UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE."

AUTOR: GALO ISRAEL ESPINOSA PADILLA

DIRECTOR: Ing. Carlos Vásquez

IBARRA – ECUADOR

2017

IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100294205-8		
APELLIDOS Y NOMBRES:	ESPINOSA PADILLA GALO ISRAEL		
DIRECCIÓN:	GONZALES SUAREZ Y GALO PLAZA (ATUNTAQUI – ANTONIO ANTE)		
EMAIL:	giespinosap@utn.edu.ec		
TELÉFONO FIJO:	062 909331	**TELÉFONO MÓVIL:**	093367379
DATOS DE LA OBRA			
TÍTULO:	IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE.		
AUTOR (ES):	ESPINOSA PADILLA GALO ISRAEL		
FECHA:			
PROGRAMA:	■ PREGRADO ☐ POSGRADO		
TITULO POR EL QUE OPTA:	INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN		
ASESOR:	ING. CARLOS VÁSQUEZ		

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Galo Israel Espinosa Padilla, con cédula de identidad Nro.100294205-8, en calidad de autor y titular de los derechos patrimoniales de la obra para trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

.....

Firma

Galo Israel Espinosa Padilla

100294205-8

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Galo Israel Espinosa Padilla, con cédula de identidad Nro.100294205-8, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor (es) de la obra o trabajo de grado denominado: "**IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE**", que ha sido desarrollado para optar por el título de: Ingeniería Electrónica y redes de Comunicación en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Firma

Galo Israel Espinosa Padilla

100294205-8

Ibarra, 2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Galo Israel Espinosa Padilla con cédula de identidad nro. 100294205-8, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido realizado, ni calificado por otro profesional, para efectos académicos y legales será de mi responsabilidad.

.....

Firma

Galo Israel Espinosa Padilla

Cédula: 100294205-8

Ibarra, 2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación "**IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE**" fue desarrollado en su totalidad por el Sr. Galo Israel Espinosa Padilla, bajo mi supervisión.

.....

Ing. Carlos Vásquez

DIRECTOR DE TESIS

DEDICATORIA

Dedico este proyecto a mi hijo Martín Israel, quien me motiva para continuar superándome y encontrar en él mi mejor propósito de vida y felicidad

A mis padres Galo Patricio y Carmen Narciza quienes me inspiran a continuar trabajando con humildad y disciplina.

A mis hermanos Jhonny Patricio y Albania Carolina que fortalecen mis emociones con su cariño.

A mis sobrinos Mateo Joaquin, Leandro Josue (+) y Julian Alessandro que con su inocencia me dan razones para sonreír cada día, a mis abuelos que con su sabiduría me han guiado por el camino del bien y del servicio.

A mis familiares y amigos que siempre están presentes en el momento que más los necesito.

Galo Israel

AGRADECIMIENTOS

Agradezco a mis padres por educarme con valores de honestidad, respeto.

A la madre de mi hijo Paola Vanessa quien cuida de mi hijo con responsabilidad y mucho amor.

A los docentes de mi querida Facultad quienes imparten conocimiento con el único interés de compartir.

A la Dirección de desarrollo tecnológico e informática UTN y de manera diferenciada al Ing. Vinicio Guerra quien supo guiarme y ayudarme en el desarrollo de este proyecto de manera incondicional.

Galo Israel Espinosa Padilla

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La red de datos de la Universidad Técnica Del Norte se encuentra administrada por la Dirección de Desarrollo Tecnológico e Informático -UTN, la misma que tiene la gestión de los segmentos de red de las diferentes dependencias de la institución, entre ellas las VLAN de cada una de las facultades.

La administración de la red de datos institucional se encuentra centralizada, lo que lleva a congestionar el tráfico y procesando la información en un solo sector. El proyecto permite gestionar el tráfico de red de cada facultad de la Universidad Técnica del Norte con el fin de optimar el acceso al servicio de Internet y gestionar el mismo de manera independiente.

Se enfocó en primera instancia en la recolección de datos y análisis de la situación, lo que permitió aclarar dudas que sirvieron de base para orientar de mejor manera la solución. El diseño del proyecto se fundamentó en un modelo por capas tomando como referencia la arquitectura de red TCP/IP.

Para la implementación de la solución y el cumplimento de los objetivos, se procuró utilizar herramientas que sean capaces y precisen desempeñar con lo planteado sobre un sistema operativo que contemple los criterios de software libre.

De esta manera se pudo concluir con la implantación de una alternativa que permite administrar el servicio de acceso a internet y gestionar el mismo de acuerdo a requerimientos solicitados por los usuarios.

ABSTRACT

The data network of the "Técnica del Norte" University is administered by the "Dirección de Desarrollo Tecnológico e Informático-UTN", which takes care of the management of the network segments from the different dependencies of the institution, including the VLANs in each Faculty.

The management of the institutional data network is centralized, leading to congestion of traffic and processing information in unique sector. The project allows to handle the network traffic of each faculty of "Técnica del Norte" University, in order to optimize access to Internet service and to manage it independently.

This was focused on the first instance on data collection and analysis of the situation, which allowed to clarify doubts which has served as a basis, guiding to get a better solution. The design of the project was based on a layer model based on the TCP / IP network architecture.

For the implementation of the solution and the enforcement of the objectives, it was tried to use some tools, which may require in order to carry out an operating system that contemplates the criteria of free software.

In this way it was possible to conclude with the implementation of an alternative, which allows to manage the internet access service and according to requirements required by users.

PRESENTACIÓN

Un firewall administra los datos que existen en un segmento de red tanto de entrada como de salida y de enrutamiento, el presente documento detalla una alternativa para gestionar el servicio de acceso a internet de las Facultades de la Universidad Técnica del Norte.

En la primera parte se detalla los antecedentes y aspectos iniciales del propósito del trabajo de grado, se puntualiza el problema y lo objetivo, se delimita el alcance y se justifica la elección del tema, en la segunda parte se detalla los conceptos involucrados el desarrollo del proyecto; el tercer apartado hace referencia al análisis de la Situación Actual; por último se presenta el diseño, instalación y pruebas de funcionamiento del proyecto realizado procurando puntualizar las conclusiones y recomendaciones que referencian el trabajo realizado

A continuación se presenta a detalle los aspectos que se tomaron en cuenta para la realización del trabajo

1. Antecedentes

1.1 Problema

Debido al incremento de flujo de información y procesamiento de los equipos en las redes computacionales se tiende a tener puntos de congestión, un firewall es un sistema que nos conlleva a tener mayor control en el filtrado y enrutamiento de los paquetes que atraviesan por un segmento de red y nos proveen alguna forma de sectorización, permitiendo gestionar de una manera más óptima el tráfico; mientras que el proxy tiene la funcionalidad de un intermediario, conservando el contenido solicitado por los usuarios, acelerando las respuestas en futuras peticiones.

La red de la Universidad técnica del Norte se encuentra administrada y gestionada de una manera centralizada, condescendiendo a congestionar el tráfico y procesando la información en un solo sector, acarreando un elevado procesamiento, no acceso a servicios, encolamiento de paquetes y saturación de los Equipos del data center.

El objetivo del proyecto es el de utilizar mecanismos que permitan liberar procesamiento de los equipos del data center por medio de la implementación de un firewall y proxy en cada facultad, bajo la plataforma de GNU/Linux, que ayuden a controlar el contenido de la información que atraviesa cada segmento de la red.

1.2 Objetivos

1.2.1 General

Mejorar el servicio de acceso a internet en la Facultad de Ingeniería en Ciencias Aplicadas con la implementación de un Servidor Firewall-Proxy bajo la plataforma de GNU/Linux, a fin de reducir procesamiento de los equipos del Data Center de la Universidad Técnica del Norte.

1.2.2 Específicos

- Respaldar mediante documentación las bases teóricas, que servirán de referencia para la estructuración del presente trabajo.
- Analizar el estado actual de la red de la Facultad de Ingeniería en Ciencias Aplicadas.
- Determinar requerimientos físicos y lógicos necesarios para la implementación del servidor Firewall-Proxy y su posterior instalación.
- Crear y configurar VLANS en la plataforma GNU/Linux que permita el enrutamiento de paquetes de las distintas redes lógicas pertenecientes a la Facultad de Ingeniería en Ciencias Aplicadas.
- Definir reglas y políticas en el firewall que permitan dirigir el tráfico, de un segmento de red, hacia el proxy y establecer funciones de filtrado de contenidos, así como horarios en los que se puede acceder a sitios no establecidos.
- Asignar memoria cache en el proxy, para mejorar los tiempos de acceso de consultas y concurrencias con el motivo de liberar carga hacia los enlaces de acceso a Internet.
- Emplear una herramienta que permita generar reportes usando la bitácora del proxy que en el futuro permita tomar decisiones administrativas.

1.3 Alcance

El propósito de este proyecto tiene como finalidad encontrar una alternativa que disminuya el procesamiento de los equipos del data center de la Universidad Técnica del Norte y contribuya al mejoramiento en el tiempo de respuesta de consultas hacia la web, y de esa manera desarrollar la ejecución de herramientas para reducir el tráfico de datos en el segmento de red de acceso a la Internet.

Se analizará la situación actual de la red. Esto implica realizar una auditoría a las políticas y reglas institucionales implementadas sobre el acceso a contenido de internet, y acceso a recursos locales lo que permite establecer pautas estrictas para la implementación del firewall acorde con las políticas institucionales.

Se estudiará la topología actual del segmento de red perteneciente a la Facultad de Ingeniería en Ciencias Aplicadas para definir donde ubicar y donde va servir el firewall-proxy. Se establecerá los requerimientos físicos y lógicos para la posterior instalación del servidor.

Configurar VLANS y enlaces troncales empleando el estándar IEEE 802.1q en la plataforma de GNU/Linux con el objetivo de gestionar los segmentos de red y brindar comunicación entre VLANS pertenecientes a la Facultad, para de esa manera distinguir el tipo de filtrado de paquetes acorde con el tipo de usuarios.

Implementar el firewall con políticas y reglas acordes con la administración de la red, que permitan dirigir el tráfico hacia el proxy, y que contengan la suficiente granularidad para distribuir el paquete que se va a aceptar o denegar. En el proxy se procurará filtrar contenido web, tomando reportes de la herramienta de gestión y administración de ancho

de banda EXINDA, filtrar el contenido por tiempos y definir horarios convenientes en el que los usuarios puedan acceder a los recursos de internet que no estén establecidos.

La asignación de memoria cache en el proxy tiene como finalidad conservar el contenido solicitado por el usuario, aspirando mejorar la velocidad en tiempo de respuesta de los sitios solicitados.

Por último, se pretende implementar una herramienta que permita generar reportes de los sitios más visitados para de esa manera permitir tomar decisiones administrativas.

Todo lo mencionado se realizará en la Facultad de Ingeniería en Ciencias Aplicadas, procurando detallar manuales de instalación del Firewall-Proxy así como un manual de implementación de políticas y reglas en el firewall y un manual de Administrador, para en un futuro ser replicada en las demás facultades, con la colaboración del Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.

1.4 Justificación

La institución al manejar un número de usuarios considerables y que la gran mayoría se respalda con las consultas de información en la web, conlleva que todo el tránsito de información genere gran procesamiento en los equipos del data center y toda la información demandada salga hacia Internet, por ello es necesario contar con alternativas que conlleven a disminuir el tamaño de los paquetes de consultas y reducir el consumo de recursos.

La implementación de un servidor proxy bajo la licencia GNU/Linux brinda la posibilidad de aprovechar sus ventajas, la principal y más significativas es que pertenece a la categoría de software libre razón por la cual implica costos bajos para su implementación.

La herramienta para generar reportes nos permite realizar informes y observar los sitios más visitados en la web y realizar evaluaciones para tomar decisiones que mejoren el performance de la red.

De acuerdo a lo manifestado, la investigación e implementación a realizarse constituye un aporte para mantener el servicio de acceso a Internet, mejorar los tiempos de respuesta de las peticiones y sustentar el tráfico de datos que atraviesa por la red institucional.

2. Marco Teórico

Las redes computacionales y las tecnologías de comunicación se han desarrollado de tal manera que se ha integrado nuevos servicios y aplicaciones que permiten el evidente proceso y perfeccionamiento de la transmisión de la información a través de las entidades y sistemas de transmisión. En este capítulo se documenta aspectos iniciales que conforman características importantes de una red de computadoras como, tipos de redes computacionales, arquitectura de redes, jerarquía de redes, servicios de seguridad en la comunicación tales como firewall y proxy.

2.1 Redes computacionales

En el siguiente apartado se clasifica las redes según su escala, esto implica categorizar las redes de computadoras tomando en consideración su tamaño físico.

2.1.1 Redes de área local

Una red de área local, como se muestra en la Figura1, interconecta dispositivos a través de un medio de comunicación que puede ser físico o inalámbrico, a continuación se menciona algunas características de este tipo de redes computacionales.

Generalmente las redes de área local son de propiedad privada que se encuentran organizadas en un espacio físico menor a un kilómetro o que se encuentran dentro de un campus o un edificio, se utilizan para conectar estaciones de trabajo de manera que se pueda compartir información y recursos tales como impresoras (Tanenbaum & Wetherall, 2012, pág. 17).

La velocidad de transmisión en una LAN es mayor que en otras redes de computadoras, van desde 10Mbps y las más actuales que podrían llegar hasta 10Gbps. Este tipo de topología es una red de difusión donde los paquetes son enviados por un

medio de transmisión y recibidos por todas las estaciones que conforman la LAN[1], cabe recalcar que la información es procesada por la estación de destino las demás escuchan y si no está destinada a estas, estos paquetes son descartados.

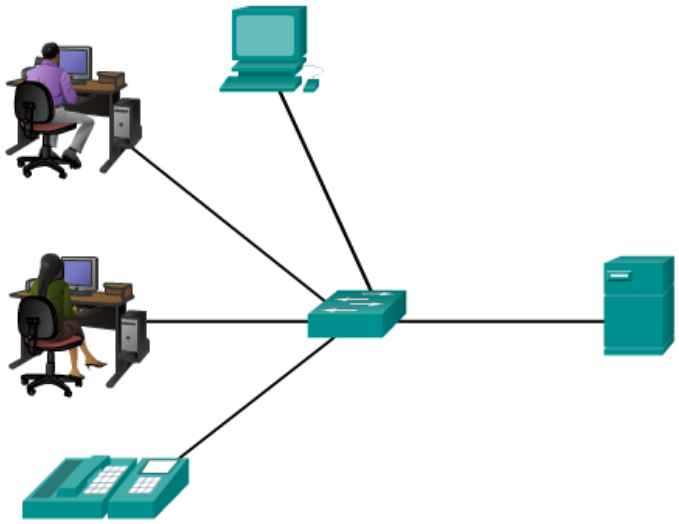


Figura 1. Topología de Red de Área Local

Fuente: Cisco Networking Academy. *Exploración de la red.* Recuperado el 04 de septiembre de 2015 de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.2.2.2

2.1.2 Redes de área metropolitana

Una red de área metropolitana es aquella que ofrece cobertura a un área geográfica más amplia por medio de una conexión de alta velocidad, el concepto de red MAN (Red de Área Metropolitana) representa una versión más grande que una LAN (Rede de Área Local), se dice que su distancia de cobertura es mayor a 4km (Tomala, 2011). Ver figura 2.

[1] LAN=Red de Área Local; por las siglas en inglés de Local Area Network.

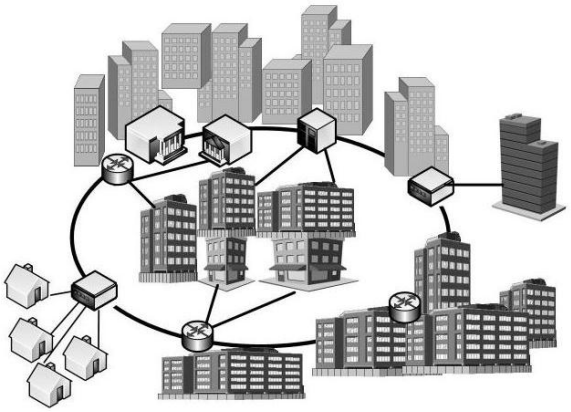


Figura 2. Topología de Red de Área Metropolitana

Redes De Datos. Recuperado el 07 de septiembre de 2015 de http://instalacionderedeslocalespatricia.blogspot.com/2014/10/redes-de-datos-red-area-local-lan-se.html

2.1.3 Redes de área amplia

Las redes de Área Amplia son consideradas aquellas que cubren una extensa área geográfica, ver Figura2, requieren atravesar rutas de acceso público, y utilizar parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicaciones.

Una WAN[2] está conformada por dispositivos de conmutación de paquetes de datos interconectados entre sí. La transmisión de información generada por cualquier dispositivo se encaminará a través de los nodos internos hasta alcanzar el destino. La función de los nodos, de la subred que conforma la WAN, es proporcionar el servicio de conmutación, necesario para transmitir los datos entre nodos hasta que los datos lleguen a su destino final. Ver figura 3.

[2] WAN: Red de Área amplia; por sus siglas en ingles Wide Área Network.

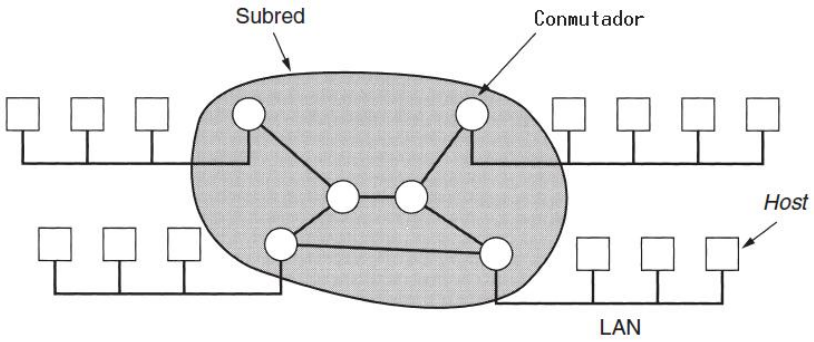


Figura 3.Topología de Red de Área Amplia

Fuente: Adaptado de Tanembaum, A. Redes de Computadoras: *Redes De Área Amplia* (p. 19).

2.1.4 Redes inalámbricas

Las redes inalámbricas se han vuelto un pilar fundamental en el acceso a una red de datos. Hoy en día, los usuarios esperan estar conectados en cualquier instante y lugar. La capacidad móvil permite que un dispositivo inalámbrico mantenga acceso a recursos de la LAN sin perder conexión (Cisco Networking Academy, 2015).

Uno de los usos que se ha venido desarrollando en lo que se refiere a redes inalámbricas es la interconexión de sistemas, componentes de una computadora que utiliza radio de corto alcance como un teclado, mouse, impresora, etc., por medio de una tecnología desarrollada por algunas compañías llamada Bluetooth, con el único requisito de que se encuentren dentro del alcance de la red. Ver Figura 4.

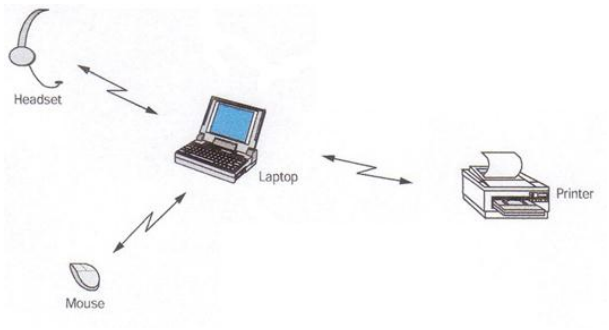


Figura 4 Red Bluetooth

Fuente: Adaptado de Garcia, A. *Estándares de Bluetooth* . Recuperado el 09 de septiembre de 2015 de http://www.info-ab.uclm.es/labelec/Solar/domotica/estandares_red_bluetooth.html

Las redes de interconexión de sistemas utilizan el concepto de maestro-esclavo. El maestro, en este caso la unidad del sistema, le dice a los esclavos (mouse, teclado, impresora, etc.) cuando difundir, durante cuánto tiempo pueden transmitir, que frecuencias pueden utilizar, etc. (Tanenbaum & Wetherall, 2012, pág. 23)

Otra categoría son las WLAN[3], se dice que tienen un alcance de unos 30m, pueden ser utilizadas en un hogar, oficina o incluso en un campus. Las WLAN conectan a los clientes de una red mediante AP's[4] inalámbricos o un router inalámbrico en lugar de hacerlo mediante un switch.

Cabe recalcar que las redes inalámbricas se enlazan en algún punto a una red cableada para proporcionar acceso a recursos. Ver Figura 5.

[3] WLAN: Redes de Área Local Inalámbricas; pos sus siglas en ingles Wireless Local Area network.
[4] AP: Punto de Acceso; es un dispositivo que interconecta computadoras en una red.

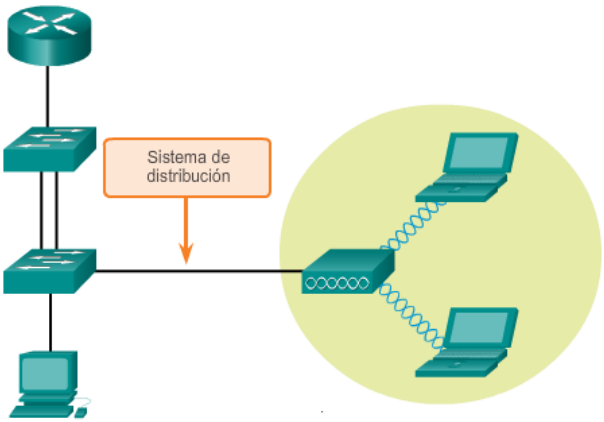


Figura 5. . Red de Área Local Inalámbrica

Fuente: Cisco Networking Academy. *Conceptos de tecnología inalámbrica.*
Los dispositivos se conectan por medio de un AP o un router inalámbrico a una red cableada.

Uno de los mayores inconvenientes de este tipo de redes es la seguridad. Las redes inalámbricas son vulnerables a las amenazas, como los intrusos inalámbricos y la intercepción de datos (Cisco Networking Academy, 2015).

2.2 Software de redes

Los programas que establecen los protocolos para que las computadoras se comuniquen entre si son denominados Software de Redes. Actualmente el software de redes está altamente estructurado.

2.2.1 Jerarquía de protocolos

Para que una comunicación entre computadoras se lleve a cabo es necesario seguir estrictas reglas, estas reglas son denominadas protocolos. La mayoría de las redes está organizada por una pila de capas, cada una construida a partir de la que está debajo de ellas.

Cada capa describe los protocolos que facilitan la comunicación y que mantiene la conversación entre capas de una y otra máquina.

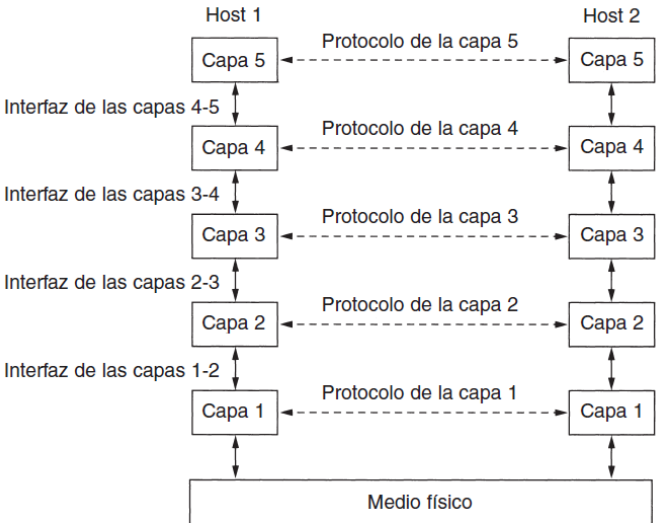


Figura 6. Capas, protocolos e interfaces.

Fuente: Tanembaum, A. Redes de Computadoras: *Jerarquía de protocolos* (p. 26).

Cada capa pasa los datos y la información de control a la capa inmediata inferior hasta alcanzar la más baja. Debajo de la capa 1 se encuentra el medio físico por el cual ocurre la comunicación real, como se muestra en la Figura 6.

La interfaz se localiza entre cada par de capaz adyacentes; esta define que operaciones y servicios primitivos pone a disposición la capa más baja a la capa inmediata superior.

El conjunto de capas y protocolos conforman una arquitectura de red, que contienen información suficiente para construir un hardware de red de modo que se cumpla correctamente con el protocolo apropiado.

En la Figura 7 se muestra un ejemplo como es el proceso para proporcionar información de una capa superior a una capa adyacente. La capa 5 produce un mensaje M y lo pasa a la capa 4 para su transmisión.

La capa 4 pone un encabezado (H4) frente al mensaje para identificarlo, e inmediatamente lo pasa a la capa inferior. El encabezado incluye información de control,

como numero de secuencia, para q la capa 4 de la maquina destino entregue los mensajes en orden correcto.

La capa 3 debe desintegrar los datos en unidades más pequeñas denominados paquetes (M1 y M2), y a cada paquete se le añade un encabezado (H3). Los paquetes son pasados a la capa 2, la cual agrega su respectivo encabezado y además un terminador (T2), por ultimo pasa, la unidad resultante, a la capa 1 para su transmisión física.

Todo este procedimiento permite a un diseñador de red fragmentar posibles problemas, El proceso se muestra en la Figura7 (Tanenbaum & Wetherall, 2012, pág. 28).

.

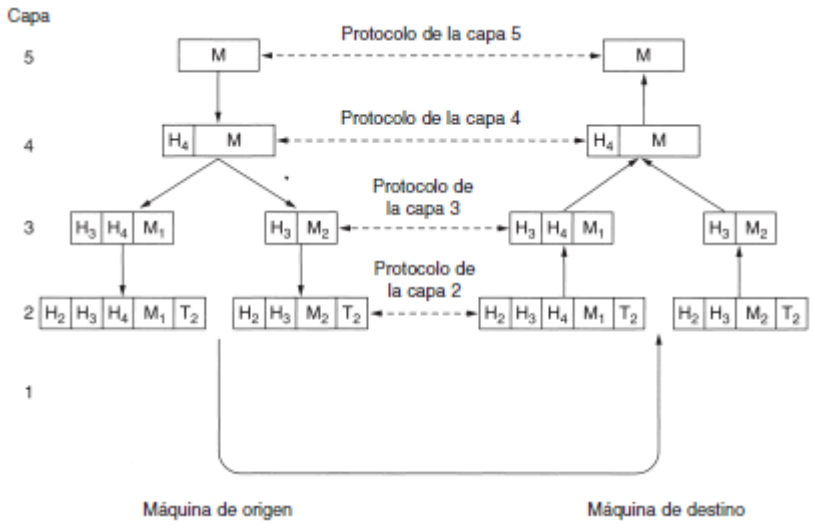


Figura 7. Flujo de información que soporta una comunicación

Fuente: Tanembaum, A. Redes de Computadoras: *Jerarquía de protocolos* (p. 30).

2.2.2 Primitivas de Servicio

Una primitiva se define como un conjunto de operaciones que especifican funciones que se deben llevar a cabo, y los parámetros que se utilizan para pasar datos de control entre capas (Barabas, 2012).

El conjunto de primitivas depende de la naturaleza del servicio que se va proporcionar. Los servicios de primitivas de un sistema orientado a conexión son diferentes de un sistema no orientado a conexión (Tanenbaum & Wetherall, 2012, pág. 32).

Los tipos de primitivas se describen en la Tabla1.

Tabla 1: Tipos de primitivas de servicio

SOLICITUD	**Primitiva emitida por el usuario del servicio para invocar algún servicio y pasar los parametros necesarios para especificar completamente el servicio solicitado.**
INDICACIÓN	Primitiva emitida por el suminstrador del servicio para: 1. Indicar que se ha sido invocado un procedimiento por el usuario de servicio par en la conexión y para suministrar los paramtros asociados, o 2. Notificar al usuario del servicio sobre una acción iniciada por el suministrador.
RESPUESTA	Primitiva emitida por el usuario del servicio para confirmar o completar algún procedimineto invocado previamente mediante una indicación a ese usuario.
CONFIRMACION	Primitiva emitida por el suministrador del servicio para confirmar o completar algún procedimiento invocado previamente mediante una solicitud por parte del usuario del servico

Fuente: Stallings, W. Comunicaciones y Redes de Computadores: *Protocolos y arquitectura* (p. 35).

Se considera un ejemplo para la transferencia de datos de una entidad N a su entidad N par en otro sistema.

1. La entidad origen (N) invoca a su entidad (N-1) con una primitiva de solicitud.
2. La entidad origen (N-1) prepara una PDU (N-1) para enviársela a su entidad par (N-1).
3. La entidad destino (N-1) entrega los datos al destino apropiado (N) a través de la primitiva de indicación, que incluye datos y dirección de origen.
4. Si se requiere una confirmación (sistema orientado a conexión), la entidad destino (N) emite una primitiva de respuesta a su entidad (N-1).
5. La entidad (N-1) convierte la confirmación en una PDU (N-1).
6. La confirmación se entrega a la entidad (N) como primitiva de confirmación.

Si la transferencia de datos recibe una confirmación se conoce como un servicio confirmado ya que lo solicitado ha tenido el efecto deseado en el otro extremo. Si la entidad que inicia la transferencia no recibe confirmación de que la acción solicitada haya tenido efecto, se denomina servicio no confirmado (Stallings, 2004, pág. 36). El diagrama de la secuencia temporal de las primitivas de servicio se muestra en la Figura 8.

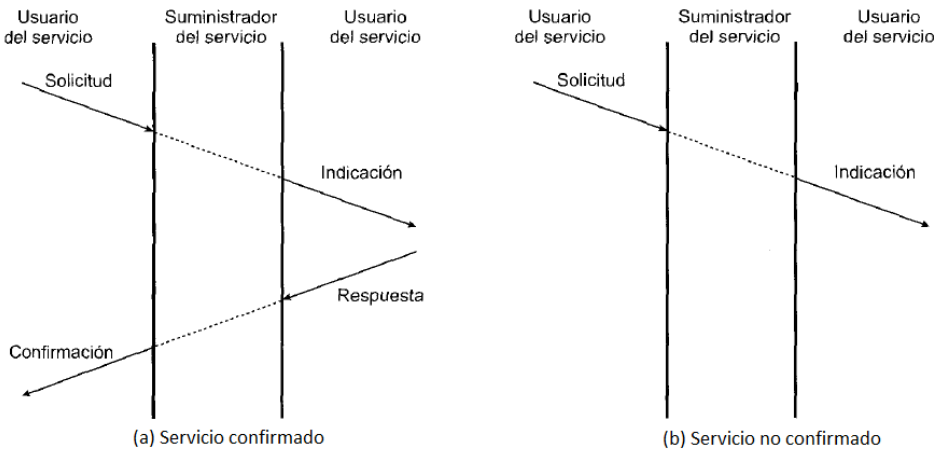


Figura 8.. Diagrma de la secuencia temporal de las primitivas de servicio.

Fuente: Stallings, W. Comunicaciones y redes de Computadores: *Protocolos y arquitectura* (p. 36).

2.2.2.1 Relación de servicios a protocolos

El servicio es un conjunto de operaciones que una capa proporciona a la capa que esta sobre ella. El servicio está relacionado con la interfaz entre dos capas, donde la capa inferior es la que provee el servicio y la superior quien lo recibe (Tanenbaum & Wetherall, 2012, pág. 34).

Los protocolos en cambio son un conjunto de reglas que rigen el formato y el significado de los paquetes que se intercambian (Tanenbaum & Wetherall, 2012, pág. 34).

Los servicios se relacionan con las interacciones entre capas. Ver Figura 9. En contraste, los protocolos (Tanenbaum & Wetherall, 2012, pág. 34)

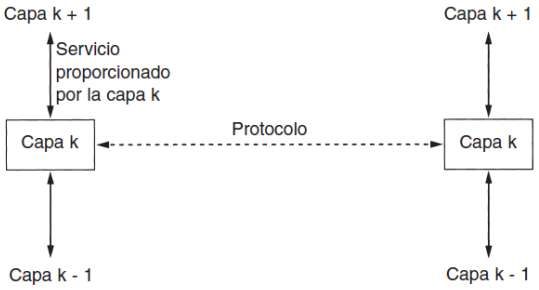


Figura 9.Relaion entre un servicio y un protocolo.

Fuente: Tanembaum, A. Redes de Computadoras: *Primitivas de Servicio* (p. 35).

2.2.3 El Modelo de referencia OSI

El modelo de referencia OSI[5], fue desarrollado por la ISO[6] como un modelo para comunicaciones entre computadores (Stallings, 2004, pág. 29).

Según Tanenbaun, para llegar a dichas capas se aplicaron algunos principios como:

1. Cada capa debe realizar una función bien definida.
2. LA función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.

2.2.3.1 Capa física

Esta capa se encarga de la transmisión de bits sobre el medio físico, están relacionadas con características mecánicas, eléctricas, funcionales y de procedimiento para acceder al medio físico. La capa acepta una trama completa de la capa de enlace de datos y la codifica como una serie de señales eléctricas, ópticas o de ondas de radio que representan

[5] OSI: Open System Interconnection; es un lineamiento funcional para tareas de comunicaciones.
[6] ISO: Organización Internacional de Estandarización; es una federación de alcance mundial integrada por cuerpos de estandarización

los bits de una trama para ser enviadas por los medios. Ver Figura 10. (Cisco Networking Academy, 2015) . Algunos ejemplos son: transmisión RS-232[7], transmisión por medio de DSL[8], entre otros.

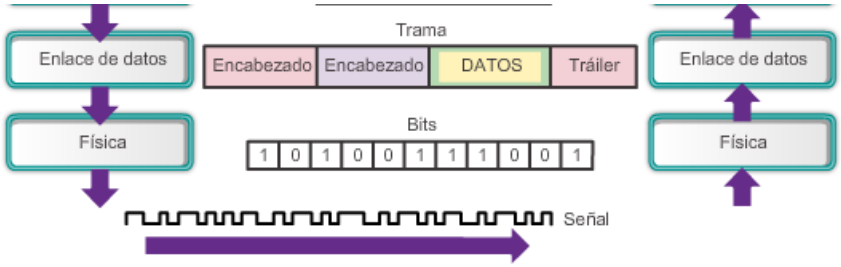


Figura 10.Capa física.

Fuente: Modificado de Cisco Networking Academy: *Protocolos de capa física*.

2.2.3.2 Capa enlace de datos

Según Stallings la capa enlace de datos "proporciona un servicio de transferencia de datos seguro a través del enlace físico; envía bloques de datos llevando a cabo la sincronización, el control de errores y el flujo necesario". El emisor fragmenta los datos y transmite las tramas de manera secuencial si el servicio es confiable el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción. Ejemplos: Ethernet[9], 802.11[10], HDLC[11], entre otros.

[7] RS-232: Es un estándar para la conexión serial de señales de datos binarias entre un equipo terminal de datos y un equipo de terminación del circuito de datos.
[8] DSL: Es una tecnología que proporciona el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica.
[9] Ethernet: es un estándar de transmisión de datos para redes de área local, con acceso al medio por detección de la onda portadora y con detección de colisiones
[10] 802.11: es un estándar internacional que define las características de una red de área local inalámbrica
[11] HDLC: sus siglas corresponden a control de enlace de datos de alto nivel, es un protocolo de comunicaciones de propósito general punto a punto

2.2.3.3 Capa de red

Proporciona independencia a los niveles superiores respecto a las técnicas de conmutación y de transmisión utilizadas para conectar los sistemas; es responsable del establecimiento, mantenimiento y cierre de conexiones (Stallings, 2004, pág. 37).

Esta capa determina como enrutar los paquetes desde su origen a su destino, además de permitir que las redes heterogéneas se interconecten. Ejemplos: IP[12], ICMP[13], entre otros.

2.2.3.4 Capa transporte

Proporciona seguridad transferencia transparente de datos entre los puntos finales; proporciona además procedimientos de recuperación de errores y control de flujo origen-destino. Determina qué tipo de servicio proporcionar a la capa de sesión y a los usuarios de la red. Ejemplos: TCP[14], UDP[15], entre otros.

2.2.3.5 Capa sesión

Proporciona el control de la comunicación entre las aplicaciones; establece, gestiona y cierra las conexiones (sesiones) entre las aplicaciones cooperadoras. Ejemplos: SSH[16], Telnet[17], entre otros.

[12] IP: Internet Protocol, es un protocolo de comunicación de datos digitales
[13] ICMP: protocolo de control y notificación de errores.
[14] TCP: Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet.
[15] UDP: es un protocolo mínimo de nivel de transporte orientado a mensajes.
[16] SSH: Intérprete de órdenes seguro, irve para acceder a máquinas remotas a través de una red.
[17] Telnet: Telecomunication Network, es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente

2.2.3.6 Capa presentación

Le corresponde la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar. Algunos ejemplos son HTML[18], .doc, .jpeg, entre otros

2.2.3.7 Capa aplicación

Contiene protocolos que los usuarios requieren con frecuencia (como HTTP[19]). Es la capa que proporciona la interfaz entre las aplicaciones que se utilizan para la comunicación a la red subyacente en la cual se transmiten los mensajes (Cisco Networking Academy, 2015).

El modelo de referencia OSI se muestra en la Figura 11.

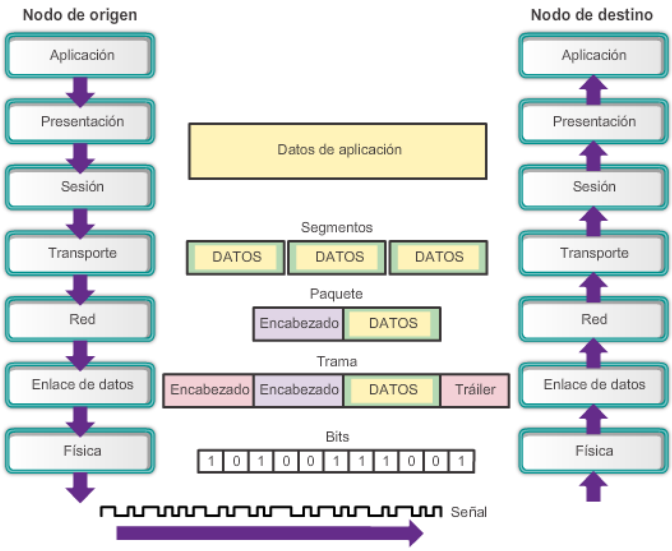


Figura 11.El modelo de referencia OSI.

Fuente: Modificado de Cisco Networking Academy: *Protocolos de capa física.*

[18] HTML: hace referencia al lenguaje de marcado para la elaboración de páginas web.
[19] HTTP: protocolo de transferencia de hipertexto; protocolo de comunicación que permite las transferencias de información en la World Wide Web.

2.2.4 Arquitectura de Red

2.2.4.1 Capa física

El propósito de la capa física es transportar un flujo de datos de una maquina a otra. Es posible utilizar varios medios físicos para la transmisión. Cada medio de transmisión tiene sus propias características como; ancho de banda, retardo, costo, facilidad de instalación y mantenimiento (Tanenbaum & Wetherall, 2012, pág. 77).

Medios de capa física

Los tres formatos básicos de medios de transmisión son:

Cable de cobre: Las señales con patrones de pulsos eléctricos. Una representación de esta señal se muestra en la Figura 12.

Figura 12.Señal eléctrica.

Fuente: Modificado de Cisco Networking Academy: *Protocolos de capa física*.

Cable de fibra óptica: las señales son patrones de luz. Ver figura 12.

Figura 13.Pulso de Luz.

Fuente: Modificado de Cisco Networking Academy: *Protocolos de capa física*.

Conexiones inalámbricas: las señales son patrones de trasmisiones de microondas. Ver Figura 14.

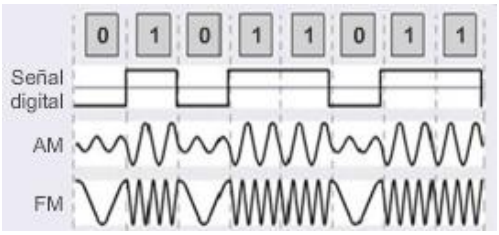


Figura 14.Señal de Microondas.

Fuente: Modificado de Cisco Networking Academy: *Protocolos de capa física*.

Estándares de capa física

La capa física consta de conectores, medios y circuitos electrónicos; por tal razón es necesario que las principales organizaciones especializadas en ingeniería eléctrica y comunicaciones definan los estándares que rigen dicho hardware (Cisco Networking Academy, 2015). Los organismos de estandarización de la capa física se muestran en la

Tabla2.

Tabla 2: Organismos de estandarización de capa física

Organismos de estandarización	Estándares de red
ISO (ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN)	ISO 887: Adoptó oficialmente los conectores RJ (p. ej., RJ-11, RJ-45) ISO 11801: Estandar de cableado de red similar a EIA/TIA 568
EIA/TIA (TELECOMUNICATIONS INDUSTRY ASSOCIATION/ELECTRONIC INDUSTRIES ASSOCIATION)	TEA-568-C Estandares de cableado de telecomunicacion, redes de datos, voz y video. TIA-569-B Estandares de constuccion comercial para rutas y espacios de telecomunicaciones. TIA-598-C Codigo de colores para fibra óptica. TIA-942 Estandar de infraestructura de telecomunicaciones para centros de datos.
ANSI (AMERICAN NATIONAL STANDARS INSTITUTE)	568-CDiagrama de pines RJ-45 desarrollado conjuntamente con EIA/TIA
ITU-T (UNION INTERNACIONAL DE TELECOMUNICACIONES)	G.992 ADSL
IEE (INSTITUTO DE INGENIEROS EN ELECTRICIDAD Y ELECTRÓNICA)	802.3 Ethernet 802.11 LAN Inalambrica 802.15 Bluetooth

Fuente: Modificado de Cisco Networking Academy: *Estándares de capa física.*

Principios fundamentales de la capa física

Ancho de Banda.- es la capacidad de un medio para transportar datos. El ancho de banda digital mide la cantidad de tatos que pueden fluir desde un lugar hasta otro en un periodo determinado**.** El ancho de banda se mide generalmente en kilobits por segundo o megabits por segundo (Cisco Networking Academy, 2015).

Rendimiento.- es la medida de transferencia de bits a través de los medios durante un periodo de tiempo determinado. Debido a diferentes factores, el rendimiento no suele coincidir con el ancho de banda especificado (Cisco Networking Academy, 2015).

2.2.4.2 Capa enlace de datos

La capa enlace de datos tiene que desempeñar varias funciones específicas, entre las que se incluyen:

1. Proporcionar una interfaz de servicio bien definida con la capa de red.
2. Manejar los errores de transmisión
3. Regular el flujo de datos para que receptores lentos no sean saturados por emisores rápidos
4. Controlar el acceso al medio físico.

La capa enlace de datos prepara los paquetes para transportarlos a través de los medio locales mediante su encapsulación con encabezado y un tráiler para crear una trama (Cisco Networking Academy, 2015).

Cada trama contiene un encabezado, un campo de carga útil (payload) para almacenar el paquete y un terminador o final (Tanenbaun, 2012, p. 168).Ver Figura 15.

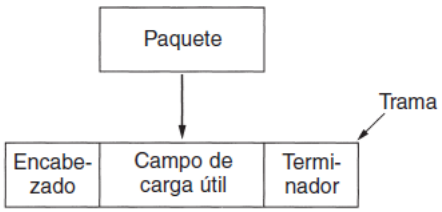


Figura 15..Relacion de Paquetes y tramas.

Fuente: Modificado de Tanembaum, A. Redes de Computadoras: *Cuestiones de diseño de la capa de enlace de*

Entramado

Es responsabilidad de la capa enlace de datos detecta y, de ser necesario, corregir los errores.

Existen algunos métodos para marcar el inicio y el final de cada trama entre ellos:

1. Conteo de caracteres.
2. Banderas, con relleno de caracteres.
3. Bandera de inicio y fin, con relleno de bits.

El conteo de caracteres, como se muestra en la Figura 16 (a), se vale de un campo en el encabezado para especificar el número de caracteres en la trama. Cuando la capa de enlace de datos del destino ve la cuenta de caracteres, sabe cuántos caracteres siguen y, por lo tanto, donde está el fin de la trama (Tanenbaun, 2012, p. 170).

El problema con este algoritmo es que la cuenta puede alterarse por un error de transmisión, como se puede apreciar en la figura 16 (b), el conteo de caracteres en la Trama 2 es 5 y se vuelve un 7, el destino perderá sincronía y será incapaz de localizar el inicio de la siguiente trama.

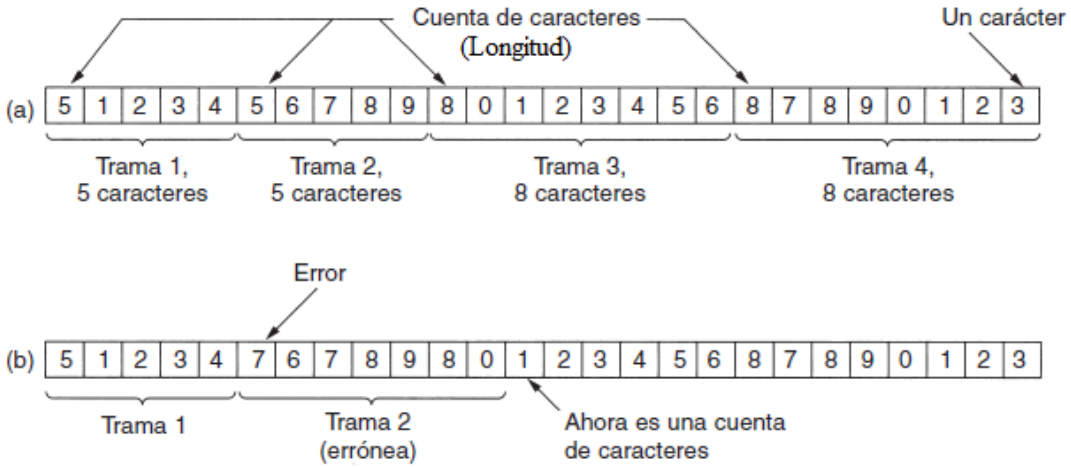


Figura 16 .Flujo de caracteres (a) Sin errores (b) Con un error.

Fuente: Modificado de Tanembaum, A. Redes de Computadoras: *Entramado.* (p. 171).

El segundo método de entramado, como se muestra en la Figura 17, evita el problema de tener que sincronizar nuevamente después de un error, haciendo que cada trama inicie y termine con bytes especiales llamado bandera (FLAG). De esta manera si el receptor pierde la sincronía, simplemente puede buscar la bandera para encontrar el final e inicio de la trama actual (Tanenbaun, 2012, p. 171).

