dirección IP y una dirección MAC. La relación entre los dos valores se denomina mapa
- Si este mapa está almacenado en la tabla, el nodo utiliza la dirección MAC como la MAC de destino en la trama que encapsula el paquete IPv4. La trama se codifica entonces en los medios de la red.

2.6.7 Medios

Los elementos físicos son los dispositivos electrónicos de hardware, medios y conectores que transmiten y transportan las señales para representar los bits.

Los medios de mayor uso son:

Cables de par trenzado

- (UTP) o cable de par trenzado sin blindaje:
- (STP) o cable de par trenzado blindado individual:
- (FTP) o cable de par trenzado apantallado

Fibraoptica

- Monomodo
- Multimodo

Medios inalámbricos

- Microondas

2.7 Firewall

Es una función diseñada para bloquear el acceso no autorizado en redes LAN hacia el internet, o desde el internet hacia nuestra red LAN.

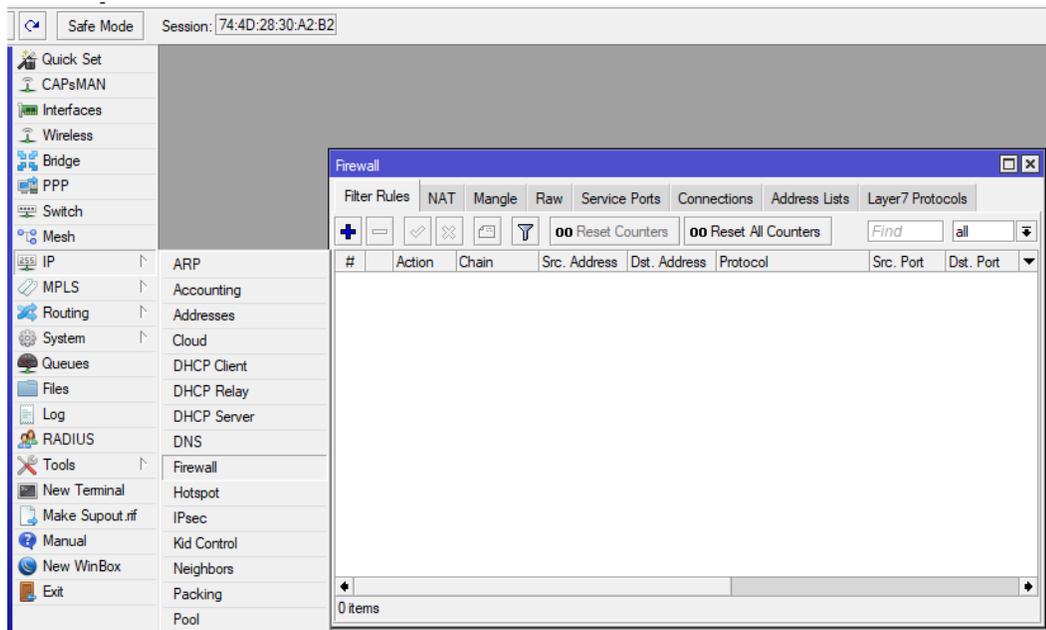
Las principales cadenas de firewall son:

- **Input:** Trafico que tenga como fin al router (webfig, winbox, ping al router, etc.)

- **Output:** Tráfico que genero el router y esta de salida (un ping del router hacia lan, dhcp del router a la lan).
- **Forward:** es el tráfico que pasa por el router simplemente cuando intento acceder a una página o algún juego etc.

En los equipos Mikrotik lo encontraremos en la pestaña de IP.

Figura 7. *Apertura de Firewall en Equipos Mikrotik*



Fuente: Elaboración propia

En el apartado de mangle tenemos varias opciones, nos enfocaremos más en el marcado de paquetes.

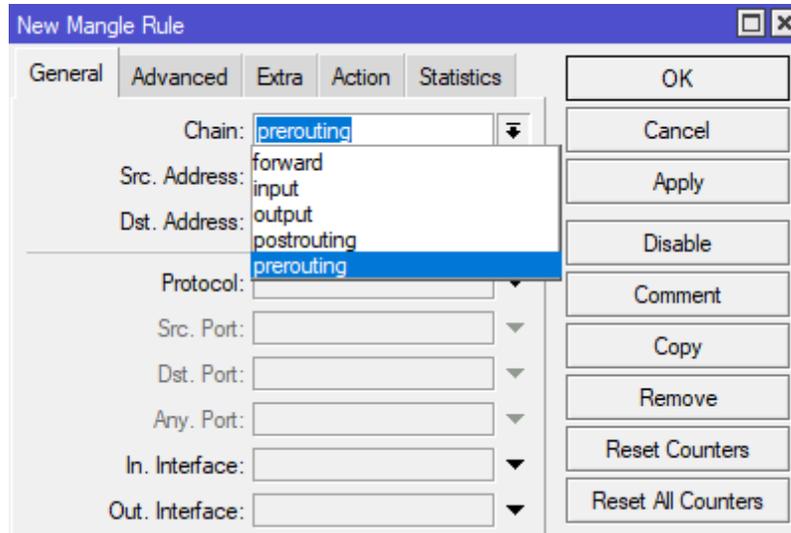
2.7.1 *Firewall Mangle*

Esta función permite marcar los paquetes IP, estas marcas son usadas por configuraciones el router como ruteo y admiración de ancho de banda para identificar los paquetes

Entre otras funciones permite modificar los campos TOS (DSCP) y TTL de la cabecera IP, como los campos.

Estas reglas de mangle están divididas en 5 cadenas en cadenas, estas cadenas están en la opción de (chain)

Figura 8. Reglas de Mangle

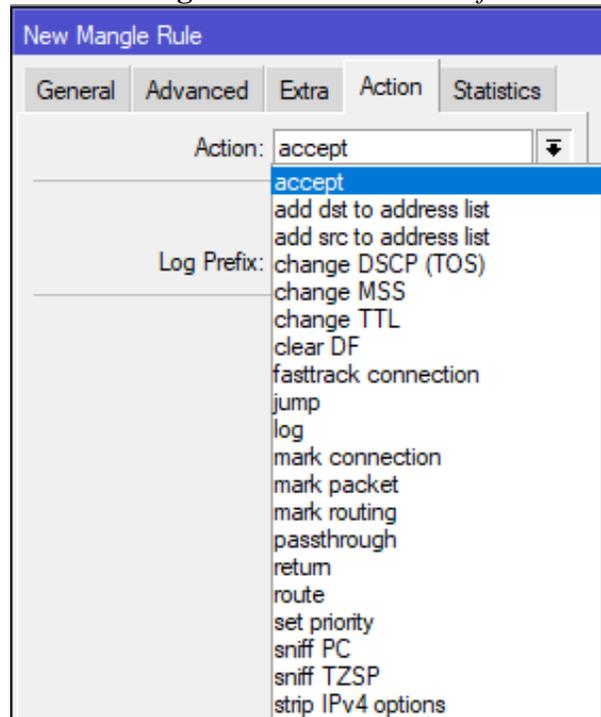


Fuente: Propio

Cadenas:

- **Prerouting:** marca los paquetes del tráfico de entrada al router que posterior saldrá a la internet o intranet. o sea, se refiere al tráfico que está entrando al router y que todavía el router no ha tomado una decisión de ruteo sobre ese tráfico.
- **Postrouting:** marca los paquetes del tráfico de afuera del internet o de la intranet y posterior ingresara a la red lan ó sea se refiere al tráfico que ya ha pasado por el router y que el mismo ya ha tomado la decisión de ruteo para ese tráfico.
- **Input:** marca de paquete antes del filtro de entrada
- **Output:** marca de paquete antes del filtro de salida
- **Forward:** marca de paquete antes del filtro Forward

Figura 9. *Acciones de firewall*



Fuente: Elaboración propia

Acciones

- **Mark connection** : marca la conexión del primer paquete
- **Mark packet** : marca un flujo de todos los paquetes.
- **Mark routing** : marca los paquetes para configuraciones de ruteo
- **Change MSS** : cambia el tamaño máximo del segmento del paquete
- **Change TOS** : cambia el tipo de servicio
- **Change TTL** : cambia el tiempo de vida de los TTL.

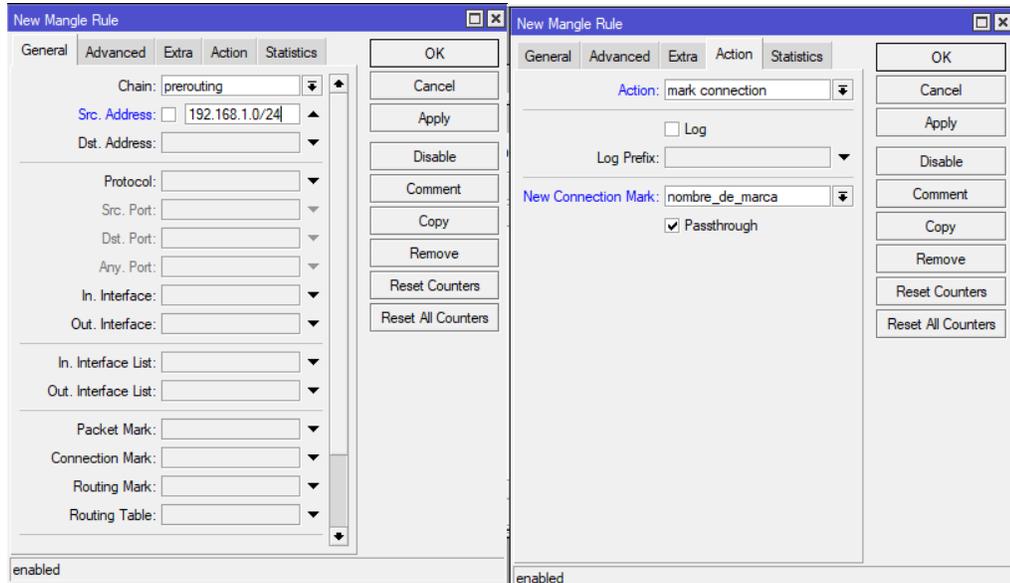
2.7.1.1 Marcado de Conexión (Mark connection)

Este marcado se la realiza a la conexión y esta marca se propaga a los demás paquetes de la misma conexión, y estas son almacenadas en connection tracking, solo puede haber una sola marca para una conexión.

En el siguiente ejemplo veremos el tráfico que esta entrando al router de una la dirección de red 192.168.1.0/24 y la marcamos la conexión con el nombre “nombre_de_conexion”, también podríamos colocar una dirección de destino,

ósea los paquetes que vienen desde una subred hacia una red en específico, y muchas otras condicionales mas como los protocolos a usar y puertos de destino etc.

Figura 10. *Marca de conexión*



Fuente: Propio

2.7.1.2 Marcado de Conexión (Mark packet)

Se aplican a un paquete en específico y no se propagan a otros paquetes de la una misma conexión.

2.7.1.3 Marcado de Conexión y paquete

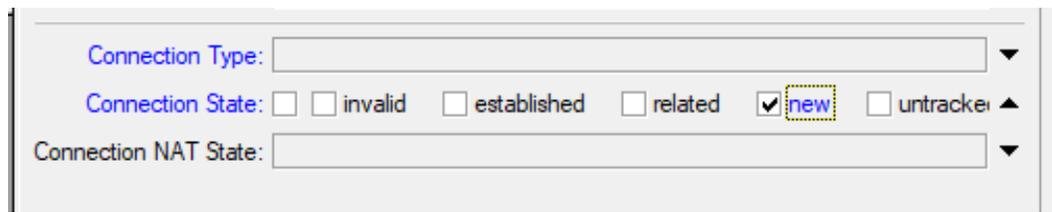
La configuración se la realiza de la misma manera solo que en la opción de acción seleccionamos mark packet.

Si realizamos el marcado de conexión y luego el marcado de paquete puede hacer más eficiente la red, ya que si solo hacemos la marca de paquete lo hará a todos los paquetes uno por uno, en cambio si realizamos el marcado de conexión y luego

el de paquete, se marcará el primer paquete de una conexión y la propagará a los demás paquetes de esa conexión.

También para que esto funcione deberemos consultar si el paquete está iniciando una nueva conexión.

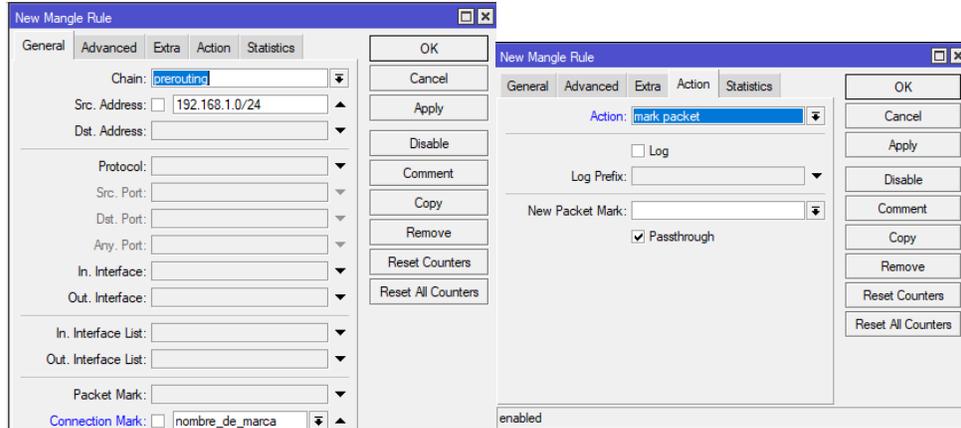
Figura 11. *Marcado de una nueva conexión.*



Fuente: Elaboración propia

Ahora si procedemos a realizar el marcado de paquete claro que también seleccionando la marca de conexión.

Figura 12. *Marcado de paquete*



Fuente: Propio

Realizar el marcado de conexión y luego el de paquete nos traera veneficios siempre y cuando tengamos tengamos que verificar de cada paquete mas de 3 parametro.

En nuestro ejemplo solo estamos verificando la direccion de origen, asi que es indistinto si marcamos solo los paquetes y no la conexión.

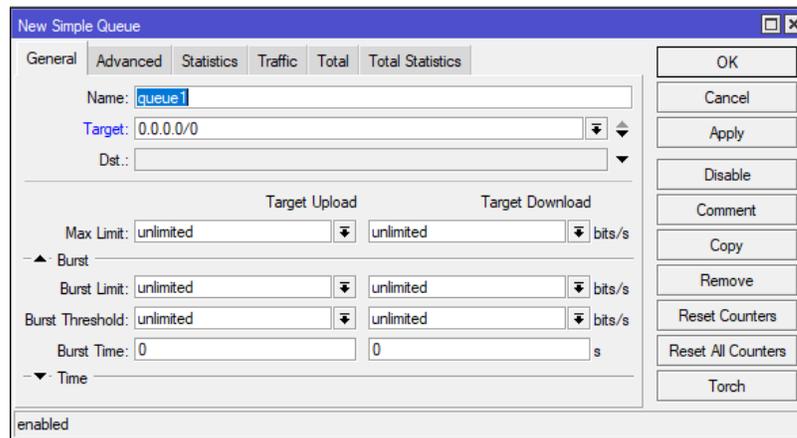
2.8 Control De Ancho De Banda

2.8.1 Cola simple (Simple Queues).

Es una manera sencilla de controlar el tráfico de nuestra red con simples reglas de prioridad hacia una IP. O una red específica.

Estas reglas te permiten establecer un límite de ancho de banda máximo y un ancho de banda garantizado:

Figura 13. Configuración general Simple Queue

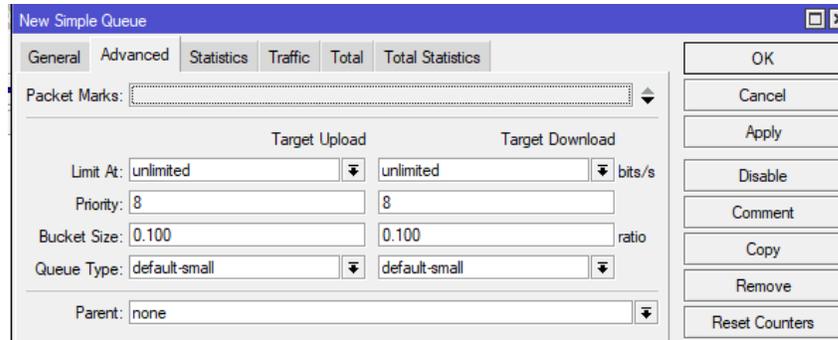


Fuente: Elaboración propia

Name: colocamos el nombre de la regla o simplemente a quien pertenece la dirección ip.
target: aquí colocaremos la dirección ip o la red a la que estamos limitando el ancho de banda

Max Limit. Aquí colocaremos el ancho de banda máximo de bajada y subida que le daremos a esa dirección ip, ese ancho de banda máximo se alcanzara siempre y cuando nadie este usando la red. y en el modo avanzado se configura el ancho de banda garantizado y la prioridad que tendrá esa direccion ip, siendo 1 la máxima prioridad y 8 la prioridad más baja.

Figura 14. Configuración general Simple Queue avanzado

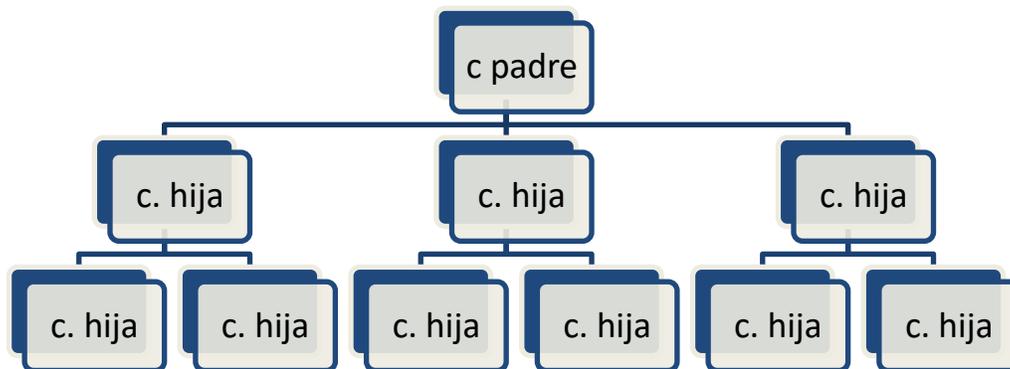


Fuente: Elaboración propia

2.8.2 Árbol de cola (Simple Queues).

Mikrotik se basa en el algoritmo Hierarchical Token Bucket para ofrecer calidad de servicio, este algoritmo permite crear una estructura jerárquica colas, con niveles de prioridad diferentes, esta estructura establece relación entre las colas padre e hijo, hijo e hijo.

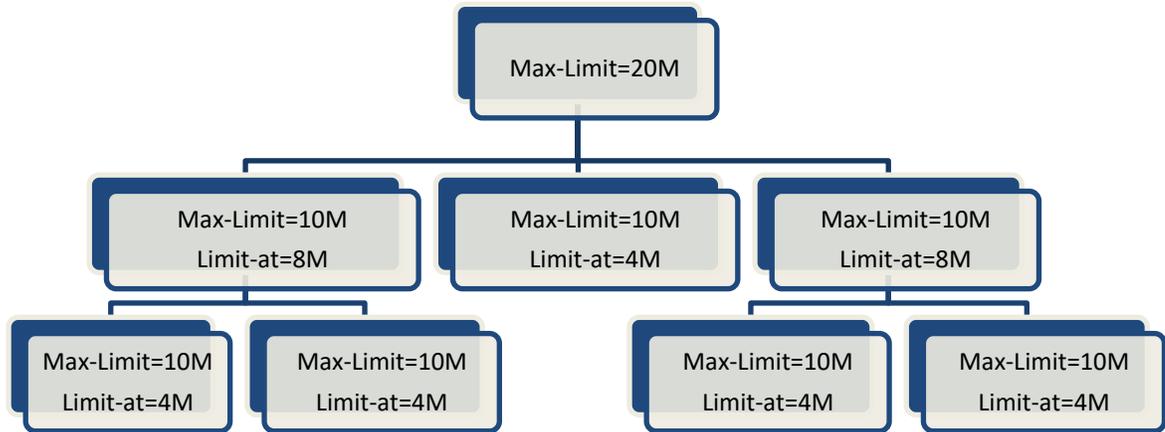
Figura 15. Diagrama de un árbol de cola



Fuente: Elaboración Propio

Las colas padres reparten el tráfico a las hijas que son las que van a consumir el tráfico, estas primero lograrán satisfacer primero el limit-at, y el tráfico restante la cola padre las repartirá.

Figura 16. *Distribución de anchos de banda*



Fuente: Elaboración Propio

El grafico anterior muestra como la cola padre tiene un ancho de banda máximo de 20Megas, este a su vez tiene tres colas hijas las cuales pueden alcanzar un ancho de banda máximo de 10Megas en caso de que nadie más este haciendo uso de él, también tenemos otro parámetro que es el limit-at que es el que nos entrega un ancho de banda garantizado, la cual la sumatoria de todos los anchos de banda garantizados no debe sobre pasar el ancho de banda del padre.

Implementación

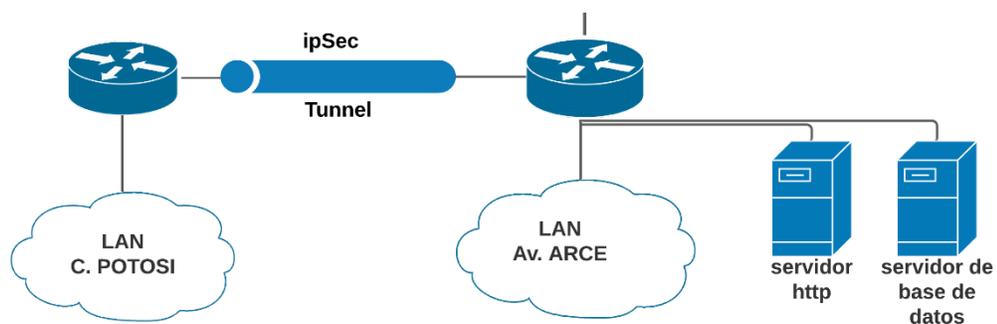
Para implementar la distribución de ancho de banda por árbol de colas necesitamos seguir los siguientes pasos.

- Marcar conexiones
- Marcar paquetes
- Crear una cola padre de bajada
- Crear una cola padre de subida
- Crear las colas hijas de bajada
- Crear las colas hijas de subida

2.9 Red Privada Virtual (VPN)

El VPN nos ayuda a interconectarnos en dos puntos de redes distintas como si estuviéramos en la misma red LAN, el sistema oculta nuestra dirección IP y nuestros datos a través de la Internet, esto lo realiza con un túnel privado

Figura 17. VPN



Fuente: Elaboración propia

Una vez nos conectamos al servicio o a la VPN, este oculta nuestra dirección IP y ubicación reales. Este sistema se hizo muy popular ya que permite a los usuarios navegar en otros países como si estuvieran en su propio país.

La intranet es una tecnología que puede funcionar tanto privada como pública, pero el fin de usar esta tecnología es la de resguardar nuestra información, de tal manera que ningún buscador lo pueda encontrar, y así la información que tengamos solo será vista por personal autorizado que este dentro de la intranet.

El acceso es un tema sumamente importante en el desarrollo de nuestra intranet ya que empleados necesitaran hacer consultas sobre cierta información. Para ellos necesitaríamos que realicen autenticaciones para ellos utilizaríamos VPN o radius

2.9.1 Protocolo de Tunelización de Punto a Punto (PPTP)

PPTP protocolo de tunelización que opera en el puerto TCP 1723, es uno de los protocolos, fue desarrollado por Microsoft para encapsular el Protocolo Punto a Punto (PPP).

Es un protocolo muy común y fácil de configurar, rápido. Por esa razón, el PPTP tiene su uso en aplicaciones en la que se requiere velocidad, como ser streaming de audio o video.

Sin embargo, el PPTP al ofrecer velocidad talvez tiene una debilidad es que ya fue descifrado su sistema de seguridad.

CAPÍTULO III.