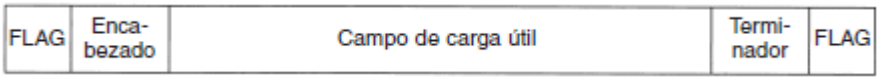


Figura 17.Una trama delimitada por banderas.

Fuente: Modificado de Tanembaum, A. Redes de Computadoras: *Entramado.* (p. 172).

Cuando el receptor ve cinco bits 1 de entrada consecutivos, seguidos de un bit 0, automáticamente extrae el bit 0 de relleno, ver Figura 18.

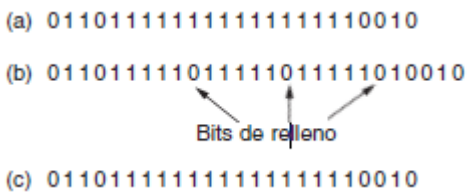


Figura 18. Relleno de bits (a) Los datos originales. (b) Los datos, según aparecen en la línea (c) Los datos según se guardan en la memoria del receptor.

Fuente: Modificado de Tanembaum, A. Redes de Computadoras: *Entramado.* (p. 173).

Subcapas de enlace de datos

La capa enlace de datos se divide en dos subcapas:

1. Control de enlace lógico (LLC).
2. Control de acceso al medio (MAC).

El control de enlace lógico es la subcapa superior, que define los procesos de software que proporciona servicios a los protocolos de capa de red. LLC coloca en la trama información que identifica qué protocolo de red se utiliza para la trama. Esta información permite que protocolos de capa de red como IPv4 e IPv6, utilicen la misma interfaz y los mismos medios de red.

El control de acceso al medio es la subcapa inferior, que define los procesos de acceso al medio que realiza el hardware, se detalla como una técnica para pasar las tramas de la capa de red hacia los distintos medios de transmisión.

La capa enlace de datos se muestra en la Figura 19.

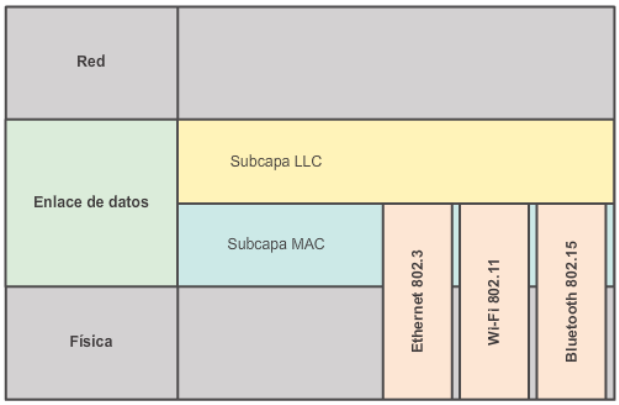


Figura 19. Subcapas de Enlace de datos

Fuente: Modificado de Cisco Networking Academy: *Subcapas de enlace de datos*.

Trama de enlace de datos

Si bien existen muchos protocolos de capa de enlace de datos diferentes que describen las tramas de la capa de enlace de datos, cada tipo de trama tiene tres partes básicas, ver Figura 20:

- Encabezado
- Datos
- Trailer

El encabezado de la trama contiene la información de control que especifica el protocolo de capa de enlace de datos para la topología lógica y los medios específicos utilizados.

Todos los protocolos de capa de enlace de datos encapsulan la PDU de la capa de red dentro del campo de datos de la trama.

El tráiler se utiliza para determinar si la trama llegó sin errores. Este proceso se denomina “detección de errores” y se logra mediante la colocación en el tráiler de un

resumen lógico o matemático de los bits que componen la trama (Cisco Networking Academy, 2015).

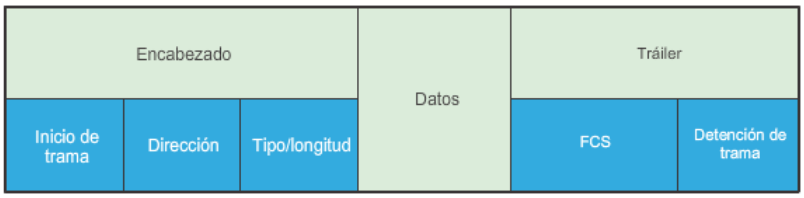


Figura 20. Trama de enlace de datos

Fuente: Modificado de Cisco Networking Academy: *Trama de enlace de datos.*

En una red TCP/IP[20], el protocolo de capa de enlace de datos que se utilice depende de la topología lógica de la red y la implementación de la capa física. Esto quiere decir que en una topología de red pueden actuar una cantidad de dispositivos de red diferentes en los cuales se utilizan una gran cantidad correspondiente de protocolos.

Trama de Ethernet

Ethernet es la tecnología LAN más utilizada y admite anchos de banda de datos de 10 Mbps, 100 Mbps, 1Gbps o 10 Gps. Ethernet utiliza CSMA/CD como método de acceso al medio, en el encabezado de la trama, utiliza una dirección de la capa de enlace de datos para identificar los nodos de origen y destino, esta dirección se llama dirección MAC (Cisco Networking Academy, 2015).

La trama Ethernet se muestra en la Figura 21.

[20] TCP/IP: Conjunto de protocolos; es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos.

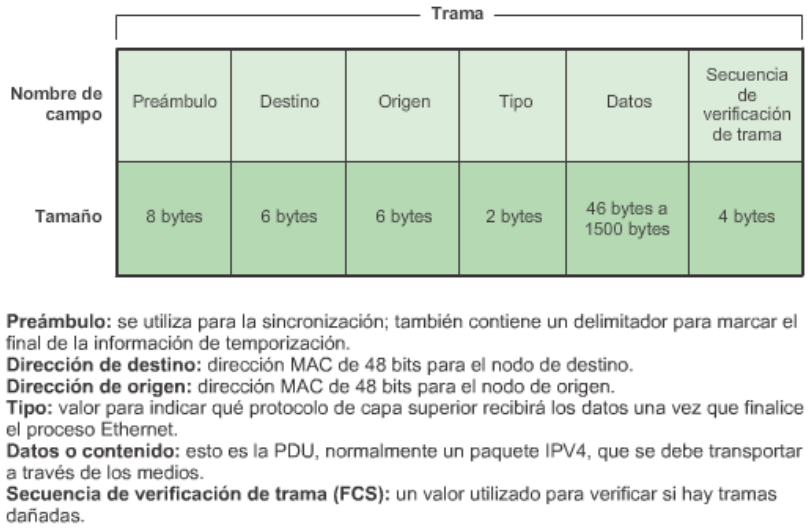


Figura 21. Trama Ethernet

Fuente: Modificado de Cisco Networking Academy: *Trama de enlace de datos.*

2.2.4.3 Capa internet

La capa de red se encarga de llevar los paquetes desde el origen hasta el destino. Llegar al destino puede requerir muchos saltos por enrutadores intermedios. Por lo tanto, la capa de red es la capa más baja que maneja la transmisión de extremo a extremo.

Encapsulación de IP

El protocolo IP es el servicio de capa de red implementado por la suite de protocolos de TCP/IP.

El protocolo IP encapsula o empaqueta el segmento de la capa de transporte agregando un encabezado IP. Este encabezado se utiliza para entregar el paquete al host de destino. La PDU de la capa de transporte encapsulada, no se modifica durante los procesos de la capa de red (Cisco Networking Academy, 2015). Ver Figura 22.

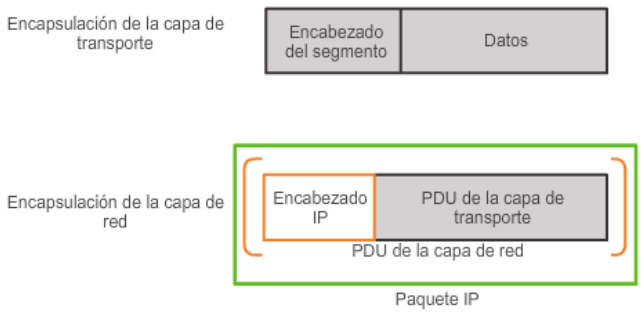


Figura 22. Generación de paquetes IP

Fuente: Modificado de Cisco Networking Academy: *Protocolos de la capa de red.*

Encabezado de paquetes IPv4

El paquete IPv4 se divide en dos partes:

- Encabezado IP: parte fija de 20 bytes que identifica las características del paquete.
- Contenido: parte opcional de longitud variable que contiene la información que permitiera a las versiones subsiguientes del protocolo incluyeran información no presente en el diseño original.

El encabezado de paquete IPv4 se muestra en la Figura 23.

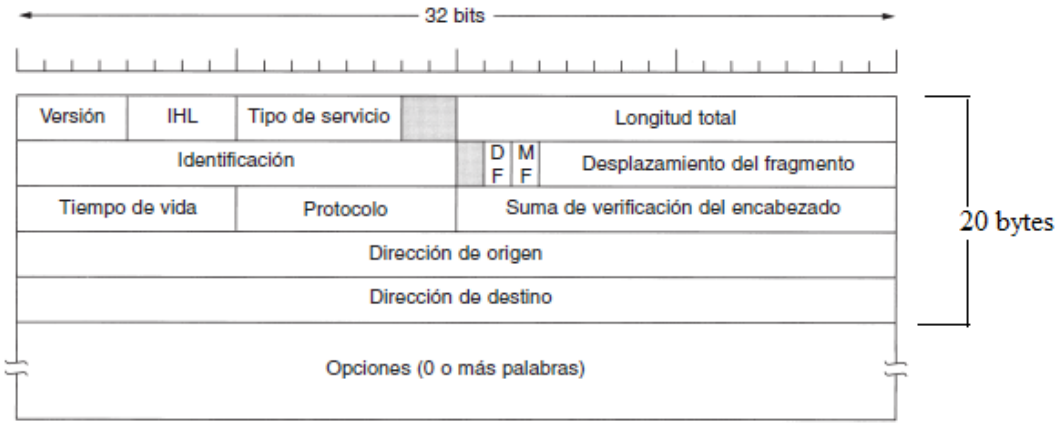


Figura 23. Encabezado de IPv4

Fuente: Modificado de Tanembaum, A. Redes de Computadoras: *El protocolo IP*. (p. 434).

El campo *versión* lleva el registro de la versión del protocolo, contiene un valor binario de 4 bits, para los paquetes IPv4[21], este campo se establece en 0100.

El *Tipo de servicio* distingue las diferentes clases de servicios, determina la prioridad de cada paquete.

IHL(Longitud del encabezado de Internet) me dice cuál es la longitud del encabezado del paquete.

Longitud total me dice el valor total del tamaño del paquete.

El campo *Identificación* es necesario para que el host de destino determine a que datagrama pertenece un fragmento recién llegado.

DF significa no fragmentar; es una orden para los enrutadores de que no fragmenten el datagrama, porque el destino es incapaz de juntar las piezas de nuevo.

MF significa más fragmentos. Todos los fragmentos excepto el último tienen establecido este bit, que es necesario para saber cuándo han llegado todos los fragmentos de un datagrama.

El *desplazamiento del fragmento* indica en que parte del datagrama actual va este fragmento.

Tiempo de vida o TTL se especifica en segundos (conteo de saltos), disminuye un punto por cada vez que el paquete es procesado por un router, el paquete es descartado cuando el contador llega a 0. El TTL evita los bucles de capa 3.

Protocolo indica el protocolo de las capas superiores al que debe entregarse el paquete. TCP es una posibilidad, pero también está UDP e ICMP.

[21] IPv4: Protocolo de Internet versión 4; es la cuarta versión del Internet Protocol (IP).

La *Suma de verificación del encabezado* verifica solamente el encabezado. Tal suma de verificación es útil para la detección de errores.

Dirección IP de origen contiene un valor binario de 32 bits que representa la dirección IP de origen del paquete.

Dirección IP de destino contiene un valor binario de 32 bits que representa la dirección IP de destino del paquete.

(Tanenbaum & Wetherall, 2012, pág. 377) y (Cisco Networking Academy, 2015)

Encabezado de paquetes IPv6

Debido al agotamiento de direcciones IP se empezó a buscar un reemplazo, esta actividad condujo al desarrollo de IP versión 6 (IPv6) que supera las limitaciones de IPv4 y constituye una mejora eficaz con características que se adaptan mejor a las demandas actuales de las redes.

El encabezado de paquete IPv6 se muestra en la Figura 24.

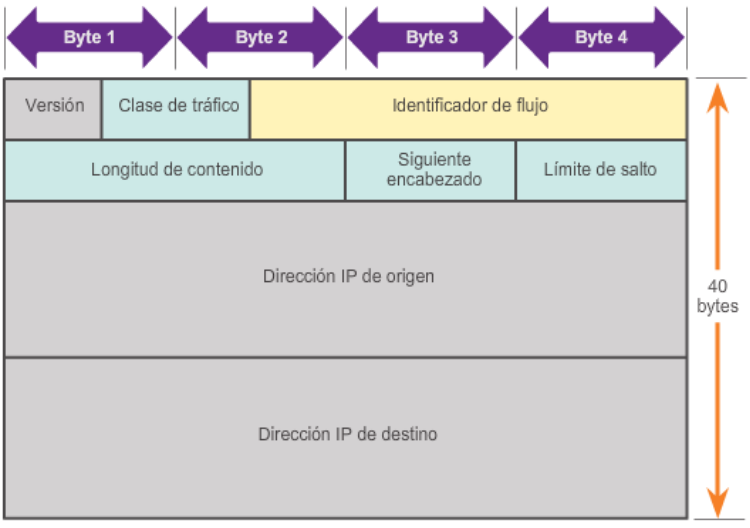


Figura 24. Encabezado de IPv6

Fuente: Cisco Networking Academy: *Encabezado de paquete IPv6.*

Versión: este campo contiene un valor binario que identifica la versión del paquete IP. Para los paquetes IPv6, este campo siempre se establece en 0110.

Identificador de flujo proporciona un servicio especial para aplicaciones en tiempo real. Se puede utilizar para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, a fin de evitar que estos se reordenen.

Longitud de contenido define el tamaño total del paquete, incluidos el encabezado y las extensiones optativas

Siguiente encabezado Indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente.

Límite de saltos, este valor disminuye en un punto, cada vez que el paquete es procesado por un router. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a destino.

Dirección de origen: este campo de 128 bits identifica la dirección IPv6 del host emisor.

Dirección de destino: este campo de 128 bits identifica la dirección IPv6 del host receptor (Cisco Networking Academy, 2015).

2.2.4.4 Capa transporte

El protocolo de transporte proporciona un servicio de transferencia de datos extremo a extremo. Los protocolos de la capa transporte pueden ser orientado a conexión como es TCP, o no orientado a conexión como es UDP (Stallings., 2004, p. 566).

La capa de transporte permite la segmentación de datos y proporciona el control necesario para rearmar estos segmentos en los distintos streams de comunicación.

Función de Capa Transporte

TCP está diseñado para proporcionar una comunicación segura entre pares de procesos a través de una gran variedad de redes interconectadas.

En la capa de transporte, cada conjunto de datos particular que fluye entre una aplicación de origen y una de destino se conoce como conversación. Un host puede tener varias aplicaciones que se comunican a través de la red de forma simultánea. Cada una de estas aplicaciones se comunica con una o más aplicaciones en uno o más hosts remotos (Cisco Networking Academy, 2015).

IP utiliza estos protocolos de transporte para habilitar la comunicación y la transferencia de datos entre los hosts.

Algunos ejemplos que proporciona cada una de las capas del modelo de referencia TCP/IP se muestra en la figura 25.

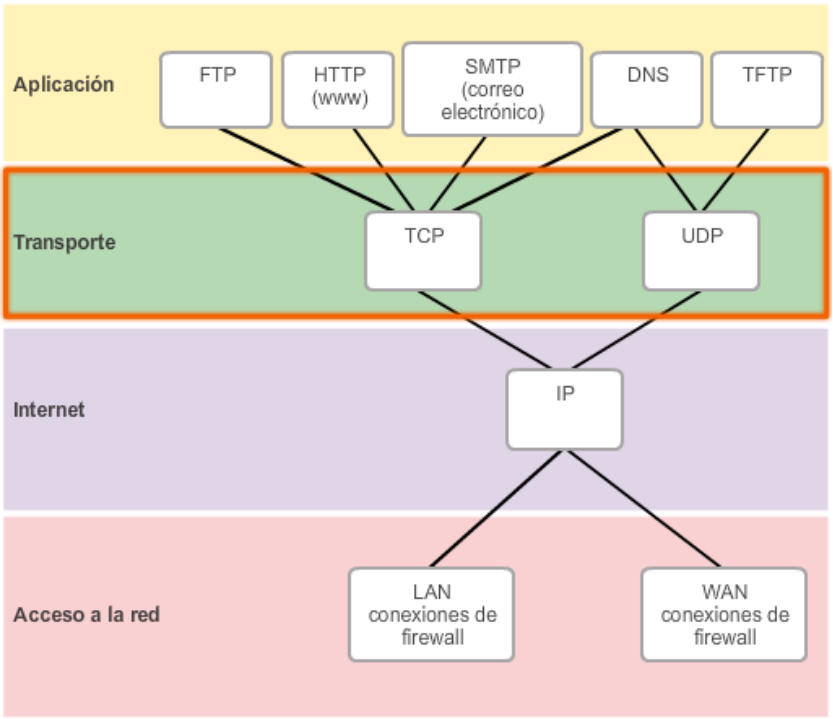


Figura 25. Transporte de Datos.

Fuente: Cisco Networking Academy: *Protocolos de la capa transporte.*

TCP

TCP se considera un protocolo de transporte confiable, lo que significa que incluye procesos para garantizar la entrega confiable entre aplicaciones mediante el uso de entrega con acuse de recibo.

Las tres operaciones básicas de confiabilidad son las siguientes:

- Seguimiento de segmentos de datos transmitidos
- Acuse de recibo de datos
- Retransmisión de cualquier dato sin acuse de recibo

Estos procesos de confiabilidad generan una sobrecarga adicional en los recursos de la red debido a los procesos de acuse de recibo, rastreo y retransmisión. Para admitir estos procesos de confiabilidad, se intercambian más datos de control entre los hosts emisores y receptores. Esta información de control está incluida en un encabezado TCP (Cisco Networking Academy, 2015).

Servicios TCP

Los servicios de confiabilidad y la forma en que realizan el seguimiento de las comunicaciones que implementa TCP son:

1. El establecimiento de una sesión garantiza que la aplicación esta lista para recibir los datos
2. La entrega confiable implica el reenvió de segmentos perdidos para que se reciban los datos en forma completa.
3. La entrega en el mismo orden garantiza que los segmentos se entreguen en el orden correcto

4. El control de flujo administra la entrega de datos si se observa congestión en el host.

Formato de la cabecera TCP

El formato de la cabecera TCP se muestra en la Figura 26.

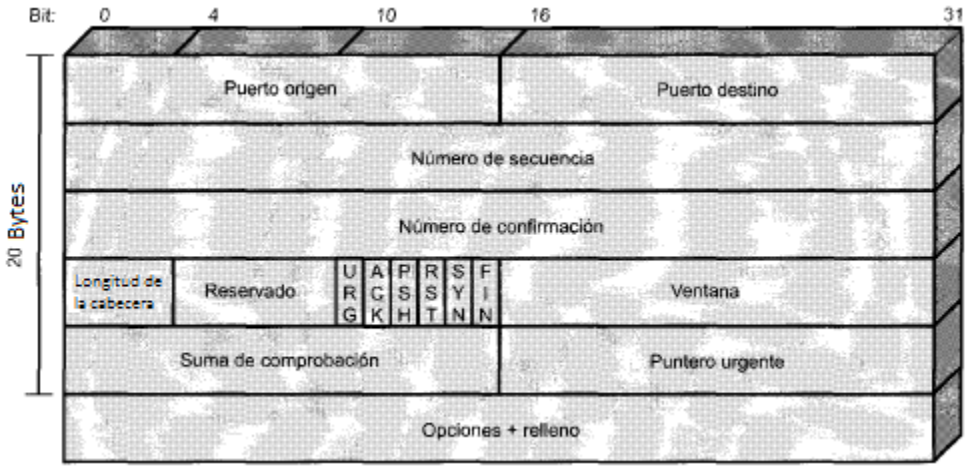


Figura 26. Cabecera TCP.

Fuente Modificado de Stallings, W. Comunicaciones y redes de computadores: *Formato de la Cabecera TCP* (p. 701).

Puerto origen.- Usuario TCP origen.

Puerto destino.- Usuario TCP destino.

Numero de secuencia.- Se utiliza para rearmar datos.

Numero de confirmación.- Indica si se recibieron los datos.

Longitud de la cabecera.- Indica la longitud del encabezado del segmento TCP.

Reservado.- Campo reservado para un uso futuro.

Indicadores.- Indican el propósito y la función del segmento TCP.

URG.- el campo puntero urgente es valido

ACK.- el campo de confirmación es válido.

PSH.- función de carga.

RST: puesta a cero de la conexión.

SYN.- sincronizar los números de secuencia

FIN.- el emisor no tiene más datos.

Suma de verificación.- se utiliza para la verificación de errores en el encabezado y los datos del segmento.

Puntero Urgente.- indica si la información es urgente.

Opciones.- si está presente, solamente se define una opción, que especifica el tamaño máximo del segmento que será aceptado.

(Tanenbaum & Wetherall, 2012, pág. 478), (Stallings, 2004, pág. 700) y (Cisco Networking Academy, 2015).

Formato de la cabecera UDP

El formato de la cabecera UDP se muestra en la Figura 27.

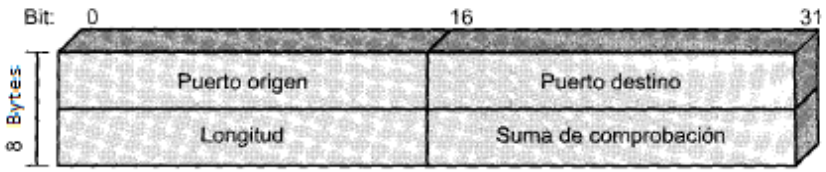


Figura 27. Cabecera UDP.

Fuente Modificado de Stallings, W. Comunicaciones y redes de computadores: *Formato de la Cabecera UDP* (p. 717).

Puerto origen.- Usuario UDP origen

Puerto destino.- Usuario UDP destino

Longitud.- Incluye el encabezado de 8 bytes y los datos

Suma de comprobación.- es opcional y se almacena como 0 si no se calcula.

(Stallings, 2004, p. 717) y (Cisco Networking Academy, 2015)

Establecimientos de la conexión

En TCP las conexiones se establecen usando el saludo de tres vías. Ver Figura 28.

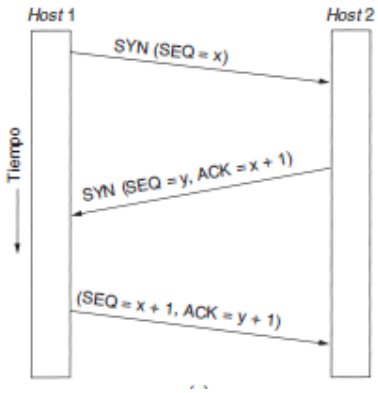


Figura 28. Establecimientos de una conexión TCP.

Fuente Modificado de Tanembaum, A. Redes de computadores: *Establecimiento de una conexión TCP* (p. 481).

El cliente de origen solicita una sesión de comunicación con el servidor.

El servidor acusa recibo de la sesión de comunicación de cliente y solicita una sesión de comunicación de servidor a cliente

El cliente de origen acusa recibo de sesión de comunicación de servidor a cliente (Cisco Networking Academy, 2015).

2.2.4.4 Capa aplicación

Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Algunos de los protocolos TCP/IP son:

HTP y HTTPS

Cuando se escribe una dirección Web o un localizador uniforme de recursos (URL) en un explorador Web, el explorador establece una conexión con el servicio Web que se ejecuta en el servidor mediante el protocolo HTTP (Cisco Networking Academy, 2015) .

Para acceder al contenido, los clientes Web establecen conexiones al servidor y solicitan los recursos deseados. El servidor responde con el recurso y, al recibirlo, el explorador interpreta los datos y los presenta al usuario (Cisco Networking Academy, 2015).

El HTTPS puede utilizar autenticación y encriptación para asegurar los datos mientras viajan entre el cliente y el servidor. HTTPS especifica reglas adicionales para pasar datos entre la capa de aplicación y la capa de transporte. El protocolo HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del servidor que HTTP, pero el stream de datos se encripta con capa de sockets seguros (SSL) antes de transportarse a través de la red (Cisco Networking Academy, 2015).

Sistema de nombres de Dominio (DNS)

En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas, los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre fácil de recordar y reconocible. El servidor DNS relaciona el nombre de dominio con la dirección numérica

Entre otros protocolos más utilizados están:

DHCP.- Se utiliza para asignar direcciones en forma dinámica a las estaciones cliente durante el inicio. Permite que las direcciones se vuelvan a utilizar cuando ya no se necesitan.

SMTP.- Permite que los clientes envíen correos electrónicos a un servidor de correo. Además que los servidores envíen correos electrónicos a otros servidores.

FTP.- permite transferir archivos hacia y desde otro host a través de una red.

2.3 Jerarquía de Redes

Antes de empezar a implementar una red es necesario preguntarse de que tamaño va a ser esta red, porque de acuerdo a esto se van a determinar los requerimientos y las posibles soluciones. Sus necesidades son totalmente diferentes, y lo que hace su diferencia es el número de dispositivos es por ello se las clasificara de la siguiente forma:

Red Pequeña.- provee servicio hasta 200 dispositivos.

Red Mediana.- provee servicios desde 200 a 1000 dispositivos

Red Grande.- provee servicio a más de 1000 dispositivos.

Para el diseño de la red se deben tomar en cuenta varios factores entre ellos que sea jerárquica esto permite facilitar el diseño de nuestra red (Vallejo, 2014).

El diseño jerárquico de una red contempla tres diferentes capas, como se muestra en la Figura 29.

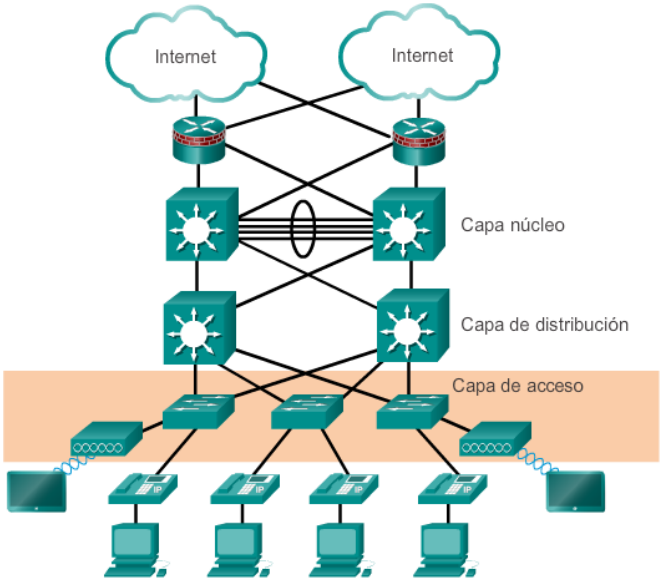


Figura 29.. Jerarquía de Redes.

Fuente: Modificado de Cisco Networking Academy: *Jerarquía en las redes conmutadas sin fronteras*).

2.3.1 Capa de acceso

Es la capa que nos brinda conectividad a los usuarios finales, típicamente está conformado solo por switch's de acceso

Dentro del modelo jerárquico en la capa de acceso no se permite conectar entre switch's de acceso. Los switch's de capa de acceso se conectan a los switch's de capa de distribución, que implementan tecnologías de base de red como el enrutamiento, la calidad de servicio y la seguridad (Vallejo, 2014).

2.3.1.1 Seguridad se puertos

La seguridad de puerto limita la cantidad de direcciones MAC[22] válidas permitidas en el puerto. Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan (Cisco Networking Academy, 2015).

[22] MAC: Media Access Control Identificador que poseen las tarjetas o dispositivos de red, este identificador es único a nivel mundial.

La seguridad de puertos se puede configurar para permitir una o más direcciones MAC. Si la cantidad de direcciones MAC permitidas en el puerto se limita a una, solo el dispositivo con esa dirección MAC específica puede conectarse correctamente al puerto.

2.3.2 Capa de distribución

Esta capa sirve para conectar la capa de acceso a la capa de núcleo. Se puntualiza los enlaces redundantes para distribuir la información del nivel de acceso.

Esta capa define políticas basadas en filtros de seguridad a nivel de servicios, enrutamiento entre VLAN´s, balanceo de cargas, sumarizaciones de subredes ya que esta capa no necesita saber a detalle de cada una de las subredes (Vallejo, 2014).

2.3.2.1 VLAN

El rendimiento de la red es un factor importante en la productividad de una organización. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños (Cisco Networking Academy, 2015).

Se puede crear diferentes LAN´s virtuales (VLAN) en un switch administrable. Una VLAN se clasifica como una LAN independiente incluso cuando comparten la misma estructura.

Definición de VLAN

Una LAN virtual se puede definir como una subred que se basa en conexiones lógicas en lugar de conexiones físicas, permiten que el administrador divida las redes en segmentos según las funciones de cada usuario sin tener en cuenta la ubicación física del dispositivo. Ver Figura 30.

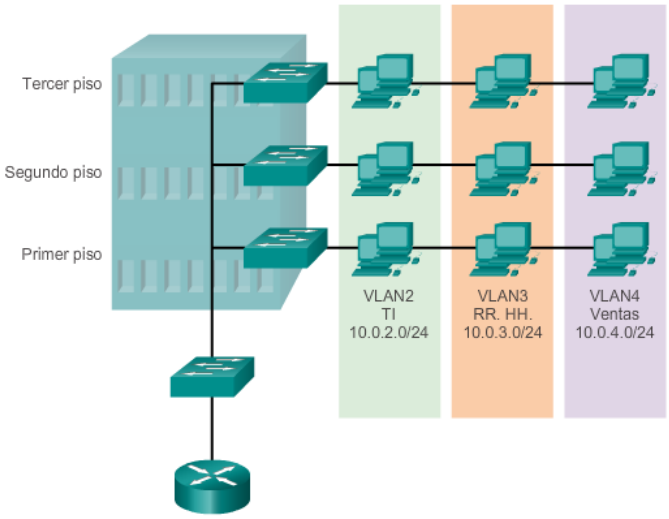


Figura 30. Definición de tipos de VLAN.

Beneficios de VLAN

Se puede mejorar la seguridad ya que permite separar los grupos con datos más sensibles del resto evitando violaciones de información confidencial.

Se puede reducir los costos haciendo un uso eficaz de enlaces y de ancho de banda.

Se mejora el rendimiento ya que la información se maneja por medio de dominios de difusión específicos y reduciendo el trafico innecesario.

La seguridad de la red y las políticas se pueden asignar a grupos definidos.

VLAN de datos

Nos permite transportar datos generados específicamente por los usuarios de la red. Se usan para dividir la red.

VLAN predeterminada

Cuando un switch es encendido todos los puertos forman parte de la VLAN predeterminada. Es una VLAN por default que está presente en el equipo.

VLAN nativa

Se utiliza para clasificar las tramas no etiquetadas, el puerto de enlace troncal 802.1Q coloca el trafico sin etiquetar en la VLAN nativa.

VLAN de administración

Es configurada para acceder a las capacidades de administración de un switch para ello es necesario asignar una dirección IP y una máscara de subred para poder gestionar el dispositivo.

VLAN de voz

Es configurado para admitir tráfico de voz sobre IP. El tráfico de voz en una red es primordial requiere como tal un ancho de banda garantizada.

Enlaces troncales

Tiene la capacidad de enviar tramas, pertenecientes a diferentes VLAN´s, a través de los switch´s; de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switch´s se puedan comunicar. Ver Figura 31.

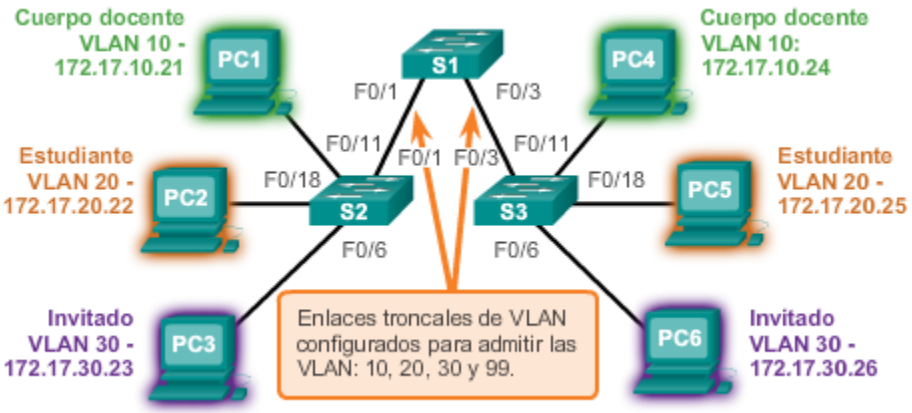


Figura 31. Enlaces troncales.

Fuente Modificado de Cisco Networking Academy: *Enlaces troncales de la VLAN.*

IEEE 802.1Q

El estándar IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos) para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Arévalo Galárraga & Vaca Tello, 2010; Laurencio, Gómez, Felipe, & Diaz).

2.3.2.2 Seguridad en la comunicación

La información es el bien más preciado de una organización, por tal motivo se ha convertido en uno de los principales desafíos, para los administradores de sistemas informáticos, en brindar una respuesta adecuada a posibles problemas de seguridad; es por ello que uno de los mecanismos más utilizados para filtrar paquetes maliciosos son los denominados Firewalls.

Firewall

Un firewall es una entidad confiable que se asienta para separar áreas sensibles dentro de una red de computadoras. El cortafuegos (firewall) se configura con un conjunto de reglas que dependen de las políticas de seguridad de la organización, que determinan a que tráfico de red se le permitirá pasar y cual será bloqueado o rechazado (Esparza Morocho, 2013; Mazzari & Monsalve Arteaga, 1998).

El esquema del funcionamiento de un Firewall se muestra en la Figura 32.

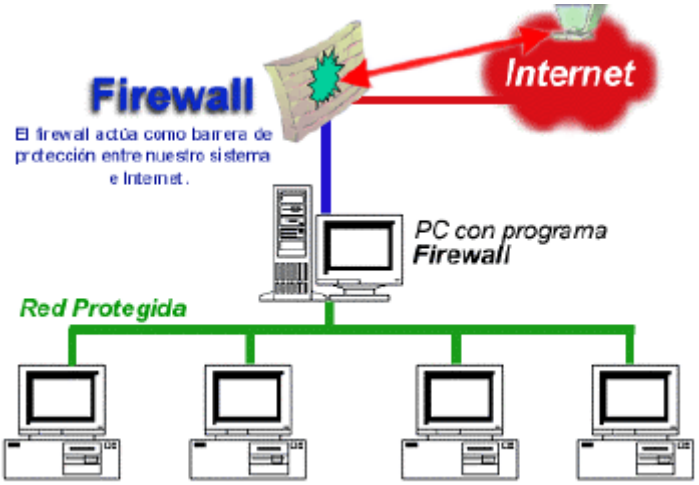


Figura 32. Esquema de un Firewall.

Fuente: Esparza J. Implementación de un Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados. *Concepto de Firewall* (p.59).

Firewalls de software

Un firewall de software es una aplicación que puede estar integrada en el mismo sistema operativo (Iptables) o puede instalarse independientemente, son fácilmente escalables ya que se pueden integrar proxies (Ferrer Berbegal, 2006).

Firewall Físicos

Un firewall físico es un hardware especifico con un sistema operativo que filtra el trafico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica o se descarta. A diferencia de los firewalls de Software estos suelen estar ya pre-configurados para su implementación (Ferrer Berbegal, 2006; Izura, 2003).

Arquitecturas de Firewalls

En este apartado se describen las diferentes características de funcionamiento de los Firewalls

Arquitectura Dual-Homed Host

Se construye en base a una computadora que tiene al menos dos interfaces de red. Esta arquitectura podría actuar como un encaminador entre las redes de estas interfaces de red que posee, encaminando paquetes IP[23] de una red a otra. Sin embargo, para aplicar esta arquitectura de cortafuegos es necesario desactivar esta función de encaminamiento. Así, paquetes IP de una red (por ejemplo, la red interna). Los sistemas dentro de cortafuegos pueden comunicarse con el anfitrión dual-homed, pero estos sistemas no pueden comunicarse directamente entre sí. El trafico IP entre ellos es completamente Bloqueado (Cuauhtémoc, 2009).

La arquitectura dual-hommed se coloca entre Internet y la red interna

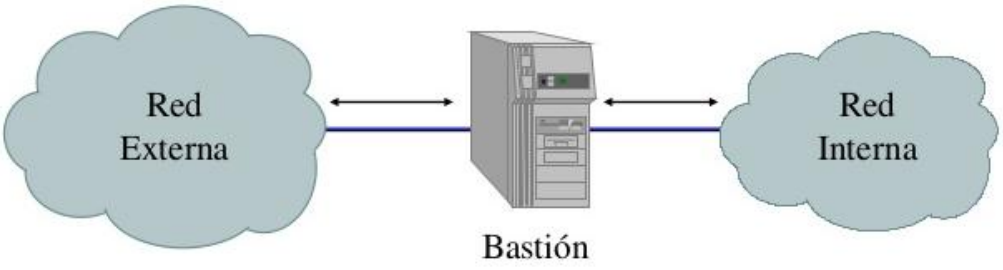


Figura 33. Arquitectura Dual-homed Host.

Fuente: Tejeda C. Estudio, diseño e implementación de un Firewall. *Dual-Homed Host* (p.22).

Esta arquitectura puede proporcionar un gran nivel de control. Si no está permitiendo que los paquetes IP puedan ir entre las redes externas e internas, puede estar seguro de que cualquier paquete de la red interna que tenga un origen externo es evidencia de algún tipo de problema de seguridad (Cuauhtémoc, 2009).

[23] IP: Protocolo internet; permite el desarrollo y transporte de paquetes de datos.

La única manera que tienen la red interna de conectase con el exterior es a través de servicios proxy localizados en el firewall, y a través de este servir de conexión. Por otra parte, el hecho de que haya un Proxy existirá una aplicación de software que permitirá un amplio número de procesos de carga y de control de acceso, lo que obliga un filtrado mucho más elaborado y consecuentemente un mayor tiempo de carga ((Ferrer Berbegal, 2006; TEJEDA, 2002).

Arquitectura Screened Host

Este tipo de arquitectura permite filtrar por direcciones origen y destino, por protocolo o por puertos origen y destino; es decir parámetros TCP/IP(Ferrer Berbegal, 2006).

Screened Host combina un router con un host bastión donde el principal nivel de seguridad proviene del filtrado de paquetes, es decir el routes es la primera y más importante línea de defensa. En la maquina bastión se ejecutan los proxies de las aplicaciones, mientras que el router se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un número reducido de servicios(Ferrer Berbegal, 2006). Ver Figura 34.

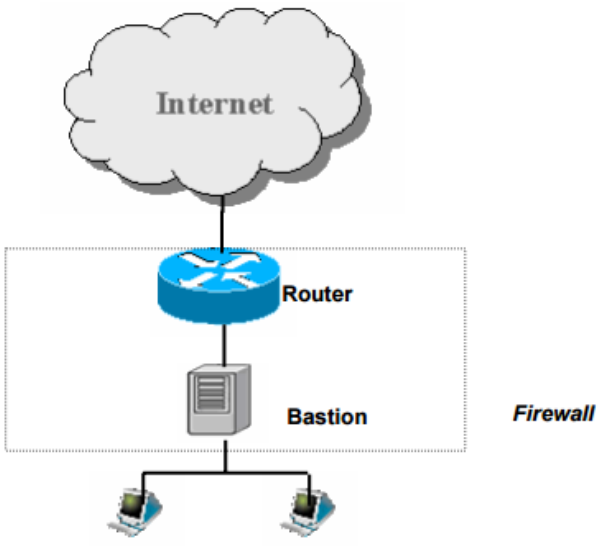


Figura 34. Arquitectura Screened Host.

Fuente: Ferrer M. Firewalls software: Estudio, Instalación, configuración de escenarios y comparativa. *Screened Host* (p.21).

Arquitectura DMZ

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, entre otros), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que se denomina DMZ[24] o zona desmilitarizada. El firewall tiene entonces tres entradas(Izura, 2003)**.** Ver Figura 35.

[24] DMZ: Zona desmilitarizada o red perimetral; es una zona segura que se ubica entre la red interna de una organización y una red externa

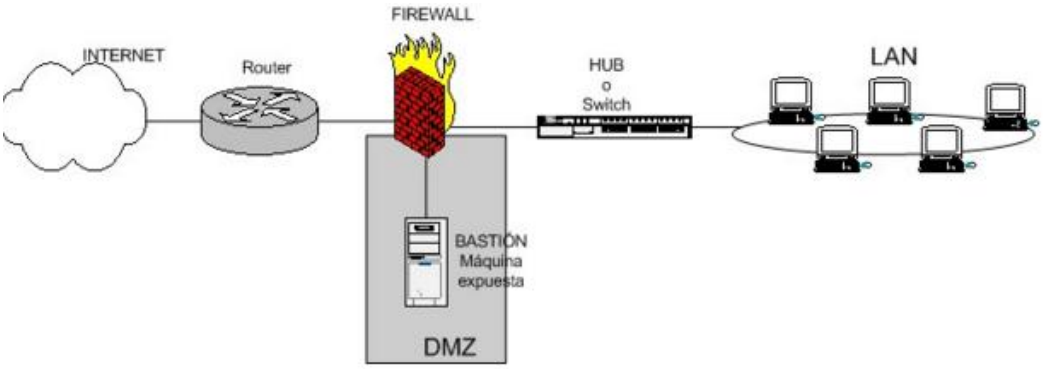


Figura 35. Arquitectura DMZ.

Fuente: Izura X. IPTABLES Manual Práctico: Estudio, Instalación. *Qué es un Firewall.*

Sea el tipo de firewall que sea, generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo TCP/IP.

Políticas de seguridad

Es importante la implementación de la política de seguridad, pues en ella se establecen las reglas básicas a través de las cuales los usuarios se guiarán para utilizar la red de una manera óptima. Definir políticas de seguridad de una red significa desarrollar procedimientos y planes que protejan a los recursos de la red contra pérdidas y daños (Mazzari & Monsalve Arteaga, 1998).

Las políticas de seguridad de la red que se implementen deben ser de tal manera que no impidan el buen funcionamiento de la organización. Si las políticas de seguridad no permiten que los usuarios ejecuten sus tareas efectivamente, los usuarios empezaran a buscar maneras de violar las seguridades; para esto es necesario distinguir que tipos de usuarios van a tener acceso a los recursos, y cuál es el comportamiento adecuado de los usuarios frente a los recursos (Mazzari & Monsalve Arteaga, 1998).

Hay dos políticas básicas en la configuración de un firewall:

Política restrictiva

Esta política, deniega todo el tráfico excepto el que esta explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten (Arévalo Galárraga & Vaca Tello, 2010).

Política permisiva

Mediante esta política, se permite todo el tráfico excepto el que este explícitamente denegado. Cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado (Arévalo Galárraga & Vaca Tello, 2010).

2.3.2.3 Proxy

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial(Arévalo Galárraga & Vaca Tello, 2010).

Definición

Un proxy es una aplicación que brinda servicios especializados que se ejecutan en un host con el propósito de enlazar directamente a los clientes internos de una red con los host externos (internet). Este tipo de servidores se colocan entre un cliente interno y un servidor externo. En vez de conectarse directamente uno al otro, cada uno se conecta a través del proxy (Mazzari & Monsalve Arteaga, 1998).

Funcionamiento

El cliente realiza una petición de un recurso de internet, cuando este desea acceder a dicha información, es el proxy quien realiza la comunicación y traslada el resultado al equipo originario.

Los Proxys pueden filtrar el contenido de las páginas Web servidas y bloquear contenido ofensivo.

En la mayoría de los casos se añade la funcionalidad adicional de mantener los resultados obtenidos en una memoria caché que permite acelerar consultas coincidentes.

Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargó en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones (Lois, 2015).

En la Figura 36 se detalla el funcionamiento de un proxy en una red de datos.

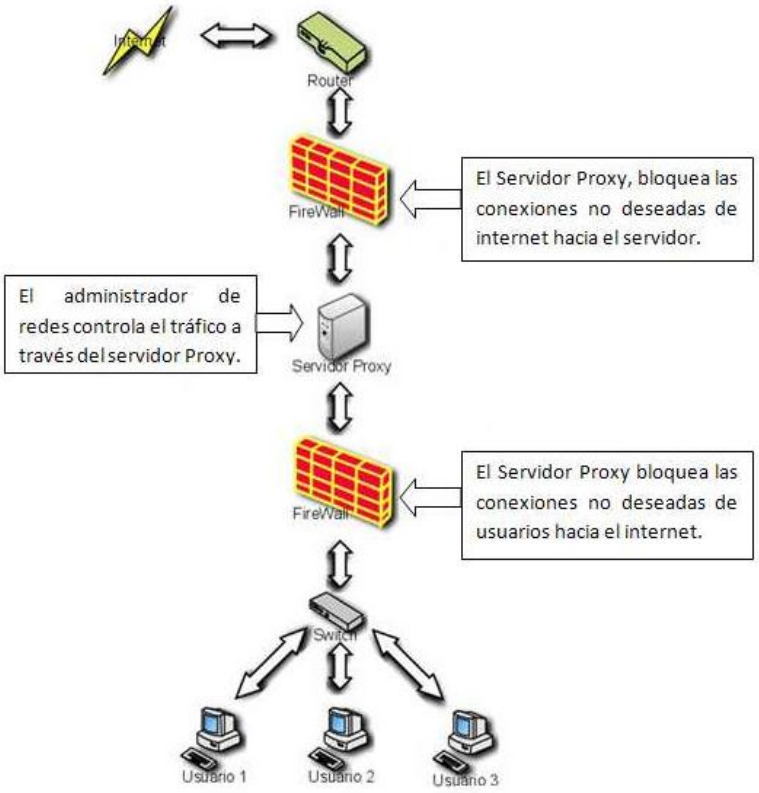


Figura 36. Funcionamiento de un servidor proxy.

Fuente: (Arévalo Galárraga & Vaca Tello, 2010). Análisis, diseño e implementación de un software prototipo de firewall y servidor proxy multiplataforma con tecnología Java. *Funcionamiento de un proxy.* (p.63).

Ventajas

- **Control:** para limitar y restringir los derechos de los usuarios, y dar permisos solo al proxy.
- **Control:** para limitar y restringir los derechos de los usuarios, y dar permisos solo al proxy.
- **Ahorro:** Solo el proxy realizará el control de la red.
- **Velocidad:** Si varios clientes van a pedir el mismo recurso, el proxy, por medio del caché proporcionará una respuesta inmediata, porque guarda en memoria las peticiones que fueron solicitadas en un principio.

- **Filtrado:** El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Anonimato:** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos(Arévalo Galárraga & Vaca Tello, 2010).
- **Anonimato:** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos.

Desventajas

- **Abuso:** Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no corresponda. Por tanto, ha de controlar quien tiene acceso y quien no a sus servicios.
- **Carga:** Un proxy ha de hacer el trabajo de muchos usuarios.
- **Intromisión:** Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy.
- **Incoherencia:** Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino(Arévalo Galárraga & Vaca Tello, 2010).
- **Incoherencia:** Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.

Tipos de Proxy

Se detallarán tres tipos de proxy: Web Proxy Cache, Proxy Inverso, Proxy Transparente.

Web Proxy Cache

Se dice que un servidor esta actuado como Web Proxy cache cuando almacena en su disco duro las páginas Web descargadas de forma que, en próximas consultas, pueda acceder a ellas de forma muy rápida. De esta forma se optimiza el canal de acceso a

Internet de la organización del usuario en momentos de ocupación importante de la línea (Rosalba Ximena & Verónica Marcela, 2008).

Este tipo de proxy se suele utilizar en los siguientes entornos:

- Cuando por motivos de seguridad, no deseas permitir acceso libre a Internet a los usuarios pero se desea proporcionarles acceso a la Web, se les proporciona a través del Proxy.
- Cuando se desea optimizar el ancho de banda y acelerar la navegación para los usuarios por ejemplo, una oficina con muchos trabajadores que sueles visitar frecuentemente las mismas páginas.

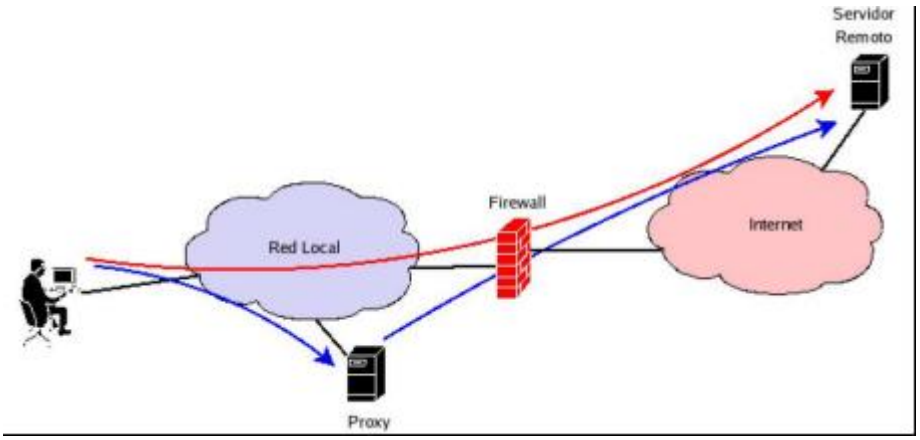


Figura 37. Web Proxy Cache.

Fuente:(Rosalba Ximena & Verónica Marcela, 2008). Desarrollo y pruebas de Servidores de Firewall y Proxy en Linux Red Hat Enterprise 4.0 mediante máquinas virtuales. *Web Proxy Cache.* (p.16).

Proxy Inverso

Un Proxy inverso (o reverse Proxy) es aquel que se sitúa cerca de uno o más servidores Web, de forma que es el Proxy quien recibe las peticiones de los clientes, las reenvía a los servidores Web Remotos y actualiza una copia en su cache para futuras peticiones. (Rosalba Ximena & Verónica Marcela, 2008).

Este tipo de Proxy se suele usar en algunos de estos entornos:

- Para añadir seguridad a los servidores Web, en ningún momento se accede directamente a ellos sino al Proxy.
- Para balancear la carga de los servidores: el servidor Proxy es el encargado de enviar las peticiones a aquellos a servidores que estén más descargados.
- Para descargar a los servidores Web de contenido estático como imágenes o documentos.
- En caso de sitios Web seguros se puede dejar al Proxy que haga el encriptado de los datos y descargar así a los servidores Web.

Proxy Transparente

Es posible usar un Proxy para aplicar políticas de control de acceso a Internet. Normalmente esa configuración no es transparente: es necesario modificar el cliente para que use el Proxy al acceder a Internet, de forma que es posible que un usuario modifique esa configuración(Rosalba Ximena & Verónica Marcela, 2008).

Una configuración de Proxy transparente hace que no sea necesaria modificación alguna en las maquinas clientes, eliminando el riesgo de que un usuario modifique dicha configuración a su antojo. El uso de un Proxy transparente combina un servidor Proxy con NAT[25], de forma que todas las conexiones son encaminadas a través del Proxy sin la intervención de la maquina cliente(Rosalba Ximena & Verónica Marcela, 2008).

Squid

Squid es un Servidor Proxy de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los

[25] NAT: traducción de direcciones de red; mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

sistemas operativos como GNU/Linux. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL)(Cholanco & Anibal, 2009).

Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para protocolos HTTP, FTP[26], Proxy transparente y otras muchas más, como filtración de contenido y control de acceso por IP y por usuario (Cholanco & Anibal, 2009).

Al iniciar Squid da origen a un número configurable de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores DNS (Cholanco & Anibal, 2009).

El servidor proxy Squid guarda los datos cacheados en la memoria RAM, realiza caché de consultas DNS, y no guarda en cache las peticiones que son rechazadas. Es decir Squid es un servidor proxy que permite utilizar una sola conexión a Internet. El servidor proxy además almacena en el disco duro las páginas más visitadas desde las estaciones, de tal manera que se realiza un ahorro significativo del ancho de banda del enlace del centro de acceso cuando se solicita la página nuevamente desde la misma u otra estación. Squid verifica si la página ha cambiado, y de ser así, vuelve a almacenarla localmente (Cholanco & Anibal, 2009).

Analizador SARG

Uno de los mecanismos que permita revisar que las acciones se estén llevando de acuerdo con las políticas establecidas, es la supervisión de la información registrada en

[26] FTP: Protocolo de Transferencia de Archivos; protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

los servidores proxy, utilizando un analizador de registros permitiendo generar un conjunto de reportes sobre la navegación de los usuarios en la red. El análisis correcto de los registros puede brindar una visión clara de las actividades realizadas durante la navegación (Santana, Barredo, Pavón, Bonachea, & Oduardo).

2.4 Plataforma Linux

2.4.1 Software libre

Software libre es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente (Cholanco & Anibal, 2009).

El software libre suele estar disponible gratuitamente, o al predio de coste de la distribución a través de otros medios; sin embargo no es obligatoria que sea así, por lo tanto no hay que asociar software libre a software gratuito, ya que, conservando su carácter de libre, puede ser distribuido comercialmente (Cholanco & Anibal, 2009).

2.4.2 Razones para utilizar Gnu/Linux

Una de las principales razones para utilizar Linux es que es que no son necesarias licencias. Linux mantiene la marca registrada Linux, el kernel de Linux se distribuye bajo la licencia GPL, esto significa que se puede obtener y modificar el código fuente(Cholanco & Anibal, 2009).

Multitarea: La palabra multitarea describe la habilidad de ejecutar varios programas al mismo tiempo. Linux utiliza la llamada multitarea preventiva, la cual asegura que todos los programas que se están utilizando en un momento dado serán ejecutados, siendo el

sistema operativo el encargado de ceder tiempo de microprocesador a cada programa mediante el scheduler[27] (TEJEDA, 2002).

Incluidas en el núcleo se tiene una gran cantidad de protocolos de red como por ejemplo: TCP/IP tanto IPversion 4 como IPversion6. Appletalk compatible con redes, entre otros (TEJEDA, 2002).

Dispone de servidores para protocolos HTTP, SMTP[28], NFS[29], SMB[30] entre otros muchos (TEJEDA, 2002).

Aunque la mejor virtud son los miles de programas a través de Internet distribuidos gratuitamente o con licencias de libre distribución.

2.4 Inter VLAN en sistemas GNU/Linux

Según GRAHAM, SHAW "Una VLAN es un tipo de red de área local que no tiene su propia infraestructura física dedicada, sino que utiliza otra LAN para llevar su tráfico. El tráfico se encapsula de manera que VLAN´s separadas lógicamente puede ser transportado por la misma LAN física".

En las redes de protocolo de Internet se considera una buena práctica utilizar una VLAN separada para cada subred IP. Las razón para hacer esto incluye evitar la necesidad de que host deban procesar tráfico de difusión procedente de otras redes.

2.4.1 Requerimientos para VLAN en GNU/Linux

[27] Scheduler: Se refiere a programar procesos dentro de un período de tiempo constante, independientemente del número de procesos se están ejecutando en el sistema operativo
[28] SMTP: protocolo para transferencia simple de correo; es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico.
[29] NFS: Network File System; utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local.
[30] SMB: Server Message Block; es un protocolo de red que permite compartir archivos, impresoras, etc. entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows

Para configurar interfaces VLAN 802.1Q debe ejecutar un kernel con soporte VLAN 802.1Q, una forma de saber si el kernel que se está ejecutando incluye el soporte del protocolo 802.1Q, es necesario la búsqueda de la etiqueta VLAN_8021Q en el archivo de configuración del kernel (Medina, J).

2.4.2 802.1Q en GNU/Linux

Linux tiene la capacidad de utilizar una interfaz Ethernet como un puerto de enlace troncal 802.1Q, lo que le permite enviar y recibir tráfico simultáneamente en múltiples VLANs. Esta es proporcionada por el módulo de kernel 802.1Q, que puede ser configurado.

La mayoría de las distribuciones GNU/Linux proporcionan un mecanismo de creación y configuración de interfaces virtuales, sin embargo, el método varía (Graham, S).

2.4.3 Distribuciones basadas en GNU/Linux

2.4.3.1 Debian

El Proyecto Debian es una asociación de personas que han hecho causa común para crear un sistema operativo libre. Los sistemas Debian actualmente usan el núcleo de Linux o. Linux es una pieza de software creada en un principio por Linus Torvalds y desarrollada por miles de programadores a lo largo del mundo (Rincón De Los Desarrolladores).

Una gran parte de las herramientas básicas que completan el sistema operativo, vienen del proyecto GNU; de ahí los nombres: GNU/Linux. Estas herramientas también son libres (Rincón De Los Desarrolladores).

Debian es famoso por filosofía de estabilidad ante todo, por eso mismo, no tiene un cronograma de lanzamiento de nuevas versiones. Estas se liberan cuando están listas. Esto hace que sea una de las opciones más estables de GNU/Linux (Garron G.).

2.4.3.2 CentOS

La distribución CentOS Linux es una plataforma estable, predecible, manejable y reproducible derivado de las fuentes de Red Hat Enterprise Linux (RHEL). Desde marzo de 2004, CentOS Linux ha sido una distribución apoyada por la comunidad derivados de fuentes proporcionadas libremente al público por Red Hat. Como tal, CentOS Linux aspira a ser funcionalmente compatible con Red Hat Enterprise Linux (Centos Project).

CentOS Linux es desarrollado por un pequeño pero creciente grupo de desarrolladores. A su vez los desarrolladores principales son apoyados por una comunidad de usuarios activa incluyendo administradores de sistemas, administradores de red, administradores, contribuyentes de Linux, y los entusiastas de Linux de todo el mundo (Centos Project).

2.4.3.3 Tabla comparativa Debian y Centos

En la Tabla 3 se muestra una comparativa y características de los sistemas operativos Debían y Centos los cuales se utilizan como sistemas de distribución y producción

Tabla 3: Comparación de Distribuciones Debían y Centos

SISTEMA OPERATIVO	DESCRIPCION	TIPO	USO
Centos	Basado sobre Red Hat™ Enterprise Linux Mantenido por comunidad	Gratuita	Servidores Est. trabajo Producción
Debian	Mantenido por comunidad	Gratuita	Multiuso Producción

Fuente: Modificado de Tabla comparativa de distribuciones Linux. (Dueñas, 2016)

2.5 Especificaciones de los requerimientos del software basado en el estándar ISO/IEC/IEEE 29148-2011

Para las especificación de los requerimientos del software a implementar se pone en consideración la norma ISO/IEC/IEEE 29148:2011 que contiene disposiciones para los procesos relacionados con la ingeniería de requisitos para los sistemas, que reemplaza a la norma IEEE 830.

1. Introducción
Se presenta la documentación de los requerimientos de software necesarios en la implementación de un servidor Firewall-Proxy para la Facultad de Ingeniería en Ciencias Aplicadas utilizando herramientas bajo la licencia de software libre GNU/Linux.
1.1.Propósito
El presente apartado pretende obtener los requisitos necesarios que debe cumplir el servidor Firewall-Proxy para su correcto diseño, desarrollo e implementación.
1.2.Ámbitos del sistema
El servidor a implementar debe tener la capacidad de ejecutar políticas de seguridad y reglas que permitan direccionar el tráfico hacia el Proxy el cual procurará gestionar contenido Web. Dicho servidor deberá proporcionar una herramienta que

permita gestionar el acceso al servicio de internet y no permita visualizar datos de la bitácora del proxy.

1.3. Acrónimos

Proxy.- es un servidor que actúa como un intermediario para solicitudes de los clientes que buscan recursos de otros servidores.

GNU.- Movimiento y comunidad de Software y Conocimiento Libres, cuyo objetivo es la Promoción del desarrollo colaborativo de software y conocimiento mediante el uso de licencias libres.

Linux.- es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre.

1.4.Referencias

Systems and software engineering — Life cycle processes — Requirements engineering. ISO/IEC/IEEE 29148.

Especificación de Requisitos según el estándar de IEEE 830.

1.5.Visión General del Documento

El documento cuenta de tres secciones: la primera parte describe el propósito y ámbito del sistema; en la segunda sección se menciona la descripción general especificando la perspectiva, características, funciones y restricciones del sistema; la tercera parte se mencionan los requisitos del servidor.

2. Descripción general

En esta sección se describen aquellos factores que intervienen en el desarrollo del sistema. Se puntualiza en contexto los detalles que permitirá definir los requisitos.

2.1.Perspectiva del Producto

El servidor permite gestionar políticas y reglas de seguridad en un segmento de red, dependiendo de estas, se direcciona el tráfico hacia el servidor Proxy el cual

procura filtrar contenido web con el fin de liberar tráfico innecesario que se transporta por el segmento de red. El generador de reportes permite generar informes de los sitios web visitado, para de esa manera tomar decisiones administrativas.

2.2.Funciones del Producto

Las funciones del servidor comprenden:

- Implementación de interfaces Virtuales por cada laboratorio
- Implementación de reglas y políticas a Firewall
- Filtrado de paquetes
- Filtrado de contenido
- Asignación de memoria cache para contenido web
- Asignación de Horarios para uso de Internet
- Herramienta para generación de reportes

2.3.Características de los Usuarios

Los usuarios están en la capacidad de restringir acceso a Sitios web, restricción de acceso por horarios, configurar memoria cache para conservar el contenido solicitado, gestionar listas y reglas de control de acceso y configurar la herramienta de reportes utilizando la bitácora del proxy.

2.4.Restricciones

El servidor se implementara en un segmento de red de la Facultad de Ingeniería en Ciencias aplicadas de la Universidad Técnica del Norte, para en un futuro con la colaboración de la dirección de desarrollo informático y tecnológico UTN sea replicado en los segmentos restantes con el objetivo de liberar procesamiento de los equipos del Data Center.

El usuario debe poseer conocimientos básicos de redes de computadores e informática para poder administrar y gestionar el servidor.

2.5.Suposiciones y Dependencias

El servidor debe disponer de al menos al menos de una tarjeta de red para implementar dicho equipo en el segmento de red.

El sistema operativo debe ser de licencia libre.

La plataforma de desarrollo debe soportar herramientas de software de Firewall-Proxy y ser compatible con herramientas de gestión y generación de reportes de los sitios visitados en la web.

El Sistema operativo debe soportar configuraciones de red y protocolos sobre los cuales se fundamenta las redes de computadoras.

2.6.Requisitos Futuros

En el futuro se puede Realizar una agregación de enlace en la tarjeta de red para de esa manera garantizar que todo el tráfico generado no sature el enlace del servidor.

3. Requisitos Específicos

3.1.Interfaces Externas

Los usuarios pueden acceder al servidor mediante el uso de una PC mediante un intérprete de comandos previamente configurado como SSH o por medio de una herramienta de configuración web denominada webmin. Con él se pueden configurar aspectos internos del sistema operativo entre ellos el servidor Proxy.

3.2.Funciones

Función de configuración de Proxy, el cual puede actuar como filtro del contenido servido, aplicando políticas de censura de acuerdo a criterios administrativos.

Función de restricción de acceso a sitios de internet, permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es

verdaderamente simple y consiste en denegar el acceso a nombres de dominio o direcciones de Internet que contengan patrones en común. *Función de asignación de memoria caché,* ayuda a ahorrar y aprovechar mejor los recursos. *Función de restricción de acceso por horarios,* denegar el acceso a ciertos en ciertos horarios permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso en horarios y días de la semana. *Función de herramienta de reportes,* permite ver con detalle la actividad de todos los equipos y/o usuarios dentro de la red de área local, registrada en la bitácora del proxy.
3.3.Requisitos de rendimiento
El servidor debe estar en la capacidad de receptar peticiones de todos los usuarios del segmento de red que va a servir.
3.4.Restricciones de diseño
El servidor se implementara bajo una plataforma de carácter de software libre GNU/Linux. El Servidor debe tener compatibilidad y disponibilidad de paquetes de software y actualizaciones necesarias.
3.5.Atributos del sistema
Para disponer de integridad en la manipulación del servidor se debe contar con mecanismos de seguridad de acceso al servidor como usuario y contraseña para acceder a la administración.

2.6 CentOS 6.5

2.6.1 Requisitos de sistema

Los sistemas GNU/Linux se pueden instalar en equipos con capacidades reducidas se recomienda un equipo con las siguientes características:

- Memoria RAM 2GB
- Espacio en Disco Duro 20 GB mínimo
- Espacio Recomendado 40 GB
- Procesador i386, x86-64
- Una Interfaz de Red

2.6.2 Arquitectura

Centos Soporta i386, x86-64

3. Análisis de la Situación Actual

Este apartado contiene la información de la situación actual de la red institucional de la Universidad Técnica del Norte, se presenta la topología Física y Lógica de cada una de las facultades procurando mencionar los equipos existentes en cada dependencia.

Se detalla las políticas de seguridad que están establecidas en la institución y se hace una auditoria y se documenta las reglas implementadas en el Firewall de seguridad institucional.

En la parte final se resume el plan de acción ante una eventual violación de las políticas de seguridad.

A continuación se presenta las consideraciones más relevantes que sirven como antecedentes para un análisis previo al diseño y puntualización de Políticas y reglas para el Firewall-Proxy.

3.1 Topología física

Esta topología detalla la disposición física donde se encuentran los equipos de red existentes como se muestra en la Figura 38. Hace mención elementos de hardware conectados entre sí.

3.2 Topología lógica

La topología lógica indica cómo se comunican los equipos dentro de la red universitaria, Figura 39. Indica la forma como los datos son transportados por las líneas de comunicación. La distribución de VLAN´s de la Universidad Técnica del Norte se muestra en la Tabla 4.

3.3 Topología física y equipos existentes

La Universidad técnica del norte cuenta con un cuarto de telecomunicaciones ubicado en la planta central, desde allí se interconectan las diferentes facultades por medio de enlaces directos de fibra óptica.

Es necesario mencionar que la universidad cuenta con instalaciones académicas alejadas de la casona universitaria: granja experimental, colegio universitario, antiguo hospital San Vicente de Paúl, estas se comunica por medio de enlaces de radio, para de esta manera acceder a los servicios disponibles en la red universitaria

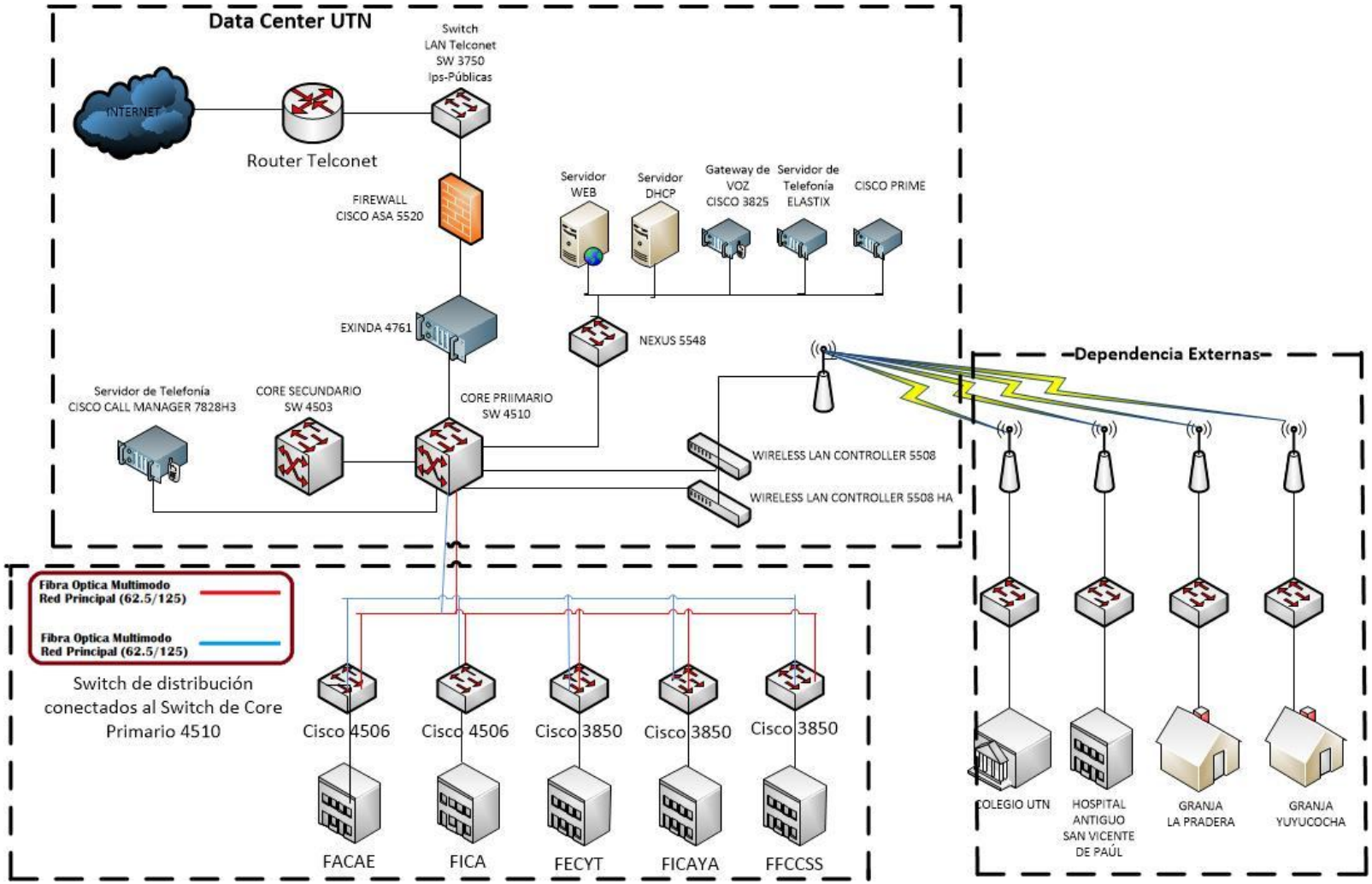


Figura 38. Diagrama Físico UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

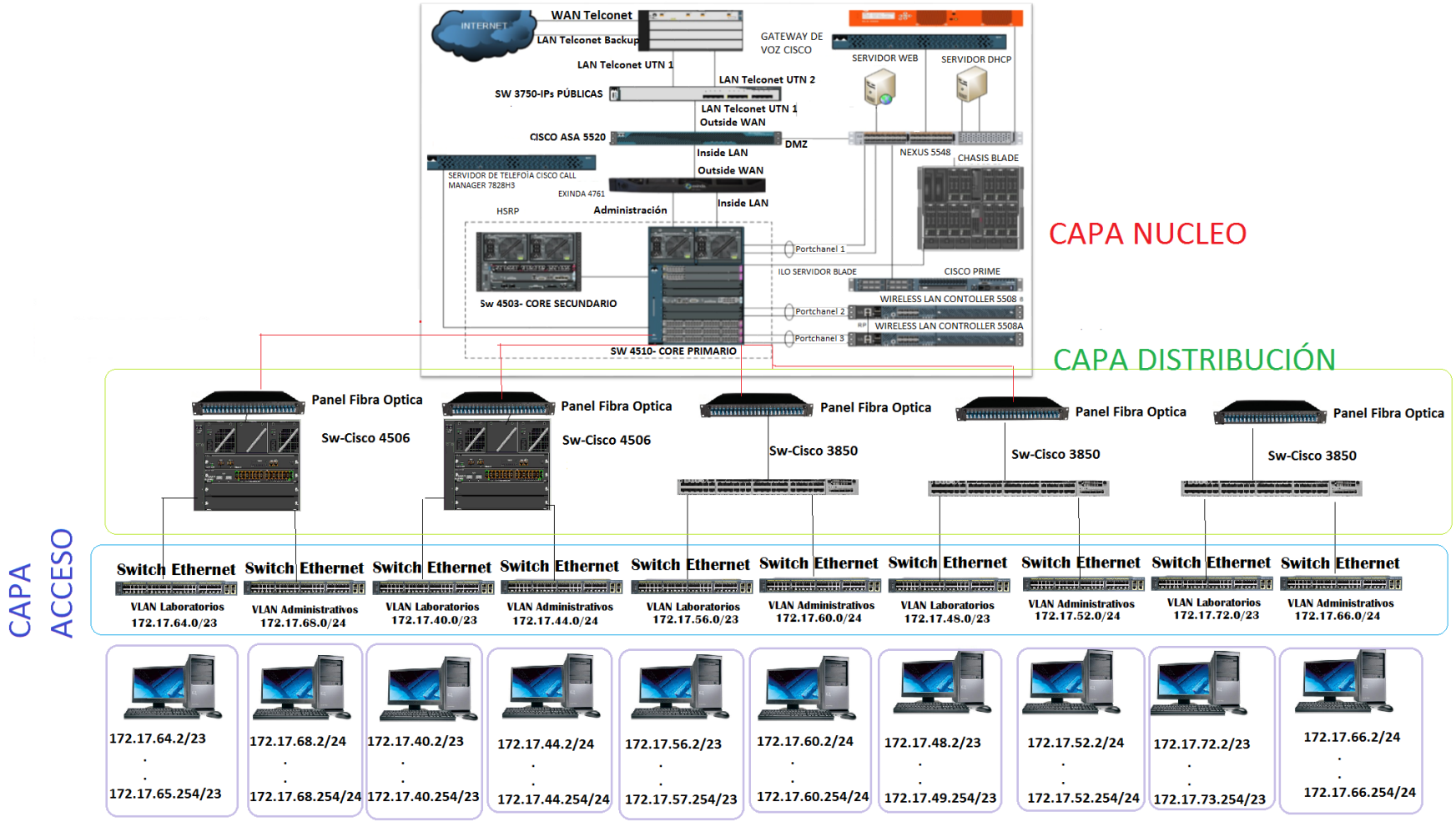


Figura 39. Topología Lógica UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

Tabla 4: Distribución de VLANs UTN

Nº	DESCRIPCIÓN	VLAN	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY
1	EQUIPOS-ACTIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
2	DMZ	X	10.24.X.X	255.255.255.0	10.24.X.X
3	NAT-INTERNO-DMZ	X	172.16.X.X	255.255.255.0	172.16.X.X
4	EQUIPOS-ACTIVOS-WIRELESS	X	172.16.X.X	255.255.255.0	172.16.X.X
5	CCTV	X	172.16.X.X	255.255.255.0	172.16.X.X
6	RELOJES-BIOMÉTRICOS	X	172.16.X.X	255.255.255.0	172.16.X.X
7	TELEFONÍA-IP-ELASTIX	X	172.16.X.X	255.255.254.0	172.16.X.X
8	TELEFONÍA-IP-CISCO	X	172.16.X.X	255.255.254.0	172.16.X.X
9	AUTORIDADES	X	172.16.X.X	255.255.255.0	172.16.X.X
10	DDTI	X	172.16.X.X	255.255.255.0	172.16.X.X
11	FINANCIERO	X	172.16.X.X	255.255.255.0	172.16.X.X
12	COMUNICACIÓN-ORGANIZACIONAL	X	172.16.X.X	255.255.255.0	172.16.X.X
13	ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
14	ADQUISICIONES	X	172.16.X.X	255.255.255.0	172.16.X.X
15	U-EMPRENDE	X	172.16.X.X	255.255.255.0	172.16.X.X
16	AGUSTÍN-CUEVA	X	172.16.X.X	255.255.255.0	172.16.X.X
17	BIENESTAR-DOCENTES	X	172.16.X.X	255.255.255.0	172.16.X.X
18	BIENESTAR-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
19	PROYECTO-INDIA	X	172.16.X.X	255.255.255.0	172.16.X.X
20	NATIVA				
21	FICA-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
22	FICA-WIRELESS	X	172.17.X.X	255.255.255.0	172.17.X.X
23	FICA-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
24	FICAYA-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
25	FICAYA-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
26	FECYT-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
27	FECYT-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
28	FACAE-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
29	FACAE-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
30	FCCSS-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
31	FCCSS-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
32	POSTGRADOS-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
33	POSTGRADOS-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
34	CAI-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
35	CAI-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
36	BIBLIOTECA-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
37	BIBLIOTECA-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
38	COLEGIO-LABORATORIOS	X	172.17.X.X	255.255.254.0	172.17.X.X
39	COLEGIO-ADMINISTRATIVOS	X	172.16.X.X	255.255.255.0	172.16.X.X
40	WIRELESS-DOCENTES	X	172.18.X.X	255.255.248.0	172.18.X.X
41	WIRELESS-ADMINISTRATIVOS	X	172.19.X.X	255.255.255.0	172.19.X.X
42	EDUROAM	X	172.20.X.X	255.255.248.0	172.20.X.X
43	WIRELESS-EVENTOS1	X	172.21.X.X	255.255.248.0	172.21.X.X
44	WIRELESS-EVENTOS2	X	172.22.X.X	255.255.248.0	172.22.X.X
45	WIRELESS-ESTUDIANTES	X	172.23.1X.X	255.255.248.0	172.23.1X.X
46	COPIADORA	X	172.24.X.X	255.255.255.0	172.24.X.X
47	BANCO-PACÍFICO	X	192.168.X.X	255.255.255.0	192.168.X.X

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

3.3.1 Fica

La facultad cuenta con equipos distribuidos en diferentes dependencias del edificio. La disposición de los equipos existentes en la facultad de ingeniería en ciencias aplicadas está representadas en la Figura 40.

- El Data Center FICA se encuentra ubicado en la planta baja del edificio, como se muestra en la Figura 41.
- El Laboratorio 1 se encuentra situado en la primera planta del edificio, como se muestra en la Figura 42.
- El Laboratorio 2 se encuentra ubicado en la primera planta del edificio, como se muestra en la Figura 42.

  El Laboratorio 3 se encuentra ubicado en la primera planta del edificio, como se muestra en la Figura 42.
- El Laboratorio 4 se encuentran ubicado en la primera planta del edificio, como se muestra en la Figura 42.
- El Laboratorio 5 y laboratorio 6 está situado en la segunda planta del edificio, como se muestra en la Figura 43.
- El Laboratorio 7 situado en la cuarta planta del edificio, como se muestra en la Figura 44.
- La Sala de Investigación se encuentra ubicado en la sala de cubículos para docentes, situados en la cuarta planta del edificio, como se muestra en la Figura 44.
- La Sala de Profesores-Uso Múltiple se encuentra ubicado en la cuarta planta del edificio, como se muestra en la Figura 44.

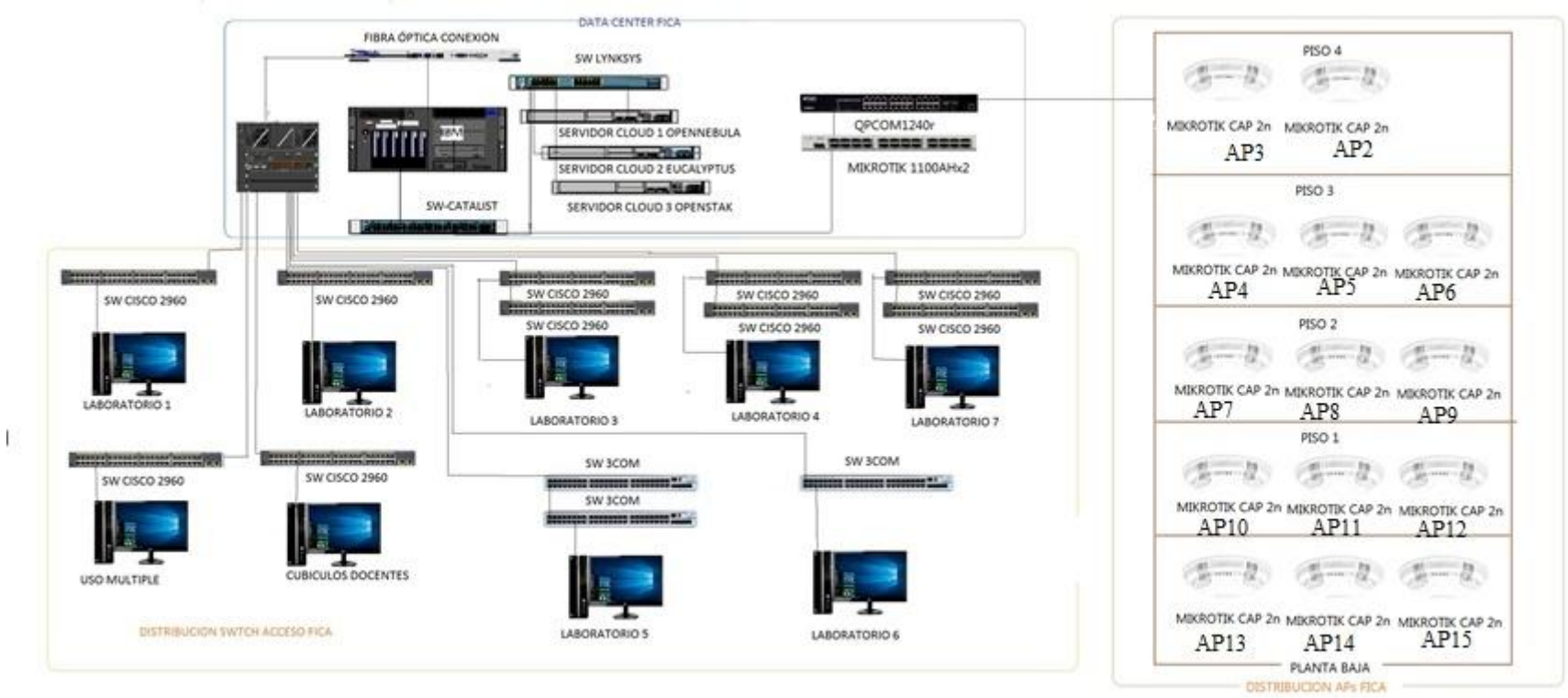


Figura 40. Topología Física FICA-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

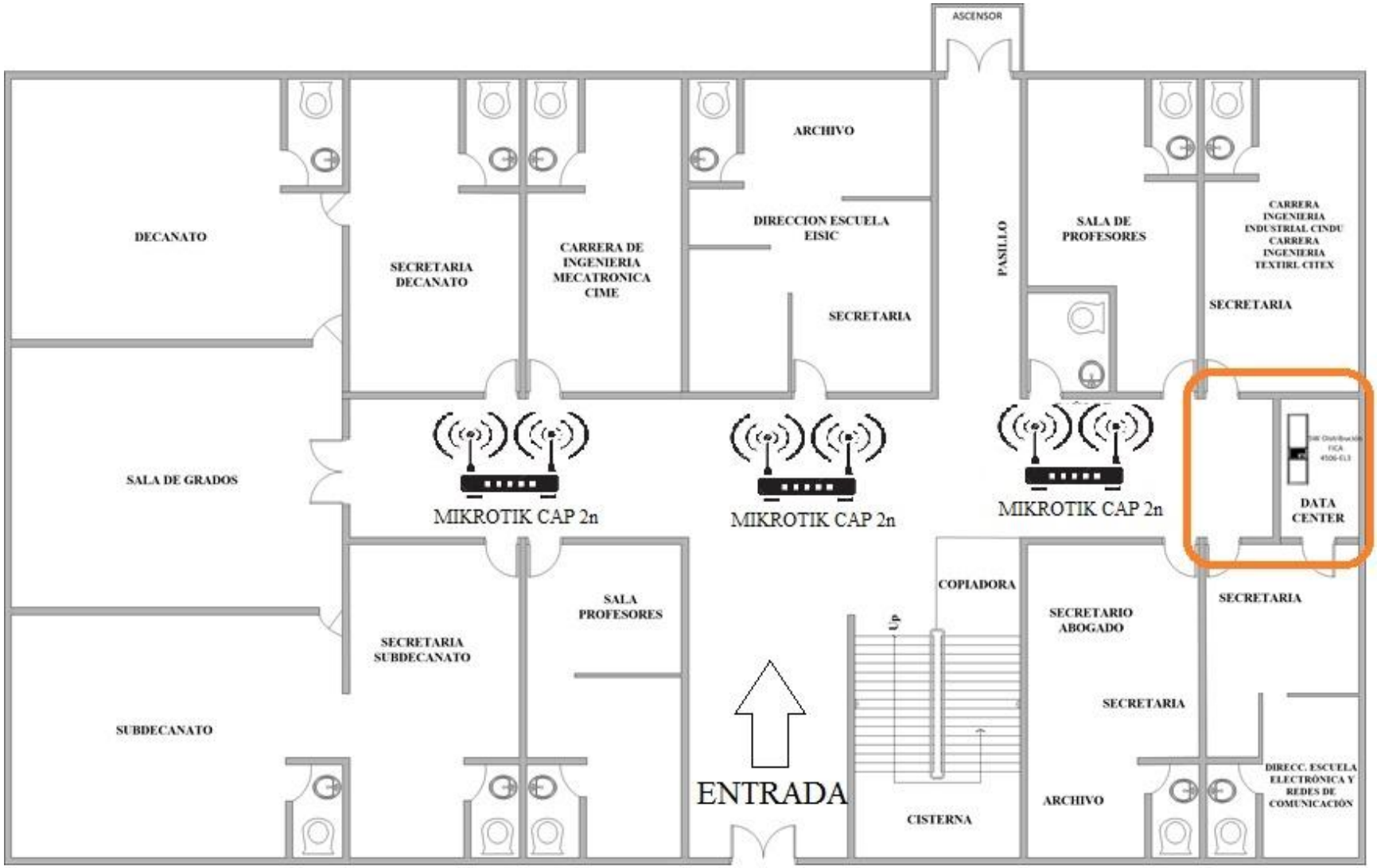


Figura 41. Planta baja FICA-UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

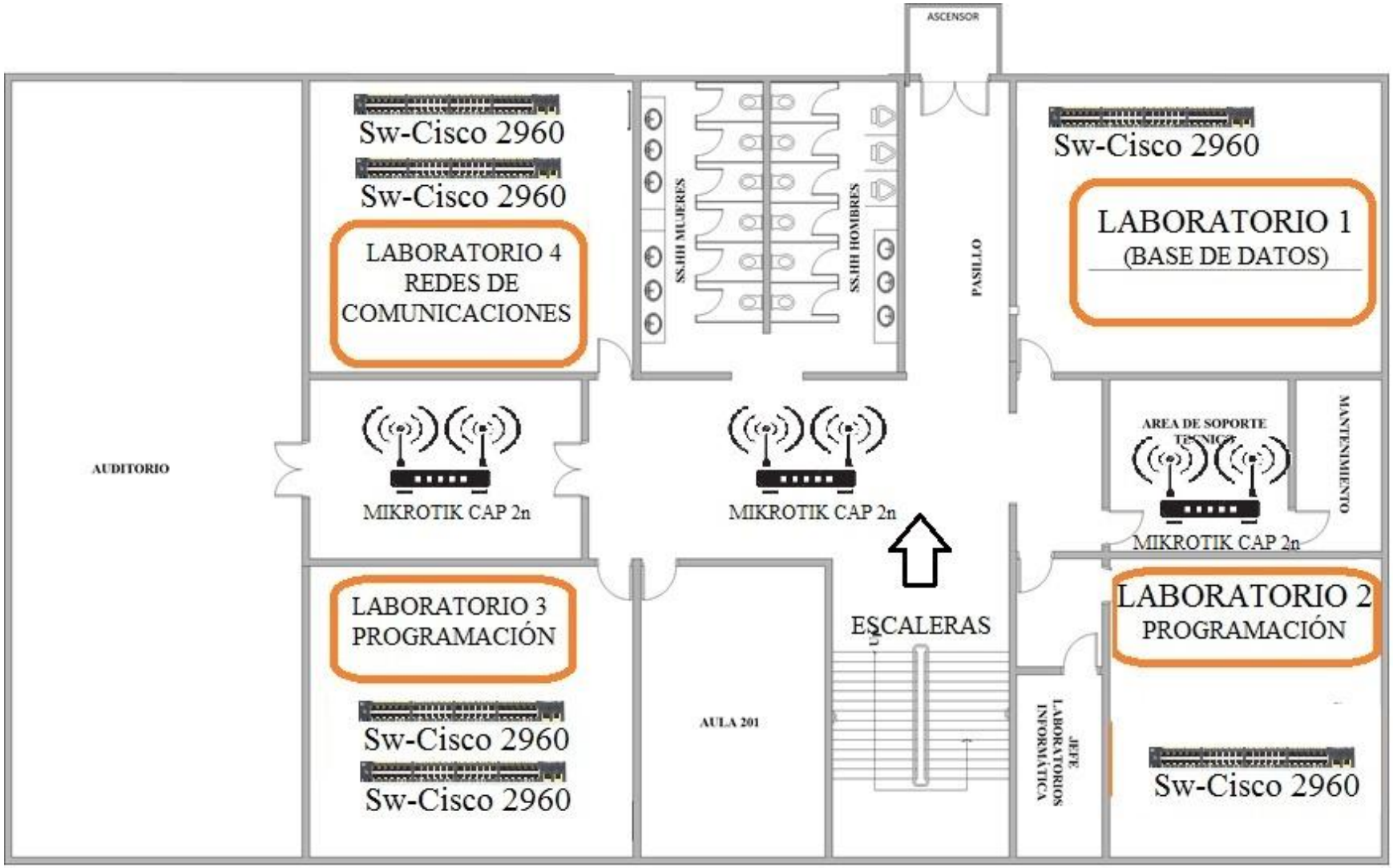


Figura 42. Primera planta FICA-UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

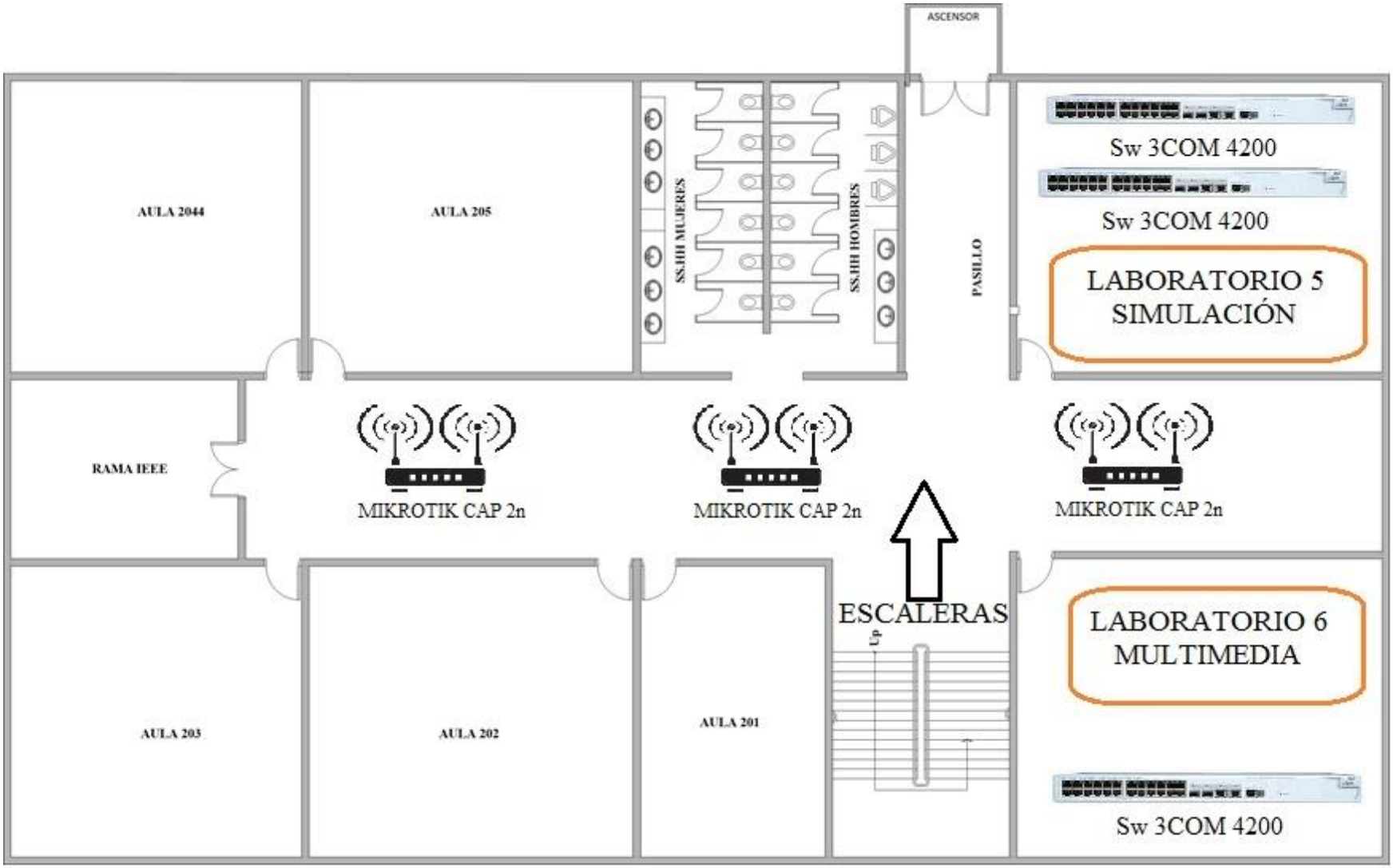


Figura 43. Segunda planta FICA-UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

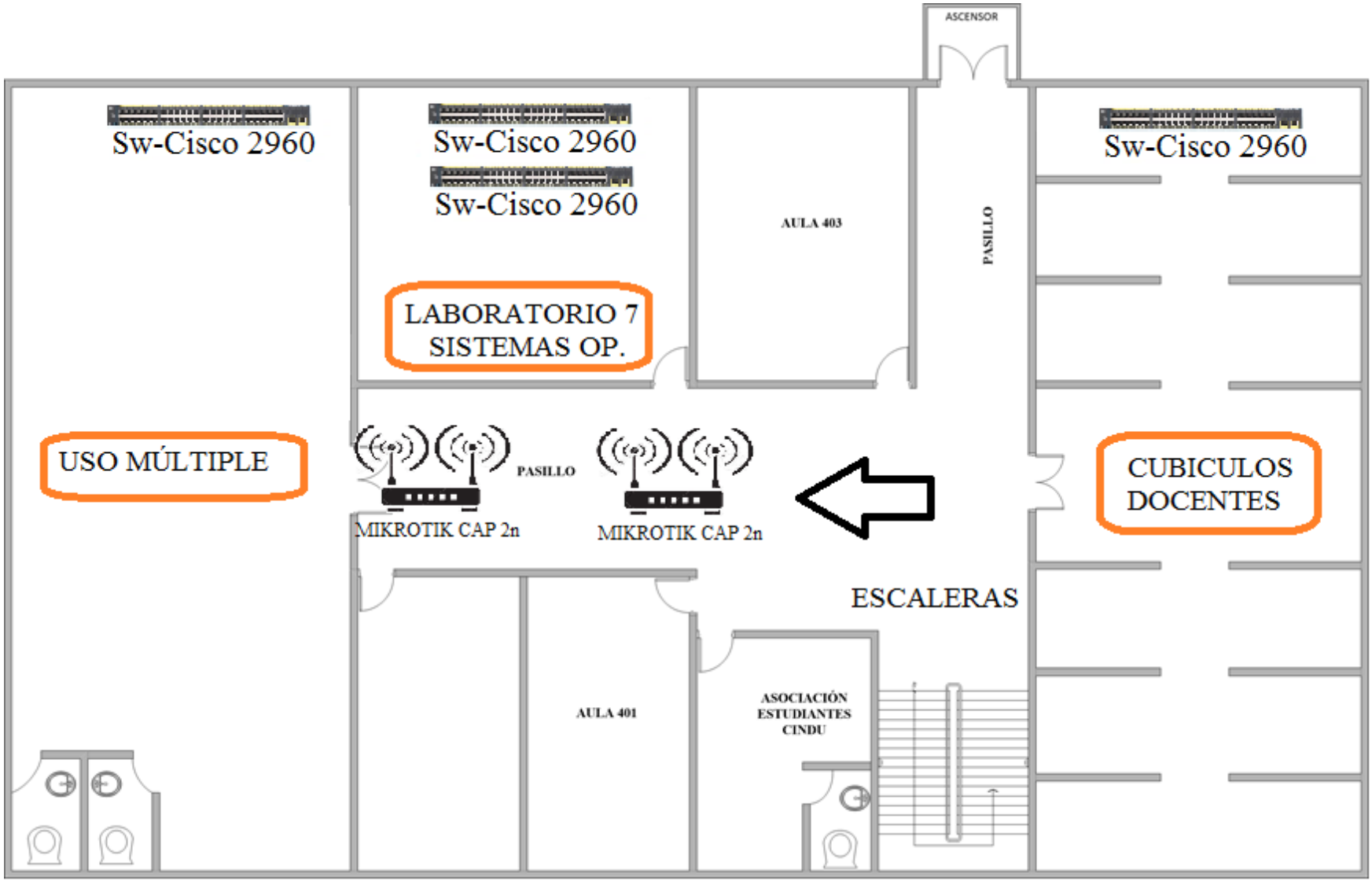


Figura 44 Cuarta planta FICA-UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

3.3.1.1 Equipos existentes

Los equipos con los que cuenta la Facultad de ingeniería en ciencias aplicadas son los siguientes:

- **Equipos en el Data Center**

En la Tabla 5 se detalla los equipos existentes en el Data Center de la FICA.