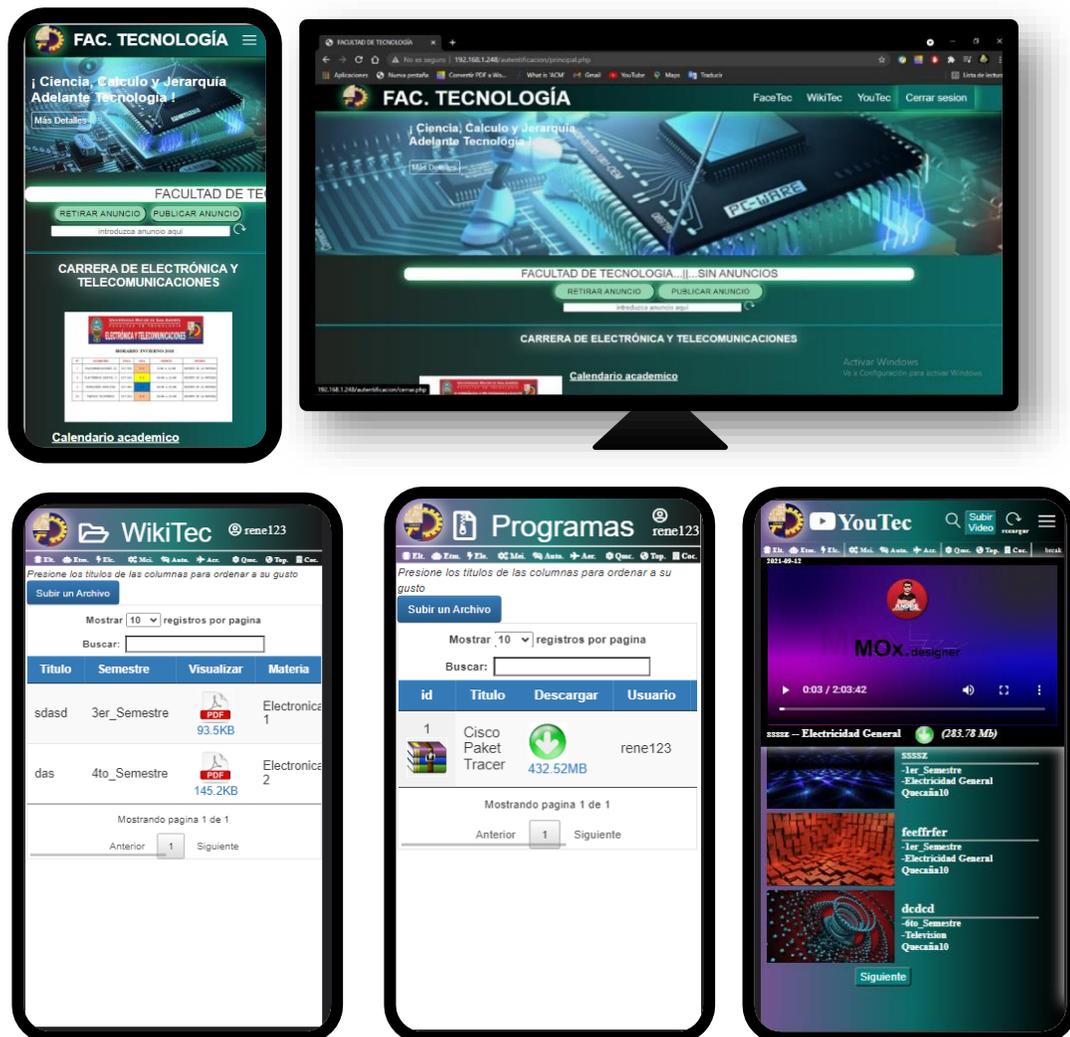
Ingeniería Del Proyecto

El desarrollo del proyecto se basará en el modelo funcional de Internet (TCP/IP), e implementaremos los protocolos y características de cada capa.

3.1 Capa De Aplicación

En esta capa desarrollaremos la interfaz con la que el usuario interactuara con servidor y con las bases de datos.

Figura 18. Aplicaciones Web



Fuente: Elaboración propia

3.1.1 XAMPP

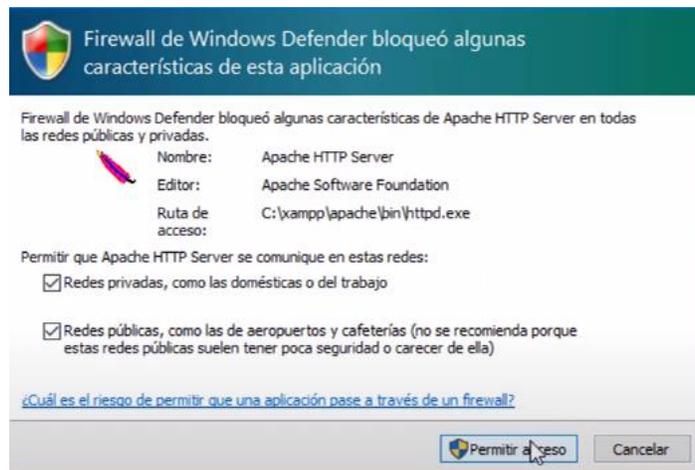
Para el desarrollo de una intranet se necesita un conjunto de servicios para nuestro servidor. XAMPP nos servicios de:

- Servidor HTTP.
- Servidor de Bases de Datos (MySQL)
- Intérpretes de lenguaje PHP

3.1.1.1 Configuraciones del servidor XAMPP

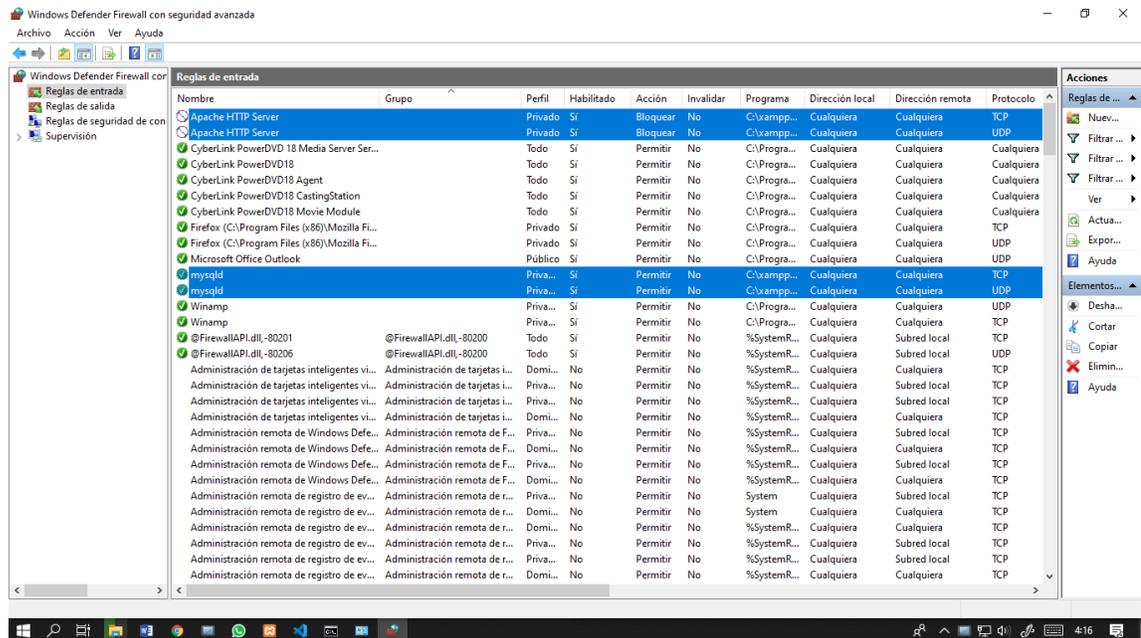
Al momento de instalar XAMPP es de vital importancia permitir que apache HTTP server ser pueda comunicarse con redes privadas debido a que la intranet es de carácter privado.

Figura 19. Comunicación con Redes Privadas



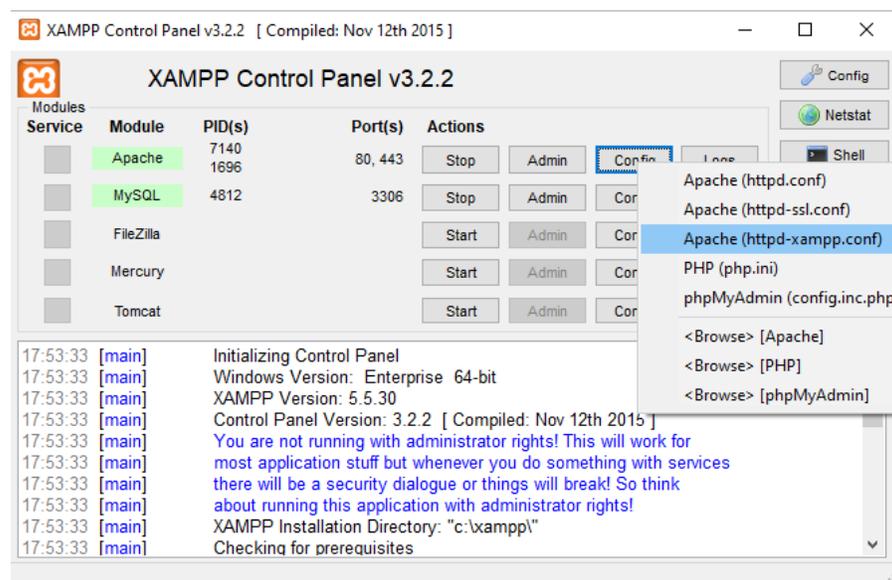
Fuente: Elaboración propia

3.1.1.2 Eliminar reglas de entrada de firewall de windows



3.1.1.2.1 Acceso De Dispositivos Móviles Al Servidor: El servidor por defecto tiene inhabilitada la conexión de dispositivos móviles, por lo que se deberá realizar unas configuraciones en el apache server.

Figura 20. Acceso de dispositivos móviles al servidor.



Fuente: Elaboración propia

En el archivo de texto que se nos abrió debemos remplazar el texto 1 por el texto 2, estos comandos nos darán los permisos necesarios para que dispositivos móviles puedan conectarse a la red de intranet.

Texto 1

```
#
# New XAMPP security concept
#
<LocationMatch “^(?i(?:xampp|security|licenses|phpmyadmin|webalizer|server-
status|server-info))”>
Require local
ErrorDocument 403 /error/XAMPP_FORBIDDEN.html.var
</LocationMatch>
```

Texto 2

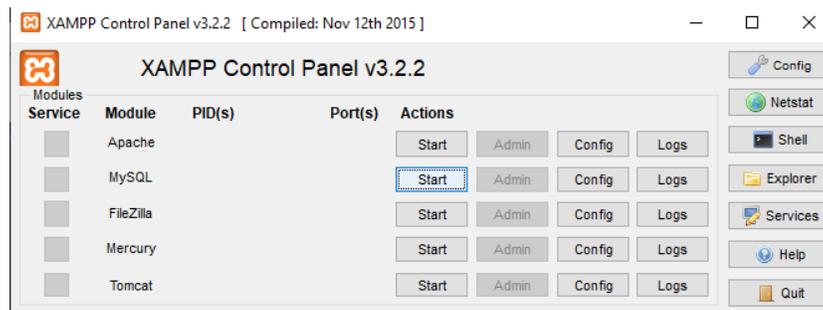
```
#
# New XAMPP security concept
#
# Close XAMPP security section here
<LocationMatch “^(?i(?:security))”>
Order deny,allow
#Deny from all
#Allow from ::1 127.0.0.0/8
Allow from all
ErrorDocument 403 /error/HTTP_XAMPP_FORBIDDEN.html.var
</LocationMatch>
# Close XAMPP sites here
<LocationMatch “^(?i(?:xampp|licenses|phpmyadmin|webalizer|server-
status|server-info))”>
Order deny,allow
#Deny from all
#Allow from ::1 127.0.0.0/8
Allow from all
ErrorDocument 403 /error/HTTP_XAMPP_FORBIDDEN.html.var
</LocationMatch>
```

3.1.1.2.2 Aumentar El Límite De Datos De Subida De Archivos A La Base De Datos:

XAMPP por defecto tiene un límite de datos de subida que es de 2MB lo cual modificaremos, ya que la subida de datos que realizaremos sobrepasará ese límite fácilmente.

Primero se desactiva el servidor.

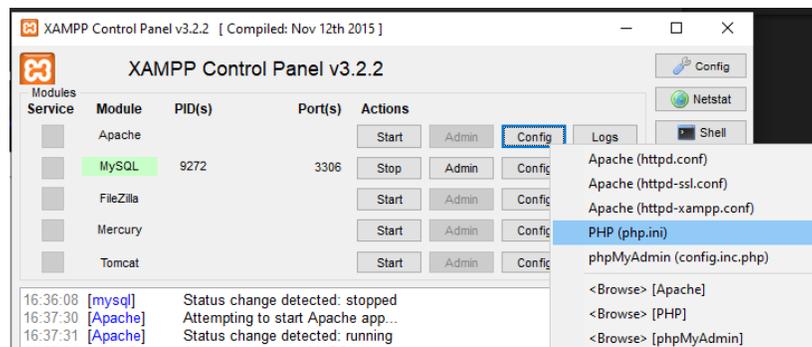
Figura 21. Desactivación de XAMPP



Fuente: Elaboración propia

Posteriormente se ingresa a la pestaña de configuraciones y a la opción de PHP (php.ini).

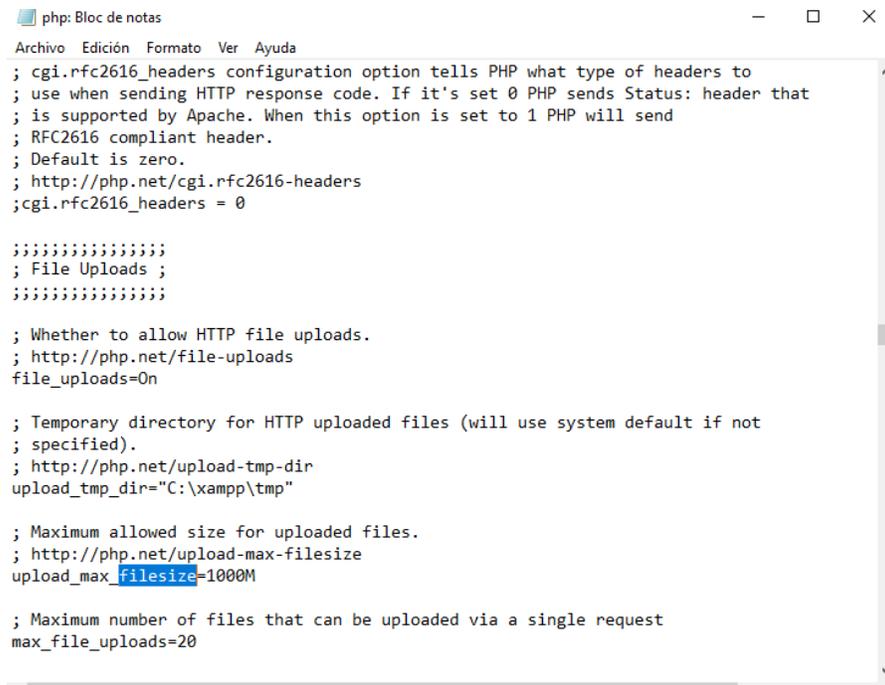
Figura 22. Ingreso a la Configuración de Apache



Fuente: Elaboración propia

Y en este script en la parte donde indica upload_max colocaremos 1000M, limitando así el límite de subida de archivos a la base de datos con un valor de 1000 Mb o 1Gb.

Figura 23. *Modificación de capacidad de subida en el Servidor*



```
php: Bloc de notas
Archivo Edición Formato Ver Ayuda
; cgi.rfc2616_headers configuration option tells PHP what type of headers to
; use when sending HTTP response code. If it's set 0 PHP sends Status: header that
; is supported by Apache. When this option is set to 1 PHP will send
; RFC2616 compliant header.
; Default is zero.
; http://php.net/cgi.rfc2616-headers
cgi.rfc2616_headers = 0

;;;;;;;;;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
; http://php.net/file-uploads
file_uploads=On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; http://php.net/upload-tmp-dir
upload_tmp_dir="C:\xampp\tmp"

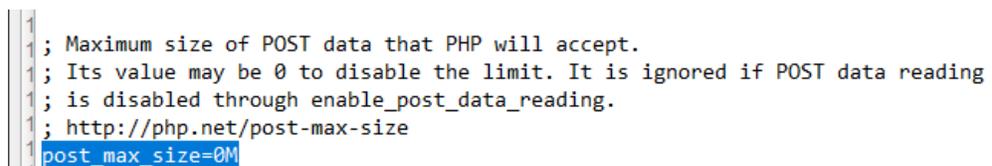
; Maximum allowed size for uploaded files.
; http://php.net/upload-max-filesize
upload_max_filesize=1000M

; Maximum number of files that can be uploaded via a single request
max_file_uploads=20
```

Fuente: Elaboración propia

También haremos una modificación en la cantidad máxima de memoria que puede consumir un script y lo colocaremos en (256 MB).

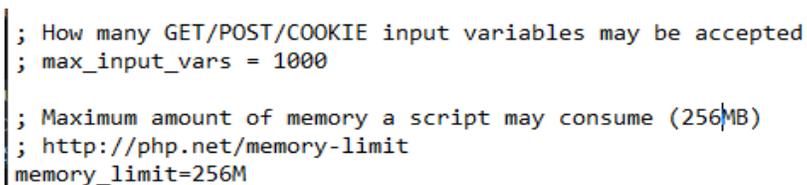
Figura 24. *Tamaño máximo de archivos post*



```
1 ; Maximum size of POST data that PHP will accept.
2 ; Its value may be 0 to disable the limit. It is ignored if POST data reading
3 ; is disabled through enable_post_data_reading.
4 ; http://php.net/post-max-size
5 post_max_size=0M
```

Fuente: Elaboración propia

Figura 25. *Modificación de capacidad de memoria para el código*



```
; How many GET/POST/COOKIE input variables may be accepted
; max_input_vars = 1000

; Maximum amount of memory a script may consume (256MB)
; http://php.net/memory-limit
memory_limit=256M
```

Fuente: Elaboración propia

3.1.2 Servidor HTTP

El Servidor HTTP que usaremos en nuestra Intranet y que viene con los servicios que nos brindó XAMPP es **Apache Server**.

3.1.2.1 Apache Server.

Es un servidor web seguro, eficiente y escalable que proporcione servicios de lenguaje de hipertexto.

Rendimiento:

Apache tiene una arquitectura para trabajar en multiprocesamiento y esta pensado en reducir la latencia y aumentar el rendimiento del servidor para así poder responder a todas las solicitudes de los usuarios de forma simultáneas.

3.1.3 Servidor DNS

Ya tenemos conocimiento que es más fácil recordar un nombre que una dirección ip, por lo que será necesario un servidor DNS.

Para ello usaremos un servidor DNS gratuito llamado No-IP, este permite identificar nuestra PC con un nombre de dominio. Un nombre de dominio es una cadena de caracteres utilizada para referirnos a una dirección ip de un host.

Este servidor tiene los siguientes planes

DNS dinámico gratuito

- Dominios Limitados
- 3 nombres De Host
- Confirmar Cada 30 Días

DNS dinámico mejorado

\$ 24.95 / año

- Más De 25 Nombres De Host
- Los Hosts Nunca Caducan
- Más De 80 Opciones De Dominio

- Incluye 1 Certificado SSL TrustCor Standard DV

DNS administrado

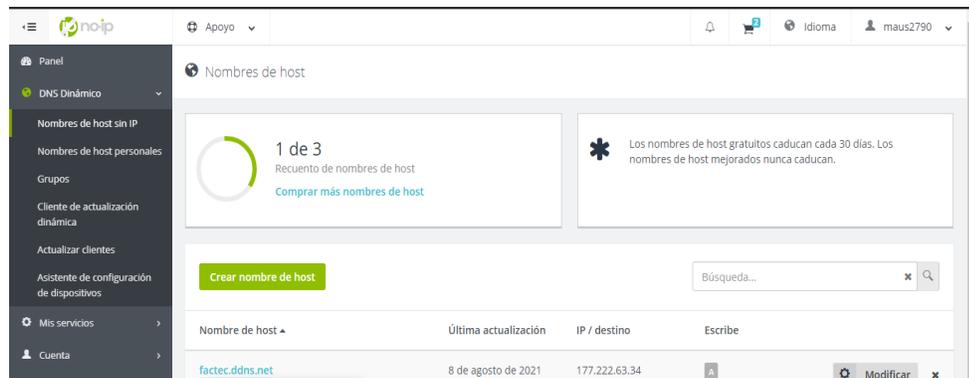
\$ 29.95 / año *

- 50 nombres De Host Incluidos
- Ahorre \$ 5 En El Registro De Dominio
- Soporte Telefónico

Para nuestro proyecto comenzaremos usando el plan gratuito este plan nos permite tener un máximo de 3 dominios y solo tenemos que confirmar el nombre de dominio una vez al mes de forma gratuita.

No ip necesita solo necesita la dirección ip publica con la que estamos saliendo a internet, por lo general las empresas ISP configuran esta ip de forma dinámica por lo que nuestra dirección ip cambiara cada cierto tiempo. No-IP tiene la ventaja añadida de que captura estos cambios de dirección y las actualiza a nuestros nombres de dominio.

Figura 26. *Interfaz de noIp*



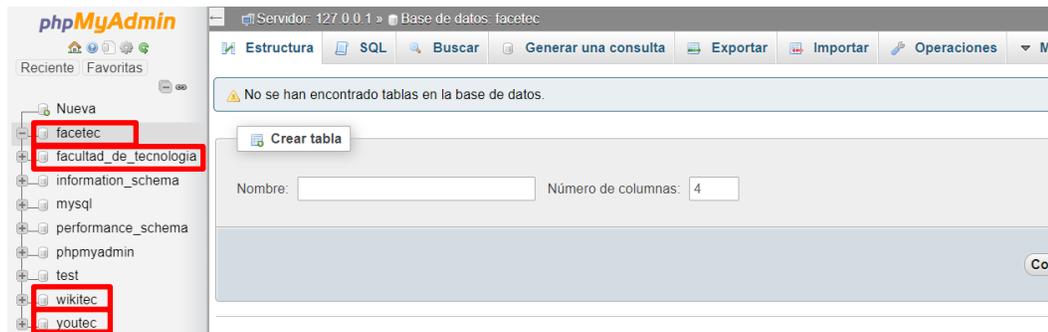
Fuente: <https://www.noip.com/>

Para nuestro proyecto crearemos un nombre de dominio llamado, “**factec.ddns.net**” el cual captara nuestra dirección ip Publica. Pero el servicio DNS va de la mano con el redireccionamiento de puertos, punto que se verá con más detalle en la capa de transporte.

3.1.4 Base De Datos

Para el almacenamiento de toda la información de la intranet se usará phpMyAdmin que es una herramienta escrita en PHP que nos permite manejar MySQL a través de la web.

Figura 27. Bases de Datos de la Intranet



Fuente: Elaboración propia

Para nuestra intranet tendremos inicialmente 4 bases de datos.

3.1.4.1 BD (facultad_de_tecnologia)

Esta base de datos tendrá contendrá 3 tablas.

- Tabla “anuncios” que me alojara los anuncios de la página principal.
- Tabla “login” que contendrá el registro de todos los usuarios
- Tabla de “matriculas” y por último y el más importante, es la que me alojará las matrículas de todos los estudiantes esto debido a que la intranet solo será usada por alumnos matriculados de la facultad.

Figura 28. Tablas de la Base de Datos Principal



Fuente: Elaboración propia

3.1.4.1.1 Tabla Anuncios

Figura 29. Entrada y salida de anuncios



Fuente: Elaboración propia

1. En este campo es donde se escribe el anuncio
2. Tenemos dos botones en las que escribiremos el anuncio
3. Y por último en este campo es donde se publicará el anuncio, el cual cuenta con una animación que hace que el mensaje se despliegue de derecha a izquierda.

Figura 30. Estructura BD Principal.

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
<input type="checkbox"/>	1	id	int(11)		No	Ninguna	
<input type="checkbox"/>	2	mensaje	varchar(500)		No	Ninguna	

Fuente: Elaboración propia

Dos columnas una que me almacena el id de tipo de dato entero, y la otra columna que almacena el mensaje con tipo de dato varchar, esta me almacenara un mensaje con un máximo de 500 caracteres.

Figura 31. Almacenamiento en B.D. Principal

	id	mensaje
<input type="checkbox"/>	1	Suspension de clases el 6 de agosto 2020 por fiest...

Fuente: Elaboración propia

El sistema de almacenamiento será muy sencillo ya que solo almacenará un mensaje, y si colocamos otro automáticamente borrará el anterior mensaje, de esta manera nuestra tabla no se llenará de mensajes pasados.

3.1.4.1.2 Tabla Login

Esta tabla contara con 5 columnas tal como se muestra en la siguiente tabla.