Tabla 5: Equipos de red en la FICA-Data Center

Data Center-Planta baja					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Equipo de distribución Switch L3	Catalyst 4506 -E	144	16
2	1	Switch	Catalyst 2960	48	
3	1	Switch	Lynksys	24	
4	3	Servidores cloud			
5	1	Router	Mikrotik 1100AHx2	24	
6	1	Switch	QPCOM 1240r	24	

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red primera planta Laboratorio 1.**

En la Tabla 6 se detalla los equipos de red existentes en el Laboratorio1 de la FICA.

Tabla 6: Equipos de red en la FICA-Laboratorio 1

Laboratorio1-PrimeraPlanta					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red primera planta Laboratorio 2.**

En la Tabla 7 se detalla los equipos de red existentes en el Laboratorio2 de la FICA.

Tabla 7: Equipos de red en la FICA-Laboratorio 2

Laboratorio1-PrimeraPlanta					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red primera planta Laboratorio 3.**

En la Tabla 8 se detalla los equipos de red existentes en el Laboratorio3 de la FICA.

Tabla 8: Equipos de red en la FICA-Laboratorio3

Equipos de red en la FICA-Laboratorio 3					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso Cisco	Catalyst 2960	48	-
2	1	Switch de acceso Cisco	Catalyst 2960	24	-

Fuente**:** Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red primera planta Laboratorio 4.**

En la Tabla 9 se detalla los equipos de red existentes en el Laboratorio 4 de la FICA.

Tabla 9: Equipos de red en la FICA-Laboratorio 4

Laboratorio4-PrimeraPlanta					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	2	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

Equipos de red segunda planta Laboratorio 5.

En la Tabla 10 se detalla los equipos de red existentes en el Laboratorio 5 de la FICA.

Tabla 10: Equipos de red en la FICA-Laboratorio 5

Laboratorio5-Segunda Planta					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	2	Switch de acceso 3Com	4200	24	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red segunda planta Laboratorio 6.**

En la Tabla 11 se detalla los equipos de red existentes en el Laboratorio 6 de la FICA.

Tabla 11: Equipos de red en la FICA-Laboratorio 6

Laboratorio6-Segunda Planta					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso 3Com	4200	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red cuarta planta Laboratorio 7.**

En la Tabla 12 se detalla los equipos de red existentes en el Laboratorio 7 de la FICA.

Tabla 12: Equipos de red en la FICA-Laboratorio 7

Laboratorio 7-Cuarta Planta					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	2	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red cubículos Docentes.**

En la Tabla 13 se detalla los equipos de red existentes en los cubiculos de docentes de la FICA.

Tabla 13: Equipos de red en la FICA- Cubículos Docentes

Sala de Investigación					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos de red Sala de profesores.**

En la Tabla 14 se detalla los equipos de red existentes en la sala de profesores de la FICA.

Tabla 14: Equipos de red en la FICA-Sala de profesores.

Sala de profesores					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso Cisco	Catalyst 2960	24	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

3.3.1.2 Mapeo de puertos del Switch de Acceso de los equipos de laboratorios.

Para el mapeo de puertos de los Switch de acceso se toma como ruta el puerto de Switch conectado al Patch Panel por medio de un Patch Cord, desde el Patch Panel a la Toma de Usuario o Punto de Red, y del punto de red a la estación de Trabajo Mediante un Patch Cord.

Se toma de ejemplo que la estación de trabajo está conectada al punto de red Si/1, este a su vez se conecta al punto de patch panel 1, el punto patch panel uno se conecta Switch 2960 por medio del puerto Fa0/1. Como se muestra en la Figura 45.

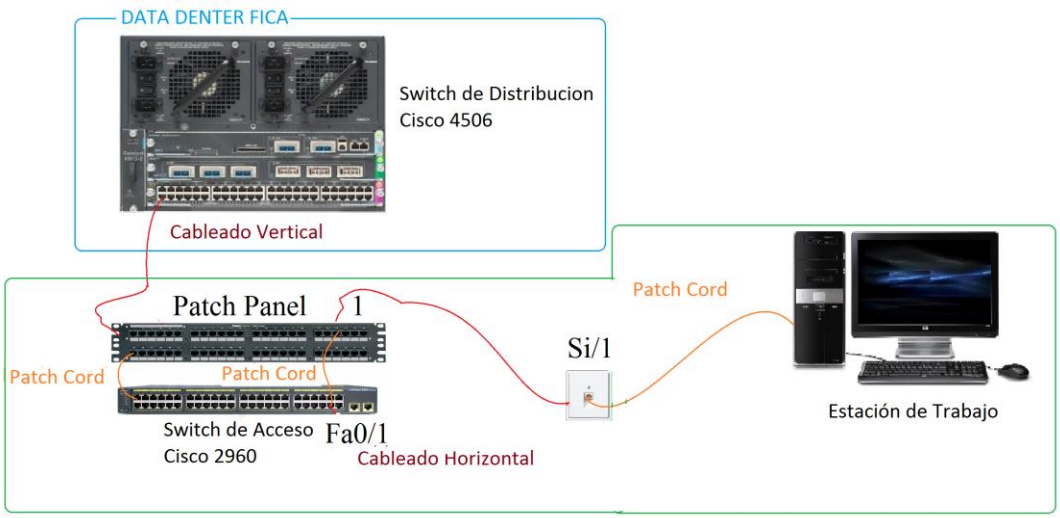


Figura 45. Ruta mapeo puerto switch de Acceso

Fuente: Elaborado por el Autor.

La facultad de ingeniería en ciencias aplicadas consta de siete laboratorios se presentan distribuidos de la siguiente manera.

- **Laboratorio 1**

Este laboratorio se encuentra ubicado en la primera planta del edificio, tiene 26 equipos conectados al switch de acceso, el switch tiene 48 interfaces FastEthernet configurados en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet uno de estos configurados en modo trunk. El detalle de este laboratorio se muestra en la tabla 15.

- **Laboratorio 2**

Se encuentra situado en el edificio en la primera planta, tiene un switch con 48 interfaces FastEthernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet uno de estos en modo trunk, este laboratorio posee 20 equipos conectados al switch. El detalle de este laboratorio se muestra en la tabla 16.

- **Laboratorio 3**

El laboratorio 3 tiene dos switch de acceso, un switch tiene 48 interfaces FastEthernet configurados en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet en modo trunk, este switch tiene interconectado 30 equipos; el segundo switch tiene 24 interfaces FastEthernet configurados en modo acceso a la VLAN financiero y dos interfaces Gigabit Ethernet configurados en modo trunk. Este laboratorio se encuentra en la primera planta. El detalle de este laboratorio se muestra en la Tabla 17.

- **Laboratorio 4**

Este laboratorio cuenta con 20 equipos conectados a un switch de acceso de 48 interfaces FastEthernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet configurados en modo trunk, además un switch de acceso adicional de 48 interfaces FastEthernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet uno de estos configurado en modo trunk; este laboratorio se encuentra ubicado en la primera planta del edificio. El detalle de este laboratorio se muestra en la tabla 18.

- **Laboratorio 5**

Este laboratorio cuenta con 30 equipos conectados a un switch de acceso de 24 interfaces FastEthernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet configurados en modo trunk, además un switch de acceso adicional de 24 interfaces FastEthernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet uno de estos configurado en modo trunk; este laboratorio se encuentra ubicado en la segunda planta del edificio. El detalle de este laboratorio se muestra en la tabla 19.

- **Laboratorio 6**

Se encuentra situado en el edificio en la seguunda planta, tiene un switch con 48 interfaces FastEthernet en modo acceso a la VLAN de laboratorios y dos interfaces Gigabit Ethernet uno de estos en modo trunk, este laboratorio posee 26 equipos conectados al switch. El detalle de este laboratorio se muestra en la tabla 20.

- **Laboratorio 7**

El laboratorio 7 se encuentra ubicado en la cuarta planta del edificio, cuenta con dos switch de acceso con 48 interfaces FastEthernet configurados en modo acceso a la VLAN de laboratorios. Este laboratorio tiene 24 equipos. El detalle de este laboratorio se muestra en la tabla 21.

- **Wireless**

  Los Access point´s de la red inalámbrica se encuentran ubicados en cada piso del edificio, estos están conectados a un switch QPCOM el detalle de los puertos utilizados se encuentra en la Tabla 22.

Tabla 15: Mapeo de puertos Laboratorio1-Fica

Switch Catalyst 2960 Laboratorio 2							Equipo conectado	
Modo VLAN	VLAN	Descripcion	PUERTO	Estado	PatchPanel	Punto de Red/N°	Nombre	IP
access	X	Laboratorios	Fa0/1	Disponible	1	Si/1		
access	X	Laboratorios	Fa0/2	Activado	2	Si/2	PCFICA-312	172.17.X.X
access	X	Laboratorios	Fa0/3	Activado	3	Si/3	PCFICA-311	172.17.X.X
access	X	Laboratorios	Fa0/4	Disponible	4	Si/4		
access	X	Laboratorios	Fa0/5	Activado	5	Si/5	PCFICA-313	172.17.X.X
access	X	Laboratorios	Fa0/6	Activado	6	Si/6	PCFICA-319	172.17.X.X
access	X	Laboratorios	Fa0/7	Activado	7	Si/7	PCFICA-318	172.17.X.X
access	X	Laboratorios	Fa0/8	Activado	8	Si/8	PCFICA-317	172.17.X.X
access	X	Laboratorios	Fa0/9	Disponible	9	Si/9		
access	X	Laboratorios	Fa0/10	Disponible	10	Si/10		
access	X	Laboratorios	Fa0/11	Activado	11	Si/11	PCFICA-325	172.17.X.X
access	X	Laboratorios	Fa0/12	Activado	12	Si/12	PCFICA-324	172.17.X.X
access	X	Laboratorios	Fa0/13	Disponible	13	Si/13		
access	X	Laboratorios	Fa0/14	Activado	14	Si/14	PCFICA-331	172.17.X.X
access	X	Laboratorios	Fa0/15	Activado	15	Si/15	PCFICA-330	172.17.X.X
access	X	Laboratorios	Fa0/16	Disponible	16	Si/16		
access	X	Laboratorios	Fa0/17	Activado	17	Si/17	PCFICA-329	172.17.X.X
access	X	Laboratorios	Fa0/18	Activado	18	Si/18	PCFICA-337	172.17.X.X
access	X	Laboratorios	Fa0/19	Disponible	19	Si/19		
access	X	Laboratorios	Fa0/20	Disponible	20	Si/20		
access	X	Laboratorios	Fa0/21	Activado	21	Si/21	PCFICA-336	172.17.X.X
access	X	Laboratorios	Fa0/22	Activado	22	Si/22	DESKTOP-5PP0IQ9	172.17.X.X
access	X	Laboratorios	Fa0/23	Disponible	23	Si/23		
access	X	Laboratorios	Fa0/24	Disponible	24	Si/24		
access	X	Laboratorios	Fa0/25	Disponible	25	Si/25		
access	X	Laboratorios	Fa0/26	Activado	26	Si/26	PCFICA-314	172.17.X.X
access	X	Laboratorios	Fa0/27	Activado	27	Si/27	PCFICA-315	172.17.X.X
access	X	Laboratorios	Fa0/28	Disponible	28	Si/28		
access	X	Laboratorios	Fa0/29	Disponible	29	Si/29		
access	X	Laboratorios	Fa0/30	Activado	30	Si/30	PCFICA-322	172.17.X.X
access	X	Laboratorios	Fa0/31	Activado	31	Si/31	PCFICA-320	172.17.X.X
access	X	Laboratorios	Fa0/32	Activado	32	Si/32	PCFICA-321	172.17.X.X
access	X	Laboratorios	Fa0/33	Disponible	33	Si/33		
access	X	Laboratorios	Fa0/34	Disponible	34	Si/34		
access	X	Laboratorios	Fa0/35	Disponible	35	Si/35		
access	X	Laboratorios	Fa0/36	Activado	36	Si/36	PCFICA-326	172.17.X.X
access	X	Laboratorios	Fa0/37	Activado	37	Si/37	PCFICA-328	172.17.X.X
access	X	Laboratorios	Fa0/38	Activado	38	Si/38	PCFICA-334	172.17.X.X
access	X	Laboratorios	Fa0/39	Activado	39	Si/39	PCFICA-332	172.17.X.X
access	X	Laboratorios	Fa0/40	Disponible	40	Si/40		
access	X	Laboratorios	Fa0/41	Activado	41	Si/41	PCFICA-333	172.17.X.X
access	X	Laboratorios	Fa0/42	Activado	42	Si/42	PCFICA-340	172.17.X.X
access	X	Laboratorios	Fa0/43	Activado	43	Si/43	PCFICA-338	172.17.X.X
access	X	Laboratorios	Fa0/44	Activado	44	Si/44	PCFICA-339	172.17.X.X
access	X	Laboratorios	Fa0/45	Disponible	45	Si/45		
access	X	Laboratorios	Fa0/46	Disponible	46	Si/46		
access	X	Laboratorios	Fa0/47	Disponible	47	No		
access	X	Administrativos	Fa0/48	Disponible	48	No		
trunk			Gi0/1					
			Gi0/2					

Tabla 16: Mapeo de puertos Laboratorio2-Fica

Switch Catalyst 2960 Laboratorio 2						Equipo conectado	
Modo VLAN	VLAN	Descripcion	PUERTO	Estado	PatchPanel	Nombre	IP
Access	X	Laboratorios	Fa0/1	Disponible	1		
Access	X	Laboratorios	Fa0/2	Disponible	2		
Access	X	Laboratorios	Fa0/3	Activado	3	PCFICA-184	172.17.X.X
access	X	Laboratorios	Fa0/4	Activado	4	PCFICA-183	172.17.X.X
access	X	Laboratorios	Fa0/5	Disponible	5		
access	X	Laboratorios	Fa0/6	Disponible	6		
access	X	Laboratorios	Fa0/7	Activado	7	PCFICA-190	172.17.X.X
access	X	Laboratorios	Fa0/8	Activado	8	PCFICA-188	172.17.X.X
access	X	Laboratorios	Fa0/9	Activado	9	PCFICA-189	172.17.X.X
access	X	Laboratorios	Fa0/10	Activado	10	172.17.40.64	172.17.X.X
access	X	Laboratorios	Fa0/11	Activado	11	PCFICA-196	172.17.X.X
access	X	Laboratorios	Fa0/12	Activado	12	PCFICA-195	172.17.X.X
access	X	Laboratorios	Fa0/13	Disponible	13		
access	X	Laboratorios	Fa0/14	Activado	14	PCFICA-199	172.17.X.X
access	X	Laboratorios	Fa0/15	Activado	15	PCFICA-243	172.17.X.X
access	X	Laboratorios	Fa0/16	Disponible	16		
access	X	Laboratorios	Fa0/17	Activado	17	PCFICA-262	172.17.X.X
access	X	Laboratorios	Fa0/18	Disponible	18		
access	X	Laboratorios	Fa0/19	Disponible	19		
access	X	Laboratorios	Fa0/20	Disponible	20		
access	X	Laboratorios	Fa0/21	Disponible	21		
access	X	Laboratorios	Fa0/22	Activado	22	PCFICA-181	172.17.X.X
access	X	Laboratorios	Fa0/23	Disponible	23		
access	X	Laboratorios	Fa0/24	Disponible	24		
access	X	Laboratorios	Fa0/25	Disponible	25		
access	X	Laboratorios	Fa0/26	Disponible	26		
access	X	Laboratorios	Fa0/27	Activado	27	PCFICA-182	172.17.X.X
access	X	Laboratorios	Fa0/28	Disponible	28		
access	X	Laboratorios	Fa0/29	Disponible	29		
access	X	Laboratorios	Fa0/30	Activado	30	PCFICA-185	172.17.X.X
access	X	Laboratorios	Fa0/31	Disponible	31		
access	X	Laboratorios	Fa0/32	Disponible	32		
access	X	Laboratorios	Fa0/33	Activado	33	PCFICA-187	172.17.X.X
access	X	Laboratorios	Fa0/34	Activado	34	PCFICA-193	172.17.X.X
access	X	Laboratorios	Fa0/35	Activado	35	PCFICA-192	172.17.X.X
access	X	Laboratorios	Fa0/36	Disponible	36		
access	X	Laboratorios	Fa0/37	Activado	37	PCFICA-191	172.17.X.X
access	X	Laboratorios	Fa0/38	Disponible	38		
access	X	Laboratorios	Fa0/39	Activado	39	PCFICA-198	172.17.X.X
access	X	Laboratorios	Fa0/40	Activado	40	PCFICA-200	172.17.X.X
access	X	Laboratorios	Fa0/41	Disponible	41		
access	X	Laboratorios	Fa0/42	Disponible	42		
access	X	Laboratorios	Fa0/43	Disponible	43		
access	X	Laboratorios	Fa0/44	Disponible	44		
access	X	Laboratorios	Fa0/45	Disponible	45		
access	X	Laboratorios	Fa0/46	Disponible	46		
access	X	Laboratorios	Fa0/47	Disponible	47		
access	X	Administrativos	Fa0/48	Activado	48		
trunk			Gi0/1				
			Gi0/2				

Fuente: Elaborado por el autor.

.

Tabla 17: Mapeo de puertos Laboratorio3-Fica

		Switch Catalyst 2960 Superior Laboratorio 3					Equipo conectado	
Modo VLAN	VLAN	Descripcion	PUERTO	Punto de Red/N°	Estado	PatchPanel	Nombre	IP
access	X	Laboratorios	Fa0/1	Si/A01	Activado	A01	PCFICA-390	172.17.X.X
access	X	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	X	Laboratorios	Fa0/3	Si/A03	Activado	A03	PCFICA-388	172.17.X.X
access	X	Laboratorios	Fa0/4	Si/A04	Activado	A04	PCFICA-389	172.17.X.X
access	X	Laboratorios	Fa0/5	Si/A05	Disponible	A05	-	-
access	X	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-382	172.17.X.X
access	X	Laboratorios	Fa0/7	Si/A07	Activado	A07	PCFICA-383	172.17.X.X
access	X	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-384	172.17.X.X
access	X	Laboratorios	Fa0/9	Si/A09	Activado	A09	PCFICA-378	172.17.X.X
access	X	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-376	172.17.X.X
access	X	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-377	172.17.X.X
access	X	Laboratorios	Fa0/12	Si/A12	Activado	A12	PCFICA-372	172.17.X.X
access	X	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-371	172.17.X.X
access	X	Laboratorios	Fa0/14	Si/A14	Disponible	A14	-	-
access	X	Laboratorios	Fa0/15	Si/A15	Disponible	A15	-	-
access	X	Laboratorios	Fa0/16	Si/A16	Activado	A16	PCFICA-370	172.17.X.X
access	X	Laboratorios	Fa0/17	Si/A17	Disponible	A17	-	-
access	X	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-366	172.17.X.X
access	X	Laboratorios	Fa0/19	Si/A19	Activado	A19	PCFICA-364	172.17.X.X
access	X	Laboratorios	Fa0/20	Si/A20	Activado	A20	PCFICA-365	172.17.X.X
access	X	Laboratorios	Fa0/21	Si/A21	Disponible	A21	-	-
access	X	Laboratorios	Fa0/22	Si/A22	Activado	A22	PCFICA-362	172.17.X.X
access	X	Laboratorios	Fa0/23	Si/A23	Activado	A23	PCFICA-361	172.17.X.X
access	X	Laboratorios	Fa0/24	Si/A24	Activado	A24	PCFICA-364	172.17.X.X
access	X	Laboratorios	Fa0/25	Si/B01	Disponible	B01	-	-
access	X	Laboratorios	Fa0/26	Si/B02	Activado	B02	PCFICA-369	172.17.X.X
access	X	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-367	172.17.X.X
access	X	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-368	172.17.X.X
access	X	Laboratorios	Fa0/29	Si/B05	Disponible	B05	-	-
access	X	Laboratorios	Fa0/30	Si/B06	Disponible	B06	-	-
access	X	Laboratorios	Fa0/31	Si/B07	Activado	B07	PCFICA-375	172.17.X.X
access	X	Laboratorios	Fa0/32	Si/B08	Activado	B08	PCFICA-373	172.17.X.X
access	X	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-374	172.17.X.X
access	X	Laboratorios	Fa0/34	Si/B10	Activado	B10	PCFICA-379	172.17.X.X
access	X	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-381	172.17.X.X
access	X	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-380	172.17.X.X
access	X	Laboratorios	Fa0/37	Si/B13	Disponible	B13	-	-
access	X	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-386	172.17.X.X
access	X	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-387	172.17.X.X
access	X	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-385	172.17.X.X
access	X	Laboratorios	Fa0/41	Si/B17	Disponible	B17	-	-
access	X	Laboratorios	Fa0/42	No	Disponible	-	-	-
access	X	Laboratorios	Fa0/43	Si/B19	Disponible	B19	-	-
access	X	Laboratorios	Fa0/44	No	Disponible	-	-	-
access	X	Laboratorios	Fa0/45	No	Disponible	-	-	-
access	X	Laboratorios	Fa0/46	No	Disponible	-	-	-
access	X	Laboratorios	Fa0/47	No	Disponible	-	-	-
access	X	Administrativos	Fa0/48	No	Disponible	-	-	-
trunk			Gi0/1					
			Gi0/2					

Fuente: Elaborado por el autor.

.

Tabla 18: Mapeo de puertos Laboratorio4-Fica

Switch Catalyst 2960 Superior Laboratorio 4							Equipo conectado	
Modo VLAN	VLAN	Descripcion	PUERTO	Punto de Red/N°	Estado	PatchPanel	Nombre	IP
access	X	Laboratorios	Fa0/1	Si/A01	Disponible	A01	-	-
access	X	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	X	Laboratorios	Fa0/3	Si/A03	Disponible	A03	-	-
access	X	Laboratorios	Fa0/4	Si/A04	Disponible	A04	-	-
access	X	Laboratorios	Fa0/5	Si/A05	Activado	A05	PCFICA-350	172.17.X.X
access	X	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-352	172.17.X.X
access	X	Laboratorios	Fa0/7	Si/A07	Disponible	A07	-	-
access	X	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-351	172.17.X.X
access	X	Laboratorios	Fa0/9	Si/A09	Disponible	A09	-	-
access	X	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-357	172.17.X.X
access	X	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-356	172.17.X.X
access	X	Laboratorios	Fa0/12	Si/A12	Disponible	A12		
access	X	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-342	172.17.X.X
access	X	Laboratorios	Fa0/14	Si/A14	Activado	A14	PCFICA-181	172.17.X.X
access	X	Laboratorios	Fa0/15	Si/A15	Activado	A15	PCFICA-341	172.17.X.X
access	X	Laboratorios	Fa0/16	Si/A16	Disponible	A16		
access	X	Laboratorios	Fa0/17	Si/A17	Activado	A17	PCFICA-347	172.17.X.X
access	X	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-346	172.17.4X
access	X	Laboratorios	Fa0/19	Si/A19	Disponible	A19		
access	X	Laboratorios	Fa0/20	Si/A20	Disponible	A20		
access	X	Laboratorios	Fa0/21	Si/A21	Disponible	A21		
access	X	Laboratorios	Fa0/22	No	Disponible	-		
access	X	Laboratorios	Fa0/23	Si/A23	Disponible	A23		
access	X	Laboratorios	Fa0/24	Si/A24	Disponible	A24		
access	X	Laboratorios	Fa0/25	Si/B01	Disponible	B01		
access	X	Laboratorios	Fa0/26	Si/B02	Disponible	B02		
access	X	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-344	172.17.X.X
access	X	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-343	172.17.X.X
access	X	Laboratorios	Fa0/29	Si/B05	Activado	B05	PCFICA-345	172.17.X.X
access	X	Laboratorios	Fa0/30	Si/B06	Activado	B06	PCFICA-348	172.17.X.X
access	X	Laboratorios	Fa0/31	Si/B07	Disponible	B07		
access	X	Laboratorios	Fa0/32	Si/B08	Disponible	B08		
access	X	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-349	172.17.X.X
access	X	Laboratorios	Fa0/34	Si/B10	Disponible	B10		
access	X	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-353	172.17.X.X
access	X	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-355	172.17.X.X
access	X	Laboratorios	Fa0/37	Si/B13	Disponible	B13		
access	X	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-354	172.17.X.X
access	X	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-360	172.17.X.X
access	X	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-198	172.17.X.X
access	X	Laboratorios	Fa0/41	Si/B17	Disponible	B17		
access	X	Laboratorios	Fa0/42	Si/B18	Disponible	B18		
access	X	Laboratorios	Fa0/43	Si/B19	Disponible	B19		
access	X	Laboratorios	Fa0/44	No	Disponible	-		
access	X	Laboratorios	Fa0/45	No	Disponible	-		
access	X	Laboratorios	Fa0/46	No	Disponible	-		
access	X	Laboratorios	Fa0/47	No	Disponible	-		
access	X	Administrativos	Fa0/48	No	Disponible	-		
trunk			Gi0/1					
			Gi0/2					

Fuente: Elaborado por el autor.

.

Tabla 19: Mapeo de puertos Laboratorio5-Fica

		Switch 3com Laboratorio 5 42000					Equipo conectado	
Modo VLAN	VLAN	Descripcion	PUERTO	Punto de Red/N°	Estado	PatchPanel	Nombre	IP
access	X	Laboratorios	Fa0/1	NO	Disponible	No	PCFICA-311	172.17.X.X
access	X	Laboratorios	Fa0/2	NO	Disponible	No	PCFICA-312	172.17.X.X
access	X	Laboratorios	Fa0/3	NO	Disponible	No	PCFICA-313	172.17.X.X
access	X	Laboratorios	Fa0/4	NO	Disponible	No	PCFICA-314	172.17.X.X
access	X	Laboratorios	Fa0/5	NO	Activado	No	PCFICA-315	172.17.X.X
access	X	Laboratorios	Fa0/6	NO	Activado	No	PCFICA-316	172.17.X.X
access	X	Laboratorios	Fa0/7	NO	Activado	No	PCFICA-317	172.17.X.X
access	X	Laboratorios	Fa0/8	NO	Activado	No	PCFICA-318	172.17.X.X
access	X	Laboratorios	Fa0/9	NO	Activado	No		
access	X	Laboratorios	Fa0/10	NO	Activado	No		
access	X	Laboratorios	Fa0/11	NO	Activado	No		
access	X	Laboratorios	Fa0/12	NO	Activado	No		
access	X	Laboratorios	Fa0/13	NO	Activado	No	PCFICA-319	172.17.X.X
access	X	Laboratorios	Fa0/14	NO	Activado	No	PCFICA-320	172.17.X.X
access	X	Laboratorios	Fa0/15	NO	Activado	No	PCFICA-321	172.17.X.X
access	X	Laboratorios	Fa0/16	NO	Activado	No	PCFICA-322	172.17.X.X
access	X	Laboratorios	Fa0/17	NO	Activado	No	PCFICA-323	172.17.X.X
access	X	Laboratorios	Fa0/18	NO	Activado	No	PCFICA-324	172.17.X.X
access	X	Laboratorios	Fa0/19	NO	Activado	No	PCFICA-325	172.17.X.X
access	X	Laboratorios	Fa0/20	NO	Activado	No	PCFICA-326	172.17.X.X
access	X	Laboratorios	Fa0/21	NO	Disponible	No		
access	X	Laboratorios	Fa0/22	NO	Disponible	No		
access	X	Laboratorios	Fa0/23	NO	Disponible	No		
access	X	Laboratorios	Fa0/24	NO	Disponible	No		
access	X	Laboratorios	Fa0/1	NO	Disponible	No		
access	X	Laboratorios	Fa0/2	NO	Activado	No	PCFICA-327	172.17.X.X
access	X	Laboratorios	Fa0/3	NO	Activado	No	PCFICA-328	172.17.X.X
access	X	Laboratorios	Fa0/4	NO	Activado	No	PCFICA-329	172.17.X.X
access	X	Laboratorios	Fa0/5	NO	Activado	No	PCFICA-330	172.17.X.X
access	X	Laboratorios	Fa0/6	NO	Activado	No	PCFICA-331	172.17.X.X
access	X	Laboratorios	Fa0/7	NO	Activado	No	PCFICA-332	172.17.X.X
access	X	Laboratorios	Fa0/8	NO	Activado	No	PCFICA-333	172.17.X.X
access	X	Laboratorios	Fa0/9	NO	Activado	No	PCFICA-334	172.17.X.X
access	X	Laboratorios	Fa0/10	NO	Activado	No	PCFICA-335	172.17.X.X
access	X	Laboratorios	Fa0/11	NO	Activado	No	PCFICA-336	172.17.X.X
access	X	Laboratorios	Fa0/12	NO	Activado	No	PCFICA-337	172.17.X.X
access	X	Laboratorios	Fa0/13	NO	Activado	No	PCFICA-338	172.17.X.X
access	X	Laboratorios	Fa0/14	NO	Activado	No	PCFICA-339	172.17.X.X
access	X	Laboratorios	Fa0/15	NO	Activado	No	PCFICA-340	172.17.X.X
access	X	Laboratorios	Fa0/16	NO	Disponible	No		
access	X	Laboratorios	Fa0/17	NO	Disponible	No		
access	X	Laboratorios	Fa0/18	NO	Disponible	No		
access	X	Laboratorios	Fa0/19	NO	Disponible	No		
access	X	Laboratorios	Fa0/20	No	Disponible	No		
access	X	Laboratorios	Fa0/21	No	Disponible	No		
access	X	Laboratorios	Fa0/22	No	Disponible	No		
access	X	Laboratorios	Fa0/23	No	Disponible	No		
access	X	Administrativos	Fa0/24	No	Disponible	No		
trunk			Gi0/1					
			Gi0/2					

Fuente: Elaborado por el autor.

.

Tabla 20: Mapeo de puertos Laboratorio6-Fica

Switch Catalyst 2960 Superior Laboratorio 4							Equipo conectado	
Modo VLAN	**VLAN**	**Descripcion**	**PUERTO**	**Punto de Red/N°**	**Estado**	**PatchPanel**	**Nombre**	**IP**
access	X	Laboratorios	Fa0/1	Si/A01	Disponible	A01	-	-
access	X	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	X	Laboratorios	Fa0/3	Si/A03	Disponible	A03	-	-
access	X	Laboratorios	Fa0/4	Si/A04	Disponible	A04	-	-
access	X	Laboratorios	Fa0/5	Si/A05	Activado	A05	PCFICA-350	172.17.X.X
access	X	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-352	172.17.X.X
access	X	Laboratorios	Fa0/7	Si/A07	Disponible	A07	-	-
access	X	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-351	172.17.X.X
access	X	Laboratorios	Fa0/9	Si/A09	Disponible	A09	-	-
access	X	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-357	172.17.X.X
access	X	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-356	172.17.X.X
access	X	Laboratorios	Fa0/12	Si/A12	Disponible	A12		
access	X	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-342	172.17.X.X
access	X	Laboratorios	Fa0/14	Si/A14	Activado	A14	PCFICA-181	172.17.X.X
access	X	Laboratorios	Fa0/15	Si/A15	Activado	A15	PCFICA-341	172.17.X.X
access	X	Laboratorios	Fa0/16	Si/A16	Disponible	A16		
access	X	Laboratorios	Fa0/17	Si/A17	Activado	A17	PCFICA-347	172.17.X.X
access	X	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-346	172.17.4X
access	X	Laboratorios	Fa0/19	Si/A19	Disponible	A19		
access	X	Laboratorios	Fa0/20	Si/A20	Disponible	A20		
access	X	Laboratorios	Fa0/21	Si/A21	Disponible	A21		
access	X	Laboratorios	Fa0/22	No	Disponible	-		
access	X	Laboratorios	Fa0/23	Si/A23	Disponible	A23		
access	X	Laboratorios	Fa0/24	Si/A24	Disponible	A24		
access	X	Laboratorios	Fa0/25	Si/B01	Disponible	B01		
access	X	Laboratorios	Fa0/26	Si/B02	Disponible	B02		
access	X	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-344	172.17.X.X
access	X	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-343	172.17.X.X
access	X	Laboratorios	Fa0/29	Si/B05	Activado	B05	PCFICA-345	172.17.X.X
access	X	Laboratorios	Fa0/30	Si/B06	Activado	B06	PCFICA-348	172.17.X.X
access	X	Laboratorios	Fa0/31	Si/B07	Disponible	B07		
access	X	Laboratorios	Fa0/32	Si/B08	Disponible	B08		
access	X	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-349	172.17.X.X
access	X	Laboratorios	Fa0/34	Si/B10	Disponible	B10		
access	X	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-353	172.17.X.X
access	X	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-355	172.17.X.X
access	X	Laboratorios	Fa0/37	Si/B13	Disponible	B13		
access	X	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-354	172.17.X.X
access	X	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-360	172.17.X.X
access	X	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-198	172.17.X.X
access	X	Laboratorios	Fa0/41	Si/B17	Disponible	B17		
access	X	Laboratorios	Fa0/42	Si/B18	Disponible	B18		
access	X	Laboratorios	Fa0/43	Si/B19	Disponible	B19		
access	X	Laboratorios	Fa0/44	No	Disponible	-		
access	X	Laboratorios	Fa0/45	No	Disponible	-		
access	X	Laboratorios	Fa0/46	No	Disponible	-		
access	X	Laboratorios	Fa0/47	No	Disponible	-		
access	X	Administrativos	Fa0/48	No	Disponible	-		
trunk			Gi0/1					
			Gi0/2					

Fuente: Elaborado por el autor.

.

Tabla 21: Mapeo de puertos Laboratorio7-Fica

Switch Catalyst 2960 Superior Laboratorio 4							Equipo conectado	
Modo VLAN	VLAN	Descripcion	PUERTO	Punto de Red/N°	Estado	PatchPanel	Nombre	IP
access	X	Laboratorios	Fa0/1	Si/A01	Disponible	A01	-	-
access	X	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	X	Laboratorios	Fa0/3	Si/A03	Disponible	A03	-	-
access	X	Laboratorios	Fa0/4	Si/A04	Disponible	A04	-	-
access	X	Laboratorios	Fa0/5	Si/A05	Activado	A05	PCFICA-350	172.17.X.X
access	X	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-352	172.17.X.X
access	X	Laboratorios	Fa0/7	Si/A07	Disponible	A07	-	-
access	X	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-351	172.17.X.X
access	X	Laboratorios	Fa0/9	Si/A09	Disponible	A09	-	-
access	X	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-357	172.17.X.X
access	X	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-356	172.17.X.X
access	X	Laboratorios	Fa0/12	Si/A12	Disponible	A12		
access	X	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-342	172.17.X.X
access	X	Laboratorios	Fa0/14	Si/A14	Activado	A14	PCFICA-181	172.17.X.X
access	X	Laboratorios	Fa0/15	Si/A15	Activado	A15	PCFICA-341	172.17.X.X
access	X	Laboratorios	Fa0/16	Si/A16	Disponible	A16		
access	X	Laboratorios	Fa0/17	Si/A17	Activado	A17	PCFICA-347	172.17.X.X
access	X	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-346	172.17.4X
access	X	Laboratorios	Fa0/19	Si/A19	Disponible	A19		
access	X	Laboratorios	Fa0/20	Si/A20	Disponible	A20		
access	X	Laboratorios	Fa0/21	Si/A21	Disponible	A21		
access	X	Laboratorios	Fa0/22	No	Disponible	-		
access	X	Laboratorios	Fa0/23	Si/A23	Disponible	A23		
access	X	Laboratorios	Fa0/24	Si/A24	Disponible	A24		
access	X	Laboratorios	Fa0/25	Si/B01	Disponible	B01		
access	X	Laboratorios	Fa0/26	Si/B02	Disponible	B02		
access	X	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-344	172.17.X.X
access	X	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-343	172.17.X.X
access	X	Laboratorios	Fa0/29	Si/B05	Activado	B05	PCFICA-345	172.17.X.X
access	X	Laboratorios	Fa0/30	Si/B06	Activado	B06	PCFICA-348	172.17.X.X
access	X	Laboratorios	Fa0/31	Si/B07	Disponible	B07		
access	X	Laboratorios	Fa0/32	Si/B08	Disponible	B08		
access	X	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-349	172.17.X.X
access	X	Laboratorios	Fa0/34	Si/B10	Disponible	B10		
access	X	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-353	172.17.X.X
access	X	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-355	172.17.X.X
access	X	Laboratorios	Fa0/37	Si/B13	Disponible	B13		
access	X	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-354	172.17.X.X
access	X	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-360	172.17.X.X
access	X	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-198	172.17.X.X
access	X	Laboratorios	Fa0/41	Si/B17	Disponible	B17		
access	X	Laboratorios	Fa0/42	Si/B18	Disponible	B18		
access	X	Laboratorios	Fa0/43	Si/B19	Disponible	B19		
access	X	Laboratorios	Fa0/44	No	Disponible	-		
access	X	Laboratorios	Fa0/45	No	Disponible	-		
access	X	Laboratorios	Fa0/46	No	Disponible	-		
access	X	Laboratorios	Fa0/47	No	Disponible	-		
access	X	Administrativos	Fa0/48	No	Disponible	-		
trunk			Gi0/1					
			Gi0/2					

Tabla 22. Mapeo Puntos de Acceso Inalámbricos

SwitchQPCOM		**Equipo conectado**	
PUERTO	Estado	Nombre/AP	IP
1	**Activo**	**AP15**	**192.168.x.x**
2	**Activo**	**AP14**	**192.168.x.x**
3	**Activo**	**AP13**	**192.168.x.x**
4	**Activo**	**AP12**	**192.168.x.x**
5	**Activo**	**AP11**	**192.168.x.x**
6	**Activo**	**AP10**	**192.168.x.x**
7	**Activo**	**AP9**	**192.168.x.x**
8	**Activo**	**AP8**	**192.168.x.x**
9	**Activo**	**AP7**	**192.168.x.x**
10	**Activo**	**AP6**	**192.168.x.x**
11	**Activo**	**AP5**	**192.168.x.x**
12	**Activo**	**AP4**	**192.168.x.x**
13	**Activo**	**AP3**	**192.168.x.x**
14	**Activo**	**AP2**	**192.168.x.x**
15	**Disponible**	**-**	**-**
16	**Disponible**	**-**	**-**
17	**Activo**	**MIKROTIK 1100**	**X.X.42.11**
18	**Disponible**	**-**	**-**
19	**Disponible**	**-**	**-**
20	**Disponible**	**-**	**-**
21	**Disponible**	**-**	**-**
22	**Disponible**	**-**	**-**
23	**Disponible**	**-**	**-**
24	**Disponible**	**-**	**-**

Fuente: Elaborado por el autor.

.

3.3.2 Ficaya

Esta facultad cuenta con switchs de acceso distribuidos en el edificio de la casona universitaria, también con dependencias fuera de la ciudadela universitaria ubicados en Yuyucocha y una granja experimental “La Pradera”, la comunicación se realiza mediante enlaces de radio. La topología física se muestra en la Figura 46.

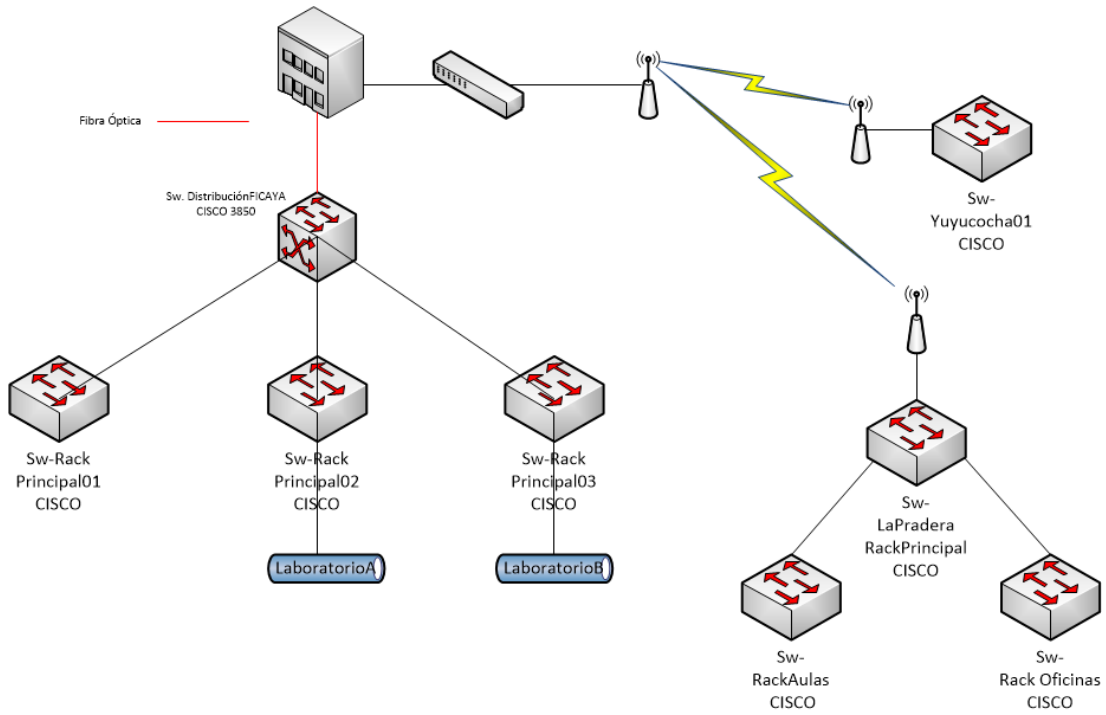


Figura 46. Topología Física FICAYA-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

El Diagrama físico del Rack Principal de la Ficaya se muestra en la Figura 47.