Figura 32. Estructura de Tabla de Logeo

#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extr
1	id	int(11)			No	Ninguna	AUT
2	correo	varchar(123)			No	Ninguna	
3	matricula	int(11)			No	Ninguna	
4	usuario	varchar(100)			No	Ninguna	
5	clave	varchar(200)			No	Ninguna	

Fuente: Elaboración propia

- Id: Como se ve en la siguiente imagen nuestra columna id será autoincrementable y nos proporcionará un identificador a cada usuario registrado,
- Correo: nos almacenara el correo del usuario
- Matricula: aquí nos almacenara la matricula del usuario previamente validada.
- Usuario: el usuario es un nombre cualquiera con que una persona se identificará.
- Clave: y por último esta clave estará cifrada con el algoritmo de encriptación sha512, para que así de esta manera solo el usuario lo conocerá su clave.

Figura 33. Cifrado de Clave

id	correo	matricula	usuario	clave
20	maus279000@gmail.com	123	marco5	3c9909afec25354d551dae21590bb26e38d53f2173b8d3d
19	maus279000@gmail.com	12	mar	5aadb45520dcd8726b2822a7a78bb53d794f557199d5d4e
18	maus2790	135	aaaxx	3c9909afec25354d551dae21590bb26e38d53f2173b8d3d
17	maus2790	123	aaax	3c9909afec25354d551dae21590bb26e38d53f2173b8d3d
16	maus2790	123	asdasd	e54ee7e285fbb0275279143abc4c554e5314e7b417ecac8

Fuente: Elaboración propia

3.1.4.1.3 Tabla Matriculas

Esta tabla solo tendra una columna del tipo de dato entero

Figura 34. Tabla Matricula

Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
matricula	int(11)			No	Ninguna	

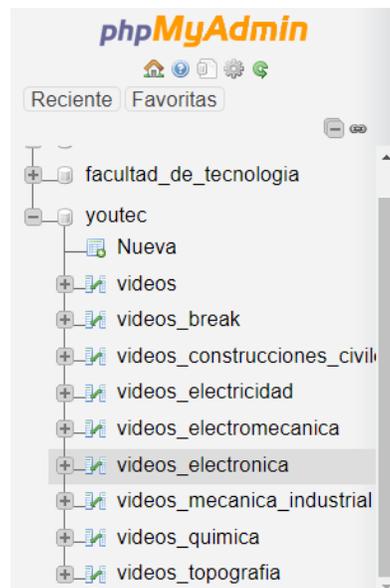
Fuente: Elaboración propia

Esta tabla almacenara todos los numeros de matricula la cual usaremos para validar el registro de todos los usuarios.

3.1.4.2 BD (youtec)

Esta base de datos permite que se almacene todos los datos de los videos que suban los usuarios.

Figura 35. Base de Datos Para Recursos Audiovisuales



Fuente: Elaboración propia

En esta base de datos cada carrera contará con una tabla que les permita almacenar los datos del video, y tendrá la siguiente estructura.

Figura 36. Estructura de la B.D. YouTec

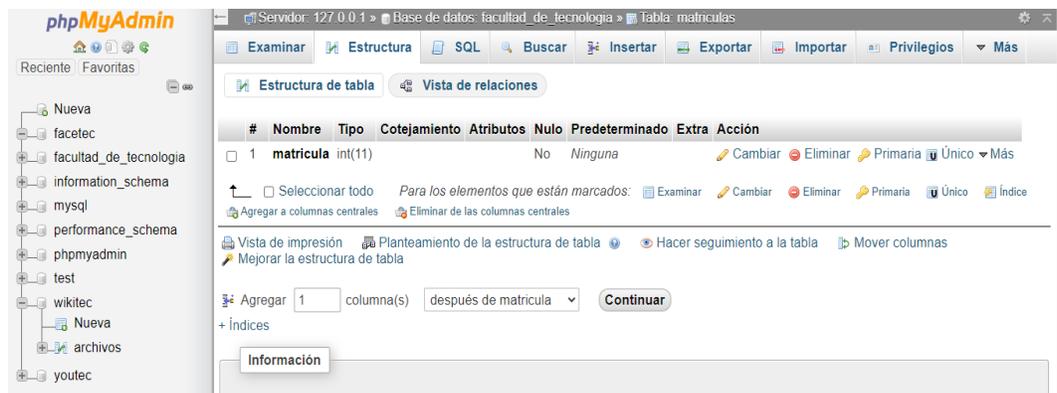
Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Extra
id	int(11)			No	Ninguna	AUTO_INCREMENT
usuario	varchar(50)			No	Ninguna	
semestre	varchar(50)			No	Ninguna	
materia	varchar(50)			No	Ninguna	
titulo	varchar(50)			No	Ninguna	
ruta	varchar(200)			No	Ninguna	
fecha	datetime			No	Ninguna	

Fuente: Elaboración propia

3.1.4.3 BD (WikiTec)

Esta base de datos mantendrá la misma estructura de los videos solo que en este caso será exclusivamente para documentos tipo texto

Figura 37. B.D. WikiTec



Fuente: Elaboración propia

3.1.5 Seguridad

El diseño de la página de autenticación tiene dos pestañas principales uno que es el de ingreso y el otro para registro. También como ya se mencionó, la contraseña de los usuarios será conocida solo por ellos ya que usaremos un algoritmo de encriptación conocido como sha512, esta será apreciada en la base de datos de la siguiente manera

Figura 38. Sistema encriptado.

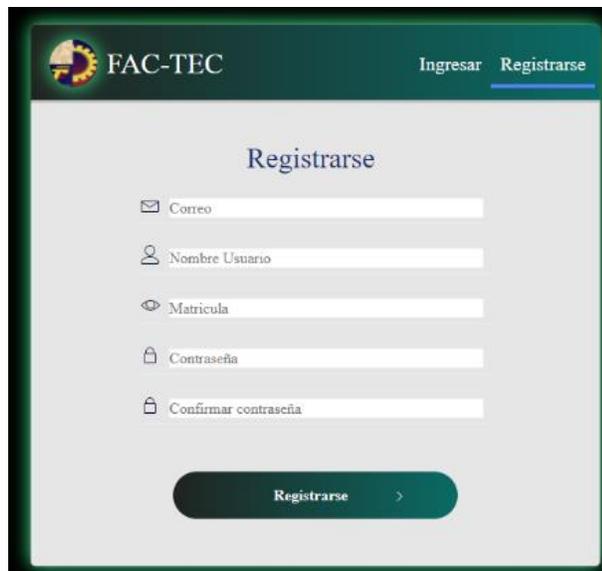
id	correo	matricula	usuario	clave
1				
20	maus279000@gmail.com	123	marco5	3c9909afec25354d551dae21590bb26e38d53f2173b8d3d
19	maus279000@gmail.com	12	mar	5aadb45520dcd8726b2822a7a78bb53d794f557199d5d4e
18	maus2790	135	aaaxx	3c9909afec25354d551dae21590bb26e38d53f2173b8d3d
17	maus2790	123	aaax	3c9909afec25354d551dae21590bb26e38d53f2173b8d3d

Fuente: Elaboración propia

También se hará uso de VPN con ipSec (Seguridad del protocolo de Internet), el cual se verá en posteriores capítulos. Pero reforzando la seguridad en nuestra intranet realizaremos un sistema de registro para los usuarios.

3.1.5.1 Registro

Figura 39. Registro HTML



The image shows a web registration form for FAC-TEC. At the top left is the FAC-TEC logo. To the right are links for 'Ingresar' and 'Registrarse'. The main heading is 'Registrarse'. Below it are five input fields: 'Correo' (with an envelope icon), 'Nombre Usuario' (with a person icon), 'Matricula' (with an eye icon), 'Contraseña' (with a lock icon), and 'Confirmar contraseña' (with a lock icon). At the bottom is a dark green button labeled 'Registrarse' with a right-pointing arrow.

Fuente: Elaboración propia

La aplicación web para el registro se lo realizo en base a la tecnología HTML y CSS. La pestaña de registro permite almacenar un nuevo usuario y contraseña en

la base de datos de phpMyAdmin. Esta página tiene 4 campos de entrada que son correo, nombre de usuario, contraseña y la confirmación de contraseña.

Análisis

1 primero comenzamos colocando el título de la página Login-Facultad De Tecnología.

2 implementamos unas etiquetas meta para que nuestra página web sea responsiva

`Viewport` es el área visible del documento

`width=device-width` hace que se adapte al ancho del dispositivo

`initial-scale=1.0` permite mantener la escala inicial para cuando volteemos la pantalla en un dispositivo móvil.

`user-scalable=no` no es permitido realizar zoom en un dispositivo móvil

3 luego tenemos los iconos que implementamos en los campos de entrada

4 vinculando todos los estilos de css utilizados en la página de login.

5 insertamos la imagen de la facultad

6 colocamos el título de la página FAC-TEC

7 colocamos un hipervínculo que nos direccionara a la página de login

8 colocamos un hipervínculo que nos direccionara a la página de registro

9 colocamos el título de la página Registrarse

10 insertamos una imagen para el campo de correo

11 colocamos un campo de entrada para correo

12 insertamos una imagen para el campo de nombre

13 colocamos un campo de entrada para nombre

14 insertamos una imagen para el campo de contraseña

15 colocamos un campo de entrada para la contraseña

16 insertamos una imagen para el campo de confirmación de contraseña

17 colocamos un campo de entrada para confirmación de contraseña

18 colocamos un botón para realizar el registro

19 creamos un apartado para la matricula

3.1.5.2 Registro PHP

PHP nos ayudara a interactuar con las bases de datos que se encuentra en nuestro servidor, en este registro tenemos una serie de condicionantes que validan el registro

Figura 40. *Registro PHP*



The screenshot shows a web interface for registration. At the top left is the FAC-TEC logo. To the right are links for 'Ingresar' and 'Registrarse'. The main heading is 'Registrarse'. Below it are five input fields: 'Correo' (with an envelope icon), 'Nombre Usuario' (with a person icon), 'Matricula' (with an eye icon), 'Contraseña' (with a lock icon), and 'Confirmar contraseña' (with a lock icon). Below the fields is a red error message: 'Esta matricula no esta registrada en la universidad o'. At the bottom is a dark green button labeled 'Registrarse' with a right-pointing arrow.

Fuente: Elaboración propia

En esta parte realizaremos la validación principalmente de la matricula, la cual se verificará con otra tabla donde estarán almacenadas las matrículas de los estudiantes.

```
<?php session_start();
```

```
if ($_SERVER['REQUEST_METHOD'] == 'POST'){ //si estamos enviando datos entonces...
```

```
    $correo = $_POST['correo']; //almacenamos los datos en una variable
```

```
    $usuario = $_POST['usuario'];
```

```
    $matricula = $_POST['matricula'];
```

```
    $clave = $_POST['clave'];
```

```
    $clave2 = $_POST['clave2'];
```

```
    $clave = hash('sha512', $clave); //almacenamos los datos encriptados en una variable
```

```
    $clave2 = hash('sha512', $clave2);
```

```
    $error = ""; //creamos una variable error en blanco
```

```

if (empty($correo) or empty($usuario) or empty($matricula) or empty($clave) or
empty($clave2)){

    $error .= '<i>Favor de rellenar todos los campos</i>'; //la variable error tomara este mensaje
    siempre y cuando no se llene algun campo
    }else{

        try{ //si es que todos los campos estan llenados nos conectamos a la base de datos
            $conexion = new
PDO(mysql:host=localhost;dbname=FACULTAD_DE_TECNOLOGIA', 'root', '');
        }catch(PDOException $prueba_error){
            echo "Error: " . $prueba_error->getMessage();
        }

        //luego con las siguientes líneas de código verificamos la matricula del usuario en la bd
        $statement = $conexion->prepare('SELECT * FROM matriculas WHERE matricula =
:matricula LIMIT 1');
        $statement->execute(array(':matricula' => $matricula));
        $resultado = $statement->fetch();//si existe el resultado será verdadero

        if ($resultado == false){ //si el resultado es falso
            $error .= '<i>Esta matricula no esta registrada en la universidad o </i>'; //la variable error
tomara un valor que será el mensaje
        }

        //luego con las siguientes líneas de código verificamos al usuario en la bd
        $statement = $conexion->prepare('SELECT * FROM login WHERE usuario = :usuario
LIMIT 1');
        $statement->execute(array(':usuario' => $usuario));
        $resultado = $statement->fetch();//si existe el resultado será verdadero
        if ($resultado != false){ //si el resultado es verdadero
            $error .= '<i>Este usuario ya existe</i>'; //la variable error tomara un valor que sera el
mensaje
        }
        if ($clave != $clave2){ //lo mismo
            $error .= '<i> Las contraseñas no coinciden</i>';
        }
    }

    if ($error == ""){// si es que la variable error no toma ningun valor entonces procedemos a
guardar en la bd
        $statement = $conexion->prepare('INSERT INTO login (id, correo, matricula, usuario,
clave) VALUES (null, :correo, :matricula, :usuario, :clave)');
        $statement->execute(array(

```

```

        ':correo' => $correo,
        ':matricula' => $matricula,
        ':usuario' => $usuario,
        ':clave' => $clave
    ));

    $error .= '<i style="color: green;">Usuario registrado exitosamente</i>'; // aquí la variable
error tomara un valor pero no de error, si no que nos dirá que nuestro registro fue exitoso en color
verde
    }
}

require 'frontend/register-vista.php'; //y nos direcciona al mismo formulario?>

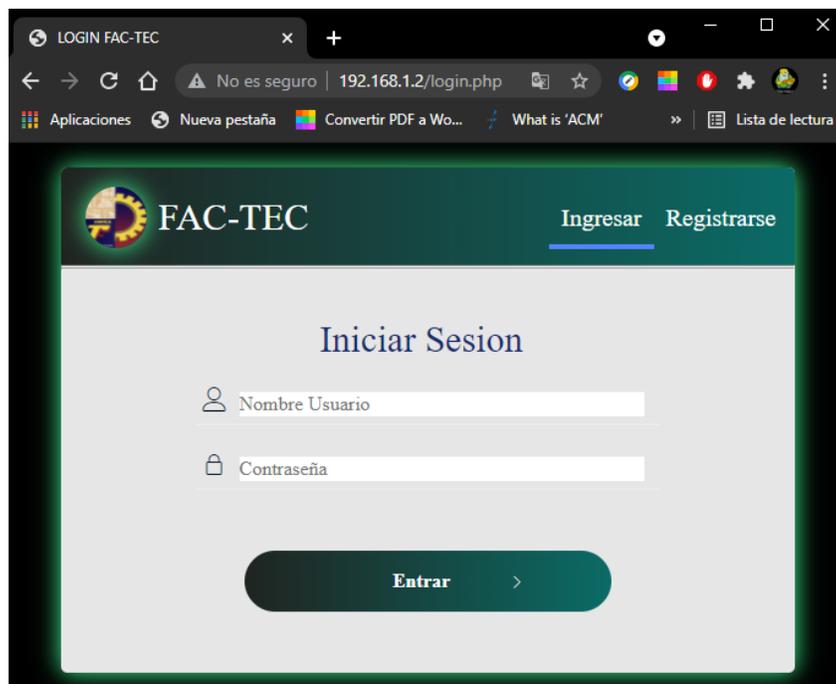
```

3.1.5.3 Ingreso HTML

La pestaña de ingreso el cual tiene dos campos que permite ingresar a la página principal y su diseño es el siguiente.

Y prácticamente es lo mismo que el registro solo que con menos campos de entrada

Figura 41. *Sistemas de Ingreso HTML.*



Fuente: Elaboración propia

Ingreso PHP

```
<?php session_start();

if(isset($_SESSION['usuario'])) {
    header('location: ../index.php');
}

$error = "";

if($_SERVER['REQUEST_METHOD'] == 'POST'){

    $usuario = $_POST['usuario'];
    $clave = $_POST['clave'];
    $clave = hash('sha512', $clave);

    try{
        $conexion =
PDO('mysql:host=localhost;dbname=FACULTAD_DE_TECNOLOGIA', 'root', "");
    }catch(PDOException $prueba_error){
        echo "Error: " . $prueba_error->getMessage();
    }

    $statement = $conexion->prepare('
SELECT * FROM login WHERE usuario = :usuario AND clave = :clave'
);

    $statement->execute(array(
        ':usuario' => $usuario,
        ':clave' => $clave
    ));

    $resultado = $statement->fetch();

    if ($resultado !== false){
        $_SESSION['usuario'] = $usuario;
        header('location: principal.php');
    }else{
        $error .= '<i>Este usuario no existe</i>';
    }
}
require 'frontend/login-vista.php';

?>
```

new

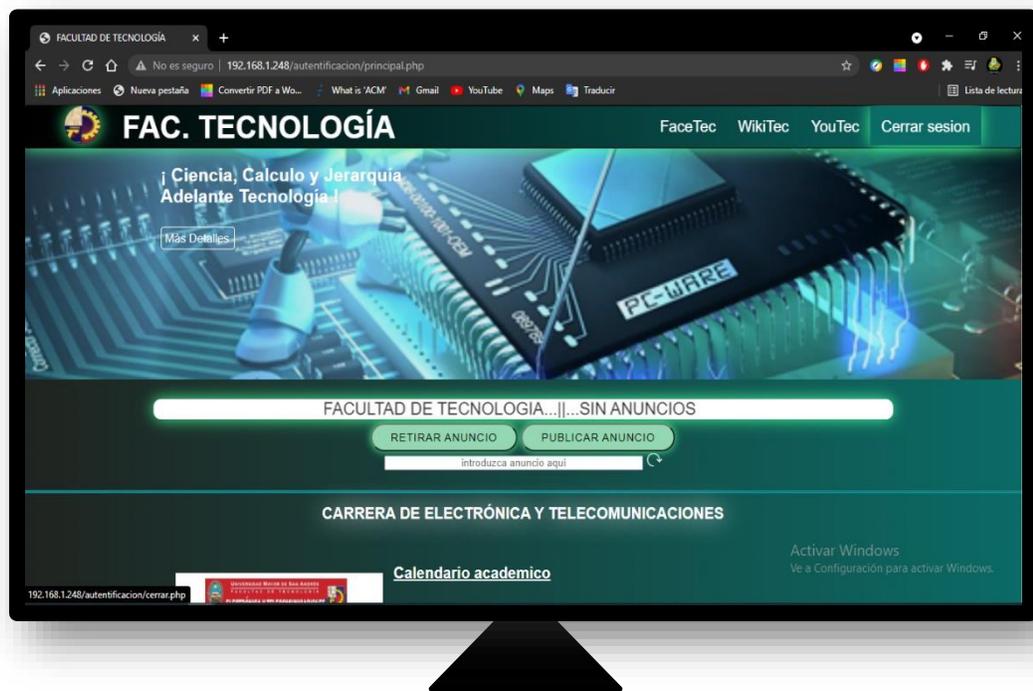
3.1.6 Sitios Web

Los sitios web brindarán el acceso a los recursos visuales y audio visuales que estarán alojados en el servidor.

3.1.6.1 Página Principal

La página principal de nuestra intranet tendrá el siguiente diseño y estructura.

Figura 42. *Página Principal de la Intranet*



Fuente: Elaboración propia

En el encabezado tendrá un navegador con tres pestañas, el primero “Cerrar sesión” finalizará nuestra conexión al servidor y a la base de datos, el segundo “YouTec” direccionará a una página de recursos audiovisuales, el tercero “WikiTec” dirigirá a una página de recursos en formato texto y por último tendremos “FaceTec” una red social exclusiva para la facultad de Tecnología.

La página principal será exclusiva para colgar anuncios por los administradores

Diseño Responsive

El diseño web responsive es una técnica de diseño web que busca adaptar paginas web al tamaño de pantalla de los celulares y dispositivos similares.

Hoy en día el acceso a sitios web no se limita para solo ordenadores, ya que es una necesidad tener el internet en nuestras manos, es por eso que todo tipo de dispositivos moviles necesitan adaptarse al internet.

Para la intranet se desarrollaron sitios web responsivos para que el usuario tenga la red en su mano.

Figura 43. páginas Principales Responsivas

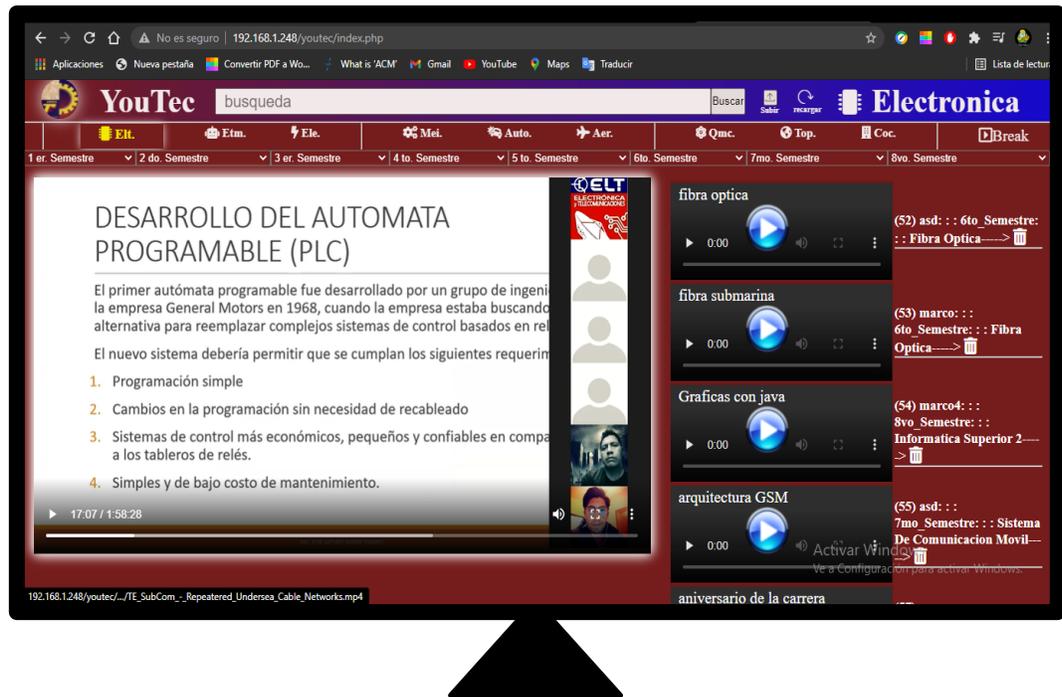


Fuente: Elaboración propia

3.1.6.2 YOUTEC

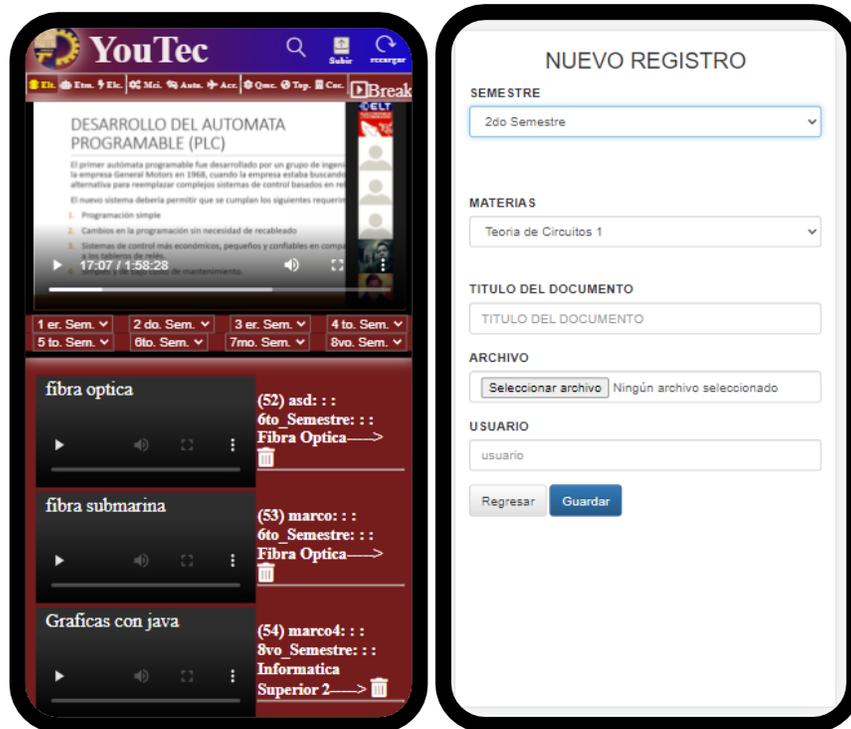
YouTec es una página dinámica donde se alojarán todos nuestros recursos audiovisuales, sera interactivo en el cual el usuario podrá colgar sus recursos en formato Mp4 con un tamaño máximo de 1Gb

Figura 44. *Página de Administración Audiovisual*



Fuente: Elaboración propia

Figura 45. *Página de Administración Audiovisual Responsiva*



Fuente: Elaboración propia

Código PHP

El código contara con dos partes muy esenciales el guardado de los videos y el eliminado también.