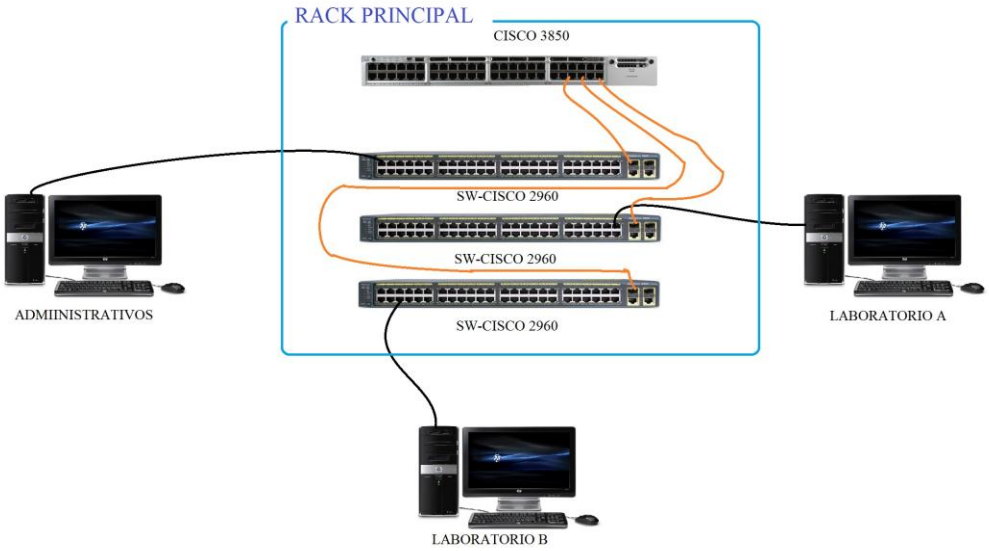


Figura 47.Diagrama Físico FICAYA-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

Todos los swtich´s se encuentran ubicados en la primera planta del edificio de la FICAYA, como se muestra en la figura 4

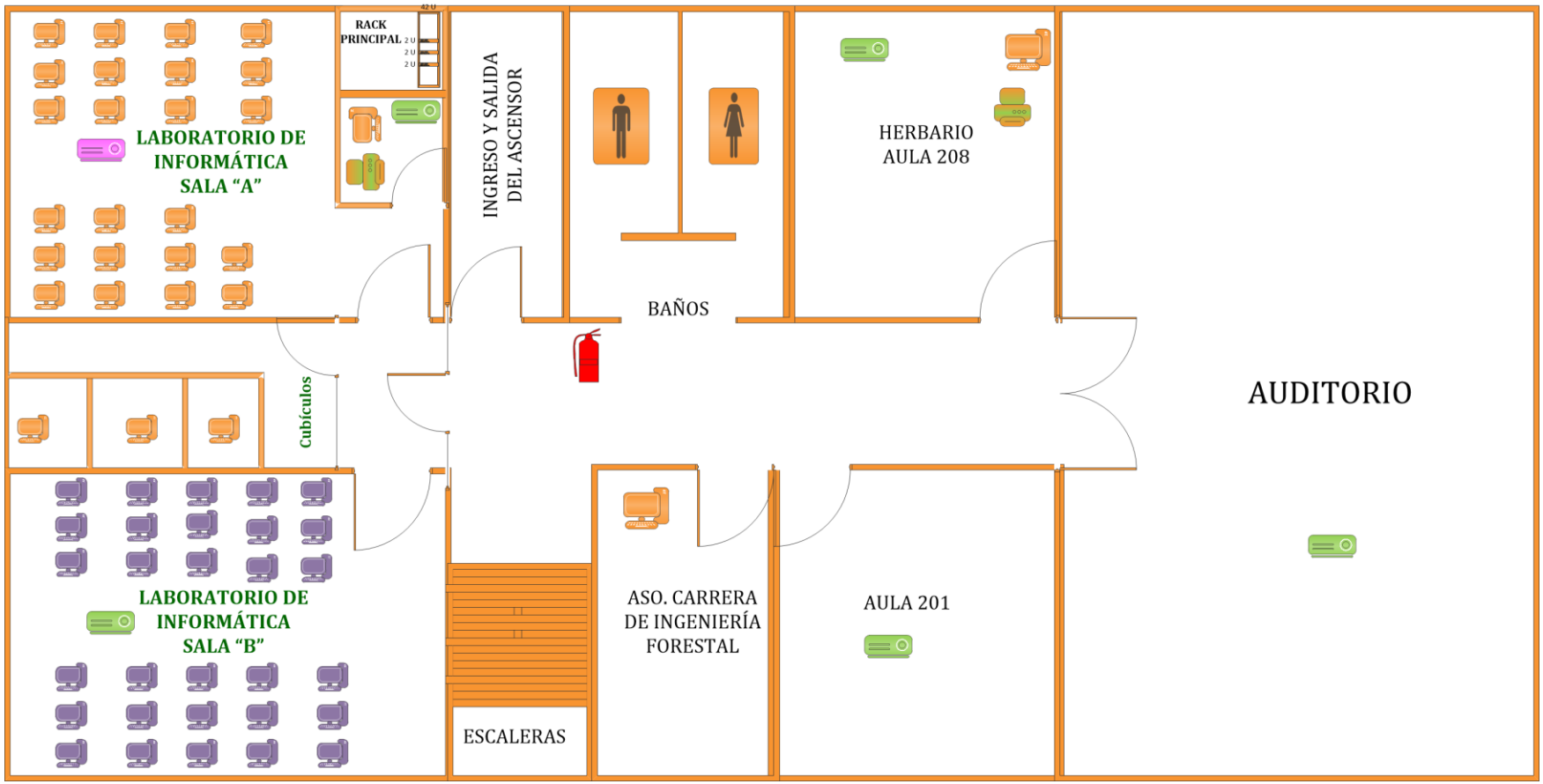


Figura 48. Segunda planta FICA-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN

.

3.3.2.1 Equipos Existentes

Los equipos con los que cuenta la Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales se muestran en la Tabla 23:

- **Rack Principal**

Tabla 23: Equipos de red en la FICAYA-Cuarto de equipos

Cuarto Equipos					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Equipo de distribución Switch Cisco	Catalyst 3850	52	4
2	3	Switch de acceso Cisco	Catalyst 2960X	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

La Facultad cuenta con dos laboratorios de computación ubicados en la primera planta del edificio.

- **Laboratorio A**

Este laboratorio cuenta con 25 equipos de cómputo disponibles, además de un área donde se encuentra ubicado el rack con los switch de acceso que abastecen a los laboratorios y a las dependencias de la Facultad.

- **Laboratorio B**

El Laboratorio B tiene a disposición 30 computadores.

3.3.3 Fecyt

La facultad cuenta con switch's de acceso distribuidos en las diferentes dependencias. La disposición física de estos equipos se muestra en la Figura 49.

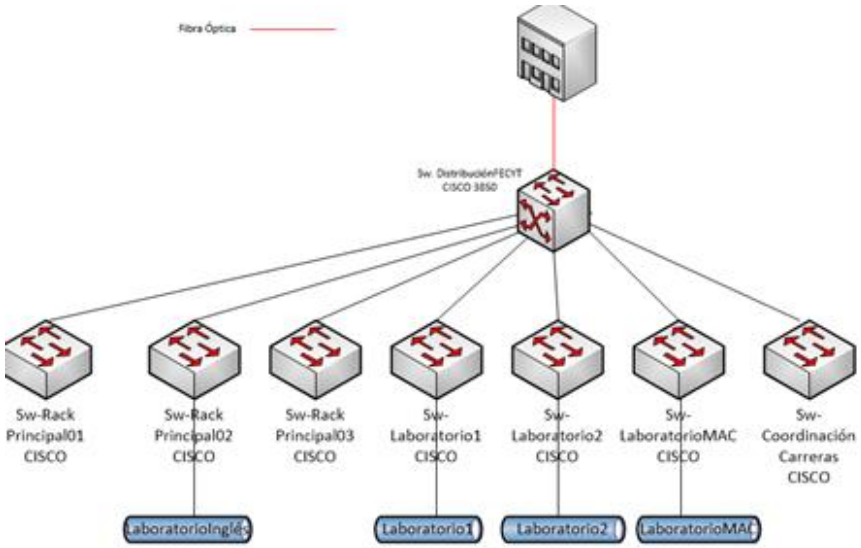


Figura 49. Topología Física FECYT-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

3.3.3.1 Equipos Existentes

El diagrama físico del rack principal de la Fecyt se muestra en la Figura 50.

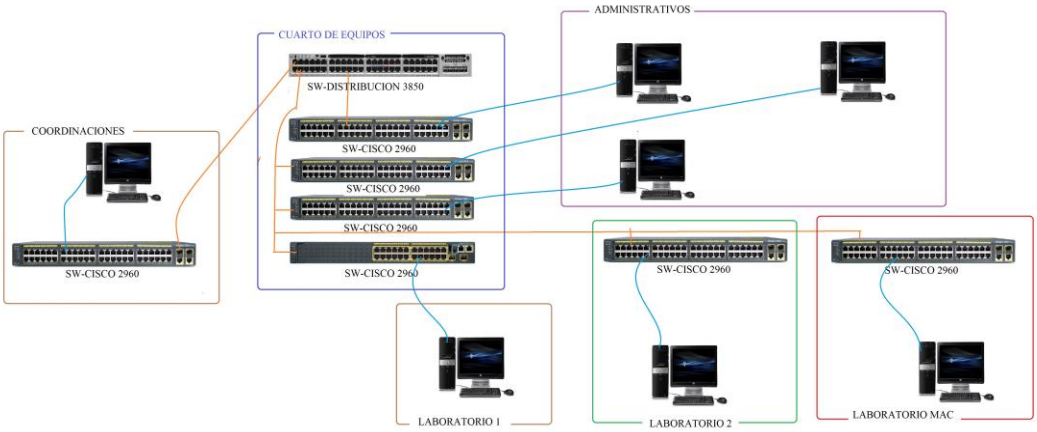


Figura 50 Diagrama Físico FECYT-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

Los equipos con los que cuenta la Facultad de Educación Ciencia y Tecnología son los siguientes.

Cuarto de Equipos

El detalle de los equipos en el cuarto de equipos se muestra en la Tabla 24.

Tabla 24: Equipos de red en la FECYT-Cuarto de equipos

Cuarto de Equipos					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de Distribucion CISCO	Catalyst 3850	52	4
2	2	Switch de acceso CISCO	Catalyst 2960	48	-
3	1	Switch de acceso CISCO	Catalyst 2960	24	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos Laboratorio 1.**

El detalle de los equipos que se encuentran ubicados en el Laboratorio 1 se muestra en la Tabla 25.

Tabla 25: Equipos de red en la FECYT-Laboratorio 1

Laboratorio1					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso CISCO	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

Equipos Laboratorio 2.

El detalle de los equipos que se encuentran ubicados en el Laboratorio 2 se muestra en la Tabla 26.

Tabla 26: Equipos de red en la FECYT-Laboratorio 2

Laboratorio2					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso CISCO	Catalyst 2960	48	-

Fuente**:** Dirección de desarrollo tecnológico e informático UTN

- **Equipos laboratorio MAC.**

El detalle de los equipos que se encuentran ubicados en el Laboratorio MAC se muestra en la Tabla 27.

Tabla 27: Equipos de red en la FECYT-Laboratorio MAC

Laboratorio Mac					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso CISCO	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos Coordinaciones.**

El detalle de los equipos que se encuentran destinados a Coordinaciones se muestra en la Tabla 28.

Tabla 28: Equipos de red en la FECYT-Coordinaciones

Coordinaciones					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso CISCO	Catalyst 2960	24	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

Esta facultad cuenta con cuatro laboratorios ubicados en la planta baja del edificio de la facultad. Ver Figura 51.

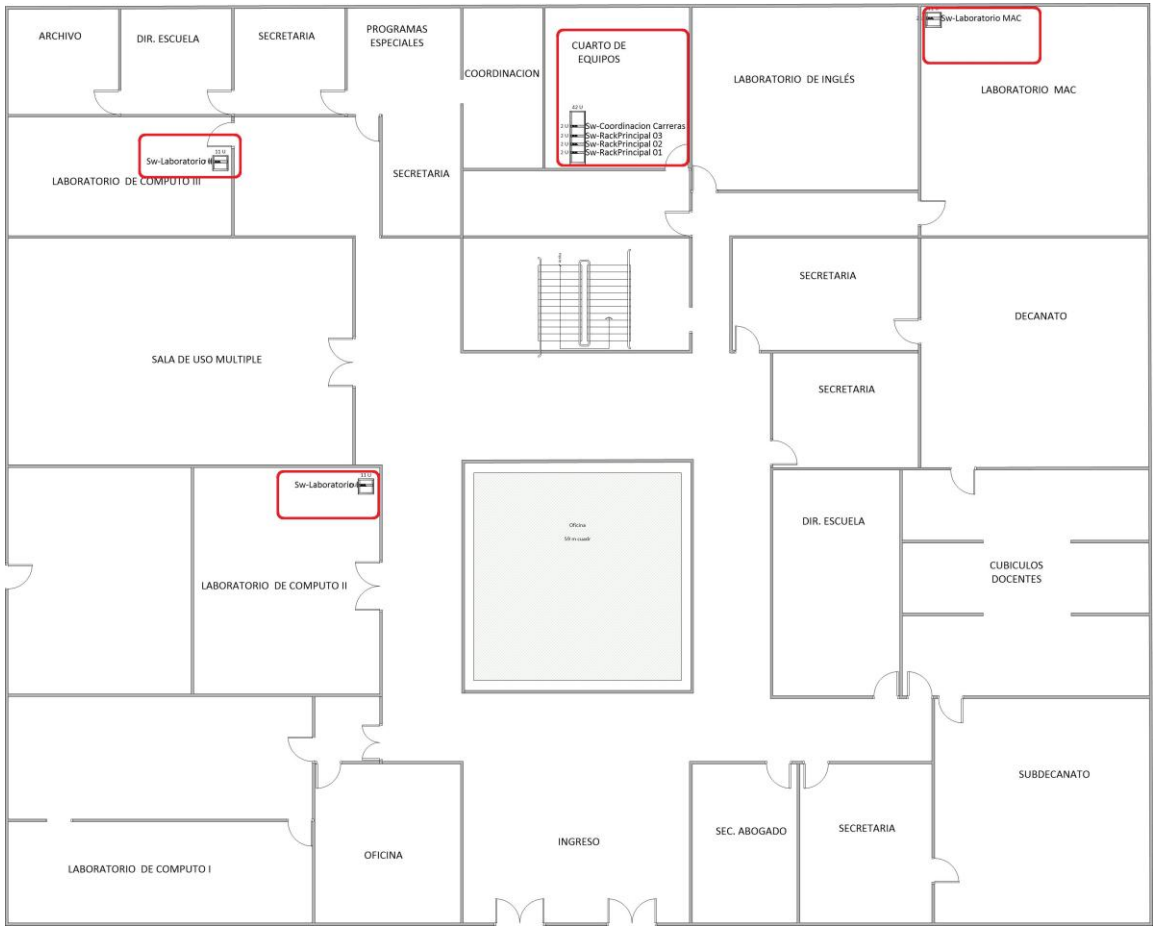


Figura 51. Planta Baja Fecyt-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

- **Laboratorio 1**

Este laboratorio cuenta con un switch de acceso que abastece a 30 computadores del laboratorio.

- **Laboratorio 2**

El laboriatorio tiene 30 equipos de computo que se conectan aun switch de acceso ubicado en el mismo.

- **Laboratorio MAC**

Este laboratorio cuenta con 38 computadores y su propio switch de acceso.

- **Laboratorio Inglés**

El labratorio de Ingles tiene 34 computadores.

3.3.4 Facae

La facultad cuenta con switchs de acceso distribuidos en las diferentes dependencias. La disposición física de estos equipos se muestra en la Figura 52.

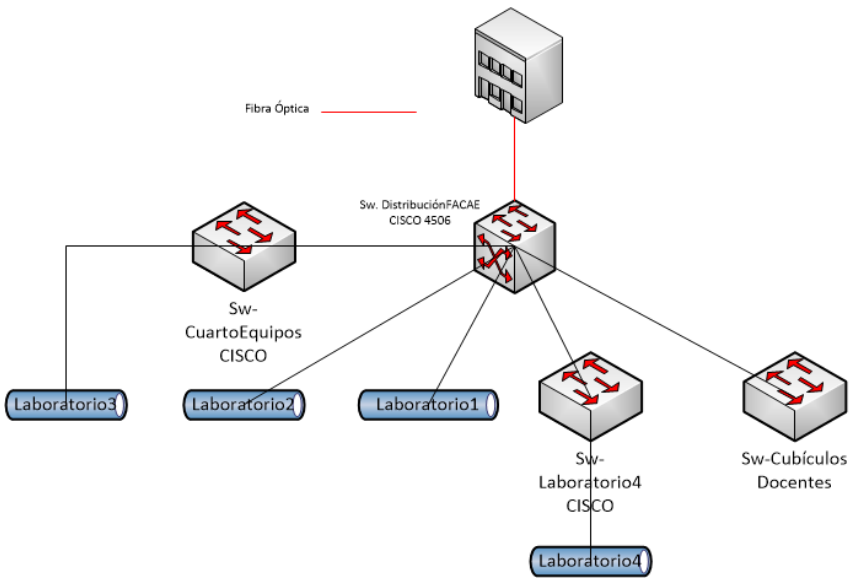


Figura 52. Topología Física FECAE-UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

El Diagrama físico del cuarto de equipos de la Facae se muestra en la Figura 53.

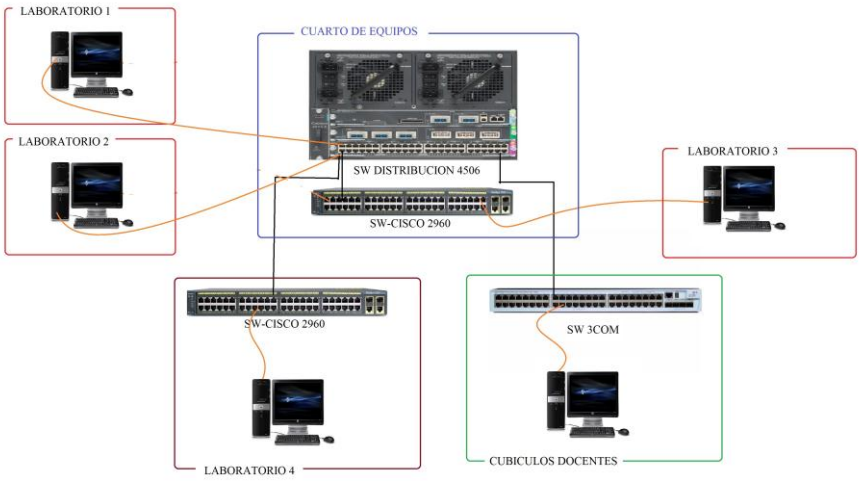


Figura 53.Diagrama Físico FACAE-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

3.3.4.1 Equipos Existentes

Los equipos con los que cuenta la Facultad Ciencias Administrativas y Económicas son los siguientes:

- **Cuarto de Equipos**

El detalle de los equipos existentes en el Cuerto de equipos se muestran en la Tabla 29.

Tabla 29: Equipos de red en la FACAE-Cuarto de Equipos

Cuarto de equipos					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de Distribución	Catalyst 4506	144	16
2	1	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos Laboratorio 4**

El detalle de los equipos que se encuentran ubicados en el Laboratorio 4 se muestra en la Tabla 30.

Tabla 30: Equipos de red en la FACAE-Laboratorio 4

Laboratorio 4					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso Cisco	Catalyst 2960	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos Cubículos**

El detalle de los equipos que se encuentran ubicados en los cubículos se muestra en la Tabla 31.

Tabla 31: Equipos de red en la FACAE-Cubículos.

Cubiculos					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso	3COM	-	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

La facultad cuenta con cuatro laboratorios ubicados en la planta baja del edificio. La disposicion de los equipos se muestra en la Figura 54.

- **Laboratorio 1**

Este laboratorio tiene a disposición 19 computadores MAC conectados al switch de acceso.

- **Laboratorio 2**

El laboratorio tiene 35 computadores.

- **Laboratorio 3**

Este laboratorio tiene 41 equipos de computo.

- **Laboratorio 4**

El laboratorio 4 tiene a disposición 33 computadores.

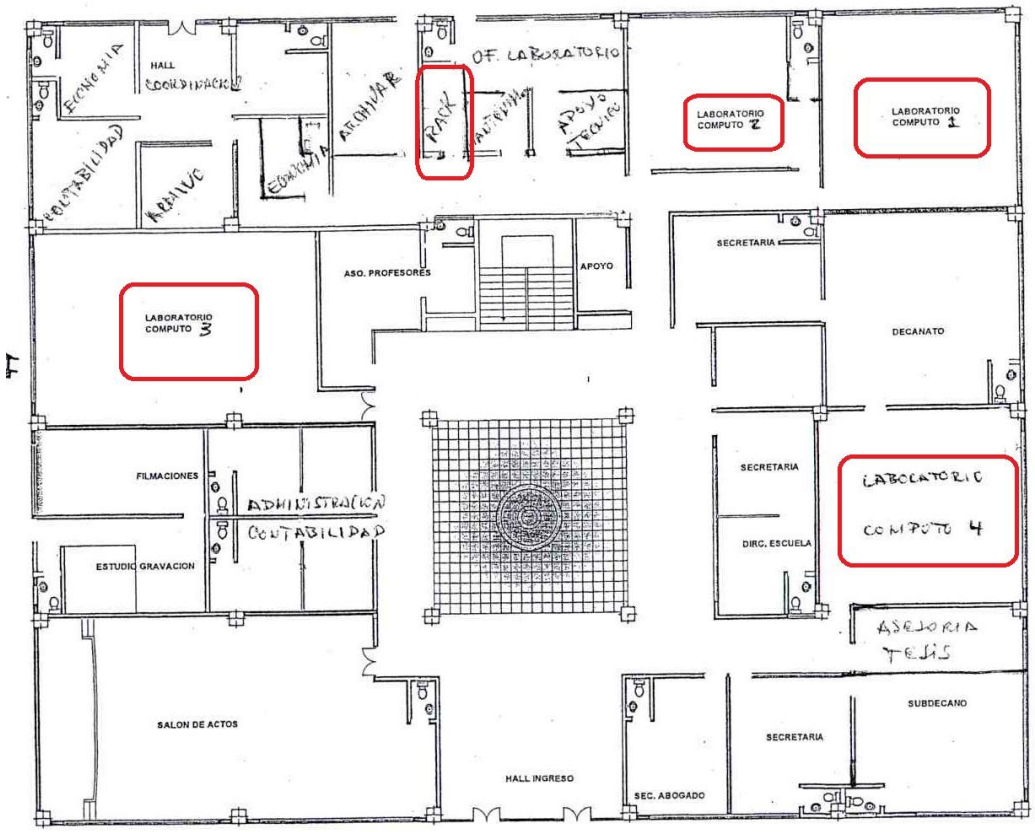


Figura 54. Planta Baja Fecyt-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

3.3.5 FFCCSS

Esta facultad cuenta con switchs de acceso distribuidos en el edificio de la ciudadela universitaria, también con dependencias fuera de la casona ubicada en el antiguo hospital San Vicente de Paul, la comunicación se realiza mediante enlace de radio. La topología física se muestra en la Figura 55.

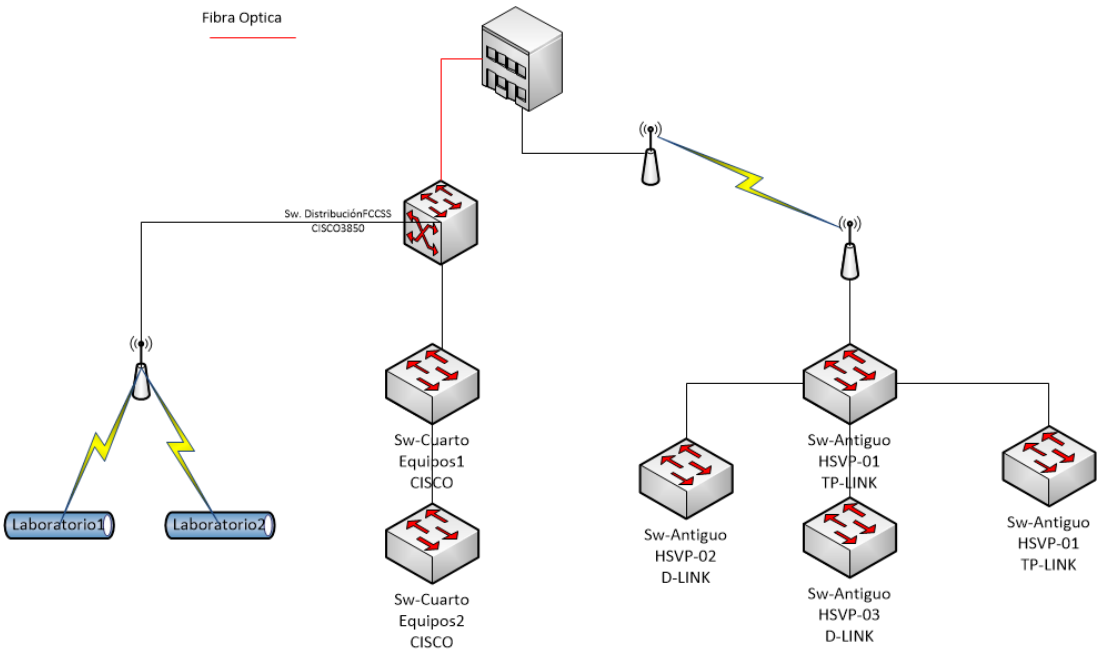


Figura 55. Topología Física FCCSS-UTN

Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

El Diagrama físico del cuarto de equipos de la FCSS se muestra en la Figura 56.

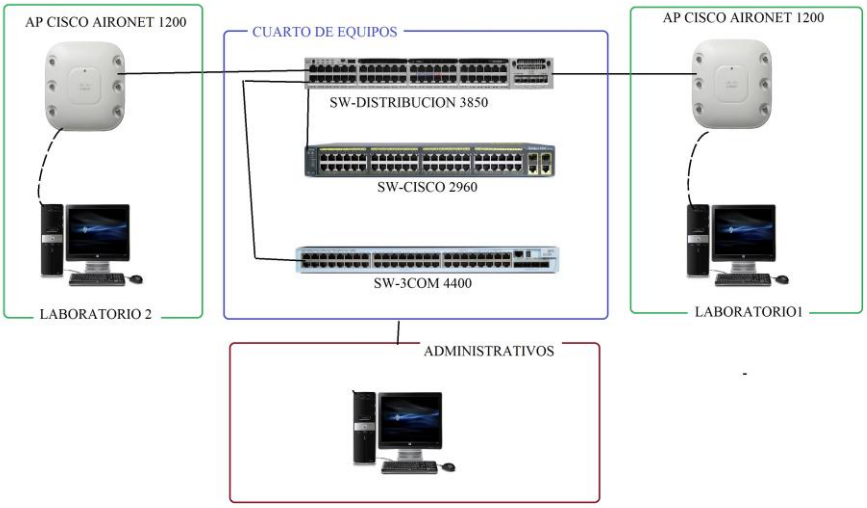


Figura 56. Diagrama Físico FFCCSS-UTN
Fuente: Dirección de Desarrollo Tecnológico e Informático-UTN.

3.3.5.1 Equipos Existentes

Los equipos con los que cuenta la Facultad de Ciencias de la Salud son los siguientes:

- **Cuarto de equipos**

Tabla 32: Equipos de red en la FCCSS-Cuarto de equipos.

Cuarto Equipos					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de Distribucion Cisco	Catalyst 3850	52	4
2	1	Switch de acceso Cisco	Catalyst 2960	48	-
3	1	Switch de acceso 3Com	SS3 SW 4400	48	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

- **Equipos antiguo hospital SVP**

Tabla 33: Equipos de red en la FCCSS-Antiguo hospital SVP.

Antiguo Hospital SVP					
N°	Cantidad	Detalle	Equipo	N° Puertos Rj45	N° Puertos FO
1	1	Switch de acceso TP-LINK	TL-SG2216WEB	16	-
2	1	Switch de acceso D-LINK	DGS-1210-28	28	-
3	1	Switch de acceso D-LINK	DGS-1210-52	52	-
4	1	Switch de acceso TP-LINK	TL-SF1024	-	-

Fuente: Dirección de desarrollo tecnológico e informático UTN

Esta facultad cuenta con dos laboratorios ubicados en la cuarta planta del edificioo el acceso a la red univesrsitaria es de forma inalámbrica. El laboratorio 1 cuenta con 27 computadores y el Laboratorio 2 tiene a disposición 30 computadores.

3.4 Políticas de seguridad en la red de la Universidad Técnica Del Norte

3.4.1 políticas basadas en el administrador de la red

Las políticas que se detallan a continuación cumplen con el escenario vigente de la red de datos institucional y la información ha sido recolectada de la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del, y corresponden a la gestión que desarrolla el administrador de Redes y Comunicaciones de la institución.

3.4.1.1 Políticas sobre el uso de los servicios de la red

- Todos los servicios que presta la universidad a su personal administrativo y estudiantil, se encuentran alojados en servidores dentro del Cuarto de Comunicaciones.
- Cada servidor debe ser administrado por el personal capacitado de la Dirección de Desarrollo Tecnológico e Informático.

- El acceso a la administración de los servidores es restringido y exclusivo de quien lo administra.
- Se debe respaldar la información una vez al mes.

3.4.1.2 Políticas de conectividad a internet

- Se permitirá el uso de internet a todos los usuarios dentro de la red de datos universitaria.
- Se bloqueará el acceso a redes sociales dentro del campus universitario.
- Se habilitará el uso de redes sociales previa autorización del señor rector de la Universidad Técnica del Norte.

3.4.2 Políticas de responsabilidades en la red de la UTN

Las responsabilidades en la red deberán estar claramente definidas y debieran realizarse en concordancia con la política de seguridad de la Universidad Técnica del Norte.

3.4.2.1 Responsabilidad del administrador de la red

- El administrador de la red tiene la responsabilidad de mantener la conectividad entre las redes de la organización.
- Debe definir y documentar claramente los niveles de autorización y privilegios de acceso de los usuarios hacia los recursos de la organización.
- Monitorear cualquier actividad relacionada con los activos de la organización
- Tener contacto apropiado con las autoridades relevantes por ejemplo, la organización puede necesitar de terceras personas como grupos de interés y profesionales en el área de seguridad.

- La información podría ser expuesta por grupos externos por lo que se podría tomar en consideración del administrador utilizar acuerdos de no-divulgación.

3.4.2.2 Responsabilidades de los usuarios de la red

- El usuario es responsable de mantener sus contraseñas en secreto.
- El usuario es responsable del uso y acceso a los servicios de la red Universitaria.
- No proporcionar datos personales por medio de correo o teléfono.
- Se prohíbe la excesiva o abusiva navegación por Internet con fines extra laborales.
- Se prohíbe la transmisión de información confidencial a personal que no labore en la Universidad Técnica del Norte.
- Los usuarios deben tener conciencia sobre las responsabilidades y problemas que comprenden la seguridad de la información.
- Los usuarios tienen la responsabilidad de reportar eventos que pongan en riesgo los activos de la organización.

3.5 Firewall cisco ASA 5520

La infraestructura de red de la Universidad Técnica Del Norte tiene un firewall de última generación cisco ASA 5520.

3.5.1 Auditoria de las reglas implementadas en el firewall

Para determinar las reglas implementadas en el firewall hay que definir el direccionamiento que utiliza, el direccionamiento utilizado se puede apreciar en la Tabla 3.

3.5.1.1 Reglas asignadas al uso de los servicios en la red

Los servidores ubicados en la DMZ de la infraestructura de red tienen un direccionamiento en el rango 10.24.X.X/24. Las reglas asignadas se describen a continuación:

- **Reglas Forward**
    - Se deniega todo trafico IP con origen en la DMZ[31] y destino a una BOTNET[32].
    - Se acepta todo tráfico (con servicios definidos por el administrador de la red) que tengan origen en la LAN interna de la universidad con destino a los servidores ubicados en la DMZ.
    - Se permite todo tráfico (con servicios definidos por el administrador de la red) que tenga origen en la DMZ hacia cualquier destino.
    - Se permite todo tráfico (con servicios definidos por el administrador de la red) que tenga origen en la red interna de la universidad con destino a internet.
    - Se deniega todo como regla implícita
- **Reglas Input**
    - Se deniega todo tráfico input al firewall como regla implícita
- **Reglas Output**
    - Se deniega todo tráfico con origen en el firewall dirigido a una BOTNET

[31] DMZ: Zona Desmilitarizada, es una zona segura que se ubica entre la red interna de una organización y una red externa.
[32] BOTNET: Hace referencia a un conjunto de red de robots informáticos que se ejecutan de manera autónoma. Esta red de ordenadores pueden controlar servidores infectados de manera remota

- Se acepta todo tráfico que el administrador de la red crea conveniente que tenga origen en el firewall.

3.5.1.2 Reglas asignadas a la conectividad a internet

- Desde la Internet hacia la DMZ y hacia la Intranet solo se habilitarán los puertos necesarios por cada uno de los servicios.
- Desde la DMZ hacia la Internet y la Intranet sólo se habilitarán los puertos necesarios por cada uno de los servicios.
- Desde la Intranet hacia la DMZ y hacia la Internet sólo se habilitarán los puertos necesarios por cada uno de los servidores, y la misma configuración servirá para cada una de las interfaces de la zona local del firewall.
- Se habilitará solamente a determinados equipos de la Dirección de Desarrollo Tecnológico e Informático para el acceso hacia el Firewall
- Se deniega todo las paquetes con servicio ip que tengan origen en la DMZ con destino a una BOTNET
- Se deniega todo tráfico con servicio http que tengan origen en la DMZ con destino a una BOTNET

Restricciones del servicio

- El acceso a páginas WEB relacionadas con pornografía, violencia, sexo, entre otros, que no tengan vinculación con sus obligaciones institucionales.

3.5.1.1 Reglas Asignadas a los Laboratorios

- Todo tráfico que tenga origen en la VLAN de laboratorios está permitido acceder a los servicios UTN.

- Se acepta todo tráfico (con servicios definidos por el administrador) que tengan origen en la VLAN de laboratorios con destino a la internet.

3.6 Plan De Acción Ante Violación De Políticas De Seguridad

- Los usuarios deben informar cualquier evento o debilidad que pueda afectar la seguridad de la información
- Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados

3.6.1 Identificación de incidente

Se debe recolectar toda la información necesaria para el análisis del evento registrando todos los antecedentes, y de esta manera el encargado de Seguridad debe clasificar el incidente, de acuerdo al origen, tipo y nivel de criticidad.

3.6.2 Atención a incidente

Una vez evaluados y conocidos los riesgos es necesario definir que se hará con cada uno de ellos. La etapa de conocimiento y evaluación de los riesgos es tan importante como la de su tratamiento.

3.6.3 Seguimiento y cierre

Al menos una vez al año el encargado de la seguridad de la información, debe revisar los incidentes, y se debe proponer medidas que sean necesarias para que no vuelvan a ocurrir, además de detectar y aprender de cada uno de ellos.

4. Diseño e Implementación Firewall-Proxy

El Firewall es un equipo perimetral que actúa sobre toda la red de datos. De acuerdo al análisis de la situación actual el enlace perimetral entre los equipos de core de la institución y los equipo de distribución de las Facultades es Fibra Óptica, se puede apreciar en la Figura 38, por lo que resulta muy costoso invertir en tarjetas de red que soporten este tipo de enlaces. En el siguiente apartado se detalla aspectos fundamentales para el diseño e implementación de Firewall-Proxy.

Para definir los requisitos de software se toma como referencia el estándar ISO/IEC/IEEE 29148-2011 antes analizados, para diseño e implementación del Firewall-Proxy se toma de referencia la Arquitectura de Red TCP/IP usado comúnmente en las comunicaciones de redes informáticas, que provee de guías generales para permitir la comunicación entre equipos.

Para el diseño e implementación del Firewall-Proxy se toma como sustento la Arquitectura de red TCP/IP usado comúnmente en las comunicaciones de redes informáticas, que provee de guías para permitir la comunicación entre equipos.

4.1 Requisitos de software basado en el estándar ISO/IEC/IEEE 29148-2011

Los requisitos de software comprenden lo analizado en el apartado de Especificaciones de los requerimientos del software basado en el estándar ISO/IEC/IEEE 29148-2011 en el Capítulo Marco Teórico del presente documento. Para ello los requisitos se resumen en la Tabla 32.

Tabla 34 Requisitos basados en el estándar ISO/IEC/IEEE 29148-2011

ESPECIFICACION DE LOS REQUISISTOS DE SOFTWARE	
AMBITOS	
AMBITOS DEL SISTEMA	
Ejecutar políticas de Seguridad	El Sistema operativo cuenta con la herramienta de cortafuegos que Permite filtrar paquetes.
Ejecutar reglas en el Firewall	El sistema operativo cuenta con iptables que nos brinda cadenas para especificar regalas de seguridad
Direccionamiento de Puertos	podemos re direccionar el trafico entrante a nuestro Firewall mediante iptables
FUNCIONES DEL PRODUCTO	
Implementación de interfaces Virtuales por cada Laboratorio	Soporta protocolo 802.1Q que permite compartir de forma transparente el mismo medio físico a diferentes redes
Implementación de políticas en Firewall	Las cadenas se las puede definir como aceptar o denegar todo como política implícita
Implementación de reglas Firewall	Cuenta de cadenas para el ingreso de tráfico, salida y enrutamiento
Filtrado de paquetes	El filtrado se lo realiza por cadenas
Filtrado de contenido Web	Mediante la implementación de proxy SQUID
Asignación de memoria cache para contenido Web	La herramienta SQUID requiere de asignación de memoria cache para almacenar contenido WEB
Asignación de Horarios para uso de Internet	El proxy tiene la características de gestionar el acceso mediante horarios
Generación de Reportes	Por medio de la herramienta de generación de reportes SARG
CARACTERISTICAS DE LOS USUARIOS	
Restricción acceso a Sitios Web	El usuario puede crear listas de acceso en el proxy
Restricción de Acceso por horarios	El administrador del sistema puede asignar horarios para el acceso a internet
Configuración de memoria cache	El administrador del sistema puede asignar memoria cache conveniente para el buen performance del sistema
Herramienta de Reportes	El usuario del sistema puede generar reportes tomando como datos la Bitácora del proxy.
SUPOSICIONES Y DEPENDENCIAS	
Al menos una tarjeta de red	Al menos el sistema operativo debe contar con el buen funcionamiento de una tarjeta de red
Sistema operativo de licencia libre	El sistema contribuye a la formación de conocimiento y es libre para usarlo de la forma que conviene
Sistema operativo con soporte de configuraciones de red.	El sistema operativo controla los procesos básicos y configuraciones de red necesarios
REQUERIMIENTOS FUTUROS	
Agregación de enlace	Se puede realizar la operación denominad Bonding
INTERFACES EXTERNAS	
Usuarios pueden acceder al servidor mediante un intérprete de comandos	Soporta la configuración SSH y administración vía WEB
FUNCIONES DEL PRODUCTO	
Configuración de Proxy	si
Restricción de acceso a sitios de internet	si
Restricción de Acceso por horarios	si
Herramienta de Reportes	si
RESTRICCIONES DE RENDIMIENTO	
Capacidad de receptar peticiones de todos los clientes	Si
RESTRICCIONES DE DISEÑO	
Compatibilidad y disponibilidad de paquetes de software	Si
Disponibilidad de actualizaciones necesarias	Si
ATRIBUTOS DEL SISTEMA	
Mecanismo de seguridad	Se utiliza autenticación por usuario y contraseña

Fuente: Elaborado por el Autor

4.2 Requerimientos de Hardware

Para la implementación de la solución tomamos en consideración algunos factores entre ellos consumo CPU, cuanta memoria RAM se requiere, cantidad de disco duro.

Para determinar características necesarias para la implementación de la solución nos basamos en un escenario experimental, donde contamos con un equipo de las características que se muestran en la Figura 57.

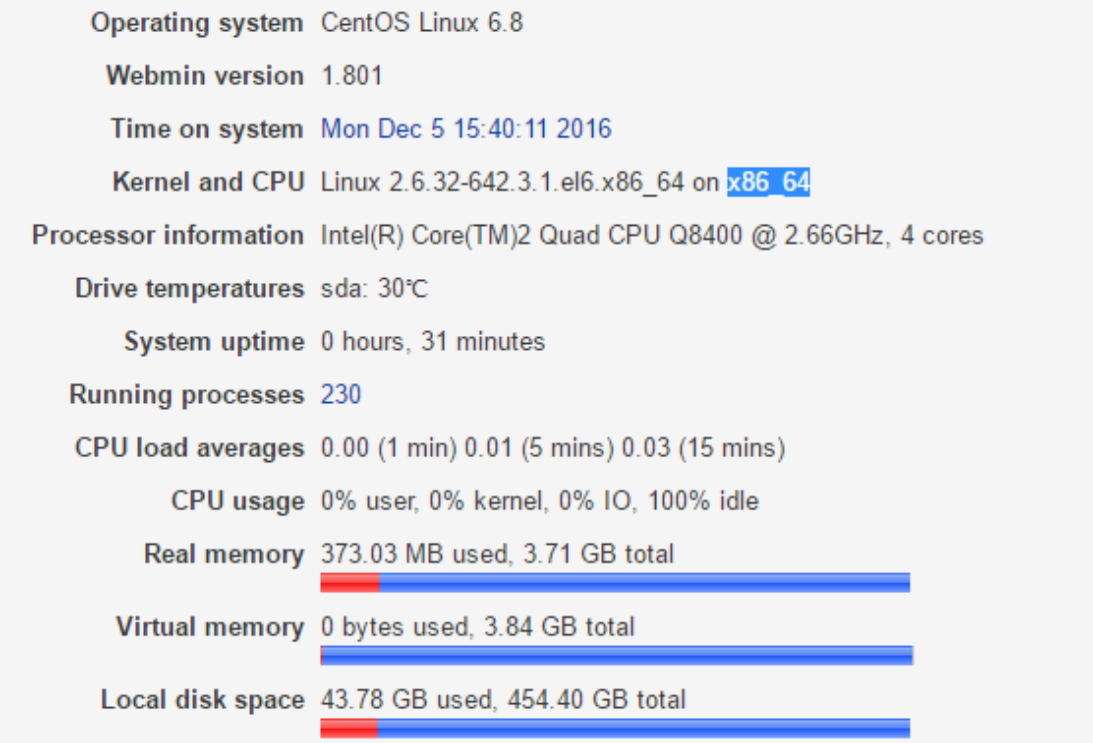


Figura 57. Características de Servidor Utilizado

Fuente: Servicio Webmin

4.2.1 CPU para Proxy Squid

La figura 57 nos muestra las características de CPU que cuenta nuestro equipo.

Squid no hace uso amplio de CPU, en las únicas ocasiones en las que hace uso intensivo de CPU es cuando el proceso es inicializado. Es posible instalar squid en sistemas con un

solo CPU de velocidades modestas. Se realizó la prueba de cantidad de procesamiento que utiliza squid al instante que se inicia el proceso y se comprobó que no realiza uso intensivo de la capacidad de CPU, llego a ocupar un 3.3% de la capacidad total como se muestra en la figura 58.

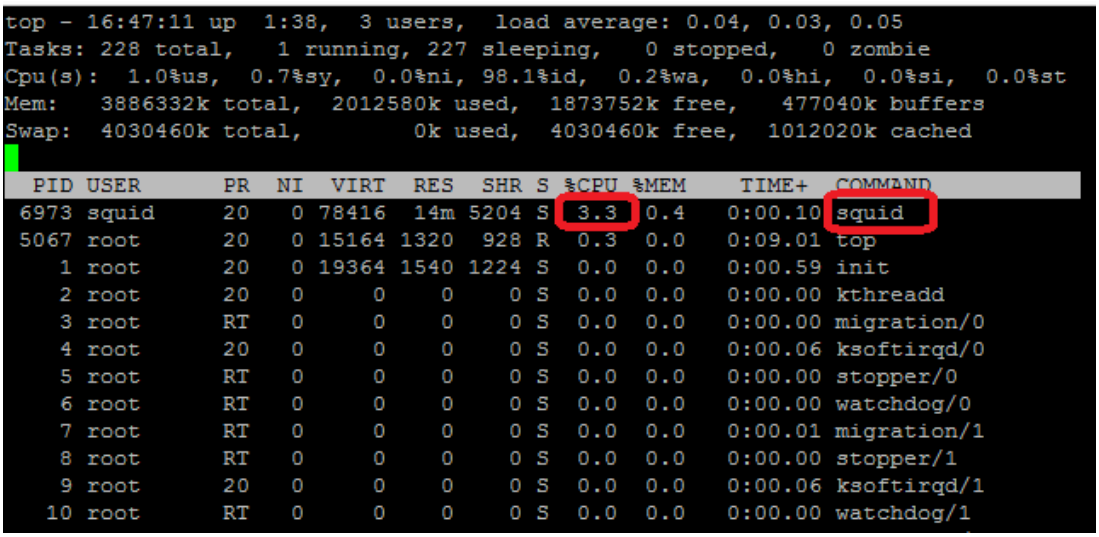


Figura 58. Uso CPU al iniciar SQUID

Fuente: Servicio Webmin

4.2.2 Disco Duro para Proxy Squid

Tomando en cuenta que el servicio de proxy va a ser utilizado durante 12 horas, ya que según el horario de uso de los laboratorios estos se usan de 7:00 am a 21:00 pm exceptuando dos horas de 13:00 a 15:00 que no se utilizan.

Según el reporte de EXINDA, tomado en el rango de tiempo de 09 de octubre de 2016 al 08 de noviembre de 2016 se puede apreciar que la cantidad procesado es de 2255988.59 MB de peticiones como se muestra en la Figura 59.

Top 40 Inbound Subnets (by Data Transfer)

Name	Data (MB)	Throughput (kbps)	
		Average	Max
FICA-Laboratorios	2255988.59	7452.53	105373.77

Figura 59. Cantidad de datos procesados 30 días
Fuente: Servicio EXINDA

Este valor hace referencia a 20 días que son los días que se usan los laboratorios por mes. Desde esta aclaración se puede obtener un valor aproximado por día que se procesa en el segmento de red de los laboratorios.

$$Procesamiento\ de\ datos\ Diario = \frac{Cantidad\ de\ datos\ Procesados}{Días\ de\ uso\ de\ Laboratorios}\ [MB/Dia]$$

Ecuación 1: Cálculo de datos procesados diariamente

El cálculo se lo realiza de la siguiente forma:

$$Procesamiento\ de\ datos\ Diario = \frac{2255988.59}{20}\ [MB/Dia]$$

$$Procesamiento\ de\ datos\ Diario = 112799.43[MB/Día]$$

$$Procesamiento\ de\ datos\ Diario = 110[GB/Día]$$

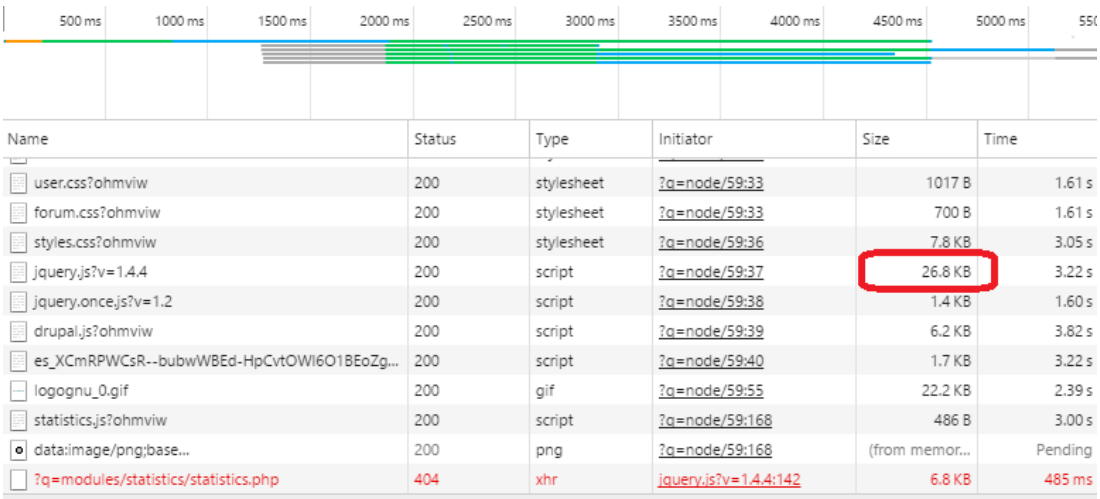
Se requiere 110 GB en disco duro para almacenar las peticiones de los usuarios de los laboratorios.