Guardar PHP

```
<?php
require './autenticacion/conexion.php';//nos direcciona a la base de datos login
$usuario = $_POST['usuario'];//obtenemos el usuario introducido en la caja de texto

//luego con las siguientes lineas de codigo verificamos al usuario en la bd
$stmt = $conexion->prepare('SELECT * FROM login WHERE usuario = :usuario LIMIT 1');
$stmt->execute(array(':usuario' => $usuario));
$resultado = $stmt->fetch();//si existe el resultado sera verdadero

if ($resultado != false) { //si el resultado es verdadero
    require 'conexion.php';
    $materia = $_POST['materia'];
```

```

    $semestre = $_POST['semestre'];
    $titulo = $_POST['titulo'];
    $nomArchivo=$_FILES["archivo"]["name");//definimos el nombre del archivo
    $sql = "INSERT INTO videos ( usuario,semestre,materia, titulo, ruta) VALUES
    ('$usuario','$semestre','$materia', '$titulo','$nomArchivo)";
    $resultado = $mysqli->query($sql); //EJECUTAMOS

    //////////::EL ARCHIVO::////////////////////
    //sacaremos el id del registro y crearemos una carpeta con ese id
    $id_insert=$mysqli->insert_id; // nos trae el id que se registro

    if($_FILES["archivo"]["error"]>0){$_FILES["archivo"]; recibimos un campo del tipo file
    evaluamos si existe un error >0
    echo "ERROR AL CARGAR ARCHIVO";
    }else {
    $limite_kb=1000000;//limite del tamaño de archivo
    if($_FILES["archivo"]["size"] <= $limite_kb*1024){//in_array($_FILES["archivo"] busca
    dentro de array archivo y el campo type y lo buscamos dentro de permitidos //evaluamos si el
    archivo corresponde al los archivos permitivos y no sobrepase el limite
    $ruta='videos/'.$id_insert.'/';//creamos una carpeta con el numero de id
    $archivo=$ruta.$FILES["archivo"]["name");//definimos el nombre del archivo
    if(!file_exists($ruta)){
    mkdir($ruta); //en caso de que no exista el archivo crea su propia carpeta
    }
    $resultado=@move_uploaded_file($_FILES["archivo"]["tmp_name"],$archivo);//que archivo
    y adonde lo voy a mover

    if($resultado){
    echo "Archivo guardado exitosamente";
    }else{
    echo "error al guardar";
    }
    } else{
    echo "archivo no permitido ";
    }
    }
    }else {
    $resultado = FALSE;
    echo "<h3 style='text-align:center'>este usuario no existe en nuestra base de datos</h3>";
    }
    ?>

    <!-------VENTANA QUE NOS REGRESARA A LA ANTERIOR VENTANA -->

    <html lang="es">

```

```

<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="css/css/bootstrap.min.css" rel="stylesheet">
  <link href="css/css/bootstrap-theme.css" rel="stylesheet">
</head>
<body>
<div class="container">
<div class="row">
<div class="row" style="text-align:center">
<?php if($resultado) { ?>
<h3>REGISTRO GUARDADO</h3>
<?php } else { ?>
<h3>ERROR AL GUARDAR</h3>
<?php } ?>
<a href="index.php" class="btn btn-primary">Regresar</a>

```

Eliminar PHP

```

<?php
require 'conexion.php';

$id = $_GET['id'];

$sql = "DELETE FROM videos WHERE id = '$id'";
$resultado = $mysqli->query($sql);
eliminarDir('videos/'.$id);
function eliminarDir($carpeta)
{
  foreach (glob($carpeta."/*") as $archivos_carpeta)
  {
    if (is_dir($archivos_carpeta)) {
      eliminarDir($archivos_carpeta);
    } else {
      unlink($archivos_carpeta);
    }
  }
  rmdir($carpeta);
}

?>

<html lang="es">
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">

```

```

<link href="css/css/bootstrap.min.css" rel="stylesheet">
<link href="css/css/bootstrap-theme.css" rel="stylesheet">
</head>
<body>
<div class="container">
<div class="row">
<div class="row" style="text-align:center">
<?php if($resultado) { ?>
<h3>REGISTRO ELIMINADO</h3>
<?php } else { ?>
<h3>ERROR AL ELIMINAR</h3>
<?php } ?>

<a href="index.php" class="btn btn-primary">Regresar</a>

```

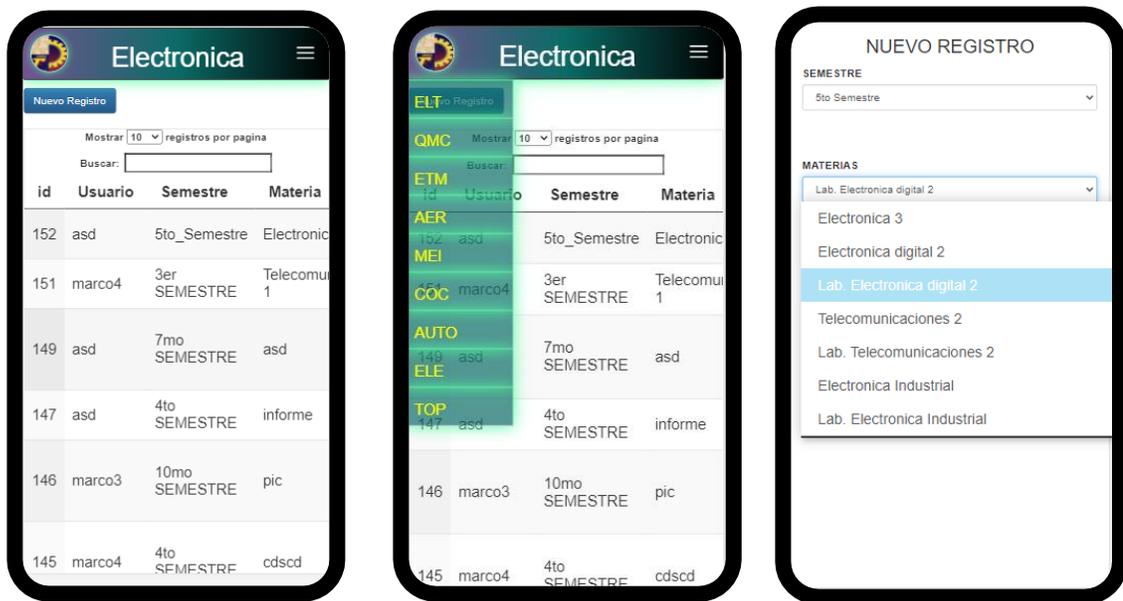
3.1.6.3 WIKITEC

Figura 46. *Página de administración de archivos*

id	Usuario	Semestre	Materia	Titulo	Documento	Descargar	Eliminar
152	asd	5to_Semestre	Electronica 3	transito	LEY CODIGO DE TRANSITO....pdf		
151	marco4	3er SEMESTRE	Telecomunicaciones 1	Laboratorio 4	Laboratorio 4.pdf		
149	asd	7mo SEMESTRE	asd	asd	ANÁLISIS DE SEÑALE 6 - espectro (Autoguardado).docx		
147	asd	4to SEMESTRE	informe	ssss	informe.docx		
146	marco3	10mo SEMESTRE	pic	video	Fundamentos BÁSICOS de dsPIC30F - Wels Theory.mp4		
145	marco4	4to SEMESTRE	cdscd	asca	ANÁLISIS DE SEÑALE 6 - espectro		

Fuente: Elaboración propia

Figura 47. *Página de Administración de Archivos Responsiva*



Fuente: Elaboración propia

WikiTec CSS

En este apartado también se hizo uso de las librerías para tablas que nos trae Bootstrap para la tabla. Y se desarrolló el siguiente archivo css para el encabezado.

WikiTec PHP

Guardar PHP

```
<?php
require './autenticacion/conexion.php';//nos direcciona a la base de datos login
$usuario = $_POST['usuario'];//obtenemos el usuario introducido en la caja de texto
```

```
//luego con las siguientes lineas de codigo verificamos al usuario en la bd
```

```

$statement = $conexion->prepare('SELECT * FROM login WHERE usuario = :usuario LIMIT
1');
$statement->execute(array(':usuario' => $usuario));
$resultado = $statement->fetch();//si existe el resultado sera verdadero

if ($resultado != false) { //si el resultado es verdadero
    require 'conexion.php';
    $materia = $_POST['materia'];
    $semestre = $_POST['semestre'];
    $titulo = $_POST['titulo'];
    $nomArchivo=$_FILES["archivo"]["name");//definimos el nombre del archivo
    $sql = "INSERT INTO archivos ( usuario,semestre,materia, titulo, ruta) VALUES
('$usuario','$semestre','$materia', '$titulo','$nomArchivo)";
    $resultado = $mysqli->query($sql); //EJECUTAMOS

//////////::EL ARCHIVO::////////////////////////////////////

//sacaremos el id del registro y crearemos una carpeta con ese id
$id_insert=$mysqli->insert_id; // nos trae el id que se registro
if($_FILES["archivo"]["error"]>0){$_FILES["archivo"]; recibimos un campo del tipo file
evaluamos si existe un error >0
echo "ERROR AL CARGAR ARCHIVO";
} else {
    $limite_kb=1000000;//limite del tamaño de archivo
    if($_FILES["archivo"]["size"] <= $limite_kb*1024){//in_array($_FILES["archivo"] busca
dentro de array archivo y el campo type y lo buscamos dentro de permitidos //evaluamos si el
archivo corresponde al los archivos permitivos y no sobrepase el limite
    $ruta='files/'.$id_insert.'/';//creamos una carpeta con el numero de id
    $archivo=$ruta.$_FILES["archivo"]["name");//definimos el nombre del archivo
    if(!file_exists($ruta)){
    mkdir($ruta); //en caso de que no exista el archivo crea su propia carpeta
    }

$resultado=@move_uploaded_file($_FILES["archivo"]["tmp_name"],$archivo);//que archivo
y adonde lo voy a mover
    if($resultado){
        echo "Archivo guardado exitosamente";
    } else{
        echo "error al guardar";
    }
    } else{
        echo "archivo no permitido ";
    }
    }
    } else {
        $resultado = FALSE;
    }
}

```

```

        echo "<h3 style='text-align:center'>este usuario no existe en nuestra base de datos</h3>";
    }
?>

<!-------VENTANA QUE NOS REGRESARA A LA ANTERIOR VENTANA -->

<html lang="es">
<head>

<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="css/bootstrap.min.css" rel="stylesheet">
<link href="css/bootstrap-theme.css" rel="stylesheet">
<script src="js/jquery-3.1.1.min.js"></script>
<script src="js/bootstrap.min.js"></script>
</head>

<body>
<div class="container">
<div class="row">
<div class="row" style="text-align:center">
<?php if($resultado) { ?>
<h3>REGISTRO GUARDADO</h3>
<?php } else { ?>
    <h3>ERROR AL GUARDAR</h3>
<?php } ?>

<a href="index.php" class="btn btn-primary">Regresar</a>

```

Eliminar PHP

```

<?php

require 'conexion.php';
$id = $_GET['id'];
$sql = "DELETE FROM archivos WHERE id = '$id'";
$resultado = $mysqli->query($sql);

eliminarDir('files/'.$id);
function eliminarDir($carpeta)
{
    foreach (glob($carpeta."/*") as $archivos_carpeta)
    {
        if (is_dir($archivos_carpeta)) {
            eliminarDir($archivos_carpeta);
        } else {

```

```

unlink($archivos_carpeta);
}
}
rmdir($carpeta);
}
?>

<html lang="es">
<head>

<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="css/bootstrap.min.css" rel="stylesheet">
<link href="css/bootstrap-theme.css" rel="stylesheet">
<script src="js/jquery-3.1.1.min.js"></script>
<script src="js/bootstrap.min.js"></script>
</head>
  <body>
    <div class="container">
      <div class="row">
        <div class="row" style="text-align:center">
<?php if($resultado) { ?>
<h3>REGISTRO ELIMINADO</h3>
<?php } else { ?>
<h3>ERROR AL ELIMINAR</h3>
<?php } ?>

<a href="index.php" class="btn btn-primary">Regresar</a>

```

Recargar PHP

Para recargar y para la búsqueda se usó la tecnología JSON ya que esa tecnología reduce y optimiza en gran manera la búsqueda de grandes cantidades de datos en bases de datos.

```

<?php
  require 'conexion.php';

  /* Nombre de La Tabla */
  $$Tabla = "archivos";

  /* Array que contiene los nombres de las columnas de la tabla*/
  $aColumnas = array( 'id','usuario','semestre','materia','titulo','ruta');

  /* columna indexada */
  $$IndexColumn = "id";

```

```

// Paginacion
$sLimit = "";
if ( isset( $_GET['iDisplayStart'] ) && $_GET['iDisplayLength'] != '-1' )
{
    $sLimit = "LIMIT ".$_GET['iDisplayStart'].", ".$_GET['iDisplayLength'];
}

//Ordenacion
if ( isset( $_GET['iSortCol_0'] ) )
{
    $sOrder = "ORDER BY ";
    for ( $i=0 ; $i<intval( $_GET['iSortingCols'] ) ; $i++ )
    {
        if ( $_GET[ 'bSortable_'.$i ] == "true" )
        {
            $sOrder .= $aColumns[ intval( $_GET['iSortCol_'.$i] ) ]."
                ".$_GET['sSortDir_'.$i].", ";
        }
    }

    $sOrder = substr_replace( $sOrder, "", -2 );
    if ( $sOrder == "ORDER BY" )
    {
        $sOrder = "";
    }
}

//Filtracion
$sWhere = "";
if ( $_GET['sSearch'] != "" )
{
    $sWhere = "WHERE (";
    for ( $i=0 ; $i<count($aColumns) ; $i++ )
    {
        $sWhere .= $aColumns[$i]. " LIKE '%".$_GET['sSearch']."' OR ";
    }
    $sWhere = substr_replace( $sWhere, "", -3 );
    $sWhere .= ')';
}

// Filtrado de columna individual
for ( $i=0 ; $i<count($aColumns) ; $i++ )
{
    if ( $_GET['bSearchable_'.$i] == "true" && $_GET['sSearch_'.$i] != "" )
    {

```

```

        if ( $sWhere == "" )
        {
            $sWhere = "WHERE ";
        }
        else
        {
            $sWhere .= " AND ";
        }
        $sWhere .= $aColumnas[$i]." LIKE '%" .$_GET['sSearch_'. $i]."%' ";
    }
}

//Obtener datos para mostrar SQL queries
$sQuery = "
SELECT SQL_CALC_FOUND_ROWS ".str_replace(" ", " ", implode(" ", $aColumnas))."
FROM $sTabla
$sWhere
$sOrder
$sLimit
";
$result = $mysqli->query($sQuery);

/* Data set length after filtering */
$sQuery = "
SELECT FOUND_ROWS()
";
$resultFilterTotal = $mysqli->query($sQuery);
$aResultFilterTotal = $resultFilterTotal->fetch_array();
$iFilteredTotal = $aResultFilterTotal[0];

/* Total data set length */
$sQuery = "
SELECT COUNT(".$sIndexColumn.")
FROM $sTabla
";
$resultTotal = $mysqli->query($sQuery);
$aResultTotal = $resultTotal->fetch_array();
$iTotal = $aResultTotal[0];

/*
    * Output
*/
$output = array(
    "sEcho" => intval($_GET['sEcho']),

```

```

    "iTotalRecords" => $iTotal,
    "iTotalDisplayRecords" => $iFilteredTotal,
    "aData" => array()
);

while ( $aRow = $rResult->fetch_array()
{
    $row = array();
    for ( $i=0 ; $i<count($aColumnas) ; $i++ )
    {
        if ( $aColumnas[$i] == "version" )
        {
            /* Formato de salida especial para la columna 'versión' */
            $row[] = ( $aRow[ $aColumnas[$i] ]=="0" ) ? '-' : $aRow[
$aColumnas[$i] ];
        }
        else if ( $aColumnas[$i] != '' )
        {
            /* General output */
            $row[] = $aRow[ $aColumnas[$i] ];
        }
    }

    $row[] = "<td><a href='files/'.${aRow['id']}. '/' .${aRow['ruta']}' target='_blank'
id='${aRow['id']}'><div class='logo'><img src='imagenes/pngegg (1).PNG'
alt='></div></a></td>";
    $row[] = "<td><a href='#' data-href='eliminar.php?id=${aRow['id']}' data-
toggle='modal' data-target='#confirm-delete'><span class='glyphicon glyphicon-
trash'></span></a></td>";

    $output['aData'][] = $row;
}

echo json_encode( $output );
?>

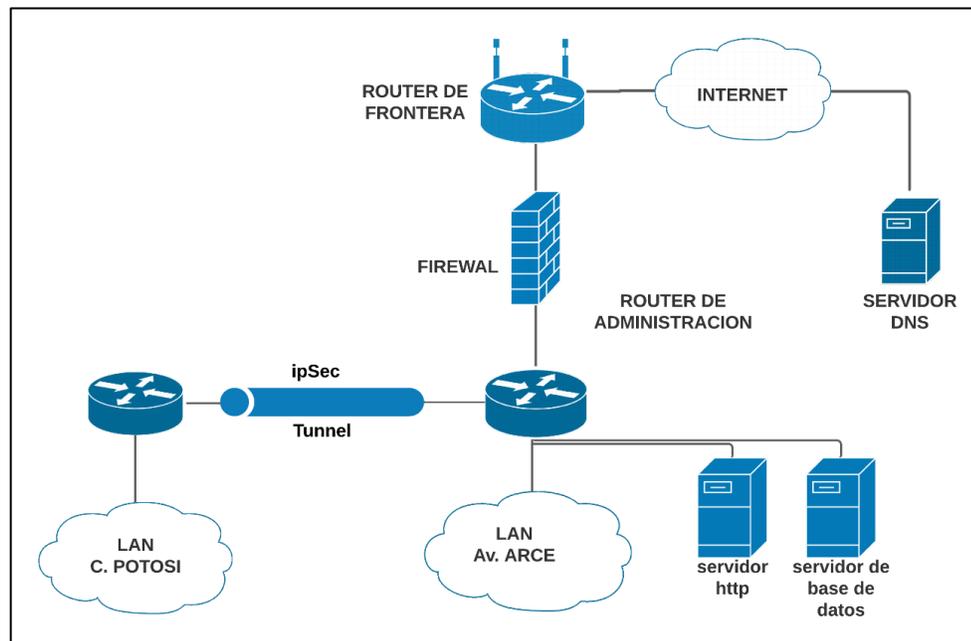
```

Fuente: Marko Robles

3.2 Capa De Transporte

En esta capa realizaremos ciertas configuraciones en el servidor HTTP y también en nuestro router de frontera y administración.

Figura 48. *Modelo General De Intranet.*



Fuente: Elaboración propia

El router de frontera es del tipo modem en la mayoría de los casos, esto debido a que la mayoría de las empresas proveedores de internet ofrecen servicios de TV y Telefonía. Estos vienen con configuraciones por defecto, así de esta manera los usuarios solo deberán realizar unas mínimas configuraciones.

La configuración de los módems de los proveedores de internet, en su mayoría tiene bloqueado el puerto 80 que será necesario activarla para que los usuarios puedan conectarse a la red.

3.2.1 Redireccionamiento de puertos

3.2.1.1 Redireccionamiento en router de frontera.

En caso de proveedores de internet Tigo el redireccionamiento se lo realiza de la siguiente forma.

Figura 49. Redireccionamiento de puertos en router de borde

HitronTechnologies Idioma: español Ayuda Cerrar Sesión

Opciones Filtrado Mac Filtrado IP **Redirección de Puertos** Activación de Puertos Pasaport

Usted puede añadir o editar las reglas de redirección de puertos acá.

Reglas de redirección de puertos

Aplicaciones comunes: -SERVICIOS-

Nombre de la Aplicación:

Protocolo: TCP / UDP

Rango de Puertos Públicos: ~

Rango de Puertos Privados: ~

Dirección IP:

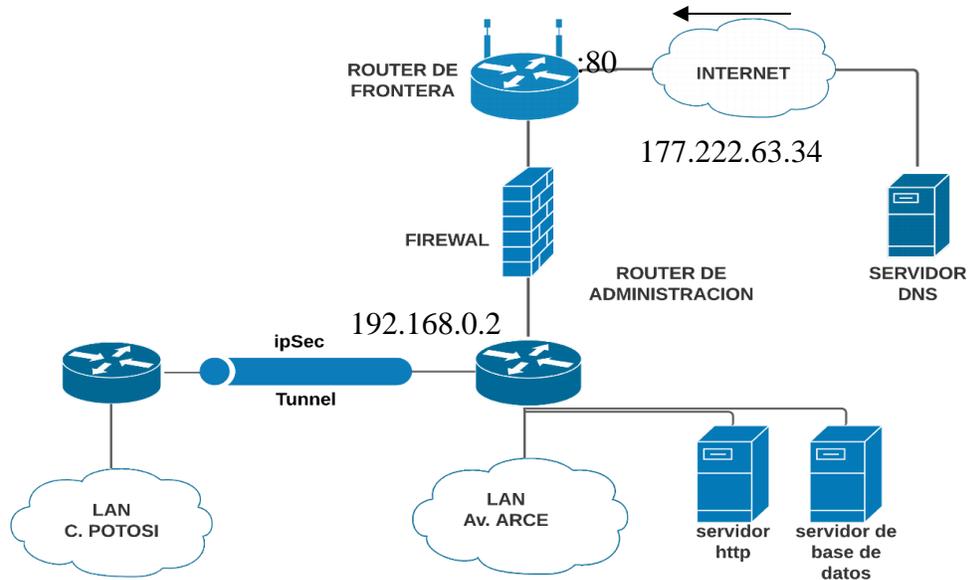
Fuente: Elaboración propia

El rango de puertos públicos colocamos el puerto 80, ya por este puerto es donde tendrá entrada de los usuarios hacia el servidor.

El protocolo de capa de transporte de datos que se usará será TCP y UDP.

En la siguiente figura muestra los usuarios remotos la manera en que accederán en primera instancia a nuestro router de administración a través del puerto 80 y lo redireccionara a su ip 192.168.0.2.

Figura 50. *Habilitación de puerto 80*

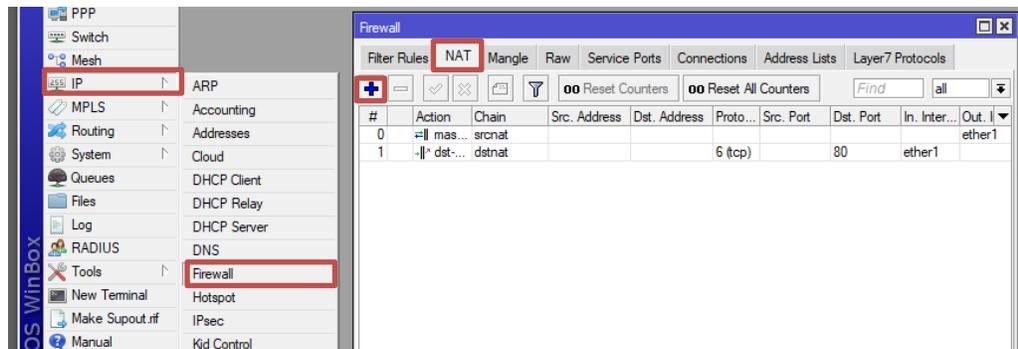


Fuente: Elaboración propia

3.2.1.2 Redireccionamiento en router de administración.

El router de administración que se usará será de tecnología mikrotik y su redireccionamiento es el siguiente. Primero se ingresa a la opción de firewall y seguidamente creamos una regla de NAT.

Figura 51. *Ingreso al NAT de Mikrotik*

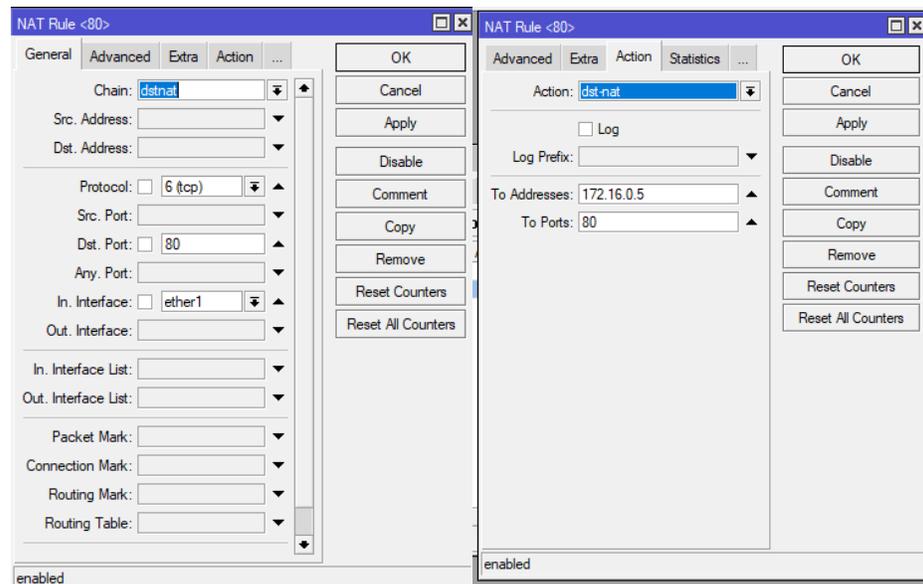


Fuente: Elaboración propia

Luego en la configuración general el tipo de tráfico que tendrá el router, el cual será de entrada a nuestro router y seleccionamos en chain como dstnat.

El protocolo que se usará será tcp y el puerto que se tendrá que abrir será el 80 en la interface de entrada ether1, la acción que realizaremos cuando tengamos un tráfico de entrada será de redireccionarlo a la ip 172.16.1.2 que de nuestro servidor http.

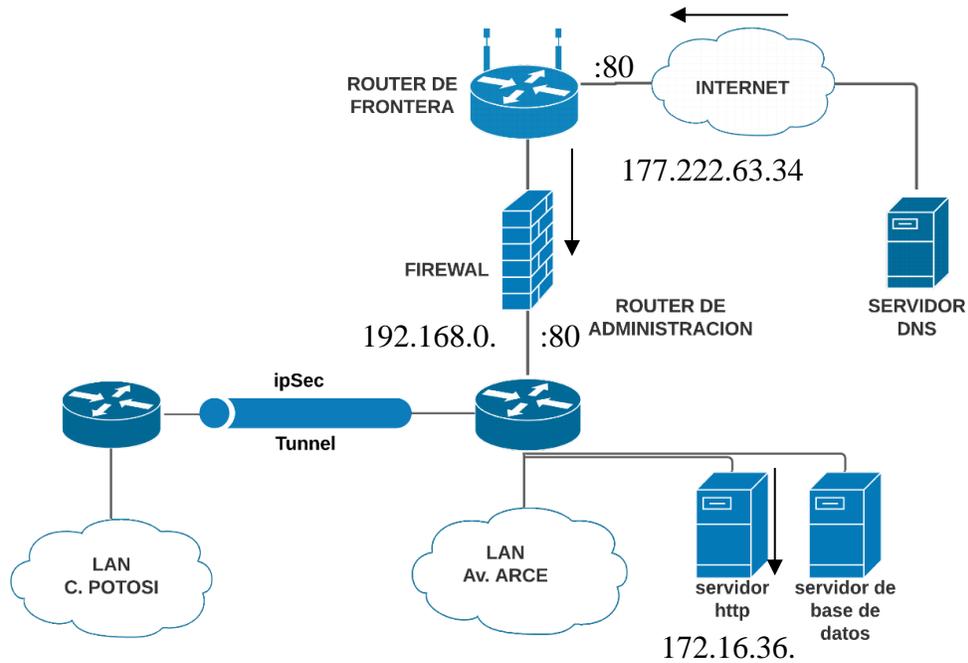
Figura 52. Redireccionamiento de puertos en router de administración



Fuente: Elaboración propia

En la siguiente figura muestra los usuarios remotos y los que están dentro de la intranet como las direcciones ip se redireccionan.

Figura 53. Diagrama de habilitación de puerto 80:

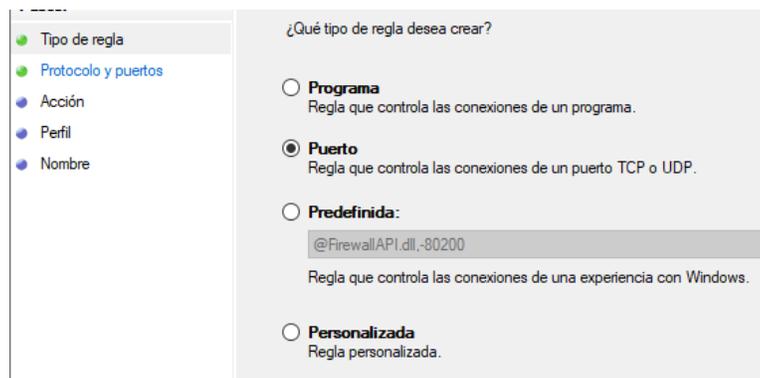


Fuente: Elaboración propia

Y finalmente procedemos a abrir el puerto 80 del servidor esto lo realiza entrando al firewall de Windows y en opciones avanzadas e ingresando a opciones avanzadas donde crearemos una regla de entrada

Primero se crea una regla para un puerto

Figura 54. Creación de regla para puerto 80



Fuente: Elaboración propia

Posteriormente se especifica el puerto y protocolo

Figura 55. *Especificación de puerto 80 en servidor.*

Asistente para nueva regla de entrada

Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

TCP

UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

Todos los puertos locales

Puertos locales específicos:

Ejemplo: 80, 443, 5000-5010

Fuente: Elaboración propia

Luego los permisos de conexión

Figura 56. *Permisos de conexión*

Asistente para nueva regla de entrada

Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

Permitir la conexión

Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

Permitir la conexión si es segura

Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Bloquear la conexión

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Cuándo se aplica esta regla?

Dominio

Se aplica cuando un equipo está conectado a su dominio corporativo.

Privado

Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

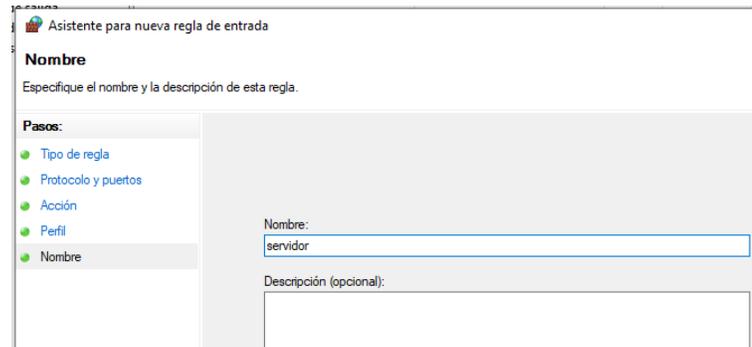
Público

Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

Fuente: Elaboración propia

Y finalmente le proporciona un nombre a la regla de entrada

Figura 57. Colocamos un nombre a la regla creada



Fuente: Elaboración propia

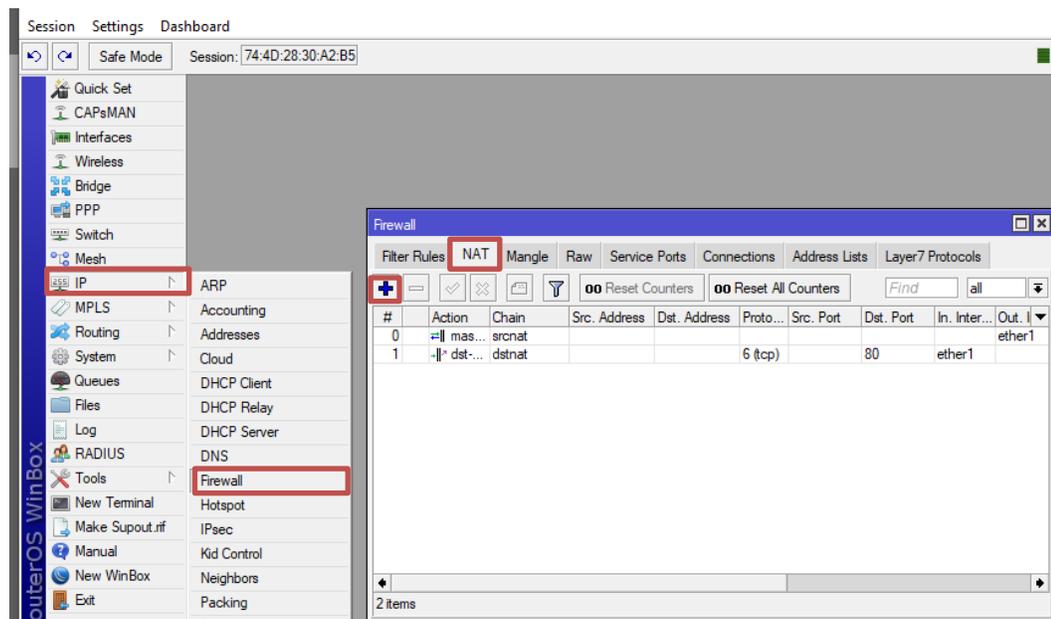
3.2.2 Nat

Es necesario crear una regla de nat para que nuestra intranet tenga salida hacia la internet.

Esto se realizará en el router de administración de la siguiente manera.

Similar a la regla de redireccionamiento, se ingresa a la pestaña nat

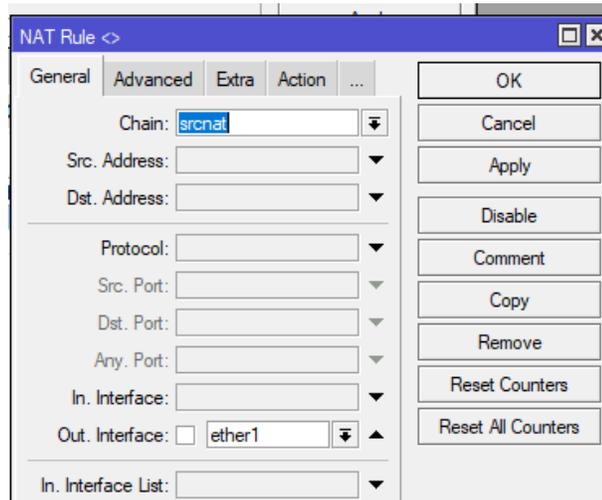
Figura 58. Ingreso a regla de NAT en mikrotik



Fuente: Elaboración propia

Seguidamente en la configuración general se especifica el tipo de tráfico, el cual será de salida por la interface ether1.

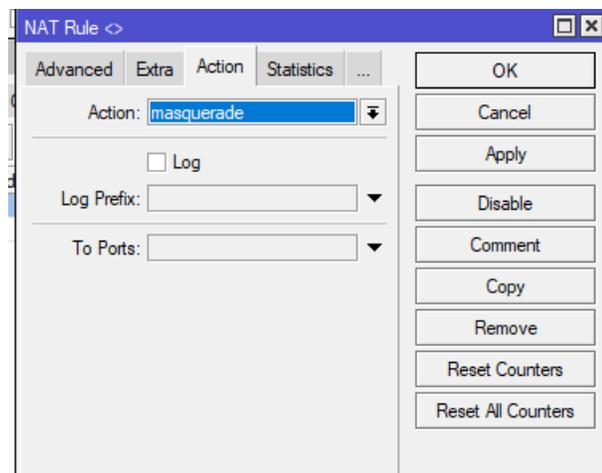
Figura 59. Configuración de regla de NAT en mikrotik



Fuente: Elaboración propia

Y en la acción se le indica que se enmascarará las direcciones ip privadas de la intranet.

Figura 60. Enmascaramiento de Dirección IP



Fuente: Elaboración propia

3.3 Capa De Red

En esta capa se hará la configuración de todo el direccionamiento ip que tendrá nuestra red.

3.3.1 Direccionamiento ip

La siguiente tabla muestra el detalle de alumnos matriculados en los últimos 5 años, estos datos nos ayudaran a dimensionar la red LAN de la facultad y el crecimiento que probablemente tendrá.

Tabla 10. Población Universitaria De La Facultad De Tecnología

POBLACION UNIVERSITARIA DE LA U.M.S.A.						
FACULTAD TECNOLOGÍA						
	Carrera	2016	2017	2018	2019	2020
TOTAL, MATRICULADOS						
1	Electrónica y Telec.	1917	1882	1841	1793	1721
2	Química Industrial	988	1023	1028	1040	1020
3	Mecánica Automotriz	912	957	970	918	897
4	Electromecánica	894	904	900	859	861
5	Aeronáutica	461	542	599	688	743
6	Construcciones Civiles	723	733	726	704	667
7	Topografía y Geodesia	604	616	617	614	602
8	Mecánica Industrial	321	305	303	369	393
9	Electricidad	329	336	332	356	374
Total		7149	7298	7316	7341	7278

Fuente: Elaboración propia

Para Una facultad con una población estudiantil de entre 7000 y 8000 estudiantes necesitamos realizar un cálculo adecuado de direcciones ip. Para ello se hace uso de la siguiente ecuación, esta nos ayudará a obtener que mascarará tendrá dicha red.

$$PARA n: 2^n - 2 \geq NH;$$

$$PARA mascara: 32 - n = /Mask;$$

Por eso calcularemos las máscaras de cada carrera.

Tabla 11. Cálculo De Numero De Host Por Carrera

	Carrera	2020	Mascara	Host	Margen de crecimiento
1	Electrónica y Telec.	1721	/21	255.255.248.0	321
2	Química Industrial	1020	/22	255.255.252.0	1026
3	Mecánica Automotriz	897	/22	255.255.252.0	125
4	Electromecánica	861	/22	255.255.252.0	161
5	Aeronáutica	743	/22	255.255.252.0	279
6	Construcciones Civiles	667	/22	255.255.252.0	355
7	Topografía y Geodesia	602	/22	255.255.252.0	420
8	Mecánica Industrial	393	/23	255.255.254.0	117
9	Electricidad	374	/23	255.255.254.0	136
	Fac. Tecnología (total)			10222	

Fuente: Elaboración propia

Como se verá, el total de host que requerirá la facultad es de 10222 así que se necesitara crear una dirección de red que soporte esa cantidad de host. Se comenzará por la máscara de la red.

$$2^n - 2 \geq 10222 \rightarrow n = 14 \rightarrow 16384 - 2 = 16382$$

$$Máscara = 32 - 14 = /18 \quad (255.255.192.0)$$

Ahora la máscara /18 está en el rango de ip privadas de clase C, el rango está en 172.16.0.0 a 172.31.255.255. la dirección que tendrá nuestra intranet será:

Dir. De Intranet. (172.16.0.0/18)

Ahora se puede calcular las direcciones de redes utilizando VLSM.

VLSM ayudará a controlar la difusión de broadcast, esto con el fin de que nuestra red no se ralentice.

Y ahora con estos datos procedemos a direccionar nuestra intranet.

Tabla 12. *VLSM para cada carrera*

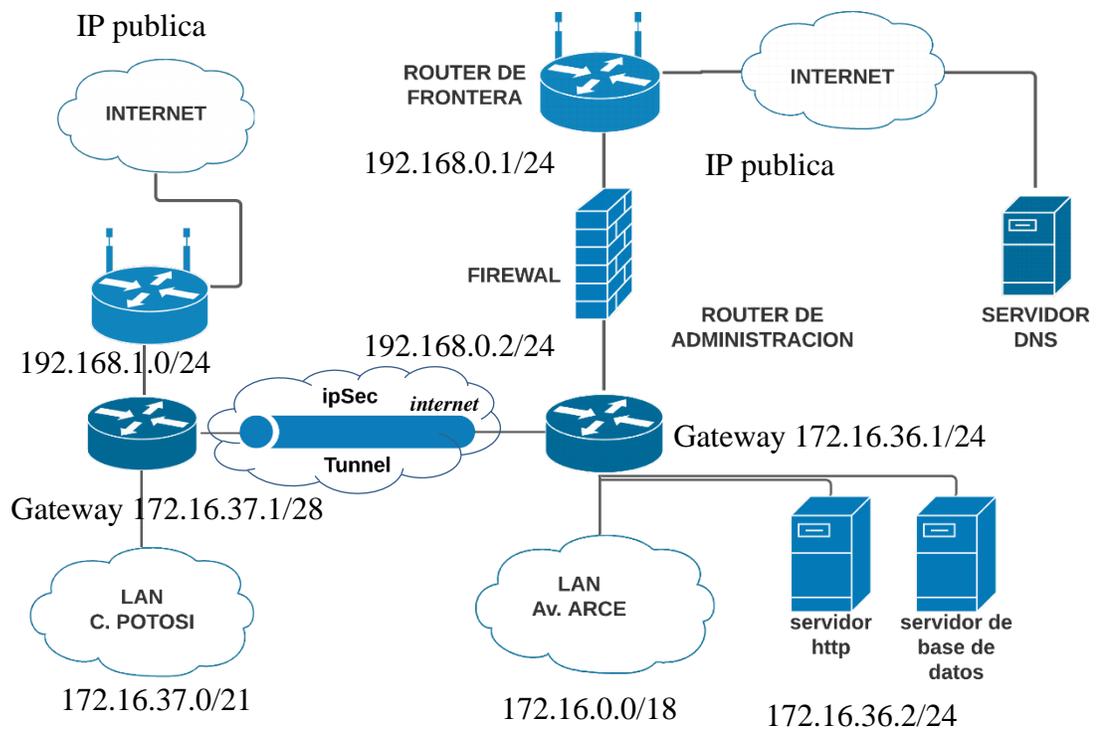
Carrera	Host	Ip de subred	Rango de host
Electrónica	2046	172.16.0.0 /21	172.16.0.1 - 172.16.7.254
Química	2046	172.16.8.0 /22	172.16.8.1 - 172.16.11.254
Automotriz	1022	172.16.12.0 /22	172.16.12.1 - 172.16.15.254
Electromecánica	1022	172.16.16.0 /22	172.16.16.1 - 172.16.19.254
Aeronáutica	1022	172.16.20.0 /22	172.16.20.1 - 172.16.23.254
Construcciones	1022	172.16.24.0 /22	172.16.24.1 - 172.16.27.254
Topografía	1022	172.16.28.0 /22	172.16.28.1 - 172.16.31.254
Mecánica Ind.	510	172.16.32.0 /23	172.16.32.1 - 172.16.33.254
Electricidad	510	172.16.34.0 /23	172.16.34.1 - 172.16.35.254
Router Administración	254	172.16.36.1/24	172.16.36.1 - 172.16.36.254

Fuente: Elaboración propia

Cabe señalar que para la red LAN de los predios de la calle potosí podrá acceder a la intranet mediante una VPN creado con L2TP/IPSEC.

La configuración de ip se la realiza en los routers mikrotik de la siguiente forma:

Figura 61. *Direcccionamiento general de la intranet*



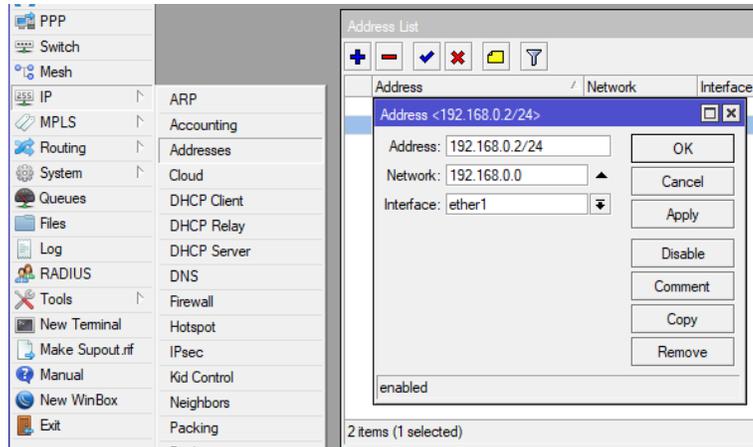
Fuente: Elaboración propia

Se asigna una ip a la interface WAN y LAN

La interfaz WAN en nuestro router de administración será el puerto ether1, y esta estará directamente conectada al modem de nuestro proveedor de internet, en caso de tener una ip pública se la colocaremos a esta interfaz.

1. Seleccionamos IP de la ventana principal
2. Seleccionamos Address
3. Clic en el signo “+”
4. En interface se selecciona Wan
5. En address se coloca la dirección ip predefinida en el diseño de red.
6. Clic en Apply y clic en OK

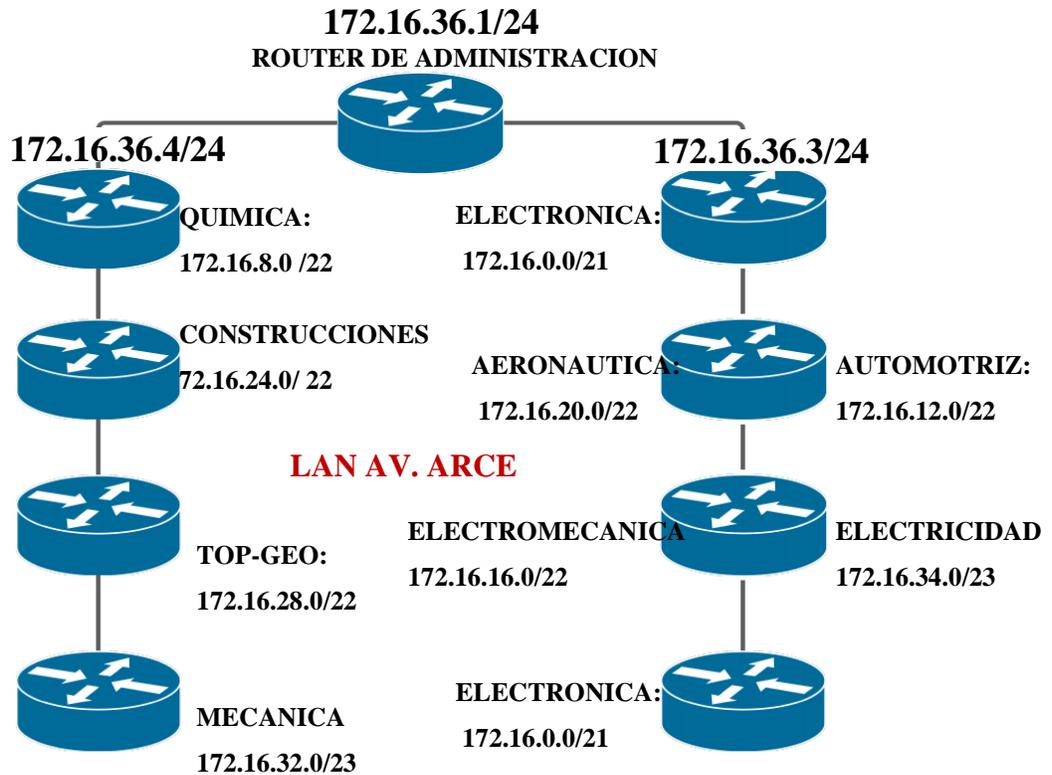
Figura 62. Asignación de Direcciones ip en Router Mikrotik



Fuente: Elaboración propia

Cada carrera contará con un router esto para configurar una red distinta, así de esta manera la difusión de broadcast será mínima, a continuación, se detalla las redes de cada carrera

Figura 63. diagrama de red con direcciones de red

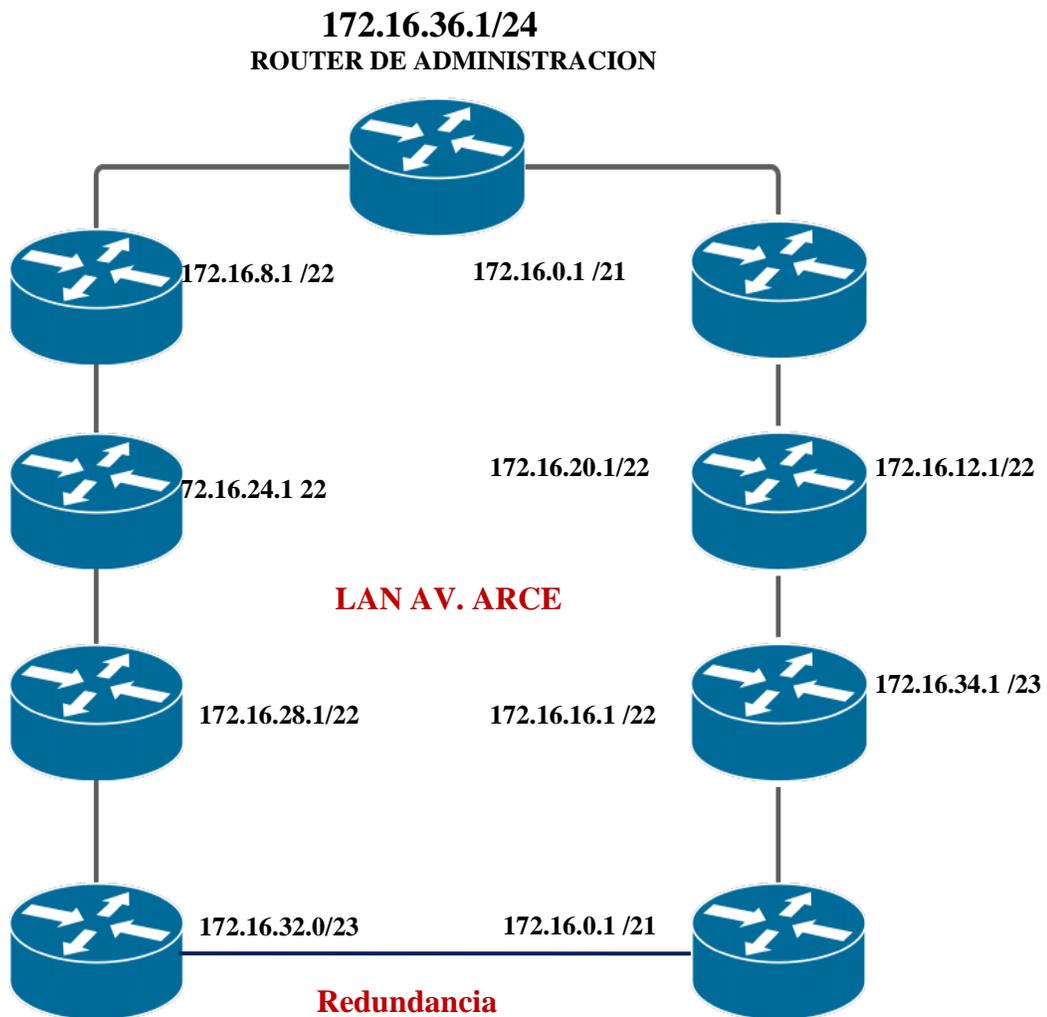


Fuente: Elaboración propia

3.3.2 Enrutamiento

Una vez direccionado todas las interfaces se procede a la interconexión de redes remotas, para ello debemos enrutar nuestra intranet.