4.2.3 Memoria RAM para Proxy Squid

El proxy squid hace uso de cache en memoria RAM para el almacenamiento de objetos en tránsito (Linux, 2016), esto permite acelerar el tiempo de respuesta a las peticiones de los clientes.

Por cada GB de espacio en disco que asigne para el cache, squid usará aproximadamente 6MB de memoria RAM para mantener una tabla o índice con la referencia a los objetos almacenados en el cache de disco. Esto significa que, entre más grande sea el cache de disco, más memoria RAM usará squid (Linux, 2016).

El tamaño promedio de un objeto que solicita un cliente es de un valor promedio de 27 KB. Como se muestra en la Figura 60.



Name	Status	Type	Initiator	Size	Time
user.css?ohmviw	200	stylesheet	?q=node/59:33	1017 B	1.61 s
forum.css?ohmviw	200	stylesheet	?q=node/59:33	700 B	1.61 s
styles.css?ohmviw	200	stylesheet	?q=node/59:36	7.8 KB	3.05 s
jquery.js?v=1.4.4	200	script	?q=node/59:37	26.8 KB	3.22 s
jquery.once.js?v=1.2	200	script	?q=node/59:38	1.4 KB	1.60 s
drupal.js?ohmviw	200	script	?q=node/59:39	6.2 KB	3.82 s
es_XCmRPWCsR--bubwWBEd-HpCvtOWI6O1BEoZg...	200	script	?q=node/59:40	1.7 KB	3.22 s
logognu_0.gif	200	gif	?q=node/59:55	22.2 KB	2.39 s
statistics.js?ohmviw	200	script	?q=node/59:168	486 B	3.00 s
data:image/png;base...	200	png	?q=node/59:168	(from memor...	Pending
?q=modules/statistics/statistics.php	404	xhr	jquery.js?v=1.4.4:142	6.8 KB	485 ms

Figura 60. Tamaño de objeto promedio de una página web

Fuente: Servicio Chrome

Si asignamos 110 GB en disco duro, la cantidad de objetos que se podrían almacenar es de aproximadamente 4.3 millones de objetos de esta manera la cantidad de memoria requerida en base a la cantidad de objetos seria de 320,4 MB.

$$Numero\ de\ Objetos = \frac{Cantidad\ Disco\ Duro}{Tamaño\ de\ Objeto}$$

Ecuación 2. *Calculo de Número de Objetos*
Fuente: Squid mejorar rendimiento en GNU/Linux. Recuperado de: http://www.linuxcolombia.com.co/?q=node/59

$$Numero\ de\ Objetos = \frac{110[GB]}{27[KB]}$$

$$Numero\ de\ Objetos = 4271976{,}30$$

Cada objeto usa 75 Bytes de RAM por lo que con 110 GB de disco duro usado se necesitan 305,6 MB de memoria RAM.

$$RAM = Numero\ de\ Objetos\ x\ 75B$$

$$RAM = 305{,}6[MB]$$

El equipo con que se cuenta tiene 4 GB de Capacidad de memoria RAM como se muestra en la Figura 61, se decidió tomar 2GB de la capacidad de memoria por la razón de que se considera el uso de memoria de otros programas que se ejecutan aparte del sistema operativo, en la Figura 61 se muestra la cantidad de memoria utilizada en RAM (used) y la cantidad de memoria libre (free).

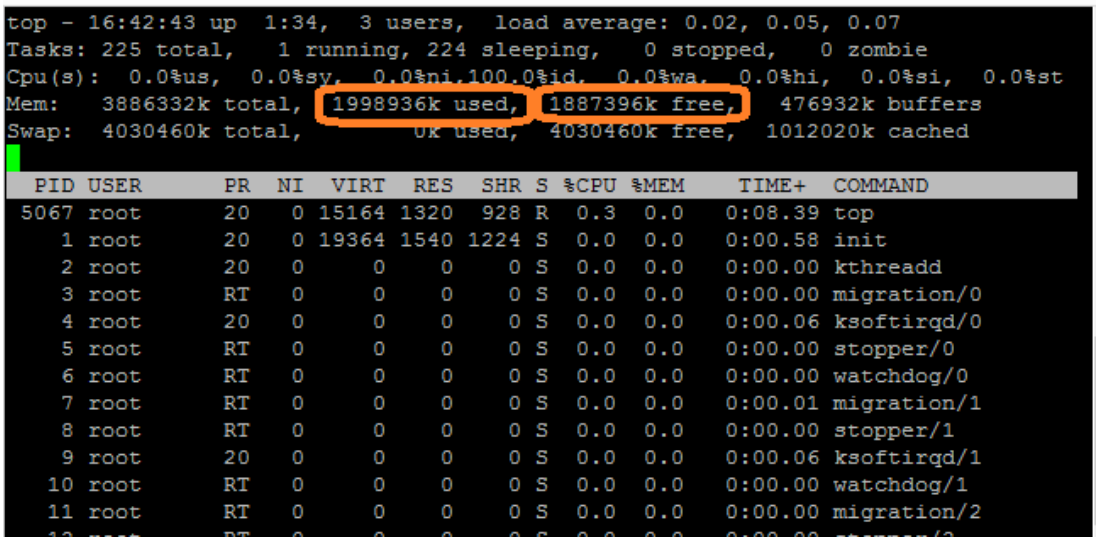


Figura 61. Uso de memoria RAM Sistema Operativo y otros procesos internos.

Fuente: Servicio Webmin

4.2.3 Firewall

Según el autor Gualoto Christian en su investigación "Desarrollo de un prototipo de solución integral Web para la administración de una red tipo SOHO bajo la plataforma GNU/Linux" el Firewall consume 128 MB de RAM y al menos se requiere 10 GB de disco duro disponible.

4.2.4 Estimación Final

La determinación del valor necesario para CPU, disco duro y RAM se realiza en base a la suma total de los valores por cada servicio, como se muestra en la Tabla 35.

De esta manera se concluye que el equipo con el que se cuenta satisface las necesidades requeridas.

Tabla 35. Estimación Requerimientos de Hardware

Servicio	RAM	Disco Duro	CPU
Firewall	128MB	10GB	250MHz
Proxy	305,6MB	110GB	250MHz
Total	**433,6MB**	**120GB**	**500MHz**

Fuente: Elaborado por el autor.

4.3 Fica

De acuerdo al análisis de situación actual realizado se pudo constatar factores que se convierten en limitantes para el desarrollo del Firewall-Proxy.

Un limitante que se manifiesta en la red de datos de la Facultad, son la velocidad de transmisión de los puertos que cuenta el Switch de distribución, ya que estos disponen de tecnología FastEthernet.

Tomando en consideración el reporte generado por la herramienta EXINDA se verificó que la red Fica-Laboratorios es la que genera mayor tráfico en la red de datos seguida por la red Fica-Wireless. Dado estas circunstancias y tomando en consideración los equipos existentes, se decidió separar los dos segmentos de red y diseñar una solución acorde a las necesidades y tecnología con que se cuenta.

4.3.1 Diseño de Capa 1

El cableado es uno de los factores a considerar más importantes en el diseño de una red LAN, en la Facultad de Ingeniería en Ciencias Aplicadas, en la actualidad se basa en su mayoría en la tecnología FastEthernet, utiliza una topología de bus lógica.

4.3.1.1 Diagrama Lógico

Este modelo detalla la topología de red de la FICA sin detalles de instalación del cableado. Es un mapa de ruta básico. Ver Figura 62.

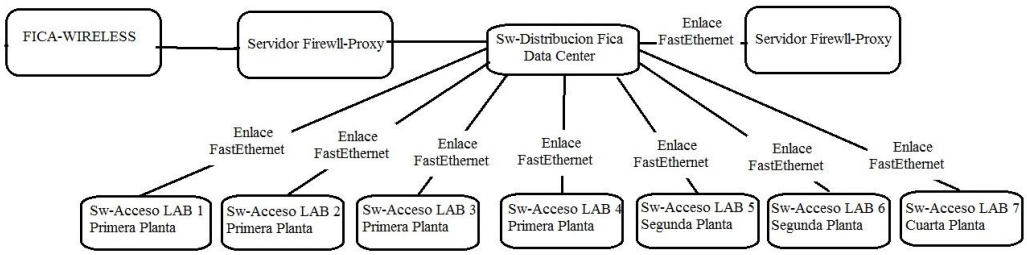


Figura 62. Diagrama Lógico FICA-UTN
Fuente: Elaborado por el Autor

4.3.2 Diseño de Capa 2

En esta sección se detalla cuantos puertos del switch están siendo utilizados y la velocidad en que trabaja cada uno medido en bits por segundo.

- **Firewall-Proxy**

El Firewall-Proxy será conectado a un puerto del Switch de distribución de la Fica tal como se muestra en la Figura 63. Este switch cuenta con 144 puertos FastEhernet pero cuenta con cuatro ranuras SFP con velocidad GigabitEthernet. Debido a la gran demanda de tráfico que genera la red de datos de los laboratorios se procuró separar el segmento de red. Para la red inalámbrica, se define que será gestionada por un router de marca Mikrotik modelo 1100AHX2 con el que cuenta la facultad cuya licencia es de nivel 6 el cual nos especifica el soporte de características de Firewall y Web proxy.

- **Laboratorio 1**

Este laboratorio cuenta con 26 equipos conectado al switch de acceso, cuenta con 48 puertos FastEthernet y 26 equipos conectados al switch como se muestra en la Figura 64.

- **Laboratorio 2**

Este laboratorio cuenta con 20 equipos conectado al switch de acceso. Ver Figura 65.

- **Laboratorio 3**

Este laboratorio tiene 30 equipos conectados al switch de acceso como se muestra en la Figura 66. Además un switch adicional de 24 puertos FastEthernet.

- **Laboratorio 4**

Este laboratorio cuenta con 20 equipos conectados a un switch de acceso de 48 interfaces FastEthernet. Además un switch de acceso adicional de 48 interfaces FastEthernet. Ver Figura 67.

- **Laboratorio 5**

Este laboratorio tiene 30 equipos conectados al switch de acceso como se muestra en la Figura 68.

- **Laboratorio 6**

Este laboratorio tiene 26 equipos conectados al switch de acceso como se muestra en la Figura 69.

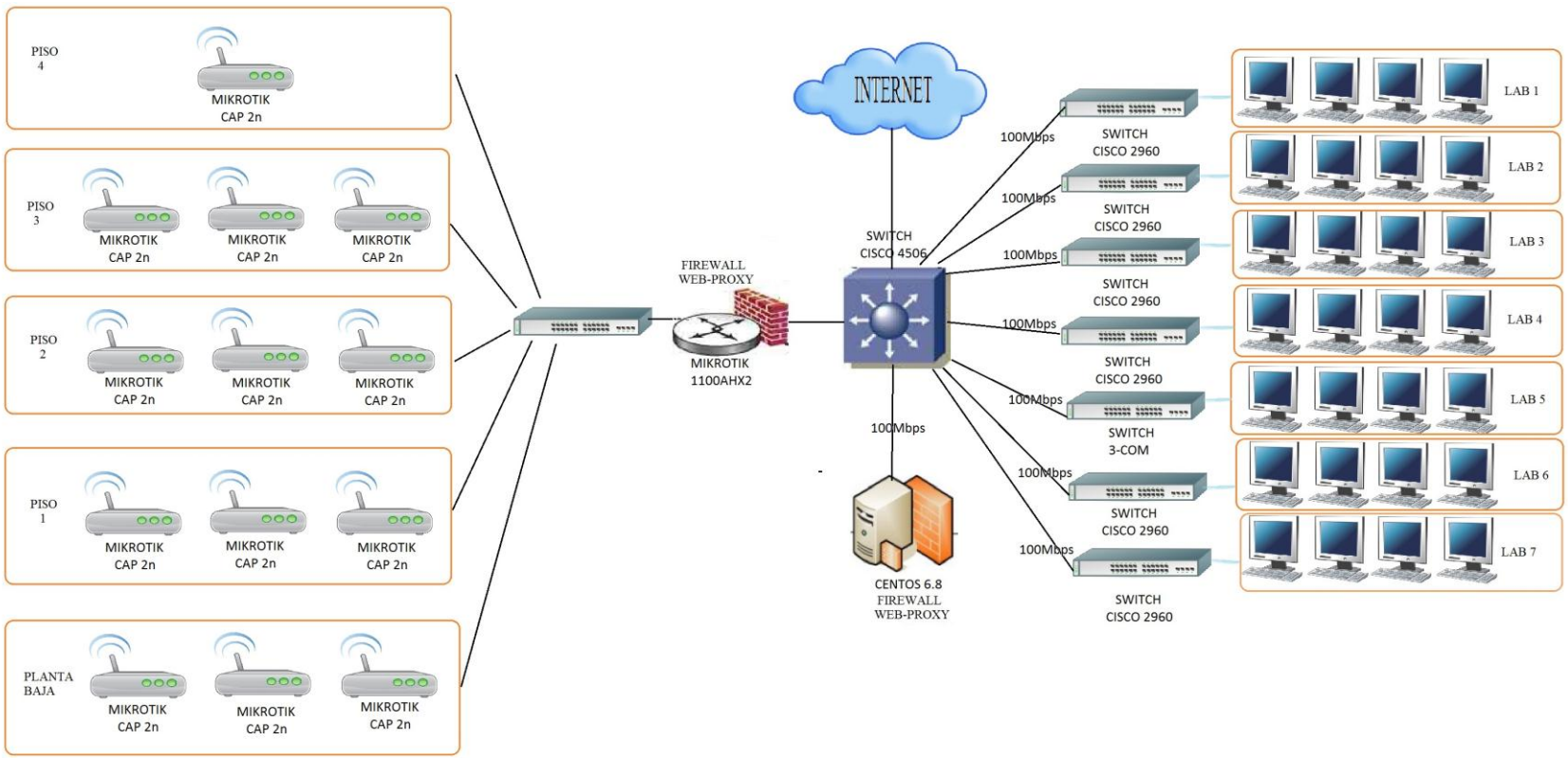


Figura 63. Diagrama de capas 2 Firewall-Proxy FICA
Fuente: Elaborado por el Autor.

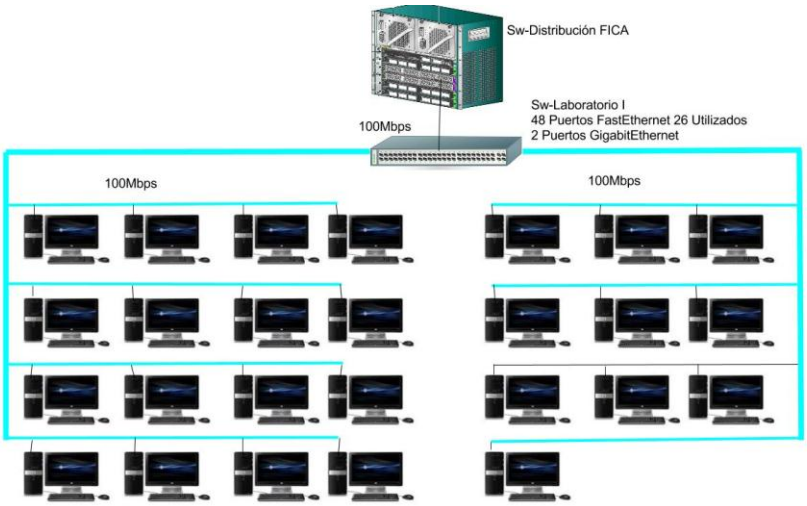


Figura 64. Diagrama de capa 2 Laboratorio 1 FICA
Fuente: Elaborado por el Autor.

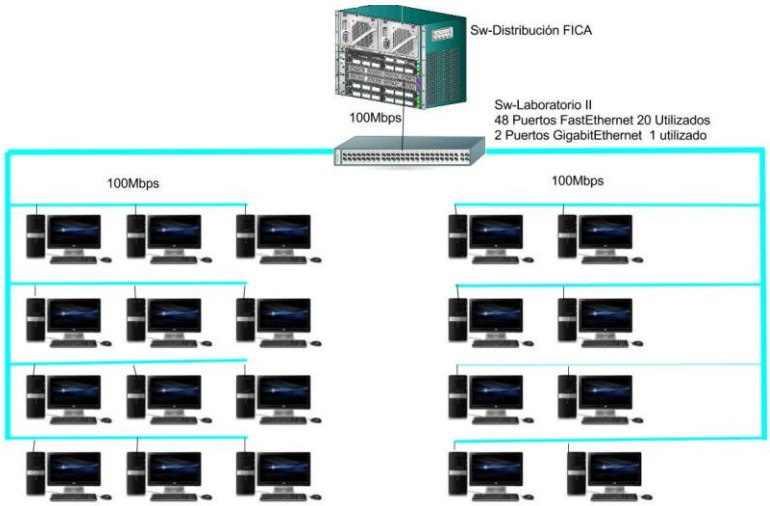
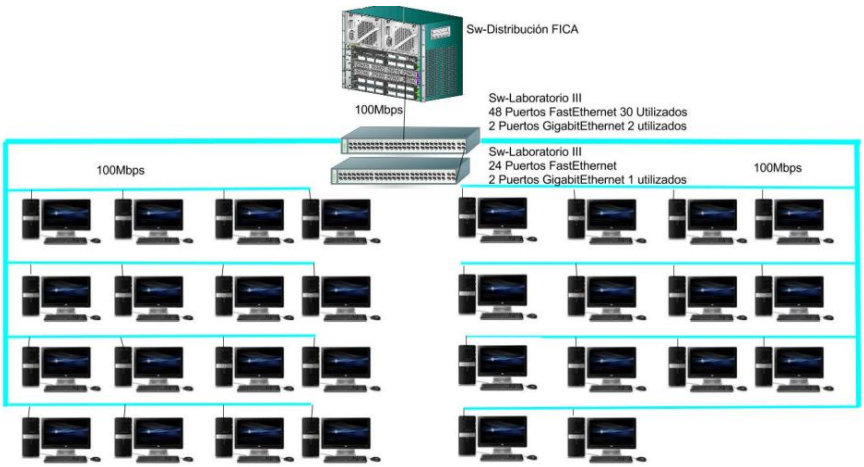


Figura 65. Diagrama de capa 2 Laboratorio 2 FICA
Fuente: Elaborado por el Autor.



.Figura 66.Diagrama de capas 2 Laboratorio 3 FICA
Fuente: Elaborado por el Autor.

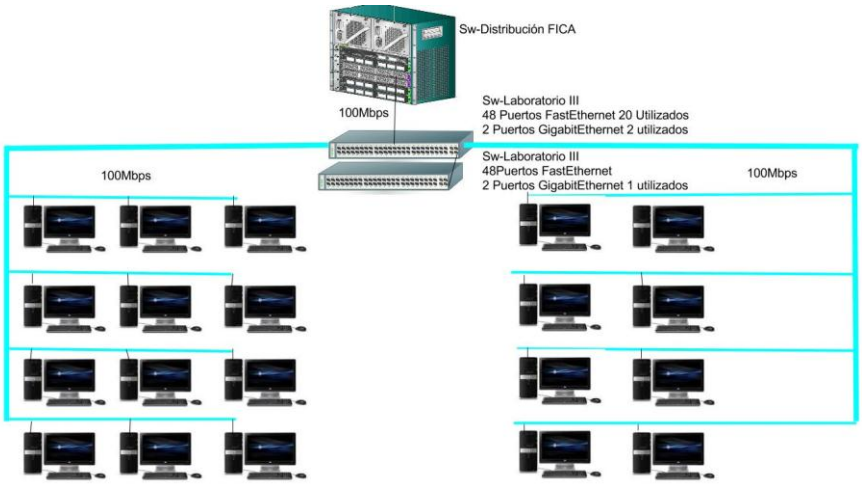


Figura 67. Diagrama de capa 2 Laboratorio 4 FICA
Fuente: Elaborado por el Autor.

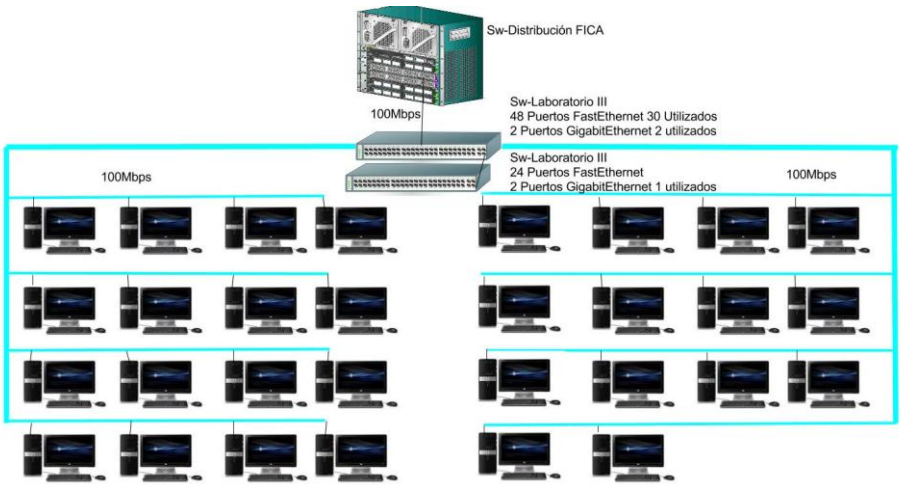


Figura 68. Diagrama de capa 2 Laboratorio 5 FICA
Fuente: Elaborado por el Autor.

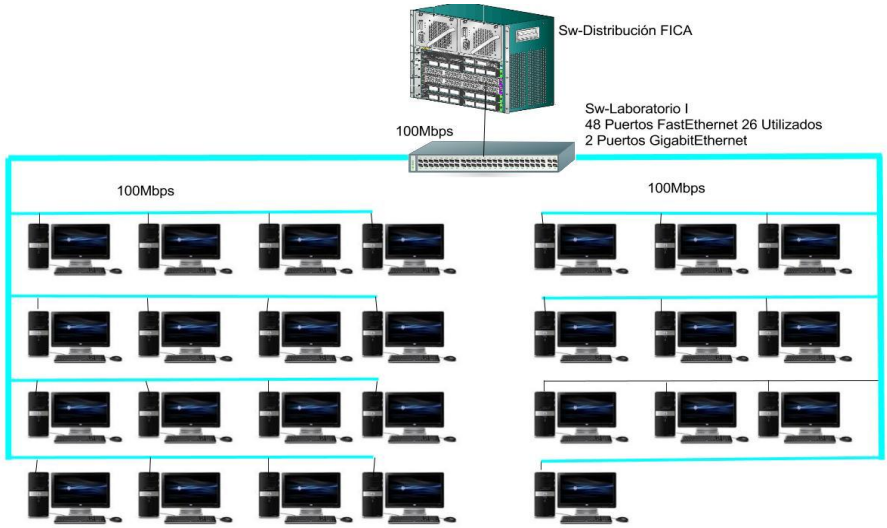


Figura 69. Diagrama de capa 2 Laboratorio 6 FICA
Fuente: Elaborado por el Autor.

- **Laboratorio 7**

Cuenta con dos switch de acceso con 48 interfaces FastEthernet y 24 equipos conectados a uno de los switch. Ver Figura 70.

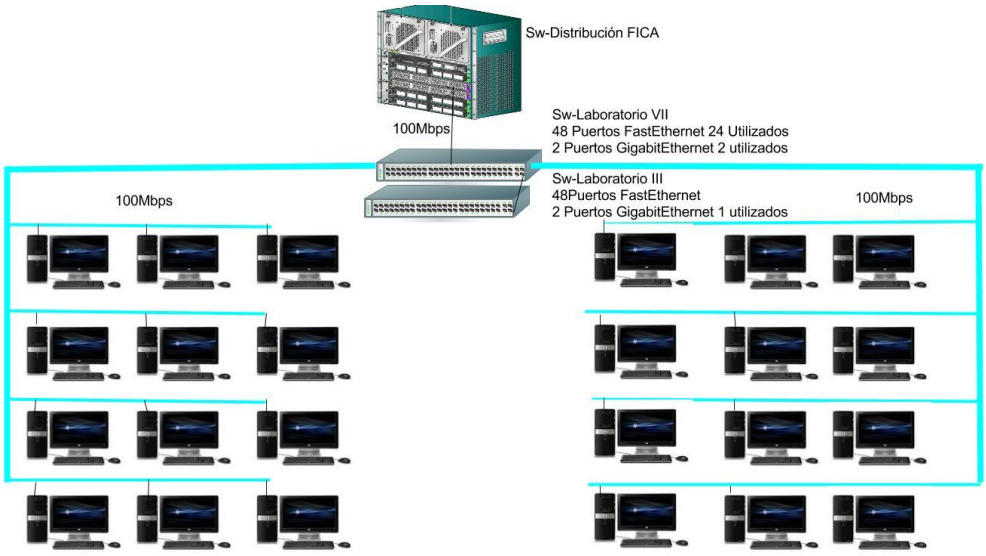


Figura 70. Diagrama de capas 2 Laboratorio VII FICA

Fuente: Elaborado por el Autor.

4.3.3 Diseño de Capa 3

Esta parte del diseño se detalla cómo fueron creadas las VLAN´s de laboratorios de la Facultad de Ingeniería en Ciencias Aplicadas (FICA). Estas subredes permiten la comunicación entre segmentos basados en direcciones de Capa 3 o direcciones IP. Por seguridad, el direccionamiento mostrado en esta sección solo hace referencia al último octeto; los primeros tres octetos son representados con letras x,y.

El diseño de la VLAN de Laboratorios de la FICA tiene definido un esquema de 512 direcciones es decir: x.x.x.0/23. A partir de esta información se procuró crear 8 subredes de 64 direcciones cada una.

El direccionamiento se muestra en la siguiente Tabla 36:

Tabla 36: Direccionamiento IP para los Laboratorios FICA.

		VLAN LABORATORIOS FICA		**X.X.X.0/23**	
N°	Subred	Máscara	Dir. IP Gateway	Dir. Broadcast	Rango IP Utilizable
1	X.X.X.0/26	255.255.255.192	X.X.X.1/26	X.X.X.63/26	X.X.X.[2-62]
2	X.X.X.64/26	255.255.255.192	X.X.X.65/26	X.X.X.127/26	X.X.X.[66-126]
3	X.X.X.128/26	255.255.255.192	X.X.X.129/26	X.X.X.191/26	X.X.X.[130-190]
4	X.X.X.192/26	255.255.255.192	X.X.X.193/26	X.X.X.255/26	X.X.X.[194-254]
5	X.X.Y.0/26	255.255.255.192	X.X.Y.1/26	X.X.Y.63/26	X.X.Y.[2-62]
6	X.X.Y.64/26	255.255.255.192	X.X.Y.65/26	X.X.Y.127/26	X.X.Y.[66-126]
7	X.X.Y.128/26	255.255.255.192	X.X.Y.129/26	X.X.Y.191/26	X.X.Y.[130-190]
8	X.X.Y.192/26	255.255.255.192	X.X.Y.193/26	X.X.Y.255/26	X.X.Y.[194-254]

Fuente: Elaborado por el autor

Del direccionamiento antes detallado se utilizaran las subredes de la 2 a la 8.

El servidor Firewall-Proxy tendrá 8 interfaces de red, se crearan siete interfaces de red virtuales a las cuales se asignarán direcciones IP que actuarán como puertas de enlace de los laboratorios 1,2,3,4,5,6 y 7 y la restante será la dirección de proxy. Ver Figura 71.

La razón por las que se crearon las interfaces virtuales es para gestionar los laboratorios de manera independiente.

La red inalámbrica de la Fica comprende de dos subredes: La WAN que proporciona el administrador de la red y la LAN que se procura diseñar de acuerdo a las necesidades existentes. El direccionamiento se puede apreciar en la Tabla 37.

Tabla 37: Direccionamiento IP para los Laboratorios FICA.

	VLAN LABORATORIOS FICA			**X.X.X.0/23**	
	Subred	Máscara	Dir. IP Gateway	Dir. Broadcast	Rango IP Utilizable
WAN	X.X.42.0/24	255.255.255.0	X.X.42.1/1	X.X.42.255/24	X.X.42.[2-254]
LAN	X.X.Y.0/24	255.255.255.0	X.X.X.1/24	X.X.X.255/24	X.X.X.[2-254]

Fuente: Elaborado por el autor.

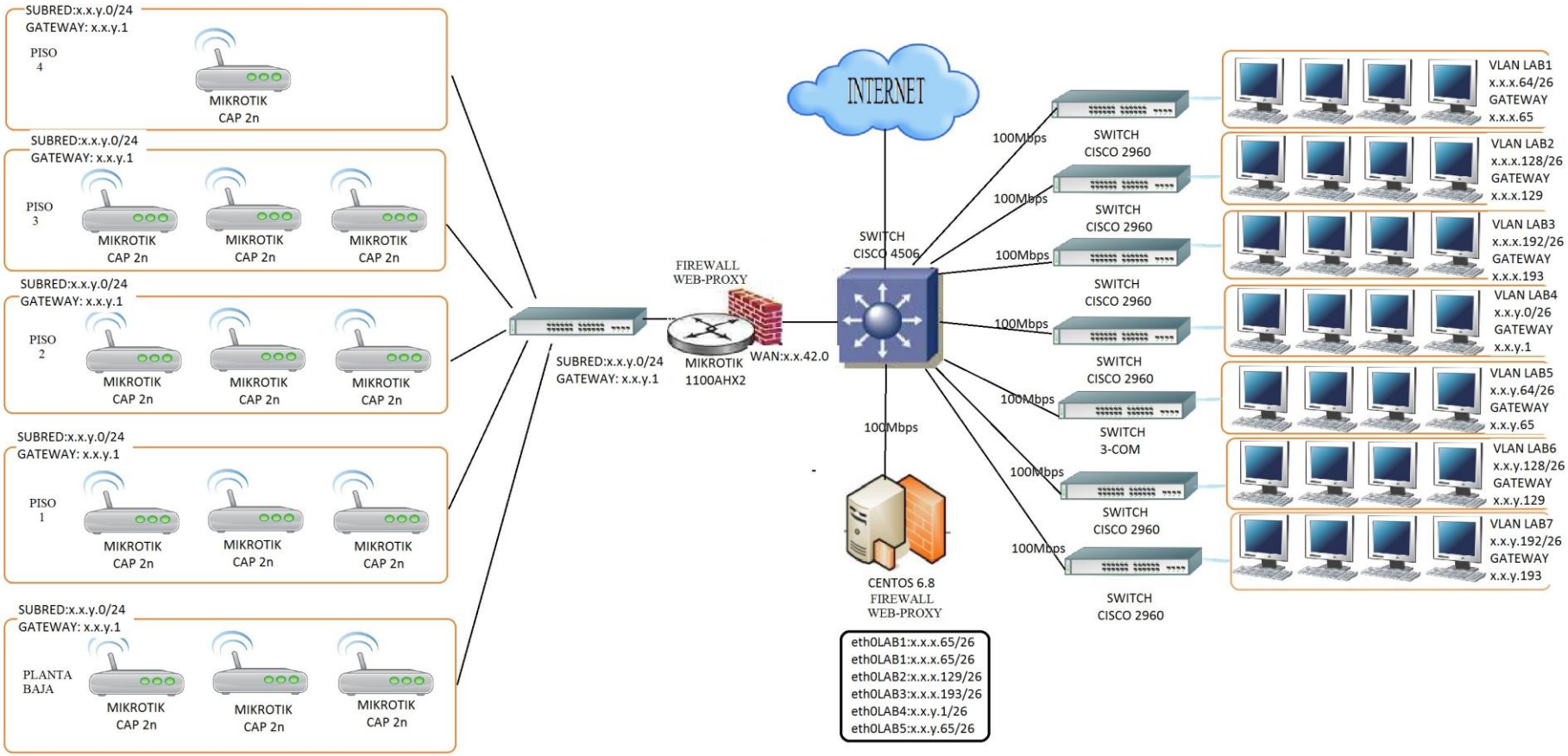


Figura 71. Diagrama de capa 3 Laboratorios FICA
Fuente: Elaborado por el Autor.

4.4 Ficaya

Para el diseño de Firewall-Proxy de la Ficaya se toma en consideración el análisis de situación actual mencionado en el capítulo 3.

4.4.1 Diseño De Capa 1

El cableado horizontal de la FICAYA incluye el par trenzado no blindado UTP categoría 6.

4.4.1.1 Diagrama Lógico

En este diagrama se muestra la topología de red de la FICAYA sin detalles de instalación. Como se muestra en la Figura 72.

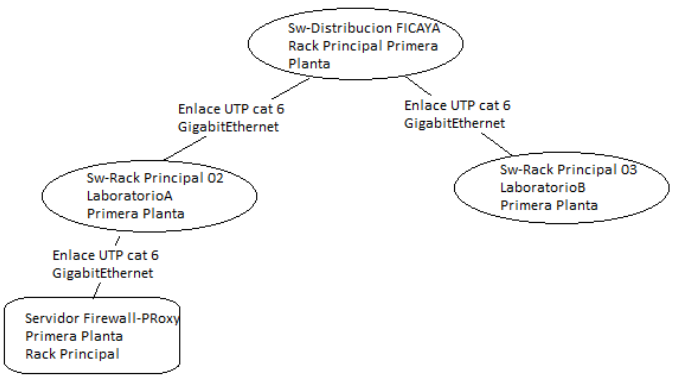


Figura 72. Diagrama Lógico FICAYA-UTN
Fuente: Elaborado por el Autor

4.4.2 Diseño De Capa 2

En esta sección se detalla cuantos puertos del switch están siendo utilizados y la velocidad en que trabaja cada uno medido en bits por segundo.

- **Laboratorio A**

Este laboratorio cuenta con 25 equipos conectado al switch de acceso, es a este switch al que se conecta el Firewall-Proxy a un puerto GigabitEthernet como se muestra en la Figura 73.

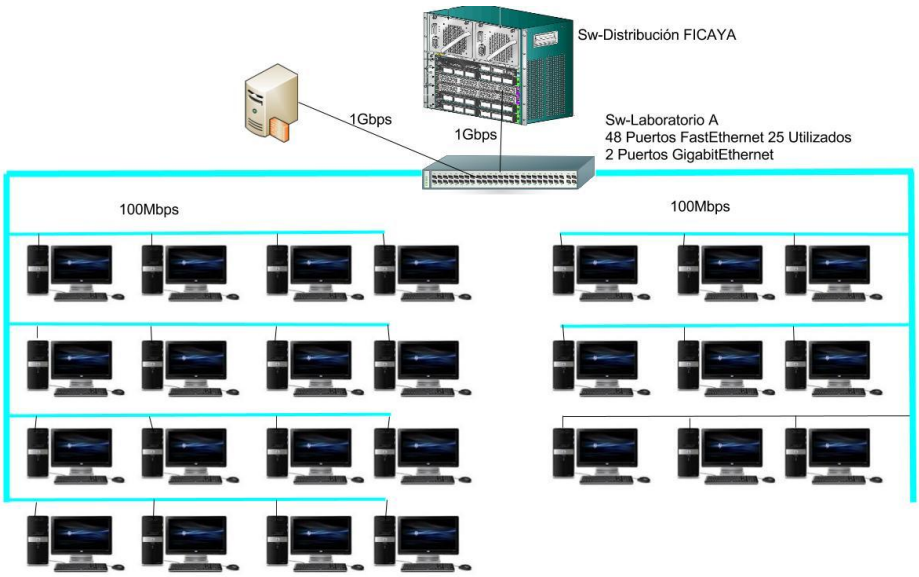


Figura 73. Diagrama de capa 2 Laboratorio I FICAYA
Fuente: Elaborado por el Autor.

- **Laboratorio B**

Este laboratorio tiene 30 equipos conectados al switch de acceso como se muestra en la Figura 74.

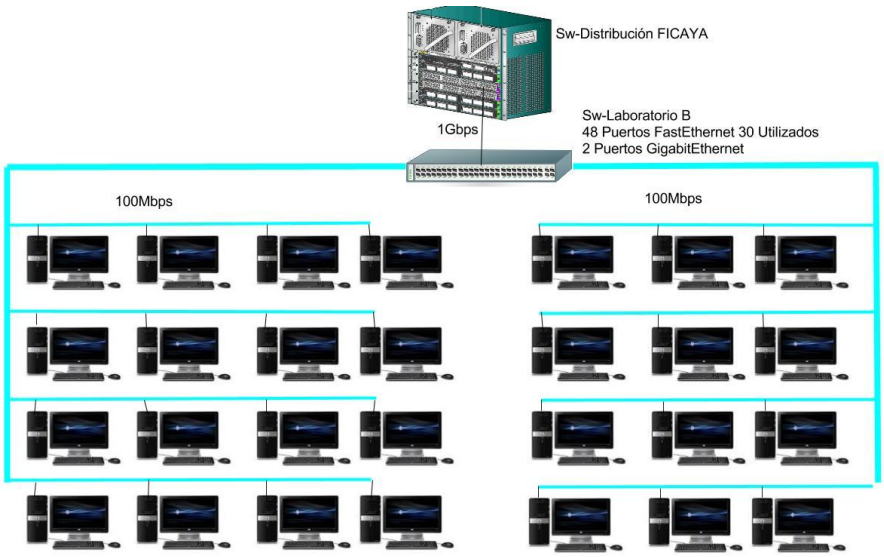


Figura 74. Diagrama de capas 2 Laboratorio B FICAYA
Fuente: Elaborado por el Autor.

4.4.3 Diseño de Capa 3

Esta parte del diseño se detalla cómo fueron creados los segmentos de red de los laboratorios de la FICAYA. Estas subredes permiten la comunicación entre segmentos basados en direcciones de Capa 3 o direcciones IP. Por seguridad, el direccionamiento mostrado en esta sección solo hace referencia al último octeto; los primeros tres octetos son representados con letras x,y.

El diseño de la VLAN de Laboratorios de la FICAYA tiene definido un esquema de 512 direcciones es decir: x.x.x.0/23. A partir de esta información se procuró crear 4 subredes de 128 direcciones cada una.

El direccionamiento se muestra en la Tabla 35:

Tabla 38: Direccionamiento IP para los Laboratorios FICAYA.

VLAN LABORATORIOS FICAYA			x.x.x.0/23		
N°	Subred	Máscara	Dir. IP Gateway	Dir. Broadcast	Rango IP Utilizable
1	x.x.x.0/25	255.255.255.128	x.x.x.1/25	x.x.x.127/25	x.x.x.[2-126]
2	x.x.x.128/25	255.255.255.128	x.x.x.129/25	x.x.x.255/25	x.x.x.[130-254]
3	x.x.y.0/25	255.255.255.128	x.x.y.1/25	x.x.y.127/25	x.x.y.[2-126]
4	x.x.y.128/25	255.255.255.128	x.x.y.129/25	x.x.y.255/25	x.x.y.[129-254]

Fuente: Elaborado por el autor.

Del direccionamiento antes detallado se utilizaran las subredes de la 2 y 3.

El servidor Firewall-Proxy tendrá 3 interfaces de red, se crearan dos interfaces de red virtuales a las cuales se asignarán direcciones IP que actuarán como puertas de enlace de los laboratorios A y B y la restante será la dirección de proxy. Ver Figura 75.

La razón por las que se crearon las interfaces virtuales es para gestionar los laboratorios de manera independiente.

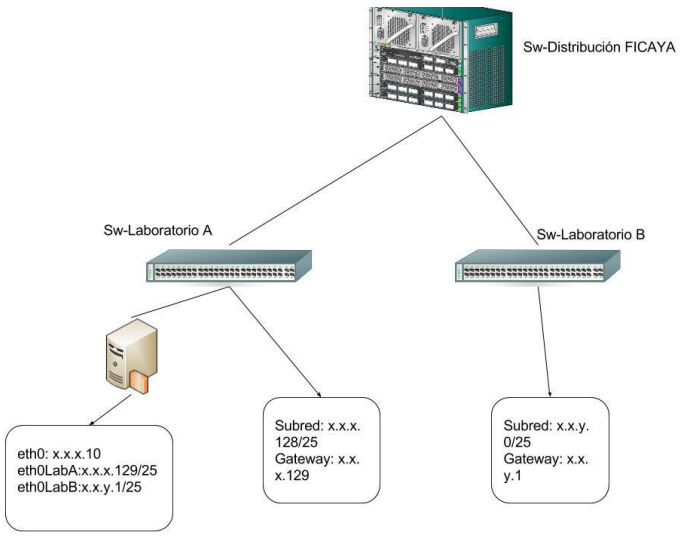


Figura 75. Diagrama de capas 3 Laboratorios FICAYA
Fuente: Elaborado por el Autor.

4.5 Fecyt

4.5.1 Diseño de capa 1

El cableado horizontal de la FECYT incluye el par trenzado no blindado UTP.

4.5.1.1 Diagrama lógico

En este diagrama se muestra la topología de red de la Facultad de Educación Ciencia y Tecnología (FECYT) sin detalles de instalación exacta del cableado. Ver Figura 76.

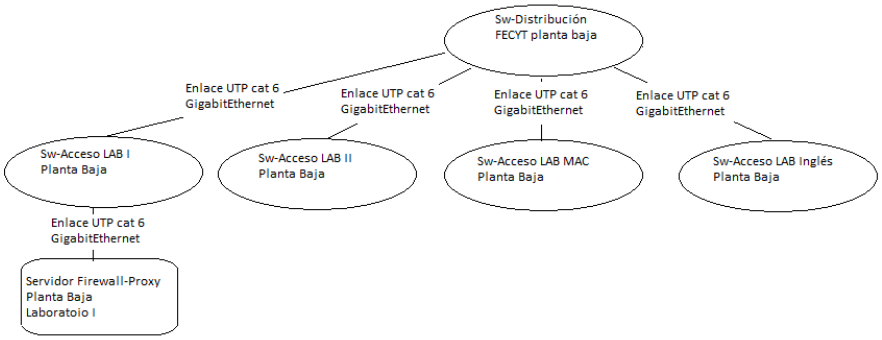


Figura 76. Diagrama Lógico FICAYA-UTN
Fuente: Elaborado por el Autor

4.3.2 Diseño de capa 2

En esta sección se detalla cuantos puertos del switch están siendo utilizados y la velocidad en que trabaja cada uno medido en bits por segundo.

- **Laboratorio 1**

Este laboratorio cuenta con 30 equipos conectado al switch de acceso, es a este switch al que se conecta el Firewall-Proxy a un puerto GigabitEthernet como se muestra en la Figura 77.

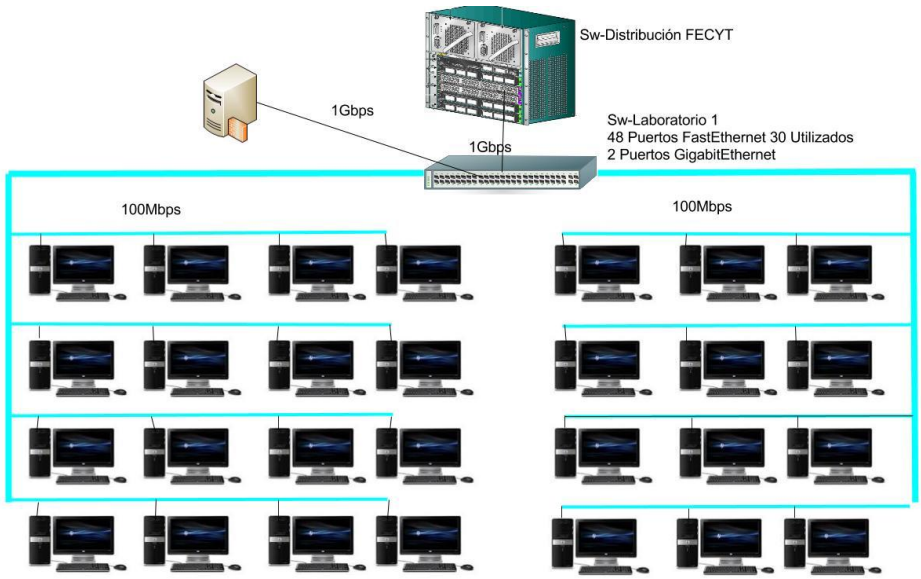


Figura 77. Diagrama de capa 2 Laboratorio I FECYT

Fuente: Elaborado por el Autor.

- **Laboratorio II**

Este laboratorio tiene 30 equipos conectados al switch de acceso como se muestra en la Figura 78.

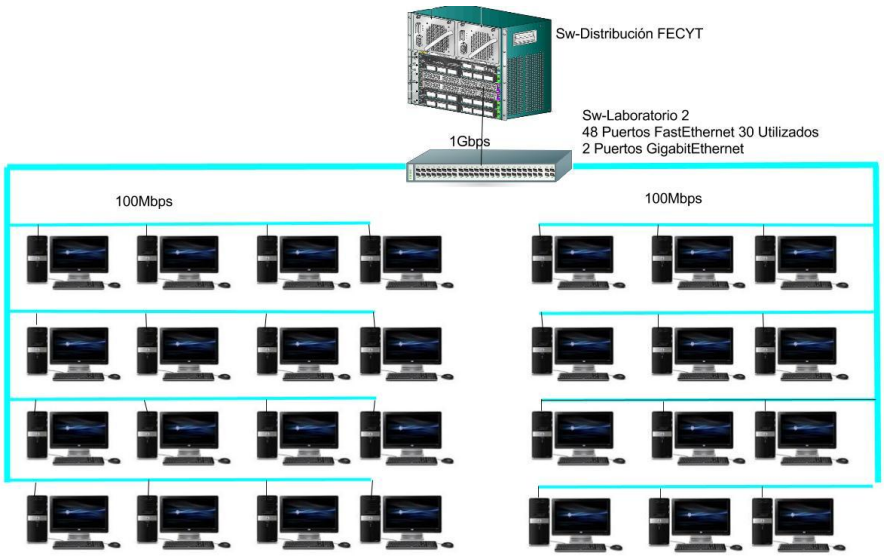


Figura 78. Diagrama de capas 2 Laboratorio 2 FECYT
Fuente: Elaborado por el Autor.