Figura 64. *Distribución De Gateway*



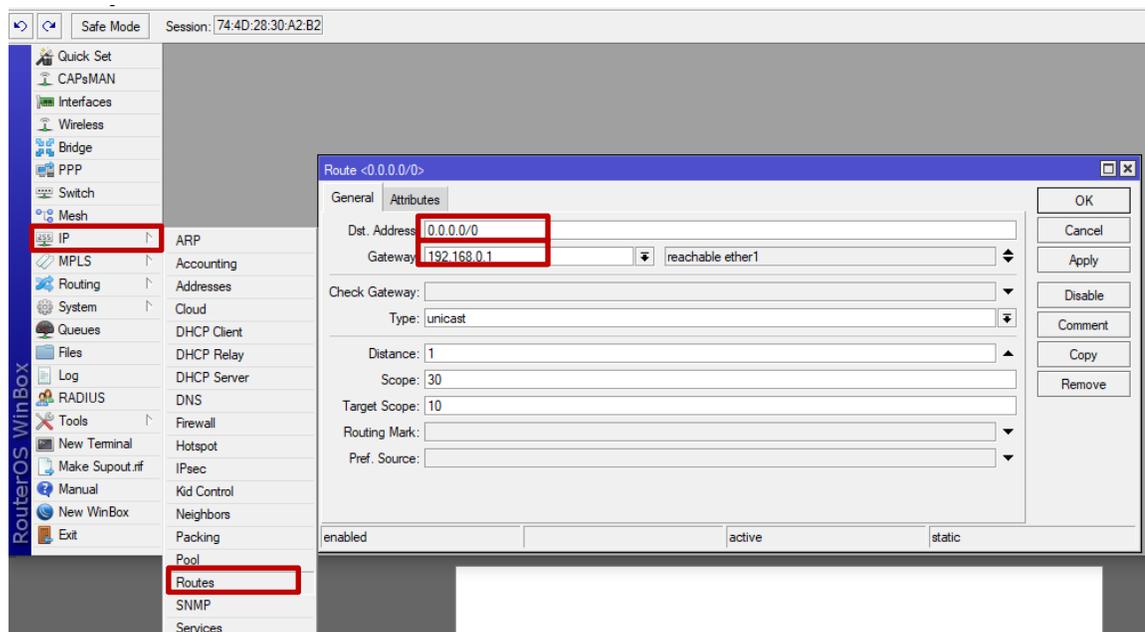
Fuente: Elaboración propia

Ruta estática para router de administración.

Ahora en los equipos mikrotik la forma de enrutar es la siguiente.

1. Se selecciona **IP** de la ventana principal
2. Se selecciona **Routers**
3. Clic en el signo “+”
4. En el espacio de **Gateway** colocar la ip del proveedor **192.168.0.1** esto en caso del router de administracion
5. Clic en **Apply** y clic en **OK**

Figura 65. Creación de rutas Estáticas



Fuente: Elaboración propia

En la dirección de red de destino (Dst Address) se coloca 0.0.0.0/0, esta dirección nos permite acceder a todas las redes remotas.

En la puesta de enlace (Gateway) se coloca la dirección de ip de nuestro router de frontera.

Ruta estática para routers de carrera

1. Seleccionamos **IP** de la ventana principal

2. Seleccionamos **Routers**
3. Clic en el signo “+”
4. En el espacio de **Gateway** colocar la ip del proveedor **172.16.35.1 esto en caso del router de administracion**
5. Clic en **Apply** y clic en **OK**

En este caso todos los routers tendrán salida a través de sus puertos 1 y 4 que estarán configurados en modo bridge juntamente con el bridge del router de administración.

3.3.3 Enlace de redundancia

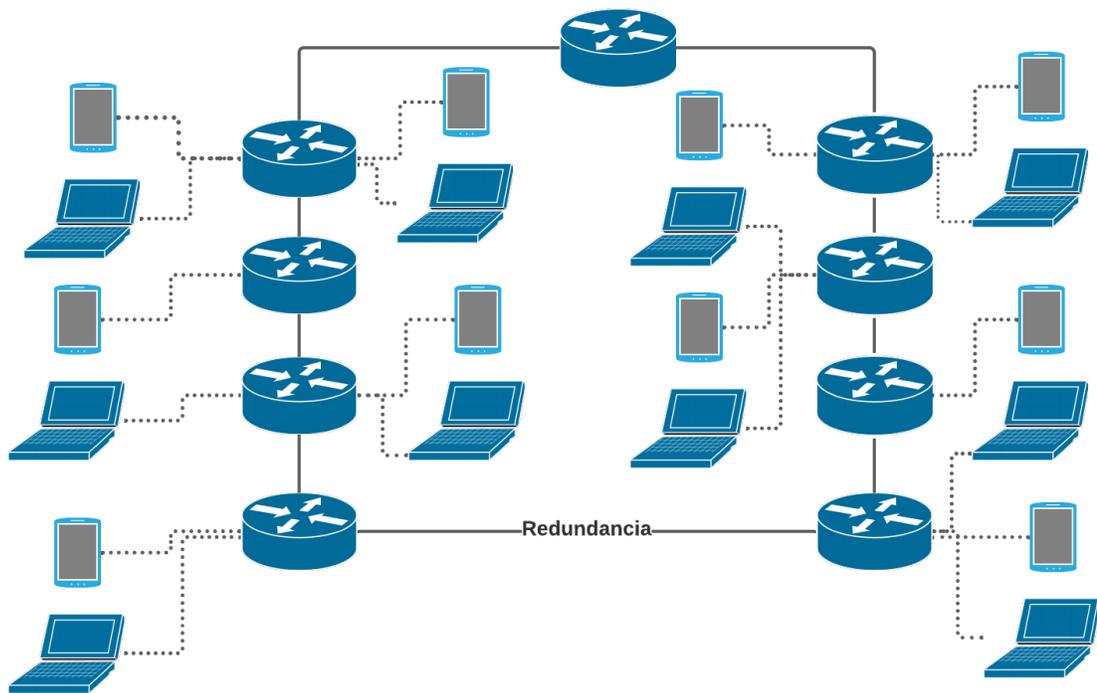
Este enlace nos permite tener otra alternativa de salida al router principal en caso de falla en los enlaces de Bridge.

3.4 Capa De Acceso A La Red

3.4.1 Topología.

La topología a implementarse será híbrida o mixta, esto debido a que los enlaces troncales serán en anillo y una conexión en estrella para los usuarios finales.

Figura 66. *Topología de red*



Fuente: Elaboración propia Propio

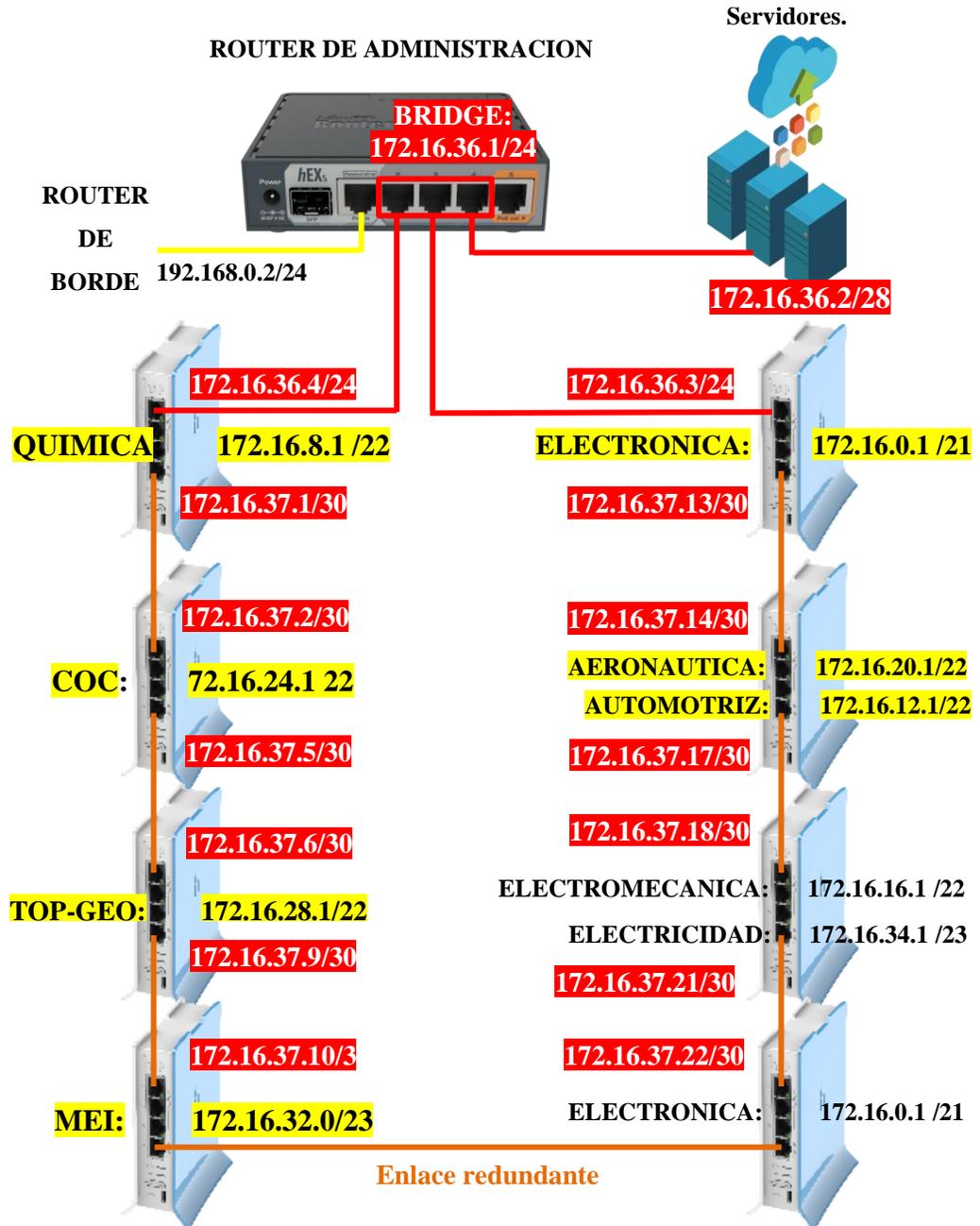
La topología en anillo de los enlaces troncales estará enlazada en dos puertos del router de administración, previamente configurada como puente, de esta forma si un enlace cae sigue se tendrá salida por el otro puerto.

Cada router de carrera estarán conectados a uno o dos routers rompe muros, así de esta manera se extenderá la intranet.

3.4.2 Bridge

El bridge tiene un papel muy importante en esta topología ya que gracias a esta no tendremos que enrutar cada puerto de nuestro router de administración.

Figura 67. Puentes en los Enlaces de Enrutamiento

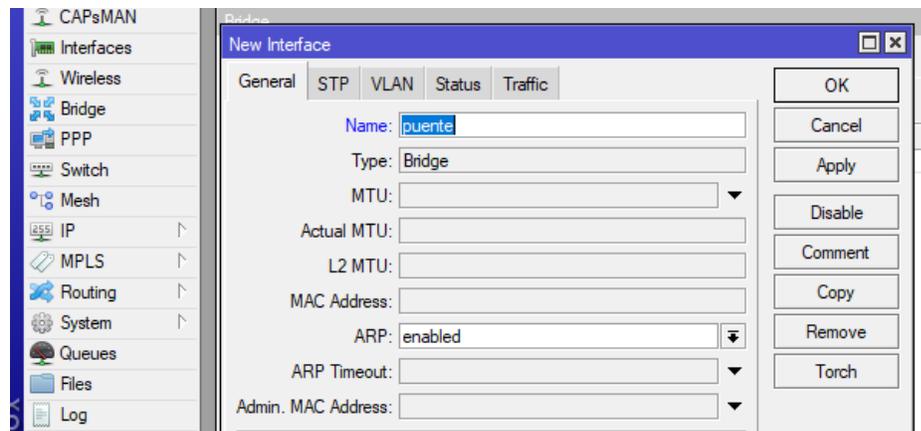


Fuente: Elaboración propia Propio

La configuración del bridge en los routers Mikrotik es la siguiente:

Accediendo a la pestaña de Bridge primero creamos un puente con el nombre puente.

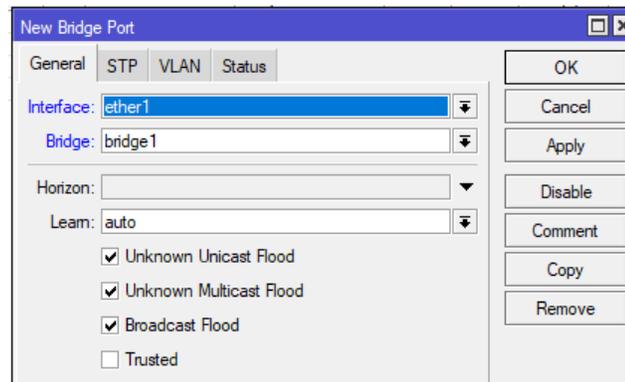
Figura 68. *Creación de Bridge en Mikrotik*



Fuente: Elaboración propia Propio

Luego añadimos los puestos a ese puente que creamos de la siguiente forma.

Figura 69. *Asignación de Interfaces al Bridge*



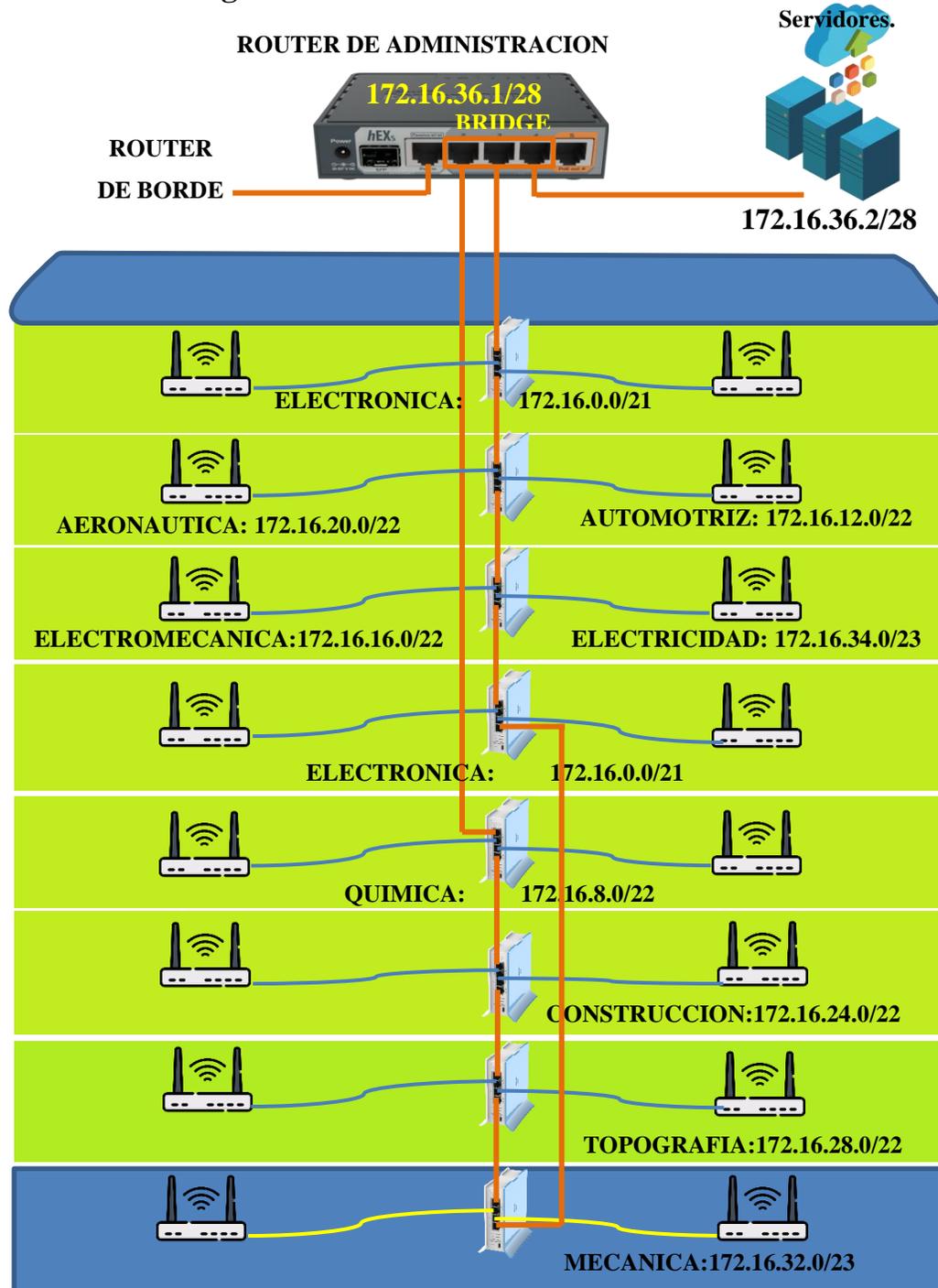
Fuente: Elaboración propia Propio

Como se mencionó a un principio de se añadirán los puestos 2,3 y 4 de router principal y los puertos 1 y 4 de los routers de carrera.

Y finalmente tendremos la siguiente estructura de la intranet de la av. Arce

RED. LAN AV. ARCE

Figura 70. Estructura de la Intranet de la av. Arce



Fuente: Elaboración propia Propio

3.4.3 Control de ancho de banda

Si se trabaja con un ancho de banda de 1Gbps, algo muy simple que podemos hacer es expresar este ancho de banda en kbps, y tendríamos que 1Gbps es 1000000kbps. Ahora esta velocidad se la divide entre la cantidad de alumnos de la facultad, y se tendrá.

$$\frac{1000000kbps}{7278} = 137.4kbps$$

Esta sería la velocidad de bajada por alumno, ahora podríamos tener el ancho de banda requerido por carrera según la cantidad de alumnado que esta tenga.

Figura 71. *Distribución de Ancho de Banda por Carrera*

	Carrera	2020	Ancho de banda
1	Electrónica y Telec.	1721	237 Mbps
2	Química Industrial	1020	140 Mbps
3	Mecánica Automotriz	897	123 Mbps
4	Electromecánica	861	118 Mbps
5	Aeronáutica	743	102 Mbps
6	Construcciones Civiles	667	92 Mbps
7	Topografía y Geodesia	602	83 Mbps
8	Mecánica Industrial	393	54 Mbps
9	Electricidad	374	51 Mbps
	total	7278	1000 Mbps

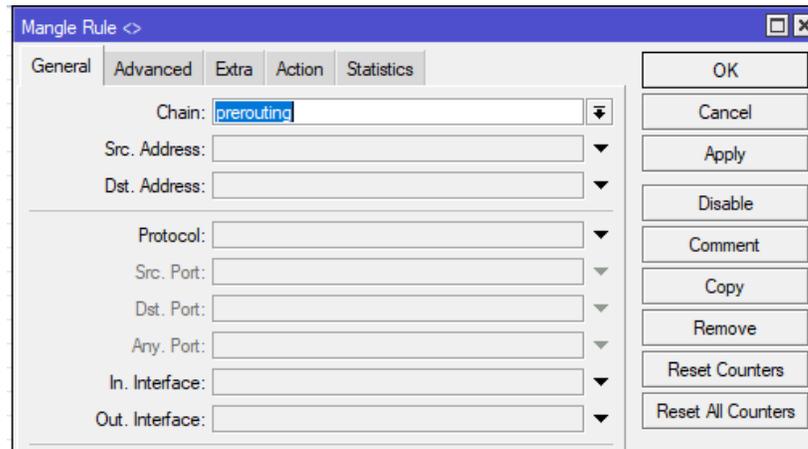
Fuente: Elaboración propia Propio

3.4.3.1 Mercado de conexión

Lo primero que se realizará será un mercado de conexión y posterior a ello el mercado de paquete. Las siguientes imágenes se realizará la configuración para una carrera. Primero se selecciona el tipo de cadena, y como vimos en la teoría

prerouting es el marcado de paquete antes que se el router tome ciertas decisiones como el enrutamiento.

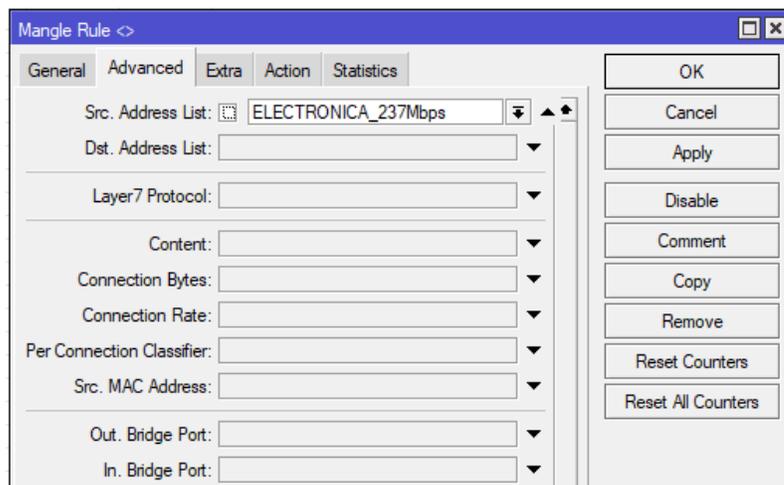
Figura 72. Preroutin En Mangle de Mikrotik



Fuente: Elaboración propia Propio

Luego asociaremos esta regla a una lista de direcciones llamada ELECTRONICA_237Mbps.

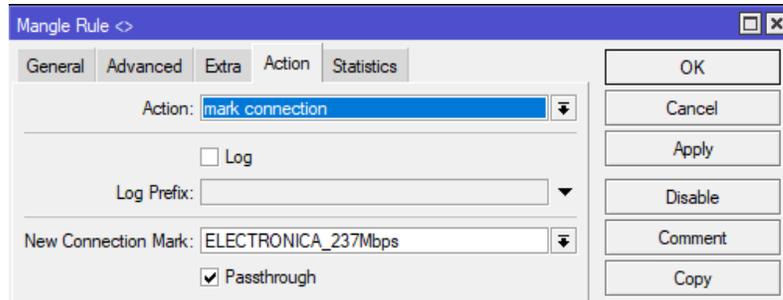
Figura 73. Asociamos mangle con una lista



Fuente: Elaboración propia Propio

Y por último en acción se selecciona marca de conexión (mark connection)ç

Figura 74. *Realizamos la marca de conexión*

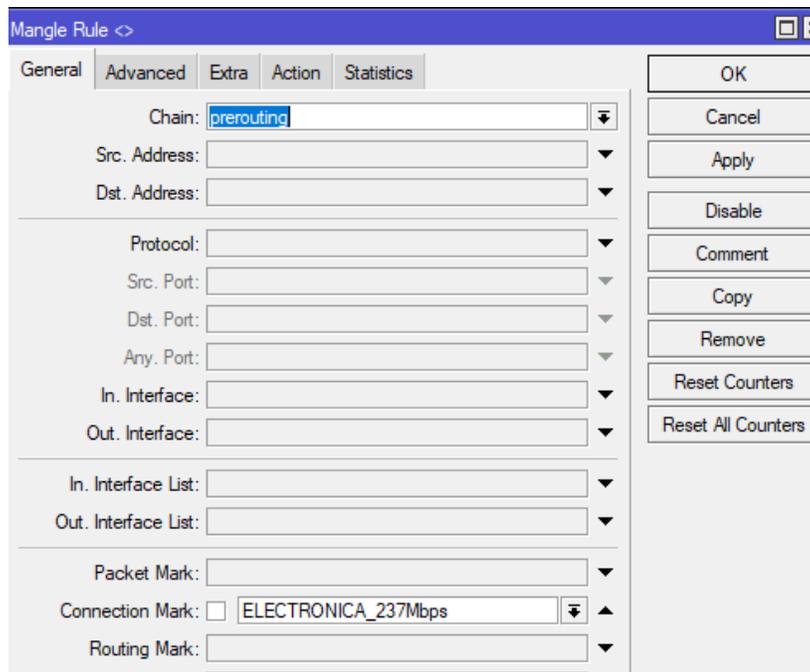


Fuente: Elaboración propia Propio

3.4.3.2 Marcado de conexión y paquetes

De igual manera se selecciona en chain prerouting y en marca de conexión seleccionamos la conexión que creamos.

Figura 75. *Relación de marca de paquete con la marca de conexión*

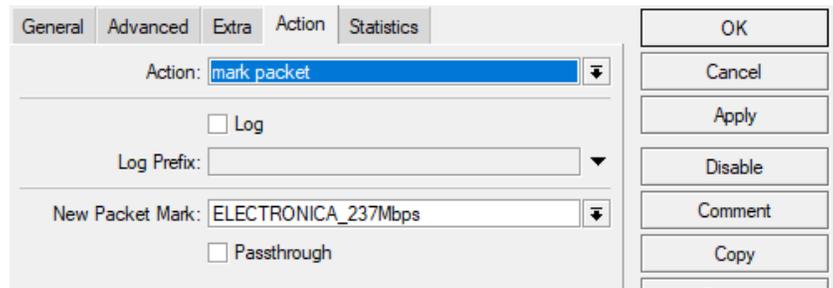


Fuente: Elaboración propia Propio

Y en acción se selecciona marcado de paquete (Mark packet), colocamos el nombre de la marca, y en la casilla de Passthrough se lo deselecciona, esto con el

fin de que si encontró la regla ya no evalué las demás reglas que sigue por debajo de ella.

Figura 76. Creamos una marca de paquete



Fuente: Elaboración propia Propio

Realizamos esta configuración para cada una de las carreras, y como resultado se tendrá las siguientes reglas de mangle.

Figura 77. Reglas de marcado de conexión y de paquetes

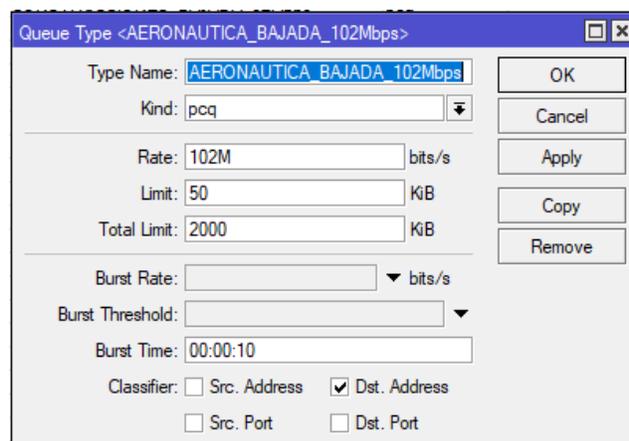
#	Action	Chain	Src. Address List	Dst. Ad...	Bytes	Packets
::: ELECTRONICA_237Mbps						
0	mark connection	prerouting	ELECTRONICA_237Mbps		0 B	0
1	mark packet	prerouting			0 B	0
::: QUIMICA_140Mbps						
2	mark connection	prerouting	QUIMICA_140Mbps		0 B	0
3	mark packet	prerouting			0 B	0
::: AUTOMOTRIZ_123Mbps						
4	mark connection	prerouting	AUTOMOTRIZ_123Mbps		0 B	0
5	mark packet	prerouting			0 B	0
::: ELECTROMECHANICA_118Mbps						
6	mark connection	prerouting	ELECTROMECHANICA_118Mbps		0 B	0
7	mark packet	prerouting			0 B	0
::: AERONAUTICA_102Mbps						
8	mark connection	prerouting	AERONAUTICA_102Mbps		0 B	0
9	mark packet	prerouting			0 B	0
::: CONSTRUCCIONES_92Mbps						
10	mark connection	prerouting	CONSTRUCCIONES_92Mbps		0 B	0
11	mark packet	prerouting			0 B	0
::: TOPOGRAFIA_83Mbps						
12	mark connection	prerouting	TOPOGRAFIA_83Mbps		0 B	0
13	mark packet	prerouting			31.4 MB	46 112
::: MECANICA_54Mbps						
14	mark connection	prerouting	MECANICA_54Mbps		0 B	0
15	mark packet	prerouting			0 B	0
::: ELECTRICIDAD_51Mbps						
16	mark connection	prerouting	ELECTRICIDAD_51Mbps		23.9 MB	51 561
17	mark packet	prerouting			84.3 MB	134 556

Fuente: Elaboración propia Propio

3.4.3.3 Tipo de cola (Queues Types)

Luego se procede a crear el tipo de cola (Queues Types), colocamos un nombre al tipo de encolamiento que usaremos, que para el caso será PCQ, y en Rate colocamos el ancho de banda para esa cola, que para el ejemplo es 102Mbps, y en classifier seleccionamos Dst. Address ya que la bajada será de una dirección de destino.

Figura 78. Creación De Un Tipo De Cola Para Control De Ancho De Banda

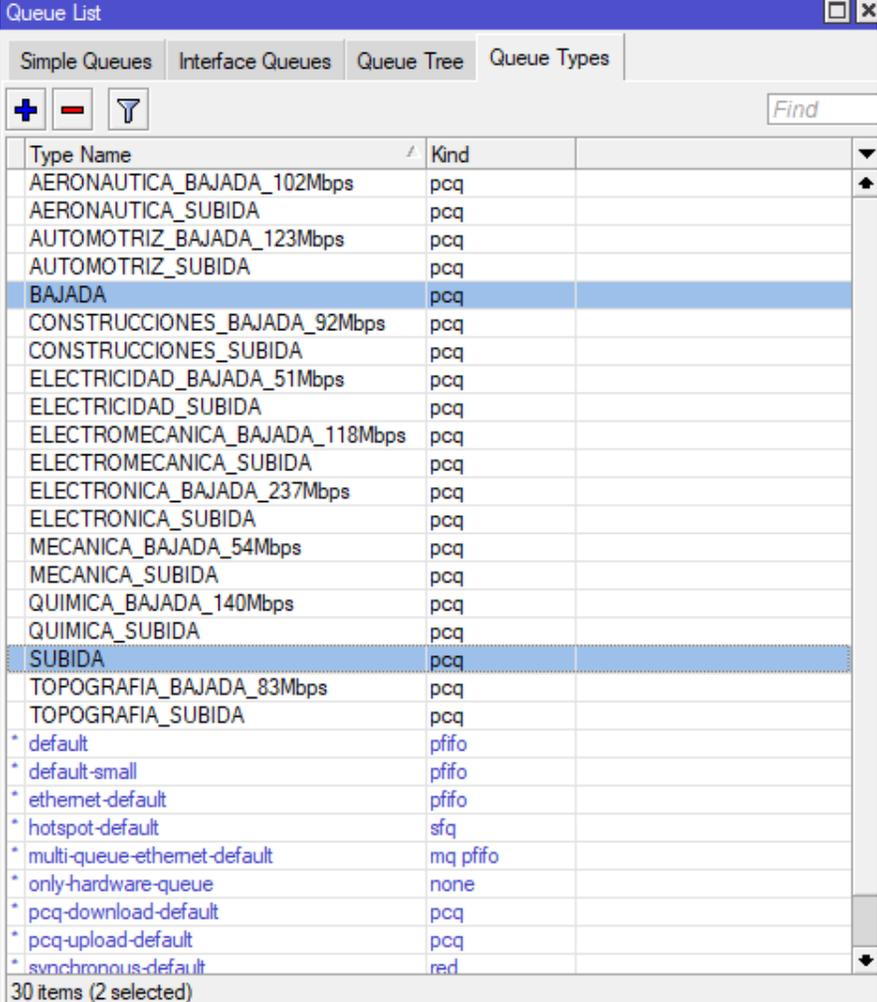


Fuente: Elaboración propia Propio

Para el tráfico de subida la casilla de classifier marcamos la casilla de Src. address esto porque es referente a un tráfico de origen.

Realizaremos esta configuración de manera similar para las demás carreras y tendremos los siguiente.

Figura 79. *Queue List*



The screenshot shows a window titled "Queue List" with tabs for "Simple Queues", "Interface Queues", "Queue Tree", and "Queue Types". Below the tabs are icons for adding (+), removing (-), and filtering (funnel), along with a "Find" search box. The main area contains a table with the following data:

Type Name	Kind
AERONAUTICA_BAJADA_102Mbps	pcq
AERONAUTICA_SUBIDA	pcq
AUTOMOTRIZ_BAJADA_123Mbps	pcq
AUTOMOTRIZ_SUBIDA	pcq
BAJADA	pcq
CONSTRUCCIONES_BAJADA_92Mbps	pcq
CONSTRUCCIONES_SUBIDA	pcq
ELECTRICIDAD_BAJADA_51Mbps	pcq
ELECTRICIDAD_SUBIDA	pcq
ELECTROMECANICA_BAJADA_118Mbps	pcq
ELECTROMECANICA_SUBIDA	pcq
ELECTRONICA_BAJADA_237Mbps	pcq
ELECTRONICA_SUBIDA	pcq
MECANICA_BAJADA_54Mbps	pcq
MECANICA_SUBIDA	pcq
QUIMICA_BAJADA_140Mbps	pcq
QUIMICA_SUBIDA	pcq
SUBIDA	pcq
TOPOGRAFIA_BAJADA_83Mbps	pcq
TOPOGRAFIA_SUBIDA	pcq
* default	pfifo
* default-small	pfifo
* ethernet-default	pfifo
* hotspot-default	sfq
* multi-queue-ethernet-default	mq pfifo
* only-hardware-queue	none
* pcq-download-default	pcq
* pcq-upload-default	pcq
* synchronous-default	red

30 items (2 selected)

Fuente: Elaboración propia Propio

También se crea dos reglas más de subida y bajada para las colas padre

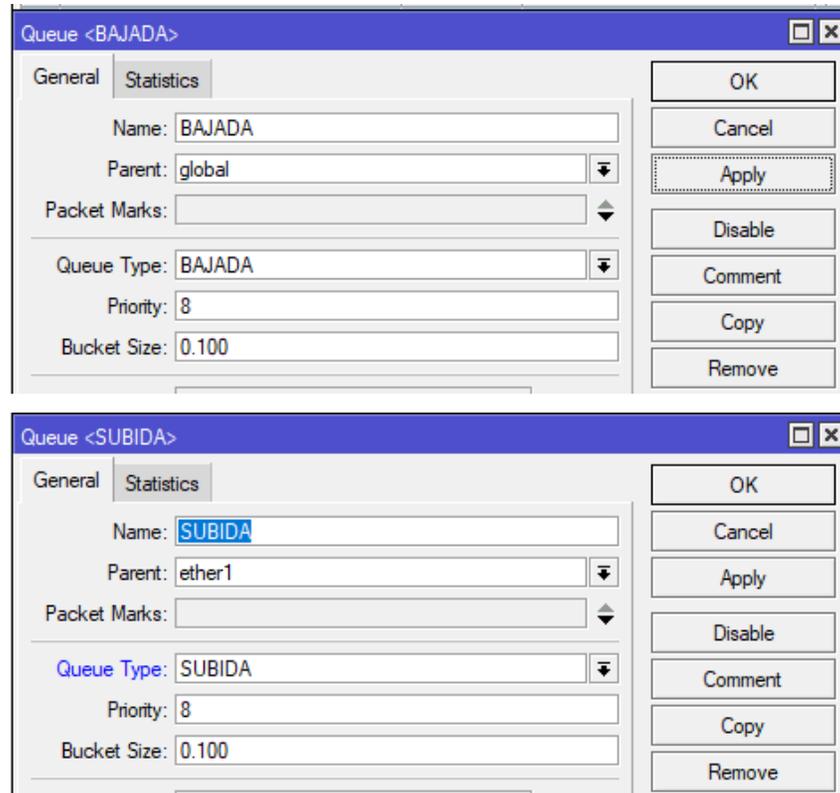
3.4.3.4 Arbol de cola (Queue Tree)

Una vez creado los tipos de cola se procede a crear la estructura del árbol de colas.

Colas padres

Primero creamos una cola global de bajada y subida de datos, y seguidamente creamos las colas hijas

Figura 80. *Queue de Bajada y Subida*



Fuente: Elaboración propia Propio

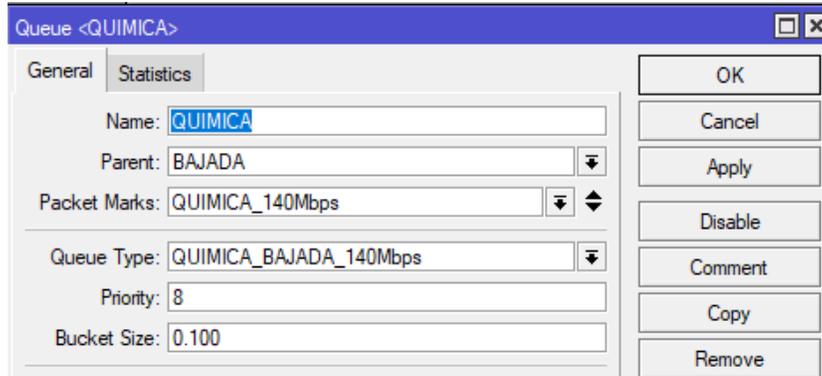
Colas hijas

Para crear las colas hijas se debe tomar más parámetros:

- Primero se coloca el nombre de la cola.
- Luego se selecciona el parentesco si es de bajada o subida
- Se selecciona la marca de paquete
- Y el tipo de cola
- También se podría colocar una prioridad

La configuración será tal como en la siguiente imagen.

Figura 81. Configuración De Ancho De Banda Por Carrera



Fuente: Elaboración propia Propio

El árbol de colas quedará así:

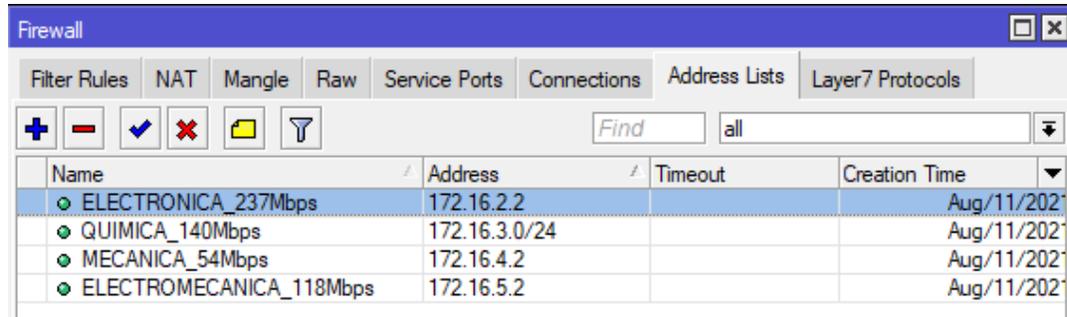
Figura 82. Árbol de colas final

Name	Parent	Packet Marks
BAJADA	global	
AERONAUTICA	BAJADA	AERONAUTICA_102Mbps
AUTOMOTRIZ	BAJADA	AUTOMOTRIZ_123Mbps
CONSTRUCCION	BAJADA	CONSTRUCCIONES_92Mbps
ELECTRICIDAD	BAJADA	paquete_Electricidad_51Mbps
ELECTROMECHANICA	BAJADA	ELECTROMECHANICA_118Mbps
ELECTRONICA	BAJADA	ELECTRONICA_237Mbps
MACANICA	BAJADA	MECANICA_54Mbps
QUIMICA	BAJADA	QUIMICA_140Mbps
TOPOGRAFIA	BAJADA	paquete_Topografia_83Mbps
SUBIDA	ether1	
AERONAUTICA_SUBIDA	SUBIDA	AERONAUTICA_102Mbps
AUTOMOTRIZ_SUBIDA	SUBIDA	AUTOMOTRIZ_123Mbps
CONSTRUCCION_SUBIDA	SUBIDA	CONSTRUCCIONES_92Mbps
ELECTRICIDAD_SUBIDA	SUBIDA	paquete_Electricidad_51Mbps
ELECTROMECHANICA_SUBIDA	SUBIDA	ELECTROMECHANICA_118Mbps
ELECTRONICA_SUBIDA	SUBIDA	ELECTRONICA_237Mbps
MECANICA_SUBIDA	SUBIDA	MECANICA_54Mbps
QUIMICA_SUBIDA	SUBIDA	QUIMICA_140Mbps
TOPOGRAFIA_SUBIDA	SUBIDA	paquete_Topografia_83Mbps

Fuente: Elaboración propia Propio

Y finalmente se agrega las direcciones ip o las direcciones de red en address list.

Figura 83. *Lista de direcciones*



The screenshot shows a 'Firewall' window with several tabs: Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. The 'Address Lists' tab is active. Below the tabs are several icons and a search box containing 'Find' and 'all'. A table lists the address lists with columns for Name, Address, Timeout, and Creation Time.

Name	Address	Timeout	Creation Time
ELECTRONICA_237Mbps	172.16.2.2		Aug/11/2021
QUIMICA_140Mbps	172.16.3.0/24		Aug/11/2021
MECANICA_54Mbps	172.16.4.2		Aug/11/2021
ELECTROMECHANICA_118Mbps	172.16.5.2		Aug/11/2021

Fuente: Elaboración propia Propio

3.4.4 Equipos

3.4.4.1 Servidor

Para la intranet haremos uso del servidor DL380p Gen8 Management Server.

Figura 84. *servidor DL380p Gen8 Management Server*



Fuente: etb-tech.com

- Alto rendimiento con dos procesadores de 6 núcleos Intel Xeon E5-2620 (2,0 GHz, 6 núcleos)
- 24 gigas de RAM con capacidad de expandirse
- 8 slots para insertar discos duro compatible con memorias SAS el cual duplica la velocidad de una conexión sata.
- 2 fuentes de de 460 watts para proporcionar un sistema ininterrumpido
- puertos rj45 GigabitEthernet

Procesador Xeon

Los procesadores Xeon está destinado a estaciones de trabajo como los servidores, capaces de funcionar ininterrumpidamente ya que su sistema siempre tiene que estar online.

Podemos mencionar 3 características principales de estos procesadores.

- **Núcleos:** Xeon cuentan con mayor cantidad de núcleos, esto nos da gran ventaja ya que el procesador será capaz de realizar múltiples procesos de usuarios y consultas a bases de datos.
- **Tiempo de uso:** El tiempo en que un procesador puede estar encendido es indefinido, esto debido a que un servidor siempre tiene que estar en línea.
- **Caché L3:** Es la memoria que se encarga de tener listos los datos para ser ejecutados, los procesadores Xeon cuentan con una mayor memoria caché L3, por lo que nos ayudara a tener un sistema más rápido para nuestra intranet.

3.4.4.2 Router de administración

El enrutador que se usara como router de administración es el RB760iGS este es un enrutador Gigabit Ethernet de cinco puertos y un puerto SFP y salida PoE en el último puerto, será adecuado con nuestro servidor ya que trabajaran a las mismas velocidades (1Gbps).

Figura 85. *RB760iGS*



Fuente: mikrotik.com

Este enrutador cuenta con las siguientes características

Especificaciones

- Recuento de núcleos de CPU 2
- Frecuencia nominal de la CPU 880 MHz
- Recuento de subprocesos de la CPU 4
- Dimensiones 113 x 89 x 28 mm
- Licencia de RouterOS 4
- Sistema operativo RouterOS
- Tamaño de RAM 256 MB
- Tamaño de almacenamiento 16 MB
- Aceleración de hardware IPsec sí

Alimentando

- Número de entradas DC 2 (toma de CC, PoE-IN)
- Voltaje de entrada DC jack 12-57 V
- Consumo máximo de energía 24 W
- Consumo máximo de energía sin accesorios 6 W
- Recuento de ventiladores Pasivo
- PoE en 802.3af / en
- PoE en voltaje de entrada 12-57 V

PoE-out

- Puertos de salida PoE Ether 5
- PoE hacia fuera PoE pasivo hasta 57 V
- Salida máxima por puerto de salida (entrada 18-30 V) 500 mA
- Salida máxima por puerto de salida (entrada 30-57 V) 500 mA
- Salida total máxima (A) 500 mA

Ethernet

- Puertos Ethernet 10/100/1000 5

Fibra

- Puertos SFP 1

Periféricos

- Tipo de tarjeta de memoria microSD
- Tarjetas de memoria 1
- Numero de puertos USB 1
- Tipo de ranura USB USB tipo A
- Corriente USB máxima (A) 1

Otro

- Monitor de temperatura de PCB sí
- Monitor de voltaje sí

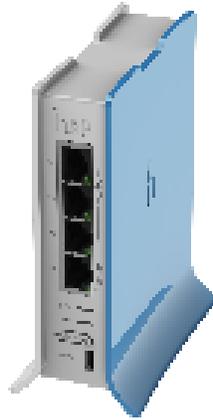
El enrutador admite el cifrado de hardware IPsec (~ 470 Mbps) y el paquete de servidor Dude.

3.4.4.3 Routers secundarios

Los router que se usará será el RB941-2nd de licencia RouterOS L4, también conocido como hAP lite está equipado con una potente CPU de 650 MHz, 32 MB de RAM, conexión inalámbrica integrada de doble cadena de 2,4 GHz, cuatro puertos Fast Ethernet.

Estos router se usarán en las carreras como routers de administración, aunque también podría usarse el RB760IGS para carreras de mayor demanda.

Figura 86. *RB941-2nd*



Fuente: mikrotik.com

3.4.4.4 Puntos de acceso

Como router para usuarios finales se usará el router TPLINK TL-WR941HP enrutador inalámbrico de alta potencia, trabaja a una velocidad de 450 Mbps.

Cuenta con amplificadores de alta potencia y las antenas de alta ganancia con una distancia que sobrepasa los 30 metros en espacio abierto.

Señal de Wi-Fi mejorada puede penetrar paredes y obstáculos, eliminando así las zonas muertas.

Figura 87. *TPLINK TL-WR941HP*

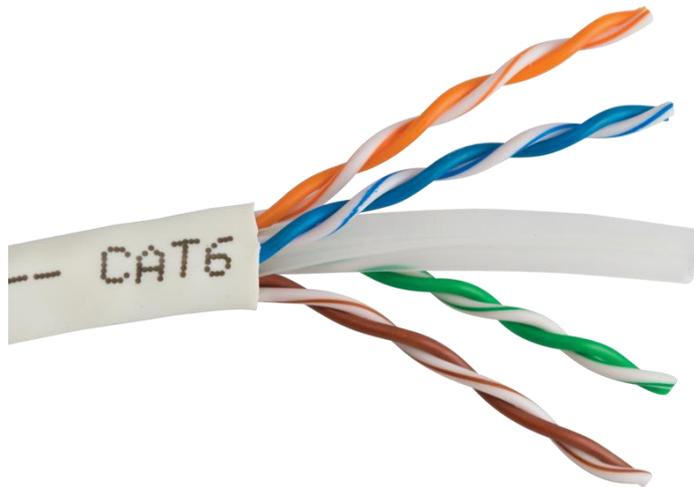


Fuente: tp-link.com

3.4.4.5 Líneas de conexión

Las líneas de conexión que usaremos para las troncales serán los cables utp CAT 6. es un cable de par trenzado estandarizado para Ethernet, estos cables admiten segmentos Gigabit Ethernet de hasta 100m, y 10 Gigabits a cortas distancias.

Figura 88. *Cable Utp CAT 6*



Fuente: alibaba.com

Ancho de banda

Esta categoría puede trabajar con velocidades de hasta 1000 Mbps, equivalente a 1 Gigabit por segundo. Esta categoría a su vez trabaja con frecuencias de hasta 250 MHz, a diferencia de la cat5e que solo trabaja a 100Mhz. Esto a su vez procesa más datos al mismo tiempo.

Velocidad

Debido a que la cat6 trabaja a 250 MHz, ofrecen velocidades de hasta 10GBASE-T o 10 Gigabits Ethernet.

3.4.5 Normas de instalación y cableado estructurado

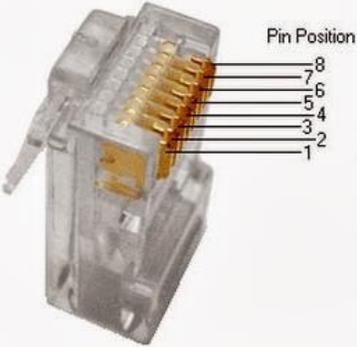
El cableado estructurado es un diseño de red de transmisión física capaz de ser adaptado a cualquier aplicación como telefonía o redes locales ethernet.

La norma ANSI/TIA/EIA-568-A, especifica ciertos criterios técnicos y de rendimiento de equipos de telecomunicaciones y sus respectivas configuraciones, así como también del sistema de cableado.

3.4.5.1.1 Norma de Código de Colores 568A y 568B Estándar para ponchado de cable UTP y el orden de los colores de estos, La Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias de Electrónica (EIA), especifican los estándares para cableado estructurado de voz y datos para las LAN.

Con esta norma no se tendrán problemas de compatibilidad en la transmisión de ciertas aplicaciones, de voz datos imágenes o videos.

Figura 89. Conexión RJ45 normas T568A y T568B

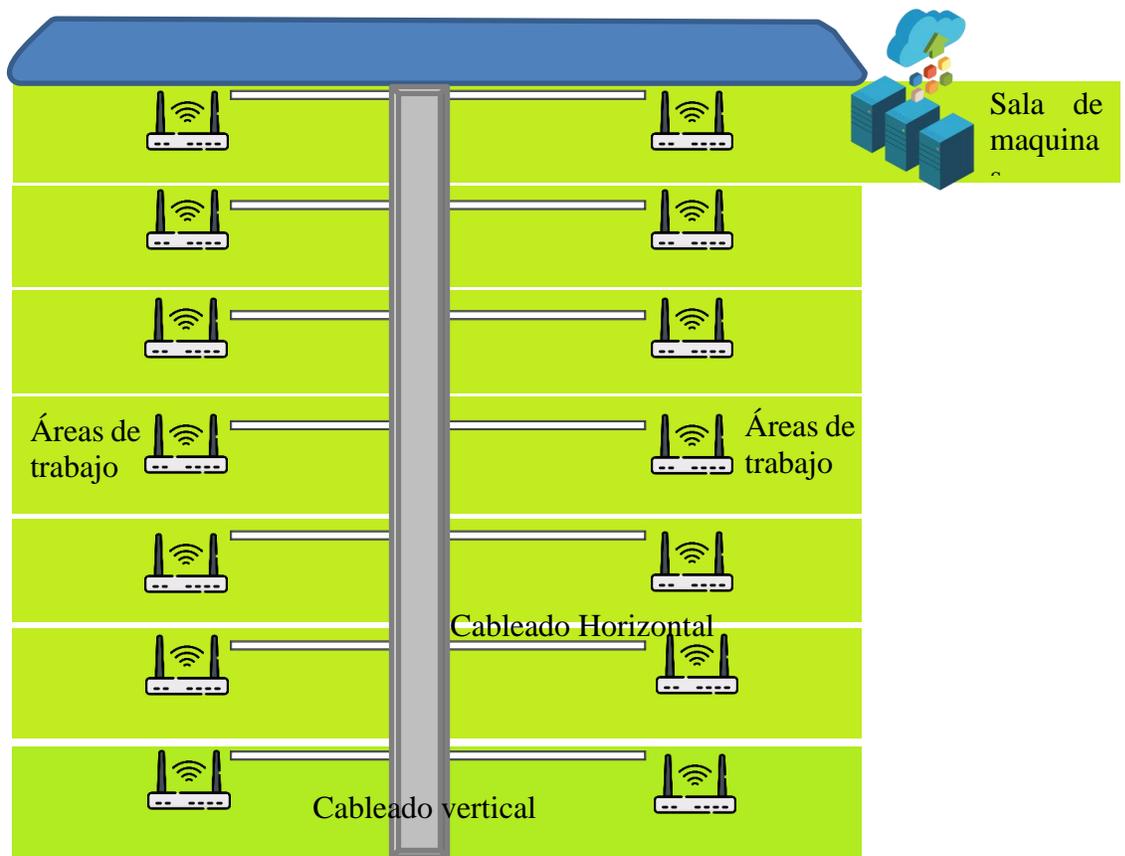
Pin	Cable	Color, T568A	Color, T568B	RJ45 pines
1	positivo	 blanco/verde rayado	 blanco/naranja rayado	
2	negativo	 verde entero	 naranja entero	
3	positivo	 blanco/naranja rayado	 blanco/verde rayado	
4	negativo	 azul entero	 azul entero	
5	positivo	 blanco/azul rayado	 blanco/azul rayado	
6	negativo	 naranja entero	 verde entero	
7	positivo	 blanco/marrón rayado	 blanco/marrón rayado	
8	negativo	 marrón entero	 marrón entero	

Fuente: elcapored.jimdofree.com

3.4.5.1.2 **ANSI/TIA/EIA 569 A.** este estándar define las normas básicas del diseño dentro de edificios, que para este estudio es la facultad de tecnología.

1. La sala de máquinas estará ubicada en el un gabinete ubicado en el 7mo piso.
2. Para el cableado central se usará la infraestructura del cableado de la facultad de tecnología
3. Para el cableado horizontal se hará uso del cable ducto horizontal de la facultad de tecnología.
4. El área de trabajo, es un área de al menos 10m², donde termina el sistema de cableado horizontal, serán las aulas de la facultad de tecnología. La ubicación por lo general es un metro de la salida eléctrica.

Figura 90. *diseño de cableado estructurado*



Fuente: Elaboración propia Propio

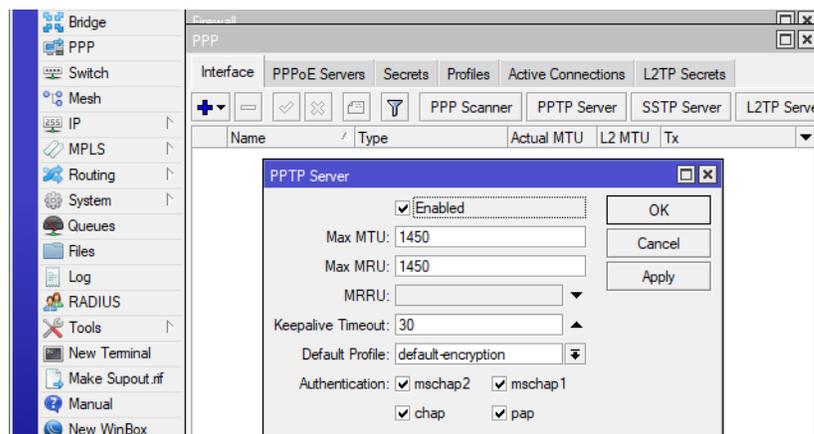
3.5 VPN

3.5.1 Protocolo de Tunelización de Punto a Punto (PPTP)

El protocolo de tunelización que usaremos en el proyecto será el PPTP, ya que a sus características será útil para aplicaciones que usan streaming de audio o video, en las cuales la velocidad es fundamental.

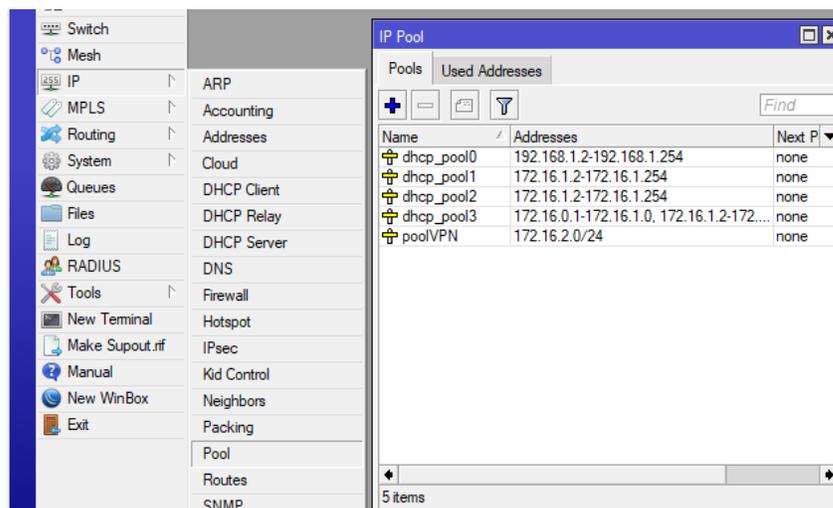
3.5.2 VPN en Mikrotik

Figura 91. *Habilitación del servicio en router De servicio*



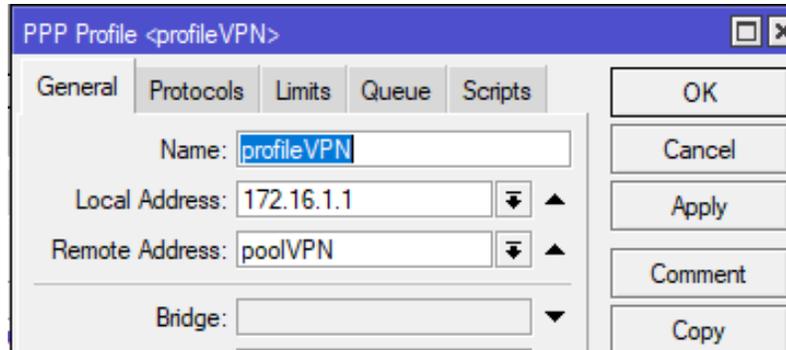
Fuente: Elaboración propia Propio

Figura 92. *Creamos un pool de direcciones*



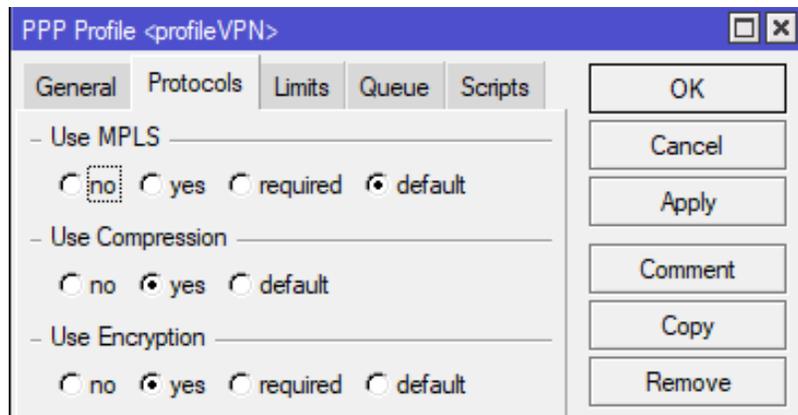
Fuente: Elaboración propia Propio

Figura 93. *Se crea un perfil VPN*



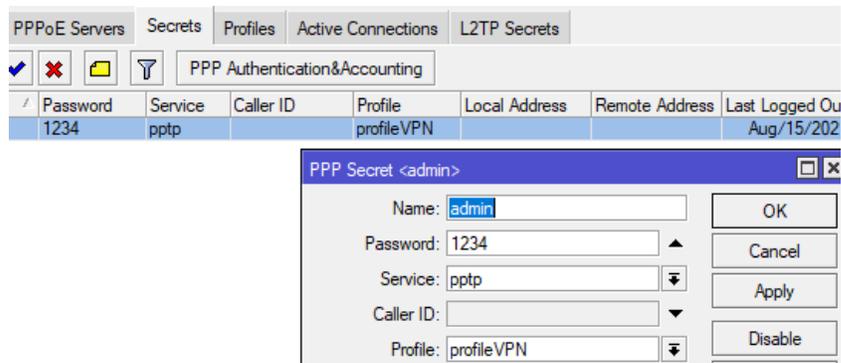
Fuente: Elaboración propia Propio

Figura 94. *Se habilita la compresión y la encriptación*



Fuente: Elaboración propia Propio

Figura 95. *Claves secretas*



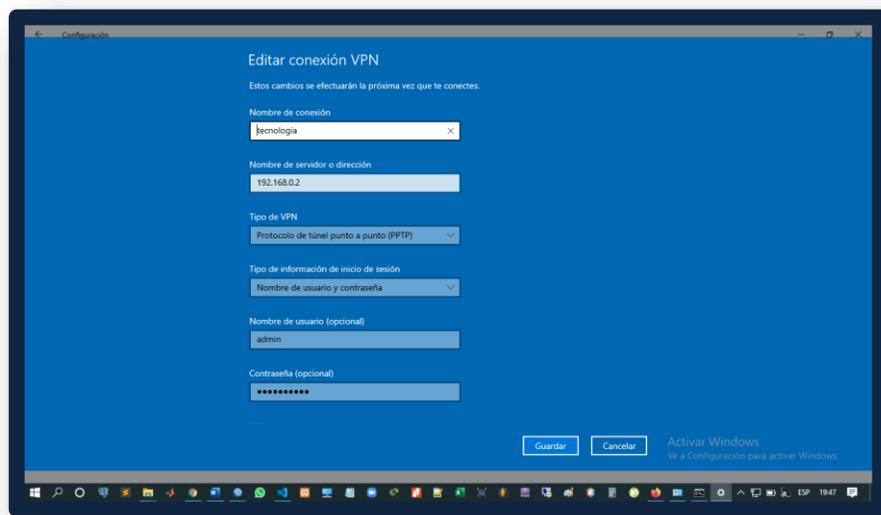
Fuente: Elaboración propia Propio

Figura 96. Configuración de VPN en celulares



Fuente: Elaboración propia Propio

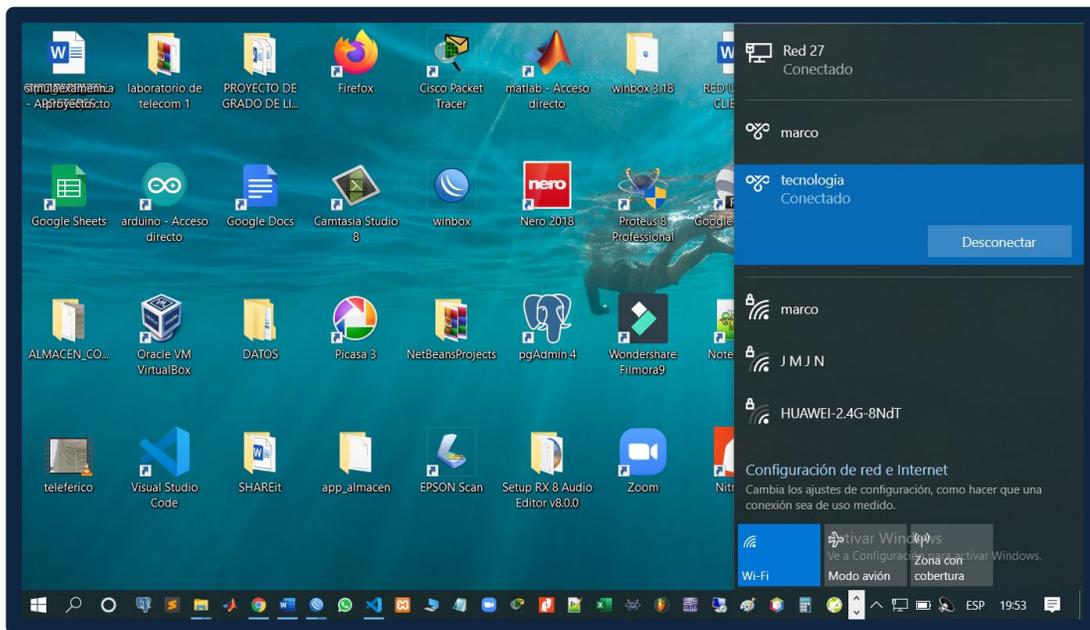
Figura 97. Configuración de VPN en PC



Fuente: Elaboración propia Propio

Usuario: admin
Contraseña: 1234

Figura 98. Activación de las VPN



Fuente: Elaboración propia Propio

CAPÍTULO IV.

4.1 Cronograma de implementación

Nro.	Nombre de tarea	Duración	Septiembre				Octubre				
			1s	2s	3s	4s	1s	2s	3s	4s	
1	Adquisición de material y equipos	1 meses									
2	Instalación del servidor en cuarto de maquinas	1 día									
3	Instalación de router de administración en cuarto de maquinas	1 día									
4	Cableado horizontal	3 días									
5	Cableado vertical	3 días									
6	Instalación de router en áreas de trabajo	3 días									
7	Configuración general del servidor	1 día									
8	Configuración general del routers	3 días									
9	Pruebas	1 semana									
10	Puesta en servicio	1 día									

4.2 Estructura De Costos

Hardware			
Nombre	Cantidad	Precio unitario (Bs)	Precio (Bs)
Servidor DL380p Gen8	1	4000	4000,00
RB760iGS	1	800	800,00
RB941-2nd	8	300	2800,00
TPLINK TL-WR941HP	16	200	3200,00
Cable UTP cat6	610m	800	1600,00
Cable ducto 20x10	610	4	2440,00
Tornillos	paquete	35	35,00
Rj45	paquete	170	170,00
Total			15045,00

Software			
nombre	Cantidad	Precio unitario (Bs)	Precio (Bs)
Licencia Windows server 12 r2.	1	1.450,00	1.450,00
Apache server	1	Libre	0
Base de datos MySql	1	Libre	0
Servidor DNS	1	Paquete gratuito	0

Total			1.450,00
-------	--	--	----------

Mano de obra			
Nombre	Cantidad	Precio unitario (Bs)	Precio (Bs)
Instalación del servidor en cuarto de maquinas	2 personas	200	400
Instalación de router de administración en cuarto de maquinas	1 persona	200	200
Cableado horizontal	2 personas	250	500
Cableado vertical	2 personas	250	500
Instalación de router en áreas de trabajo	1 persona	200	200
Configuración general del servidor	1 persona	400	400
Configuración general del routers	1 persona	400	400
Pruebas	1 persona	200	200
Total			2800,00

Costo total

nombre	Precio unitario (Bs)
Hardware	15045,00
Software	1.450,00
Mano de obra	2800,00
Total	19295

4.3 Conclusiones

- Utilizando tecnologías de software libre y con hardware asequible a la nuestra economía, se diseñó una intranet capaz de gestionar recursos académicos para los estudiantes, se presentó algo de inconvenientes con la velocidad, esto debido a que también dependerá de la cantidad de procesadores que tendrá nuestro servidor. Respecto al ancho de banda no se tuvo ningún problema ya que actualmente se cuentan con medios de transmisión y equipos capaces de trabajar en 1000BASE-T
- Implementado el servidor HTTP se logró que usuarios de la intranet puedan acceder a él, se tubo cierta complicación con el acceso de dispositivos móviles ya que XAMPP tiene desactivado esta opción por defecto. Respecto a la subida de archivos de gran tamaño se presentó un problema, esto porque XAMPP por defecto permite subir archivos de un tamaño máximo de 2MB, se solucionó realizando configuraciones en el servidor
- Con las tecnologías HTML, CSS, JS, PHP y JSON Se implementó con éxito aplicaciones web que pueden gestionar los recursos ofrecidos por la intranet, ya sea desde una computadora o dispositivos móviles, se tuvo algunas complicaciones a la hora de implementar nuevas tecnologías como HTML5 Y NODE, esto porque algunos navegadores web no lo soportan, se usó PHP en remplazo de NODE.
- Se dimensiono se manera óptima la distribución del ancho de banda según la población estudiantil de cada carrera, esto se logró realizando un marcado de paquete, conexión y Queue Tree de Mikrotik.
- La velocidad de conexión se logró dimensionar relativamente bien, aunque tomando en cuenta que se está transmitiendo streaming de video utilizando la VPN puede

reducir un poco la velocidad, esto debido a que todo el contenido este comprimido y cifrado.

- La VPN se implementó con PPTP, esto debido a que manejaremos streaming de video y nos ayudara a optimizar la transmisión.

4.4 Recomendaciones

Los servidores de hoy en día tienen mucha más capacidad de los servidores, se recomienda actualizar los procesadores que usara el servidor de nuestra intranet, para evitar que se lentee el sistema.

Utilizar transceptores SFP si quiere trabajar con fibra óptica o en su defecto cables utp con el mayor porcentaje de aleación de cobre que sea posible.

Se recomienda implementar un sistema de monitoreo como el dude de Mikrotik, pero también se recomienda dividir las funciones del router de administración si es que se quiere implementar un servidor en ese router, esto con el fin de no forzar el procesamiento del router.

Por el momento el sistema de gestión audiovisual está trabajando en la tecnología PHP, presentara un poco de lentitud si se habla de almacenar millones de archivos, para ello se recomienda usar tecnología JSON.

Si se pretende implementar un sistema de video conferencias como zoom se recomienda quitar la VPN ya que podría traer retrasos en la comunicación.

Si se pretende que la intranet se pueda acceder desde la internet se recomienda alquilar una dirección ip Publica o contratar una empresa de internet que tengan liberados los puertos 80, esto con el fin de que los usuarios no tengan problemas de conexión hacia el servidor.

Se recomienda usar discos SAS para el servidor, debido a su comunicación serial, lo hace mucho más rápido en la transmisión de datos. También se recomienda el uso de procesadores Xeon estos porque pueden procesar más tareas al mismo tiempo, de esta manera nuestra intranet será más rápido y eficiente.

Si se pretende subir la seguridad de la VPN, se recomienda utilizar L2TP/IPsec.

En caso de tener routers que no soporten el sistema de gestión DUDE se recomienda virtualizar un sistema operativo ROUTEROS en el servidor.

Con el fin de no perder datos por fallas en discos duros se recomienda crear un respaldo en el servidor con arreglo RAID 1.

Académicamente si se desea subir clases virtuales se lo haga con previa edición de video para eliminar inconvenientes o hacer más dinámico el recurso.

Se recomienda a los administradores de la intranet colocar una clave segura y no compartir su contraseña, ya que ellos tienen privilegios de eliminar y modificar cualquier información de su carrera.

Referencias Bibliográficas

BCHILLERATO CD. SAHAGUN (agosto-2018) *Navegadores y buscadores*

ÁNGEL COBO, PATRICIA GÓMEZ (2005) php y mysql tecnologías para el desarrollo de aplicaciones web: Díaz de santos

WILLIAM STALLINGS (s/f) comunicaciones y redes de computadoras: 6ta edición

MONICA CRISTINA LIBERATORI (mayo-2018) redes de datos y sus protocolos: 1ra edición

JOSÉ MANUEL ALBORNOZ (mayo-2018) radioenlaces digitales: editorial académica española

LÓPEZ YEPES, (1997), Alfonso. *Documentación informativa: Sistemas, Redes y Aplicaciones*

JUAN JOSÉ MURILLO, (2008) Fuentes Fundamentos de Radiación y Radiocomunicación: 2da edición

JORGE GONZALEZ S. (2010), *Diseño de un proveedor de servicio de internet inalámbrico*:1ra edición.

GEROMETTA (2012), *Guía de preparación para el examen de certificación CCNA*

MIKROTIK (s/f) *CCR1009-7G-1C-1S+* mikrotik.com/product/CCR1009-7G

EUSKADI (s/f) *Navegadores web* <https://www.euskadi.eus/navegadores-web/web01-a2wz/es/>

EXPRESSVPN (s/f) *Protocolos VPN: PPTP* <https://www.expressvpn.com/es/what-is-vpn/protocols/pptp>

FALCONMASTERS (8 ene. 2020) Programa *la Página Principal de Youtube con HTML, CSS, Flexbox y GRID* <https://www.youtube.com/watch?v=KWmMzM7tHGY>

GHM (s/f) *Router Wifi D-Link DIR-865L posiblemente el más vulnerable.* <https://ghmsolucioneswifi.es/router-wifi-d-link-dir-865l-posiblemente-el-mas-vulnerable/>

HARDWAREVIEWS (s/f) *Intel y los procesadores Xeon ¿son para Gaming? ¿diferencias contra los Intel Core?* <https://hardwareviews.com/intel-y-los-procesadores-xeon/>

HOW TO MASTER CCNA (*HTMC-V3*)

INITCOMS (15/07/20) *mobile first y cómo puede mejorar tu posicionamiento* <https://www.initcoms.com/que-es-mobile-first-posicionamiento/>

VEXELS (s/f) *Servidores de computación en la nube isométrica* consultado <https://es.vexels.com/png-svg/vista-previa/128104/servidores>

WIKIPEDIA (12 ago 2021) *Internet* <https://es.wikipedia.org/wiki/Internet>

WIKIPEDIA *red de área local virtual* <https://es.wikipedia.org/wiki/VLAN>

ZENITX (s/f) *Simple Queues and Queue Tree* <https://blog.zenitx.com/mikrotik-simple-queues-and-queue-tree/>