- **Laboratorio Inglés**

Este laboratorio tiene 34 equipos conectados al switch de acceso como se muestra en la Figura 79.

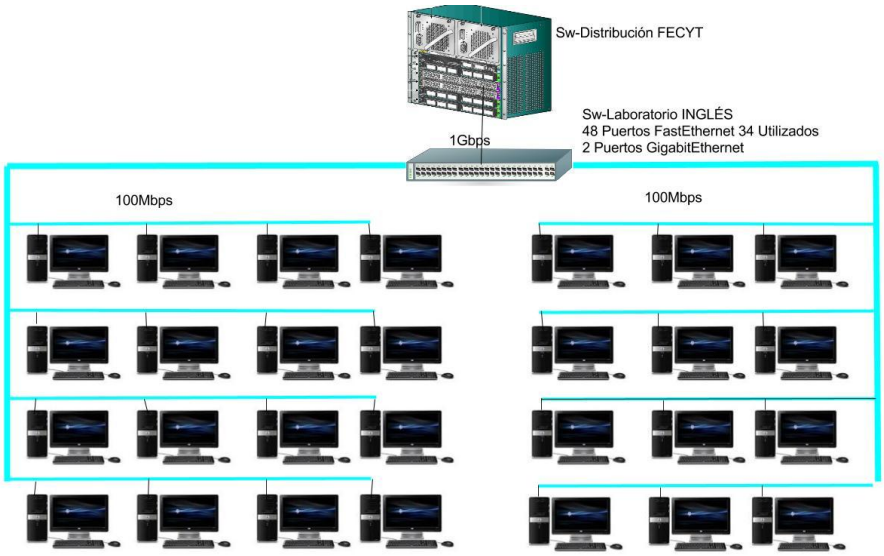


Figura 79. Diagrama de capas 2 Laboratorio Inglés FECYT
Fuente: Elaborado por el Autor.

- **Laboratorio MAC**

Este laboratorio tiene 38 equipos conectados al switch de acceso como se muestra en la Figura 80.

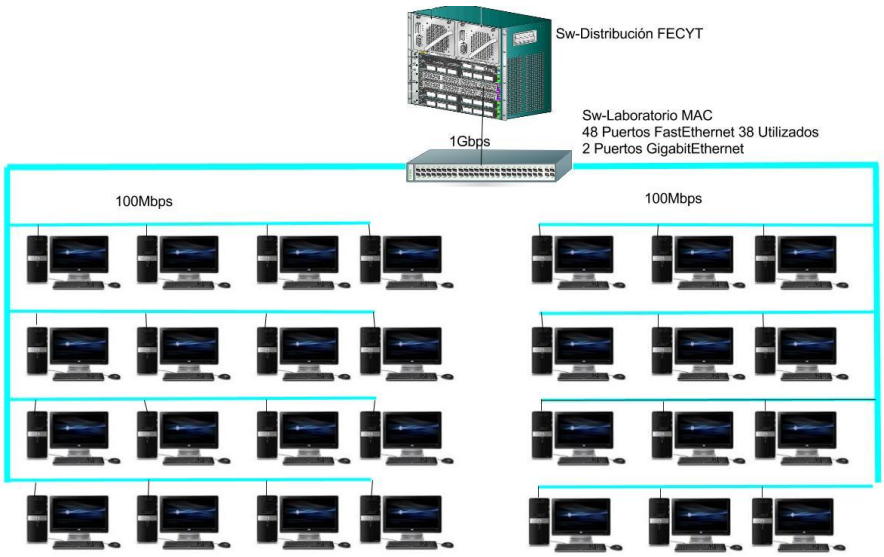


Figura 80. Diagrama de capas 2 Laboratorio MAC FECYT

Fuente: Elaborado por el Autor.

4.5.3 Diseño de capa 3

Esta parte del diseño se detalla cómo fueron creados los segmentos de red de los laboratorios de la FECYT. Estas subredes permiten la comunicación entre segmentos basados en direcciones de Capa 3 o direcciones IP. Por seguridad, el direccionamiento mostrado en esta sección solo hace referencia al último octeto; los primeros tres octetos son representados con letras x,y.

El diseño de la VLAN de Laboratorios de la FECYT tiene definido un esquema de 512 direcciones es decir: x.x.x.0/23. A partir de esta información se procuró crear 8 subredes de 64 direcciones cada una.

El direccionamiento se muestra en la Tabla 39:

Tabla 39: Direccionamiento IP para los Laboratorios FECYT.

VLAN LABORATORIOS FECYT		X.X.X.0/23			
N°	Subred	Máscara	Dir. IP Gateway	Dir. Broadcast	Rango IP Utilizable
1	X.X.X.0/26	255.255.255.192	X.X.X.1/26	X.X.X.63/26	X.X.X.[2-62]
2	X.X.X.64/26	255.255.255.192	X.X.X.65/26	X.X.X.127/26	X.X.X.[66-126]
3	X.X.X.128/26	255.255.255.192	X.X.X.129/26	X.X.X.191/26	X.X.X.[130-190]
4	X.X.X.192/26	255.255.255.192	X.X.X.193/26	X.X.X.255/26	X.X.X.[194-254]
5	X.X.Y.0/26	255.255.255.192	X.X.Y.1/26	X.X.Y.63/26	X.X.Y.[2-62]
6	X.X.Y.64/26	255.255.255.192	X.X.Y.65/26	X.X.Y.127/26	X.X.Y.[66-126]
7	X.X.Y.128/26	255.255.255.192	X.X.Y.129/26	X.X.Y.191/26	X.X.Y.[130-190]
8	X.X.Y.192/26	255.255.255.192	X.X.Y.193/26	X.X.Y.255/26	X.X.Y.[194-254]

Fuente: Elaborado por el autor.

Del direccionamiento antes detallado se utilizaran las subredes de la 2 a 5.

El servidor Firewall-Proxy tendrá 5 interfaces de red, se crearan cuatro interfaces de red virtuales a las cuales se asignarán direcciones IP que actuarán como puertas de enlace de los laboratorios 1,2,3,4 y la restante será la dirección de proxy. Ver Figura 81.

La razón por las que se crearon las interfaces virtuales es para gestionar los laboratorios de manera independiente.

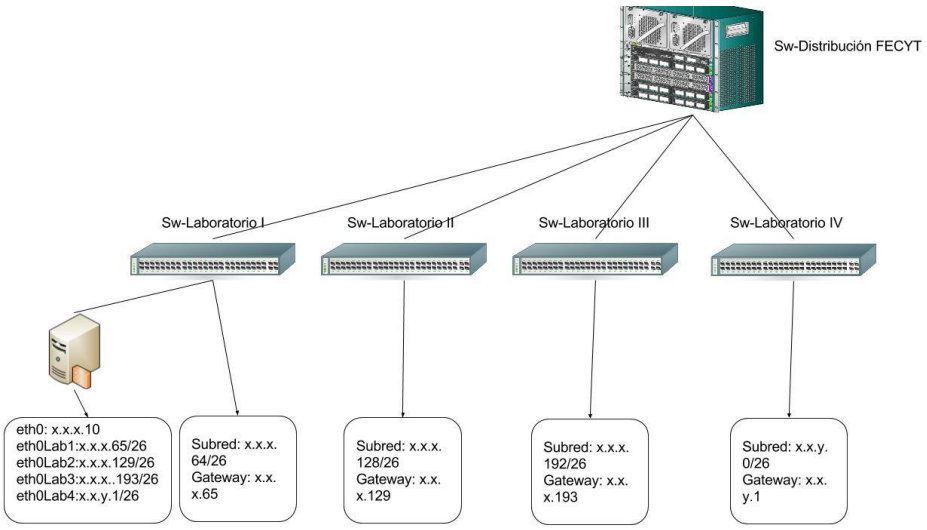


Figura 81. Diagrama de capas 3 Laboratorios FECYT
Fuente: Elaborado por el Autor.

4.6 Facae

4.6.1 Diseño de capa 1

El cableado horizontal de la Facultad de Ciencias Económicas y Administrativas incluye el par trenzado no blindado UTP categoría 6.

4.6.1.1 Diagrama lógico

En este diagrama se muestra la topología de red de la FACAE sin detalles de instalación exacta del cableado. Ver Figura 82.

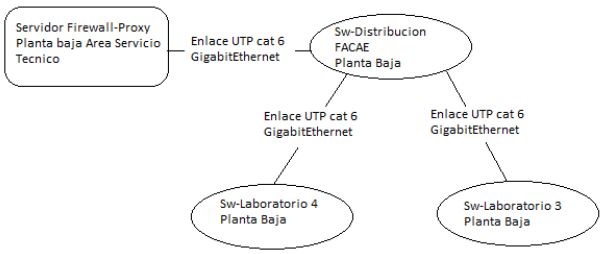


Figura 82. Diagrama Lógico FACAE-UTN
Fuente: Elaborado por el Autor

4.6.2 Diseño de capa 2

En esta sección se detalla cuantos puertos del switch están siendo utilizados y la velocidad en que trabaja cada uno medido en bits por segundo.

El Servidor Firewall se conecta al Switch de distribución

- **Laboratorio 1**

Este laboratorio cuenta con 19 equipos conectado al switch de acceso. Ver Figura 83.

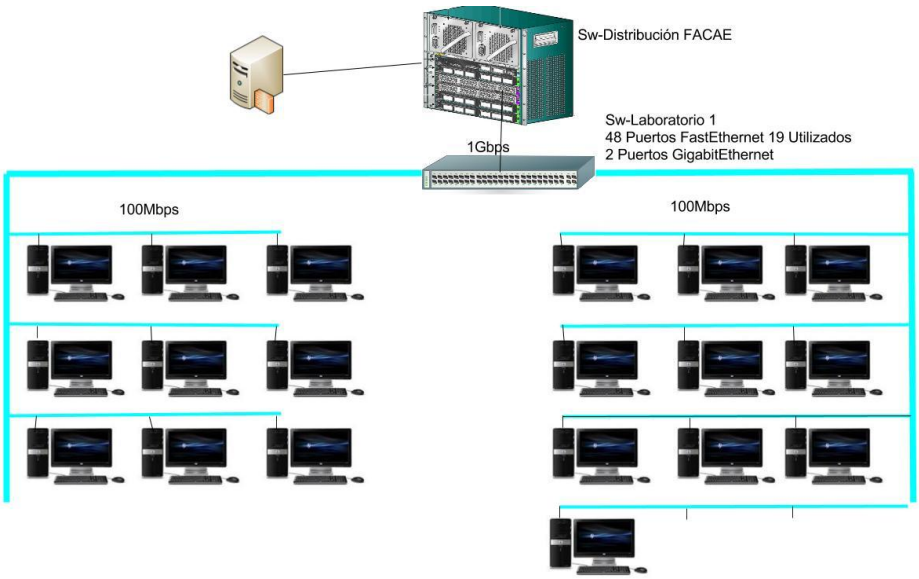


Figura 83. Diagrama de capa 2 Laboratorio I FACAE
Fuente: Elaborado por el Autor.

- **Laboratorio II**

Este laboratorio tiene 35 equipos conectados al switch de acceso como se muestra en la Figura 84.

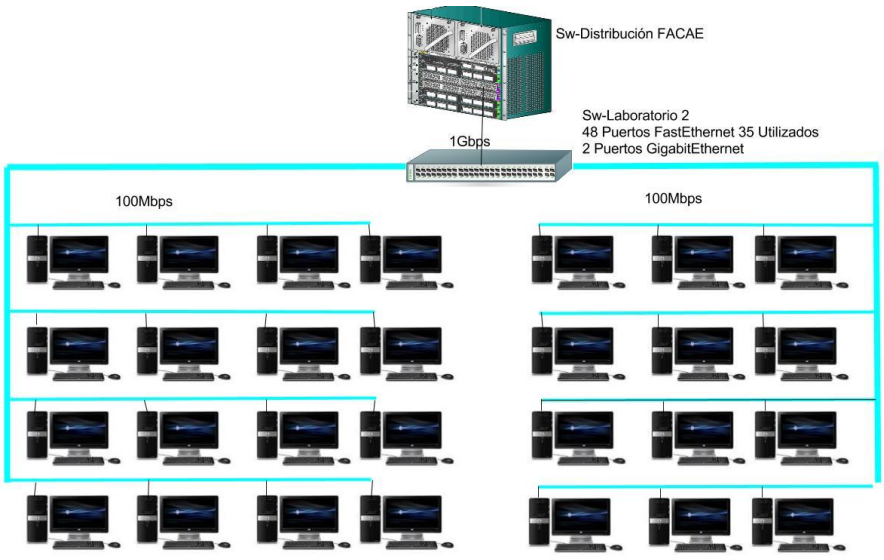


Figura 84. Diagrama de capas 2 Laboratorio 2 FACAE
Fuente: Elaborado por el Autor.

- **Laboratorio III**

Este laboratorio tiene 41 equipos conectados al switch de acceso como se muestra en la Figura 85.

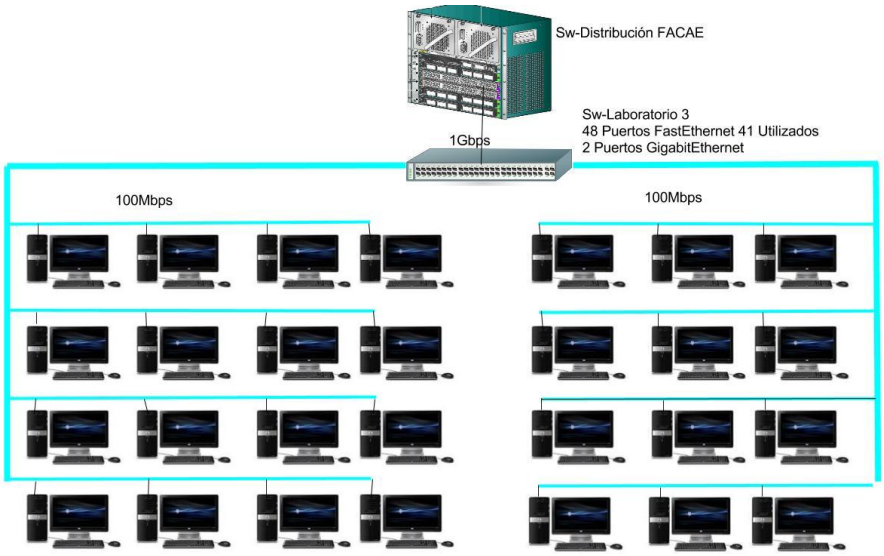


Figura 85. Diagrama de capas 2 Laboratorio III FACAE
Fuente: Elaborado por el Autor.

- **Laboratorio IV**

Este laboratorio tiene 33 equipos conectados al switch de acceso como se muestra en la Figura 86.

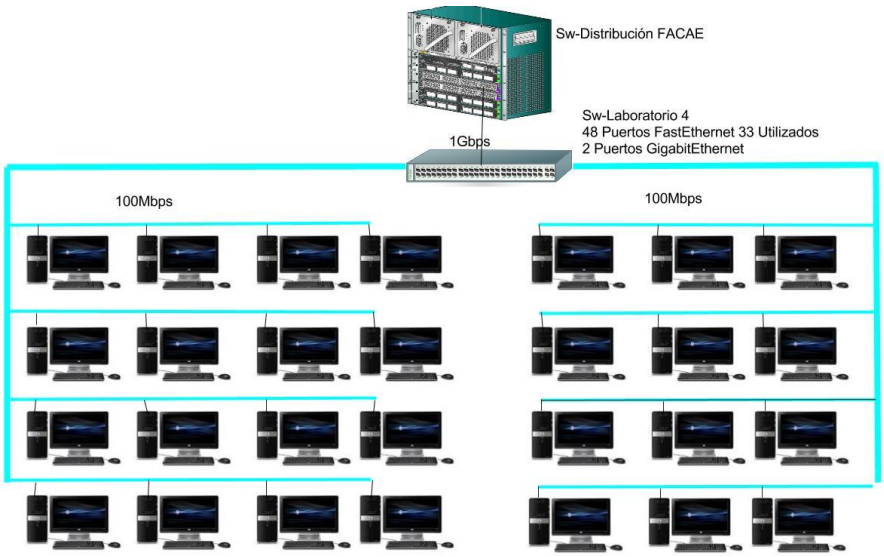


Figura 86. Diagrama de capas 2 Laboratorio IV FACAE
Fuente: Elaborado por el Autor.

4.6.3 Diseño de capa 3

Esta parte del diseño se detalla cómo fueron creados los segmentos de red de los laboratorios de la FACAE. Estas subredes permiten la comunicación entre segmentos basados en direcciones de Capa 3 o direcciones IP. Por seguridad, el direccionamiento mostrado en esta sección solo hace referencia al último octeto; los primeros tres octetos son representados con letras x,y.

El diseño de la VLAN de Laboratorios de la FACE tiene definido un esquema de 512 direcciones es decir: x.x.x.0/23. A partir de esta información se procuró crear 8 subredes de 64 direcciones cada una.

El direccionamiento se muestra en la Tabla 40:

Tabla 40: Direccionamiento IP para los Laboratorios FACAE.

		VLAN LABORATORIOS FACAE	X.X.X.0/23		
N°	Subred	Máscara	Dir. IP Gateway	Dir. Broadcast	Rango IP Utilizable
1	X.X.X.0/26	255.255.255.192	X.X.X.1/26	X.X.X.63/26	X.X.X.[2-62]
2	X.X.X.64/26	255.255.255.192	X.X.X.65/26	X.X.X.127/26	X.X.X.[66-126]
3	X.X.X.128/26	255.255.255.192	X.X.X.129/26	X.X.X.191/26	X.X.X.[130-190]
4	X.X.X.192/26	255.255.255.192	X.X.X.193/26	X.X.X.255/26	X.X.X.[194-254]
5	X.X.Y.0/26	255.255.255.192	X.X.Y.1/26	X.X.Y.63/26	X.X.Y.[2-62]
6	X.X.Y.64/26	255.255.255.192	X.X.Y.65/26	X.X.Y.127/26	X.X.Y.[66-126]
7	X.X.Y.128/26	255.255.255.192	X.X.Y.129/26	X.X.Y.191/26	X.X.Y.[130-190]
8	X.X.Y.192/26	255.255.255.192	X.X.Y.193/26	X.X.Y.255/26	X.X.Y.[194-254]

Fuente: Elaborado por el autor

Del direccionamiento antes detallado se utilizaran las subredes de la 2 a 5.

El servidor Firewall-Proxy tendrá 5 interfaces de red, se crearan cuatro interfaces de red virtuales a las cuales se asignarán direcciones IP que actuarán como puertas de enlace de los laboratorios 1,2,3,4 y la restante será la dirección de proxy. Ver Figura 87.

La razón por las que se crearon las interfaces virtuales es para gestionar los laboratorios de manera independiente.

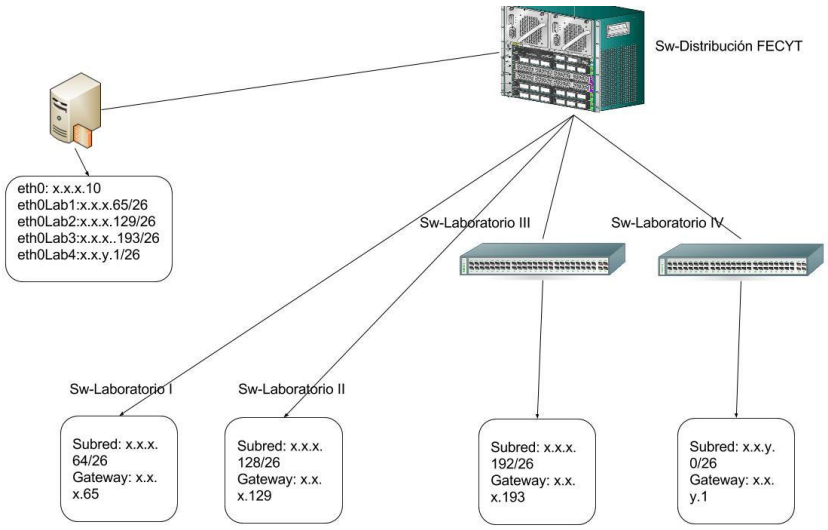


Figura 87. Diagrama de capas 3 Laboratorios FACAE
Fuente: Elaborado por el Autor.

4.7 Análisis de Encuesta y entrevistas

Para definir las políticas y reglas que serán asignadas al Firewall-Proxy se realizó una entrevista al Administrador de la red de datos de la Universidad Técnica del Norte de igual manera a los jefes de laboratorios de cada una de las facultades y respaldando algunas de las preguntas en encuestas realizadas dando como resultado lo siguiente. El Modelo de la Encuesta realizada se puede apreciar en el Anexo 3.

- **¿Cuenta con un sistema que impida tráfico malicioso que se genera por el uso de los equipos en los laboratorios?**

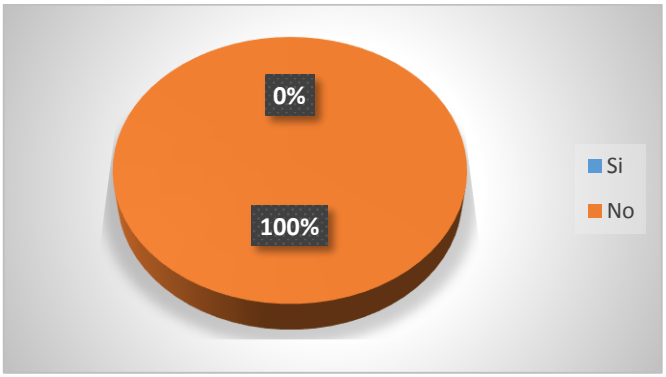


Figura 88. Grafica Respuesta Encuesta Pregunta 1.
Fuente: Elaborado por el Autor.

La Figura 88 nos da como resultado que ningún laboratorio cuenta con un sistema que impida tráfico malicioso que puede ser generado por el uso de los laboratorios.

- **¿Gestiona el acceso a Internet relacionado con sitios web maliciosos?**

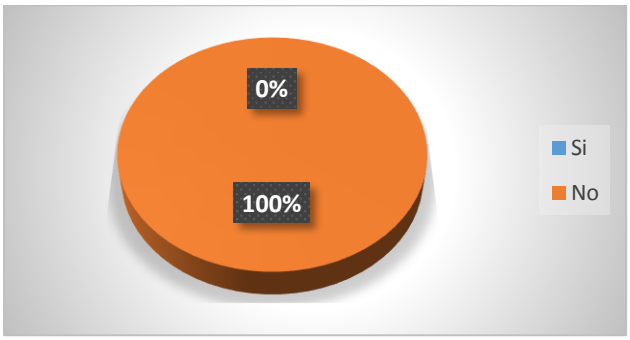


Figura 89. Grafica Respuesta Encuesta Pregunta 2.
Fuente: Elaborado por el Autor.

La figura 89 nos muestra que ningún administrador de laboratorios gestiona el acceso a internet, por lo que el sistema es una gran alternativa para implementar y que permite gestionar el acceso a sitos web.

- **De la siguiente lista ¿qué tipo de sitios web restringiría?**

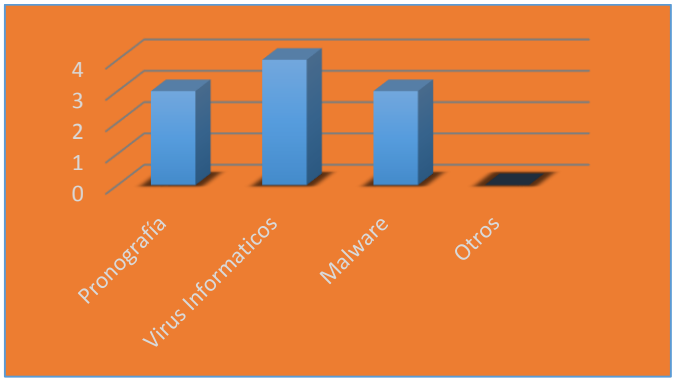


Figura 90.Grafica Respuesta Encuesta Pregunta 3.
Fuente: Elaborado por el Autor.

La Figura 90 nos revela que 4 de las cinco personas encuestadas restringirían sitios Web relacionados con pornografía, y que las 5 personas evitarían el acceso a sitios Web relacionados con Virus informáticos.

- **¿Evitaría las actualizaciones Automáticas de Windows?**

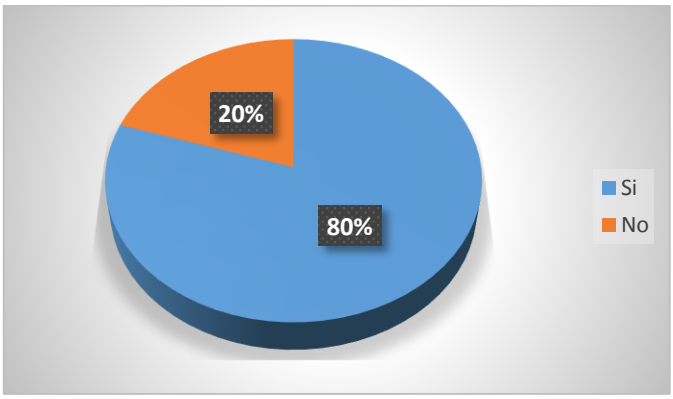


Figura 91.Grafica Respuesta Encuesta Pregunta 4.
Fuente: Elaborado por el Autor.

La Figura 91 muestra que el 80% de los encuestados evitaría las actualizaciones automáticas de Windows.

- **¿Registra la actividad de los usuarios de los equipos de cómputo de los laboratorios?**

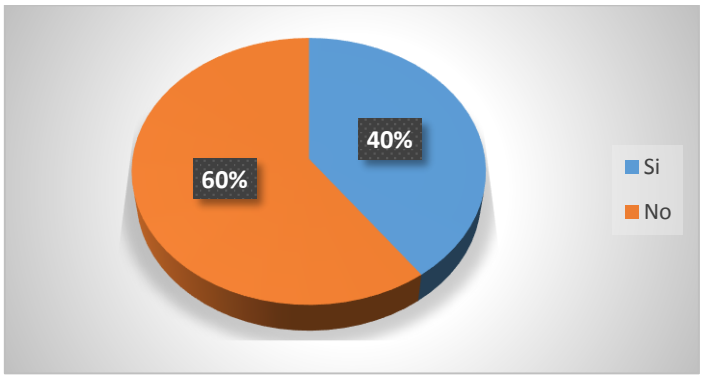


Figura 92.Grafica Respuesta Encuesta Pregunta 5.
Fuente: Elaborado por el Autor.

La Figura 92 nos muestra que 2 de los 5 jefes de laboratorio registra la actividad de los usuarios de los equipos de cómputo mientras que el resto no registra la actividad de los usuarios

.

- **¿Restringiría el acceso al servicio de internet, si en algún horario se lo requiere?**

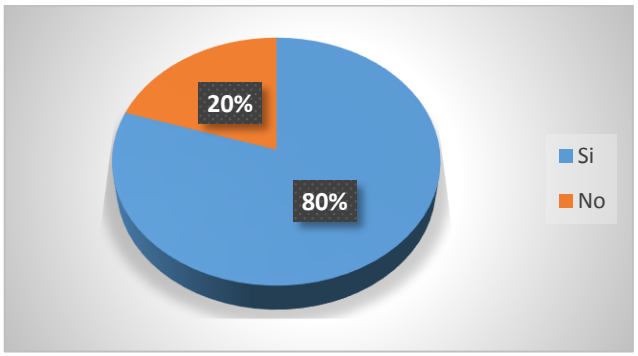


Figura 93.Grafica Respuesta Encuesta Pregunta 6.
Fuente: Elaborado por el Autor.

La figura 93 demuestra que la mayoría de jefes de laboratorios específicamente 4 está de acuerdo en restringir el acceso a internet si en algún horario se lo requiere.

- **En los horarios que no se usan los laboratorios ¿evitaría generar tráfico en la red?**

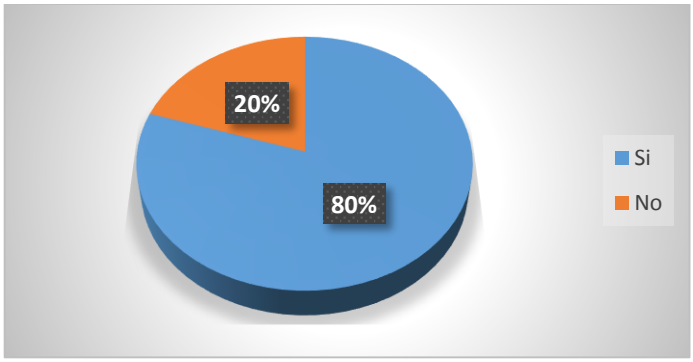


Figura 94.Grafica Respuesta Encuesta Pregunta 7.
Fuente: Elaborado por el Autor.

La figura 94 demuestra que la mayoría de jefes de laboratorios específicamente 4 está de acuerdo en evitar tráfico en la red en los horarios que no se usan los laboratorios.

- **De la siguiente lista ¿qué servicios ofrece los laboratorios de cómputo?**

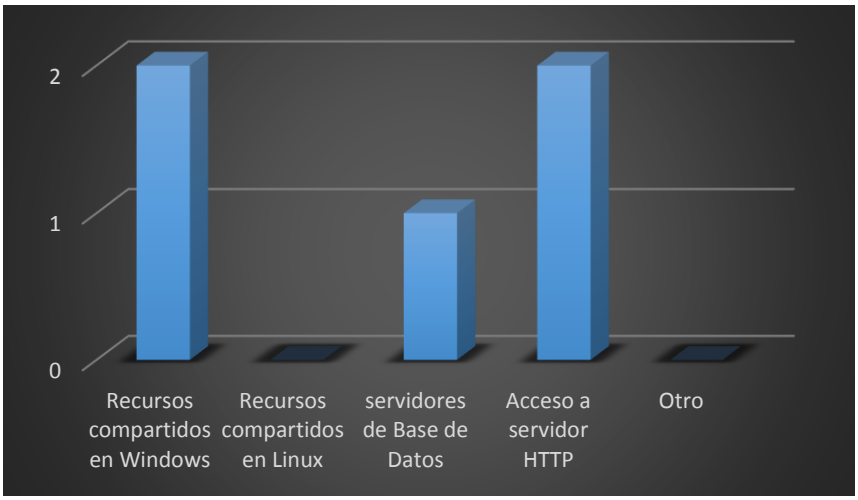


Figura 95.Grafica Respuesta Encuesta Pregunta 8.
Fuente: Elaborado por el Autor.

La Figura 95 nos revela que dos Facultades acceden a Recursos compartidos en Windows, una facultad tiene acceso a un servido de base de datos y dos facultades tienen acceso a servido HTTP.

- **¿En qué medida esta Ud. interesado en gestionar el acceso al servicio de Internet de los laboratorios?**

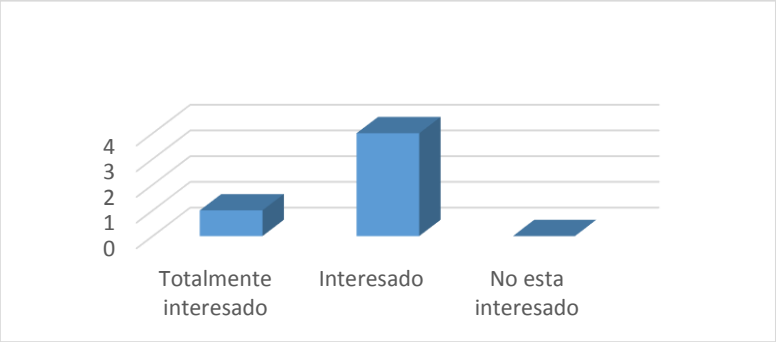


Figura 96.Grafica Respuesta Encuesta Pregunta 9.
Fuente: Elaborado por el Autor.

La Figura 96 muestra que en una facultad se encuentran totalmente interesados en gestionar el acceso a internet mientras que en las demás facultades se encuentran interesadas lo que demuestra que el proyecto se sustenta para su diseño e implementación.

4.8 Políticas de uso de la red de datos

INFORMACIÓN	
Políticas de acceso a recursos y servicio de Internet.	V. 1.0
Autor: Galo Espinosa.	
Aprobado por: Ing. Carlos Vásquez	
I. INTRODUCCION	

Las Facultades de la Universidad Técnica del Norte proporcionan a sus estudiantes recursos informáticos, servicios de acceso a la red de datos y de acceso a Internet para su utilización en actividades de investigación, desarrollo e innovación de proyectos académicos. Por otro lado, es de conocimiento que existen diversos sitios web alojados en la Internet pudiendo acertar en sitios de uso comercial, redes sociales entre otros.

En los institutos educativos, el uso de los recursos debe ser racional y apuntando siempre al buen servicio, dando prioridad a procesos que permiten llevar a cabo la función para la cual la institución fue establecida.

El propósito de esta Política es establecer normas para optimizar y facilitar el uso del servicio de acceso a Internet en las Facultades de la Universidad Técnica del Norte., tomando en consideración una entrevista realizada al administrador de la red de datos, el análisis de la situación de la red de datos, el reglamento de uso de laboratorios en vigencia, el reporte de análisis de tráfico generado por la herramienta EXINDA y analizando los resultados de una encuesta expuesta a los jefes de Laboratorios.

II. OBJETIVO

Definir normas informativas a los usuarios de la red de datos sobre uso y restricciones a recursos de la red de datos y acceso a servicio de Internet.

III. ALCANCE

Se aplica a todos los usuarios con acceso a Internet y servicios relacionados.

IV. RESPONSABILIDADES

A. DIRECCION DE DESARROLLO TECNOLOGICO E INFORMATICO (DDTI) UTN.

Proveer el servicio de Internet a las Facultades de la Universidad Técnica del Norte.

Bloquear cualquier tráfico no autorizado que dificulte la libre circulación de información útil para la universidad

B. SERVICIO TÉCNICO DE LABORATORIOS

Reportar los incumplimientos del presente reglamento que se detecte.

Controlar la navegación hacia internet de los usuarios de los laboratorios de cómputo.

V. POLITICAS Y DIRECTRICES

A. Aspectos Generales

Art1.- La presente Política, es aplicable para los usuarios que utilicen los servicios de acceso a recursos de la red de datos e Internet.

Art2.- El jefe de laboratorios y administradores de la red de datos serán los encargados de disponer la presente política, velar por su cumplimiento y aplicabilidad, así como de modificarlo y actualizarla en el caso de ser necesario.

Art3.- que esta política, será aplicable a todos los usuarios de los laboratorios de computación y red de acceso inalámbrico que pertenezcan a las facultades de la Universidad Técnica del Norte, así como quienes hagan uso de los recursos de la red, incluyendo ciudadanía en general.

B. Conectividad a los servicios de Laboratorios

Art4.- Se permite el acceso a los recursos compartidos de Windows que disponen los Laboratorios de Computo.

Art5.- Se permite el acceso a servidores de Base de Datos que disponen los laboratorios de Cómputo.

Art6.- Se permite el acceso a servidor HTTP que disponen los Laboratorios.

Art7.- Desde el Firewall se habilitaran los puertos necesarios por cada uno de los servicios que deponga los Laboratorios.

C. Conectividad a los servicios de red Inalámbrica

Art8. El servicio de acceso a la Red Inalámbrica será proporcionado a los usuarios de la comunidad universitaria de forma gratuita.

Art9. El encargado de la gestión de la red inalámbrica activara el acceso al servicio.

D. Uso del Firewall-Proxy

Art10.- El servidor debe ser administrado por el personal capacitado.

Art11.- El acceso a la administración del Servidor es restringido y exclusivo de quien lo administra.

Art12.- El acceso a la administración del servidor será vía Web mediante la herramienta de configuración de sistemas WEBMIN o por medio de un intérprete de ordenes SSH.

E. Conectividad al servidor Firewall-Proxy

Art13.- Los equipos de cómputo deben ser direccionados al Servidor Firewall-Proxy.

Art14.- El firewall será quien se encargue de gestionar tráfico relacionado con Sitios Web Maliciosos.

Art15.- Evitar actualizaciones automáticas de Windows.

Art16.- Gestionar horarios para el acceso al servicio de Internet.

Art17.- Desde el Firewall se habilitaran los puertos necesarios por cada uno de los servicios.

F. Conectividad al servicio de Internet

Art18.- El servicio de acceso a Internet es gratuito y exclusivo de los estudiantes, docentes y personal administrativo de la Institución.

Art19.- El servicio a Internet es exclusivo para actividades de investigación, desarrollo e innovación de proyectos académicos que apoyen y mejoren las funciones de los usuarios.

Art20.- El uso de Internet podrá ser registrado de tal forma que sirva como antecedente ante una investigación.

Art21.- Por razones de buen servicio la Dirección de Desarrollo Tecnología e Informático UTN, o le departamento del área técnica de Laboratorios de Computo tiene la facultad de filtrar cualquier tipo de contenido NO útil para la Institución.

Art22.- Cada usuario deberá responsabilizarse por el buen uso de los equipos de cómputo.

4.9 Políticas y reglas asignadas al Firewall Linux.

El Firewall trabaja en la capa de red y capa transporte tomando de referencia la arquitectura de red TCP/IP. En Linux la gestión del Firewall se desarrolla por medio de reglas iptables.

Para definir políticas y reglas del servidor Firewall-Proxy se toma en cuenta la arquitectura que manejan las iptables en LINUX.

Iptables en Linux está conformada por tablas y cadenas:

- Tablas: filter, nat y mangle

En el diseño del firewall se hace referencia exclusiva a la tabla filter que se encarga del filtrado del tráfico la cual presenta las siguientes cadenas: Input, Output, Forward.

- **INPUT**

Son todos los paquetes de la LAN destinados al Firewall, los paquetes tienen dirección IP destino la dirección del Firewall. Ver Figura 72.

- **OUTPUT**

Hace referencia a los paquetes que salen exclusivamente del Firewall hacia cualquier destino, estos paquetes tienen IP origen la dirección del Firewall. Ver Figura 72.

- **FORWARD**

Hace referencia a los paquetes que pasan por el Firewall pero no están destinados al Firewall. Ver Figura 97.

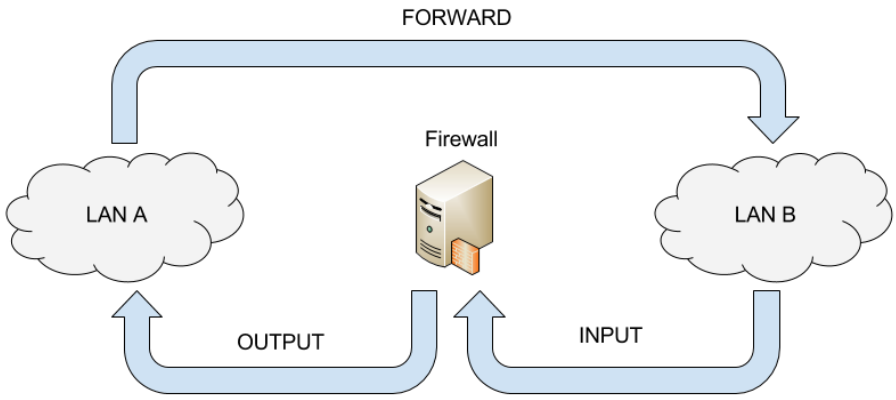


Figura 97. Arquitectura Iptables-LINUX
Fuente: Elaborado por el Autor.

4.9.1 Reglas asignadas Al Firewall

- Las políticas del firewall por defecto estarán establecidas para denegar todo tipo de tráfico ya sea Input, Output o Forward.
- Se habilitan todas las conexiones Establecidas y relacionadas.

Las políticas antes dispuestas hacen que sea necesario implementar reglas para el tráfico de paquetes ya sea Input, Output o Forward.

- **INPUT**
    - Se permite tráfico de interfaz de Loopback.
    - Se deniega tráfico que tenga origen en una BOTNET.
    - Se acepta tráfico que tenga destino al puerto que usa Webmin de nuestro servidor.
    - Se acepta tráfico con destino al puerto SSH de nuestro servidor.

- Se acepta tráfico ICMP que tenga origen en la VLAN de laboratorios.
- Se acepta todo tráfico que tenga origen en la VLAN de laboratorios con destino al puerto de proxy.

- **OUTPUT**
  - Se permite tráfico de interfaz de Loopback.
  - Se deniega tráfico a una BOTNET.

- **FORWARD**
  - Se deniega tráfico a una BOTNET.
  - Se permite consultas de servidor DNS con origen en la VLAN de Laboratorios.
  - Se permite el tráfico con destino a Servidor de Archivos Windows de los Laboratorios.

4.10 Implementación en la Fica

La implementación del Firewall inicia con la instalación del Sistema Operativo, el proceso de instalación se puede apreciar en el Anexo 1, para el desarrollo del proyecto se seleccionó CentOs 6.8 con los requerimientos antes analizados. Ver Figura 98.

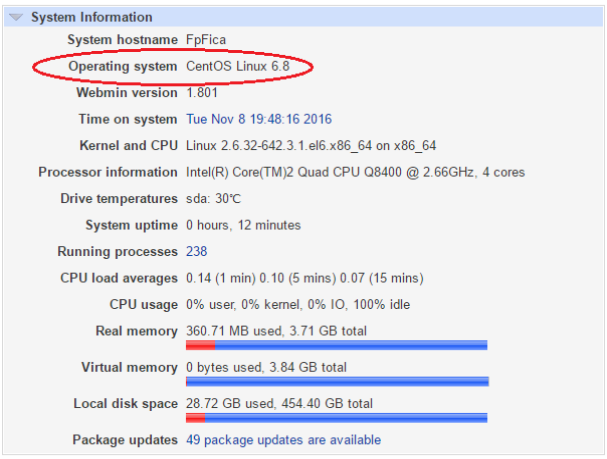


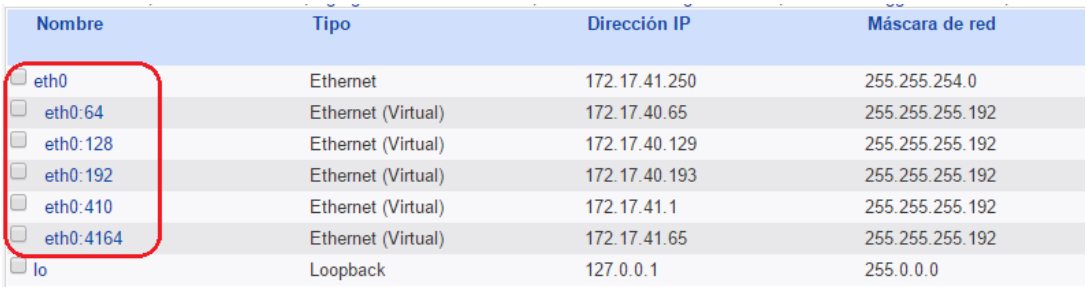
Figura 98.Versión Linux Instalada
Fuente: Servicio Webmin.

4.10.1 Implementación de VLAN's

Son todas las interfaces instaladas en el servidor y que se configurarán para la implementación de las reglas de seguridad en el Firewall de la Facultad, el proceso de instalación se observa en el Anexo 1, y el proceso de configuración se aprecia en el Anexo 2 del presente documento, se necesita una interfaz física Ethernet 10/100/1000 y siete interfaces virtuales que servirán como Gateway para los laboratorios, se encuentran distribuidas de la siguiente manera, ver Figura 99.

- eth0: Interfaz física.
- eth0:64 Interfaz virtual que sirve de puerta de enlace para Laboratorio 1.eth0:128 Interfaz virtual que sirve de puerta de enlace para Laboratorio 2
- eth0:192 Interfaz virtual que sirve de puerta de enlace para Laboratorio 3
- eth0:410 Interfaz virtual que sirve de puerta de enlace para Laboratorio 4
- eth0:4164 Interfaz virtual que sirve de puerta de enlace para Laboratorio 5
- eth0:41128 Interfaz virtual que sirve de puerta de enlace para Laboratorio 6

- eth0:41192 Interfaz virtual que sirve de puerta de enlace para Laboratorio 7



Nombre	Tipo	Dirección IP	Máscara de red
eth0	Ethernet	172.17.41.250	255.255.254.0
eth0:64	Ethernet (Virtual)	172.17.40.65	255.255.255.192
eth0:128	Ethernet (Virtual)	172.17.40.129	255.255.255.192
eth0:192	Ethernet (Virtual)	172.17.40.193	255.255.255.192
eth0:410	Ethernet (Virtual)	172.17.41.1	255.255.255.192
eth0:4164	Ethernet (Virtual)	172.17.41.65	255.255.255.192
lo	Loopback	127.0.0.1	255.0.0.0

Figura 99. Interfaces de red configuradas en Webmin

Fuente: Servicio Webmin.

4.10.2 Políticas y reglas iptables

La lista de reglas asignadas se puede ver en la Figura 100. El proceso de configuración se muestra en el Anexo2.

Las políticas se orientan en denegar todo tráfico Input, Output y Forward.

- iptables -P INPUT DROP
- iptables -P OUTPUT DROP
- iptables -P FORWARD DROP

Input

- Se aceptan todo tráfico que se origina en la interfaz de loopback, esto permite procesar tareas que se originan en el sistema.
  - iptables -A INPUT -i lo -j ACCEPT
- Se acepta tráfico que sea relacionado y establecido, esto permite el tránsito de datos que sea peticionado por los clientes de los laboratorios.

    - iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
- Se permite tráfico con destino al puerto SSH.
    - iptables -A INPUT -p tcp --dport 22 -j ACCEPT
- Se permite el tráfico a Webmin.
    - iptables -A INPUT -p tcp --dport 10000 -j ACCEPT
- Se permite tráfico ICMP
    - iptables -A INPUT -s $SUBREDLABS -p icmp -j ACCEPT
- Se Acepta tráfico entrante por el puerto 80 ya sea udp o tcp
    - iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
    - iptables -A INPUT -p udp -m state --state NEW --dport 80 -j ACCEPT
    - iptables -A INPUT -p tcp -m state --state NEW --dport 80 -j ACCEPT
- Se acepta trafico que este direccionado al puerto del proxy
    - iptables -A INPUT -s $SUBREDLABS -p tcp --dport 3128 -j ACCEPT

Output

- Se permite todo tráfico Loopback
    - iptables -A OUTPUT -o lo -j ACCEPT
- Se permite todo tráfico establecido
    - iptables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT

Forward

- Se permite el tráfico Relacionado y establecido
    - iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

- Se permite tráfico SSH.
    - iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
- Se permite tráfico destinado al servidor de archivos.
    - iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 139 -j ACCEPT
    - iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 445 -j ACCEPT
    - iptables -A FORWARD -s $SUBREDLABS -p udp --dport 137 -j ACCEPT
    - iptables -A FORWARD -s $SUBREDLABS -p udp --dport 138 -j ACCEPT
- Se permite consultas de servidor DNS con origen en la VLAN de Laboratorios.
    - iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
    - iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT

```
[root@FpFica ~]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ndmp
ACCEPT     icmp --  172.17.40.0/23       anywhere
ACCEPT     udp  --  anywhere             anywhere             state NEW udp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:http
ACCEPT     tcp  --  172.17.40.0/23       anywhere             tcp dpt:squid
ACCEPT     udp  --  172.17.40.0/23       anywhere             state NEW udp spts:bootps:bootpc dpts:bootps:bootpc
DROP       udp  --  anywhere             anywhere             udp spts:bootps:bootpc dpts:bootps:bootpc
ACCEPT     tcp  --  172.17.40.0/23       anywhere             state NEW tcp dpt:domain
ACCEPT     udp  --  172.17.40.0/23       anywhere             state NEW udp dpt:domain
DROP       tcp  --  anywhere             anywhere             tcp dpt:domain
DROP       udp  --  anywhere             anywhere             udp dpt:domain

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  172.17.40.0/23       anywhere             tcp dpt:netbios-ssn
ACCEPT     tcp  --  172.17.40.0/23       anywhere             tcp dpt:microsoft-ds
ACCEPT     udp  --  172.17.40.0/23       anywhere             udp dpt:netbios-ns
ACCEPT     udp  --  172.17.40.0/23       anywhere             udp dpt:netbios-dgm
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             state NEW,ESTABLISHED
```

Figura 100. Reglas implementadas Firewall-Proxy
Fuente: Servicio Terminal Linux.

4.10.3 Reglas Proxy

Para implementar las reglas en el Proxy hay que establecer los puertos y trabajo en red en la que va actuar el servidor. Para ello en la Figura 62 se muestra la dirección ip de proxy el puerto de comunicación. Todo el proceso de configuración se muestra en el Anexo 2.

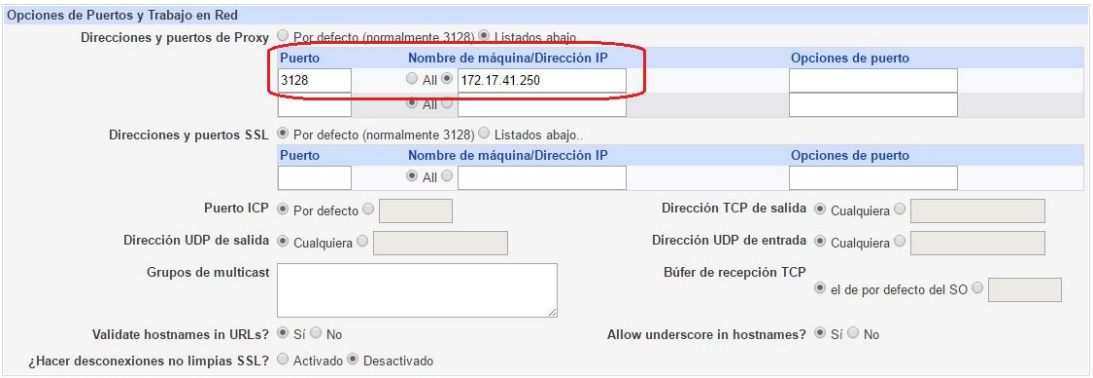


Figura 101. Dirección y Puerto de Comunicación de Proxy

Fuente: Servicio Webmin.

4.10.3.1 Control de Acceso

Se han implementado seis listas de control de acceso cada una de estas representa la VLAN de cada laboratorio como se muestra en la Figura 102, y una que representa a todo el segmento de red de los laboratorios.

La razón por la que se segmento la red de laboratorios es para gestionar de manera independiente cada VLAN de laboratorio.

Nombre	Tipo	Coincidiendo con...
manager	Protocolo URL	cache_object
localhost	Dirección de Cliente	127.0.0.1/32 ::1
to_localhost	Dirección de Servidor Web	127.0.0.0/8 0.0.0.0/32 ::1
SUBREDLAB1	Dirección de Cliente	172.17.40.64/26
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	591
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT
SUBREDLAB2	Dirección de Cliente	172.17.40.128/26
SUBREDLAB3	Dirección de Cliente	172.17.40.192/26
SUBREDLAB4	Dirección de Cliente	172.17.41.0/26
SUBREDLAB7	Dirección de Cliente	172.17.41.64/26
Restringidos	Expresión Regular URL	-i facebook
LABS	Dirección de Cliente	172.17.40.0/23
snmppublic	Comunidad SNMP	public

Figura 102. Listas de control de acceso Proxy

Fuente: Servicio Webmin.

4.10.3.2 Fecha y Hora

Para definir hora y fecha como control de acceso de cada laboratorio hay que crea nuevas listas como se muestra en la Figura 64.

Figura 103. Listas de control de acceso Proxy-Horarios
Fuente: Servicio Webmin.

4.11 Pruebas de funcionamiento en la Fica

Las pruebas de funcionamiento se realizaron en un laboratorio de la Facultad de Ingeniería en Ciencias Aplicadas una vez implementado del servidor Firewall-Proxy.

4.11.1 Prueba de implementación de VLAN´s

Para esta prueba se hace uso del intérprete de comandos cmd de un cliente Windows que direcciona el tráfico hacia el servidor, como se puede observar en la Figura 104 el cliente tiene asignado una dirección ip perteneciente a la VLAN de laboratorio 4 y su Gateway es la interfaz virtual del servidor.

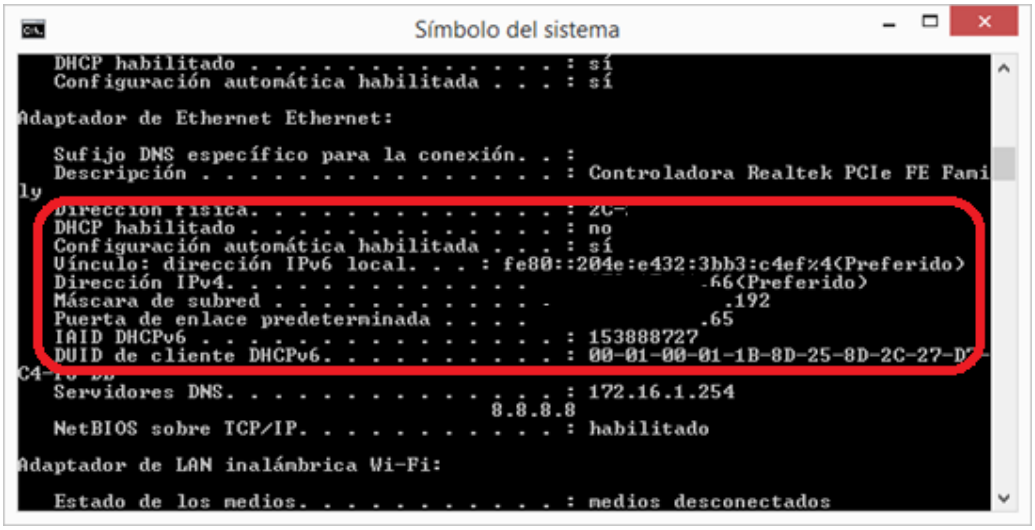


Figura 104. Parámetros configurados en cliente perteneciente a VLAN de Laboratorio 4
Fuente: Servicio CMD Windows.

Se puede demostrar que tiene conectividad, mediante el comando ping, hacia los otros equipos pertenecientes a otras redes, en el caso se hace una prueba de conectividad desde un equipo que esta direccionando su tráfico al servidor Firewall Proxy que se encuentra ubicado en uno de los laboratorios, hacia un equipo que pertenece a otra VLAN como se muestra en la Figura 105.

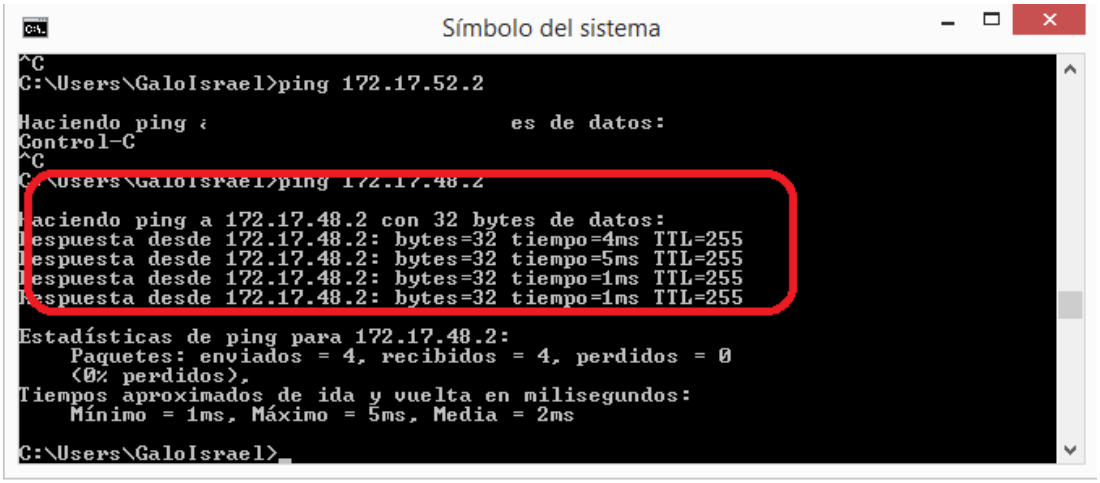


Figura 105.Prueba de conectividad mediante el comando ping.
Fuente: Servicio CMD Windows.

4.11.2 Políticas y reglas iptables

Se demuestran el funcionamiento de las reglas asignadas al Firewall

- Se permite tráfico con destino al puerto SSH, en el caso necesitamos una interfaz para acceder vía SSH al servidor Firewall-Proxy y configuramos los parámetros solicitados con dirección IP y puerto por el cual se comunica. En la Figura 106 se puede apreciar el acceso a nuestro servidor vía SSH por medio de un intérprete de comandos.

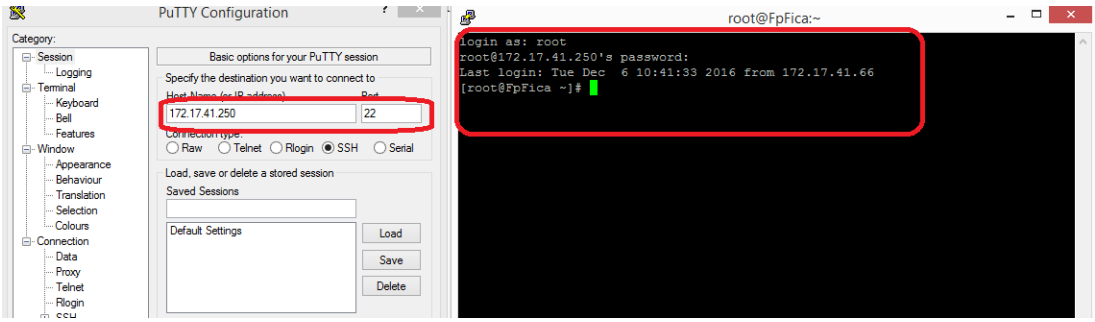


Figura 106.Acceso Vía SSH al Servidor Firewall-Proxy
Fuente: Servicio Putty.

- Se permite el tráfico a Webmin. Para esta prueba se necesita de un navegador Web, en la barra de direcciones escribimos la dirección IP de nuestro servidor, y se puede apreciar la comunicación de la comunicación. Ver Figura 107.

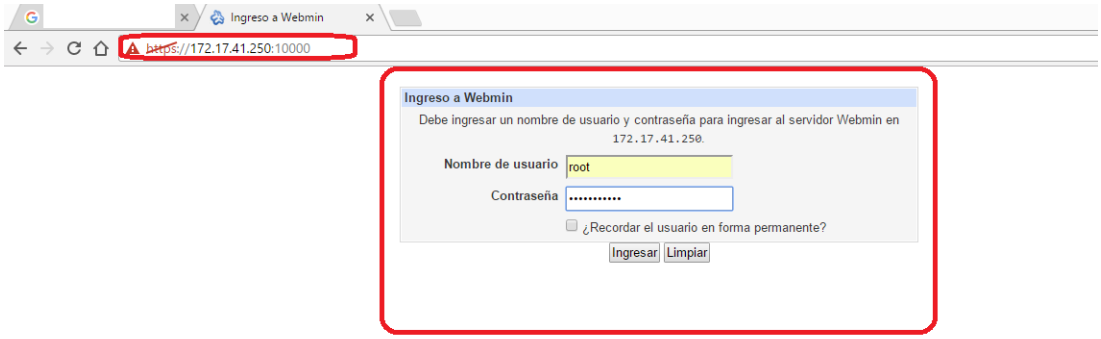


Figura 107. Acceso Vía Web al Servidor Firewall-Proxy
Fuente: Servicio Chrome.

- Se permite tráfico ICMP. En la figura 108 se muestra que se puede realizar una prueba de conectividad, mediante el comando ping, desde un equipo ubicado en un laboratorio hacia el servidor de google.

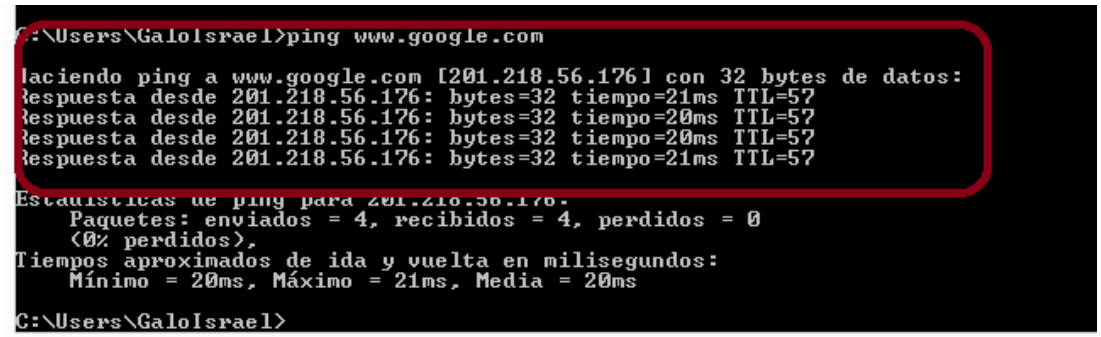


Figura 108.Trafico
Fuente: Servicio CMD Windows.

- Todo tráfico http esta direccionado al puerto del proxy

En la Figura 109 se puede verificar que se hace una petición al sitio Web Facebook pero la respuesta siempre la hace el servidor Firewall-Proxy implementado.

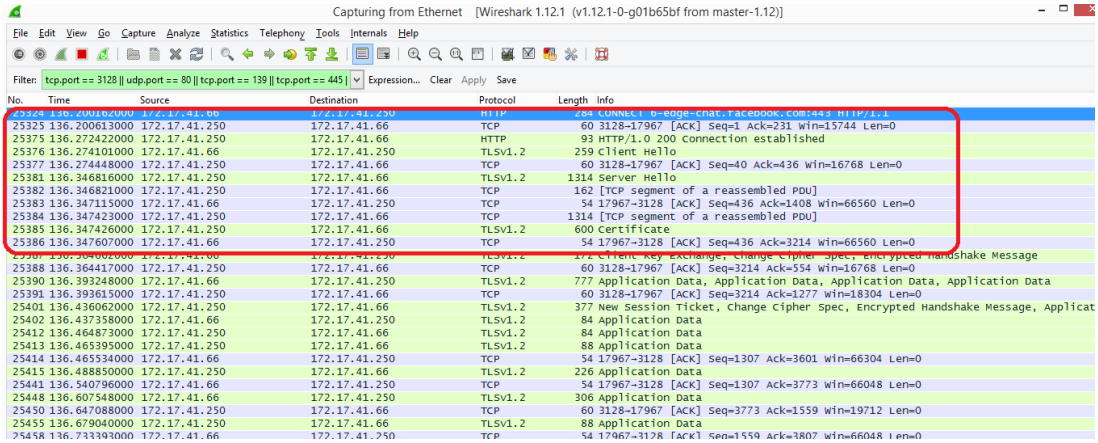


Figura 109.Trafico que responde el Proxy
Fuente: Servicio Wireshark

4.11.3 Reglas Proxy

El proxy está configurado para que trabaje con una determinada dirección IP y un puerto especifico. Ver Figura 110.

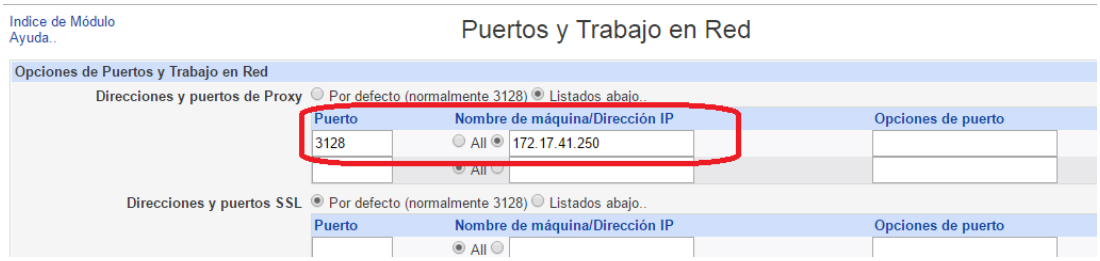


Figura 110. Puertos y trabajo en Red Webmin
Fuente: Servicio Webmin

4.11.4.1 Control de Acceso

Se asigna una lista de control de acceso una por cada VLAN de laboratorio, esto permite gestionar el acceso al servicio de internet de manera independiente. La configuración se muestra en el Anexo 2. Ver Figura 111.

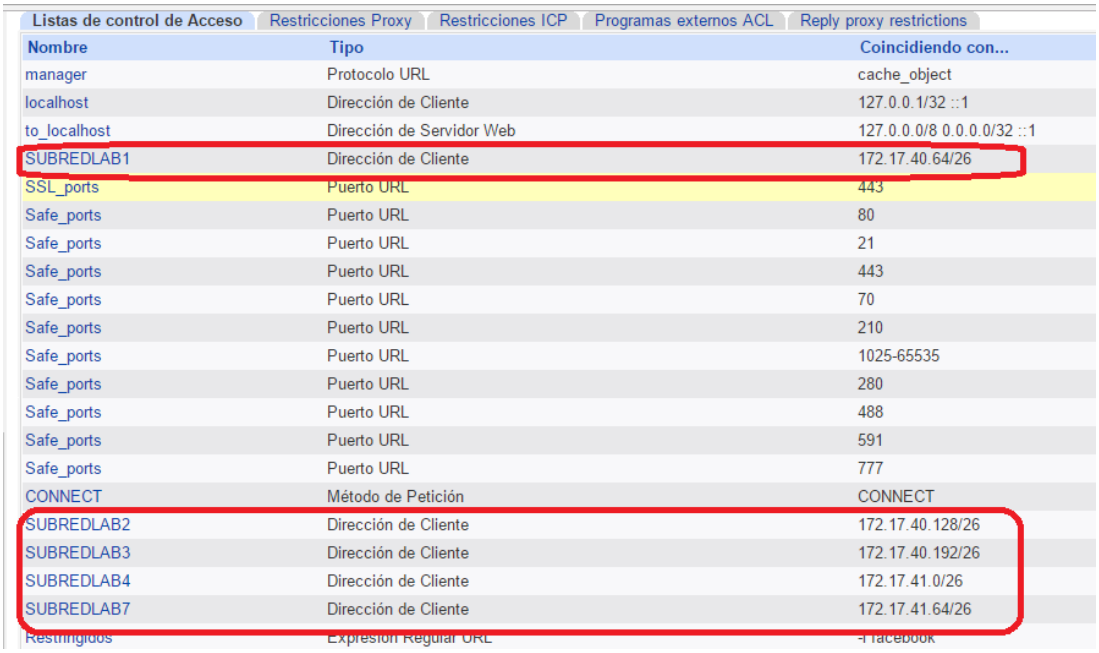


Figura 111. Lista Control de Acceso Webmin
Fuente: Servicio Webmin

4.11.4.2 Fecha y Hora

Se creó una lista de control de acceso en el que se gestiona un horario para permitir o denegar al acceso al servicio de internet. Ver Figura 112.

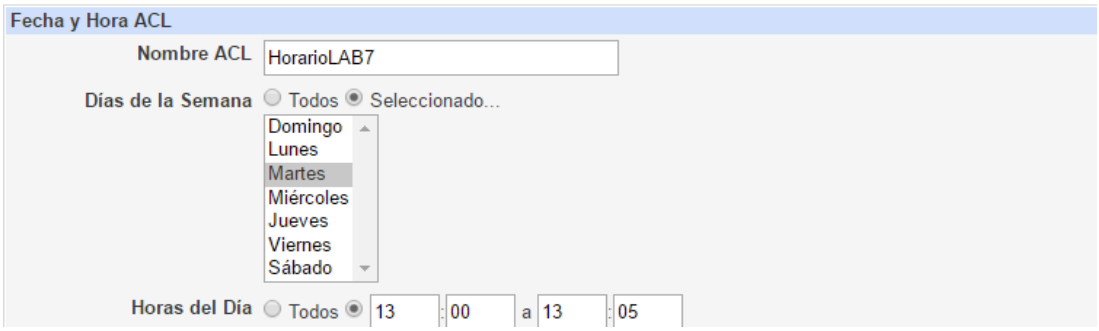


Figura 112. Lista Control de Acceso Webmin Horario
Fuente: Servicio Webmin

4.11.4.3 Comprobación de las listas de control de acceso

Para la comprobación de las restricciones se empleó una regla donde se deniegue el acceso a internet en horario del día martes de 12:40 a 12:45 pm para el Laboratorio 7 ver Figura 107.

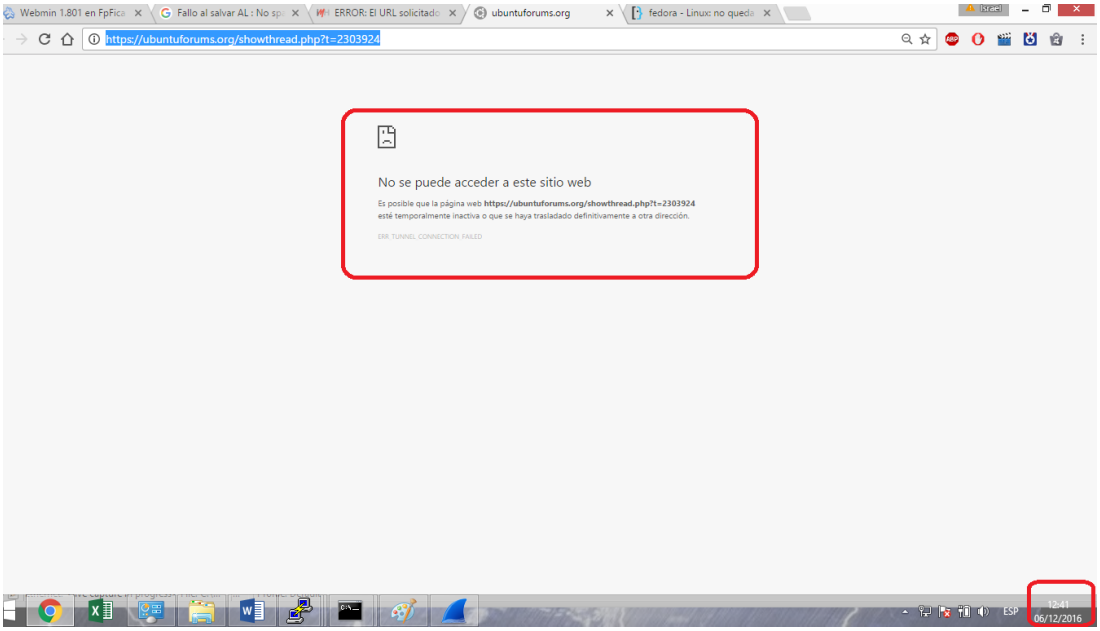


Figura 113.Restricción de Acceso Webmin Horario
Fuente: Servicio Webmin

4.11.5 Tiempos de Acceso

Se puede comprobar que los tiempos de acceso se reducen debido al uso del servidor proxy.

El método de prueba se presenta mediante la carga de un sitio web sin el direccionamiento hacia el proxy y otra con direccionamiento al servidor.

En la figura 113 se muestra la carga de un sitio Web sin el direccionamiento al Proxy. El tiempo de respuesta es de 2.51 segundos.

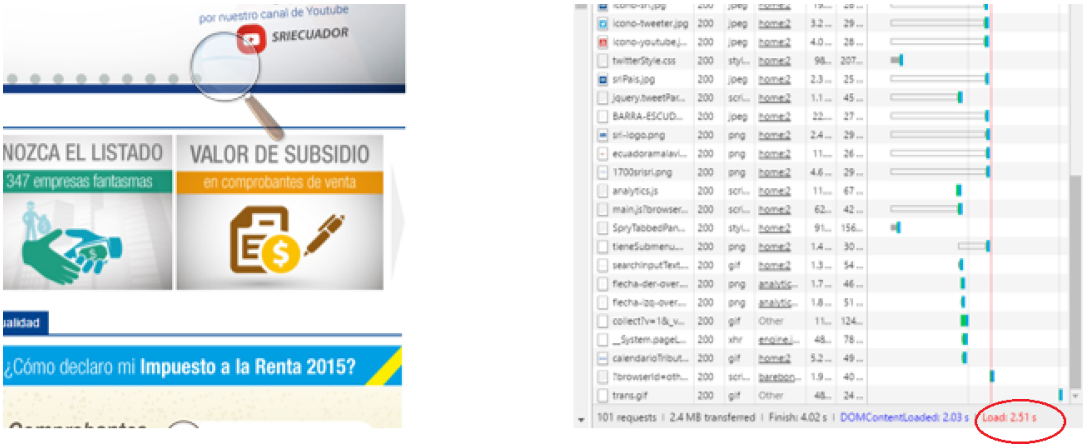


Figura 114. Tiempo de respuesta de un Sitio web sin el direccionamiento de Proxy.

Fuente: Servicio Chrome.

En la figura 115 se muestra la carga de un sitio web y se puede verificar el tiempo de respuesta es menor. El tiempo de respuesta que se muestra es de 2.01 segundos.

Figura 115. Tiempo de respuesta de un Sitio web con el direccionamiento de Proxy.

Fuente: Servicio Chrome.

Esta prueba se realizó en un escenario experimental en el mismo computador ya que los tiempos de carga dependen de los procesos que realice el Sistema Operativo, cantidad de memoria RAM y procesador. En la Figura 108 se puede evidenciar que el tiempo de carga disminuyó asignando la dirección del proxy el cliente. Esta prueba se realizó en una muestra considerable dando resultados similares.

Figura 116. Resultado tiempo de respuesta de acceso a sitio Web

Fuente: Elaborado por el autor.

4.11.6 Generador de reportes SARG

El generador de reportes SARG es una herramienta de desarrollo libre que se implementó en el proxy nos presenta detalles en forma gráfica y en tiempos de la cantidad de Bytes que se han transportado por la red como se muestran en la Figura 117 y 118.

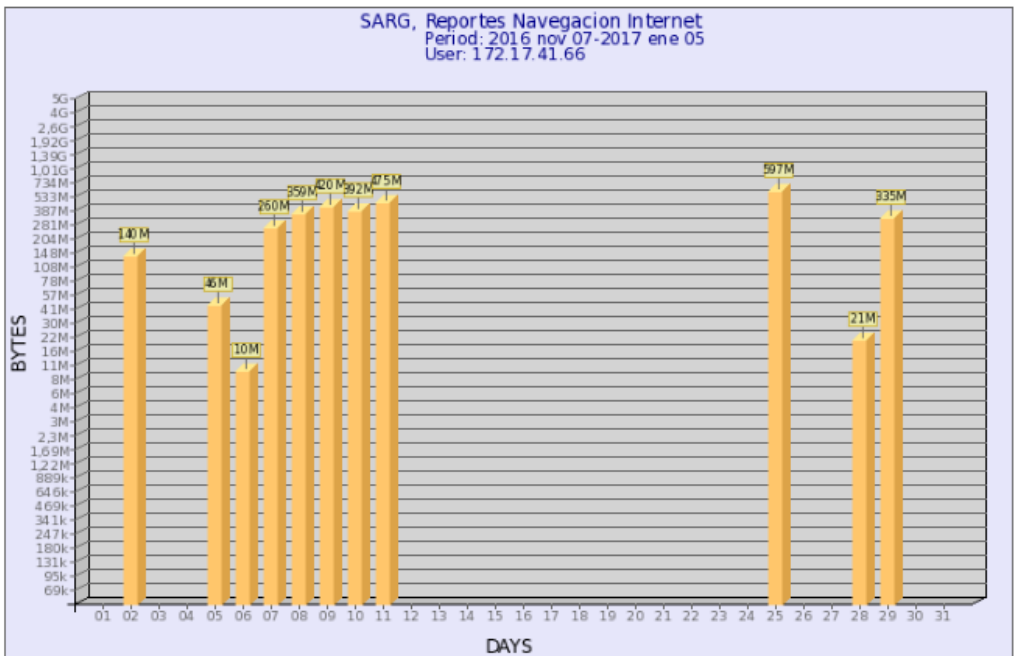
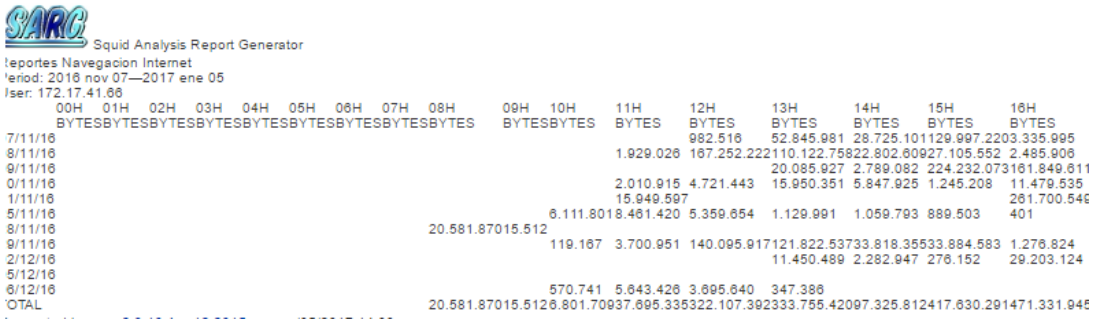


Figura 117. Generador de Reportes Gráfico SARG.

Fuente: Servicio Webmin.


Squid Analysis Report Generator

eportes Navegacion Internet
eriod: 2016 nov 07—2017 ene 05
ser: 172.17.41.66

	00H BYTES	01H BYTES	02H BYTES	03H BYTES	04H BYTES	05H BYTES	06H BYTES	07H BYTES	08H BYTES	09H BYTES	10H BYTES	11H BYTES	12H BYTES	13H BYTES	14H BYTES	15H BYTES	16H BYTES
7/11/16													982.516	52.845.981	28.725.101	129.997.220	3.335.995
8/11/16												1.929.026	167.252.222	110.122.758	22.802.609	27.105.552	2.485.906
9/11/16														20.085.927	2.789.082	224.232.073	161.849.611
0/11/16												2.010.915	4.721.443	15.950.351	5.847.925	1.245.208	11.479.535
1/11/16												15.949.597					261.700.546
5/11/16											6.111.801	8.461.420	5.359.654	1.129.991	1.059.793	889.503	401
8/11/16										20.581.870	15.512						
9/11/16											119.167	3.700.951	140.095.917	121.822.537	33.818.355	33.884.583	1.276.824
2/12/16														11.450.489	2.282.947	276.152	29.203.124
5/12/16																	
6/12/16											570.741	5.643.426	3.695.640	347.386			
OTAL										20.581.870	15.512	6.801.709	37.695.335	322.107.392	333.755.420	97.325.812	417.630.291

Figura 118. Generador de Day Report SARG

4.11.7 Procesamiento en equipos

Para esta prueba de funcionamiento se toma como escenario experimental con los siguientes detalles:

- Se realiza en un laboratorio con 34 equipos.
- El procesamiento se mide en el switch de distribución del data center de la Fica.
- Se mide el procesamiento del equipo de distribución con el servidor Firewall-proxy y la otra medición se realiza sin el servidor Firewall-proxy.
- Se realizan dos mediciones: una en horario normal de uso de los laboratorios de 14:50 pm durante 20 minutos y otra en un horario donde se pueda registrar el procesamiento de los equipos en un horario donde no existe mucho tráfico de datos 20:30 pm durante 15 min. En los dos casos se procuró generar la mayor cantidad de tráfico posible.

4.11.7.1 Primer escenario experimental

En la Figura 117 se puede constatar el tráfico generado durante el periodo de 20 minutos. Se logró transmitir un máximo de 40 Mbps.

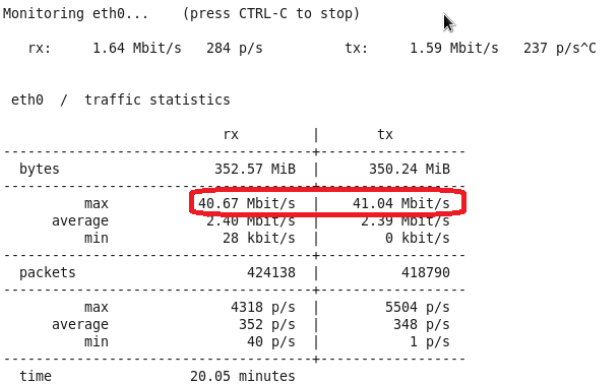


Figura 119. Máximo tráfico generado Tx y Rx escenario1
Fuente: Elaborado por el autor.

En la Figura 118 se puede observar que el uso de memoria RAM aumenta en el servidor pero que el procesamiento de CPU no es intensivo en el proceso del proxy squid.

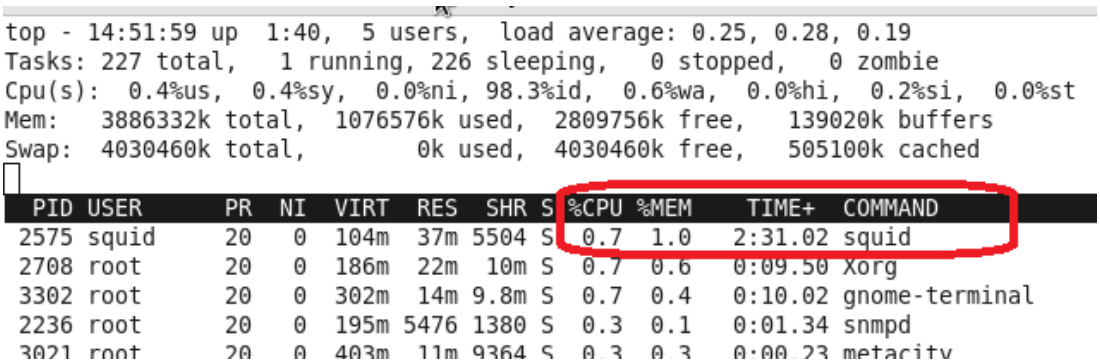


Figura 120. Consumo de Ram y CPU squid
Fuente: Elaborado por el autor.

4.11.7.2 Segundo escenario experimental

En la Figura 119 se puede constatar el tráfico generado durante el periodo de 15 minutos. Se logró transmitir un máximo de 91 Mbps.

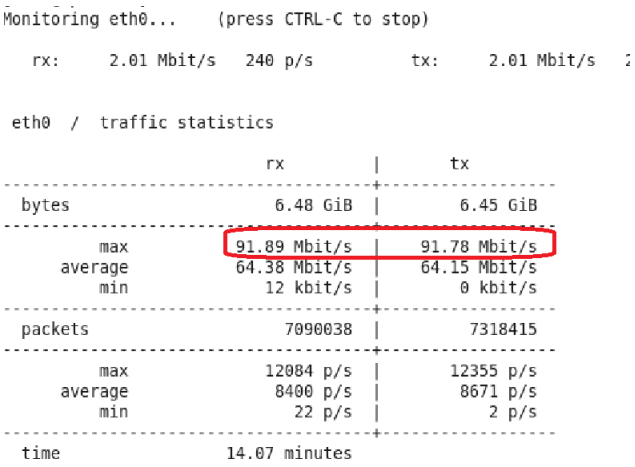


Figura 121. Máximo tráfico generado Tx y Rx escenario 2
Fuente: Elaborado por el autor.

En la Figura 120 se puede observar que el uso de memoria RAM aumenta en el servidor pero que el procesamiento de CPU no es intensivo en el proceso del proxy squid, al igual que en el escenario 1.

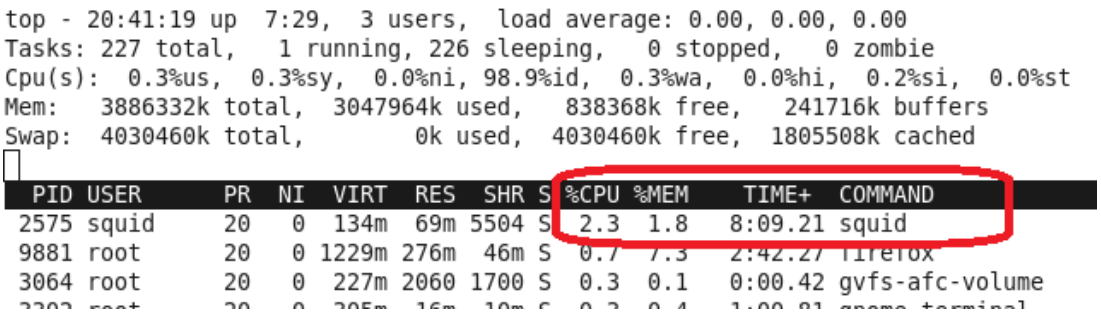


Figura 122. Consumo de Ram y CPU squid escenario 2
Fuente: Elaborado por el autor.

4.11.7.3 Estimación de los escenarios experimentales

Según la experimentación realizada se puede estimar un ahorro de procesamiento de los equipos del data center de la Fica y este procesamiento lo realiza el servidor Firewall Proxy como se puede evidenciar en la Figuras 122 y 124. Esto puede influir, en un futuro, si el desarrollo de este proyecto se lo realiza en todas los laboratorios de todas las facultades.

En la Figura 121 y 123 se observa el ahorro de procesamiento resumido mediante la experimentación de la implementación del Servidor Firewall-Proxy.

El uso de CPU en el primer escenario llega a un 30% sin el uso del proxy, mientras que con la implementación del servidor este uso de procesamiento se ve aumentado hasta un 20 %.

En el escenario dos el resultado es similar, el uso de cpu pasa el 1|9% debido a la mayor demanda de tráfico, pero se puede evidenciar que al implementar el servidor esta demanda de uso de CPU se reduce a un pico máximo de uso de 20 %. El detalle del monitoreo del equipo de distribución del data center de la Fica Se muestra en el Anexo 4.

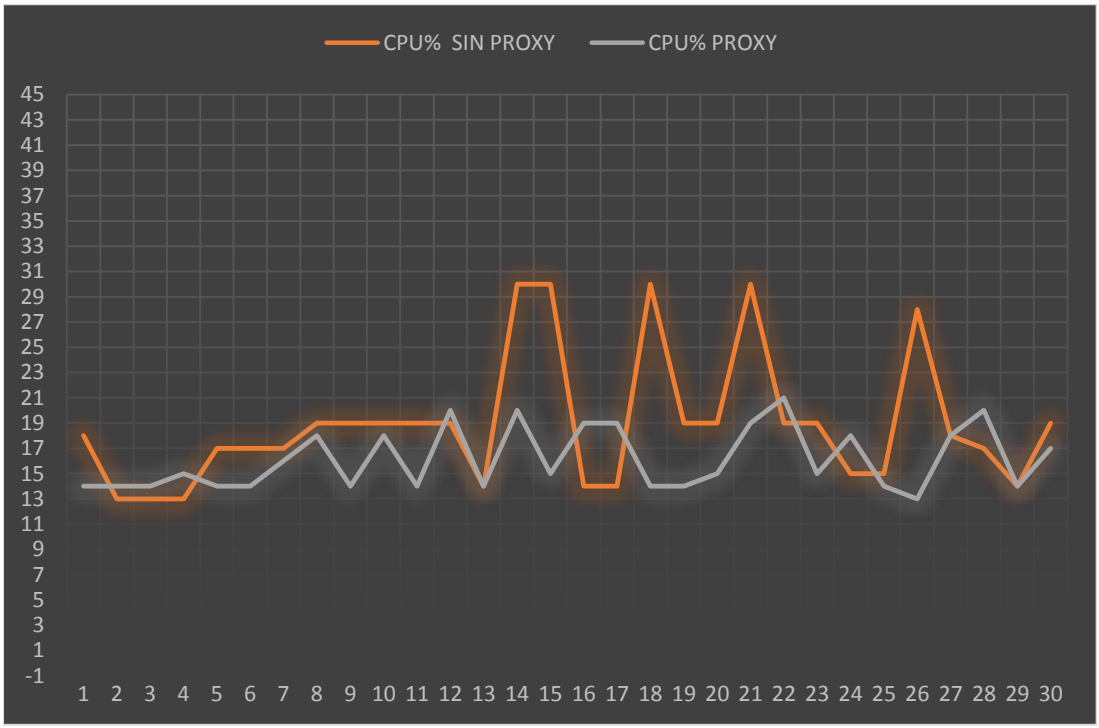


Figura 123. Consumo de Procesamiento Sw-Dist. con servidor Firewall-Proxy y sin Firewall Proxy escenario 1
Fuente: Elaborado por el autor.

```
top - 14:51:59 up  1:40,  5 users,  load average: 0.25, 0.28, 0.19
Tasks: 227 total,   1 running, 226 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.4%us,  0.4%sy,  0.0%ni, 98.3%id,  0.6%wa,  0.0%hi,  0.2%si,  0.0%st
Mem:   3886332k total,  1076576k used,  2809756k free,   139020k buffers
Swap:  4030460k total,        0k used,  4030460k free,   505100k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2575 squid     20   0  104m  37m 5504 S  0.7  1.0   2:31.02 squid
 2708 root      20   0  186m  22m  10m S  0.7  0.6   0:09.50 Xorg
 3302 root      20   0  302m  14m 9.8m S  0.7  0.4   0:10.02 gnome-terminal
 2236 root      20   0  195m 5476 1380 S  0.3  0.1   0:01.34 snmpd
 3021 root      20   0  403m  11m 9364 S  0.3  0.3   0:00.23 metacity
 3028 root      20   0  332m  14m  10m S  0.3  0.4   0:00.43 gnome-panel
```

Figura 124 Consumo de Procesamiento en servidor Firewall-Proxy escenario 1
Fuente: Elaborado por el autor.

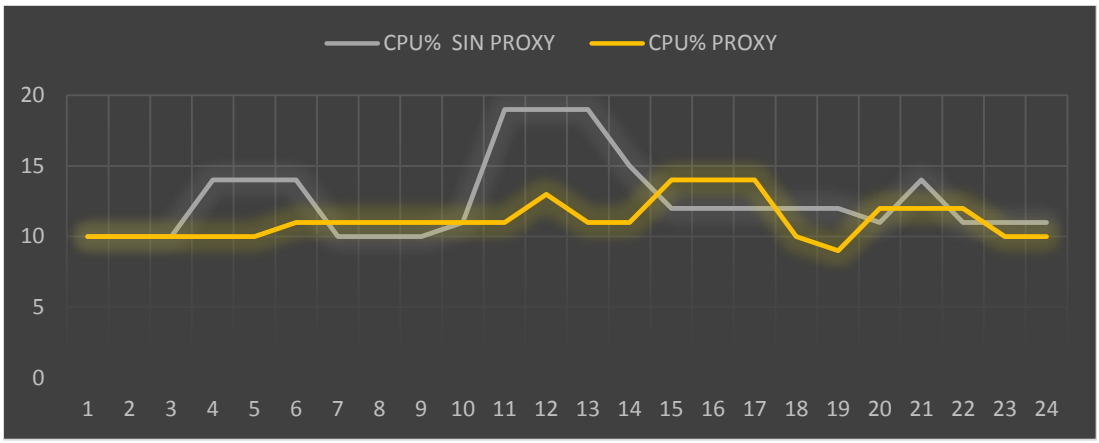


Figura 125.Consumo de Procesamiento Sw-Dist. con servidor Firewall-Proxy y sin Firewall Proxy escenario 2
Fuente: Elaborado por el autor.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
top - 20:04:30 up  6:52,  7 users,  load average: 0.01, 0.02, 0.00
Tasks: 233 total,   2 running, 231 sleeping,   0 stopped,   0 zombie
Cpu(s):  2.7%us,  3.2%sy,  0.0%ni, 91.8%id,  0.0%wa,  0.0%hi,  2.3%si,  0.0%st
Mem:   3886332k total,  3041268k used,   845064k free,   236404k buffers
Swap:  4030460k total,        0k used,  4030460k free,  1805104k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2575 squid     20   0  134m  69m 5504 S 29.2  1.8   5:58.48 squid
 2708 root      20   0  198m  26m  14m S  1.0  0.7   1:07.40 Xorg
 3302 root      20   0  309m  20m 9.8m S  0.7  0.5   0:55.62 gnome-terminal
 9881 root      20   0 1229m 276m  46m S  0.7  7.3   2:27.13 firefox
  173 root      20   0     0    0    0 S  0.3  0.0   0:01.99 usb-storage
 3348 root      20   0  100m  736  624 S  0.3  0.0   0:01.39 ping
```

Figura 126Consumo de Procesamiento en servidor Firewall-Proxy escenario 2
Fuente: Elaborado por el autor.

El consumo de CPU se ve disminuido en el swich de distribución de la Fica, en ambos casos ese procesamiento se ve aumentado en el servidor Firewall-Proxy implementado.

5. Conclusiones Y Recomendaciones

5.1 Conclusiones

El servidor Firewall-Proxy se instaló sobre el sistema operativo CentOs, el mismo que cumple los conceptos de libertad, y se implementó en la Facultad de Ingeniería en Ciencias Aplicadas, verificando el ahorro en tiempo de respuestas de páginas web y constatando la disminución de procesamiento de los equipos del Data Center mismo que se ve afectado en el aumento del porcentaje de uso de CPU del servidor Firewall-Proxy.

La documentación de las bases teóricas, permitió esclarecer dudas sobre el proceso que se tomó en consideración para el desarrollo del proyecto, se concluyó que para el diseño fue fundamental tomar como referencia la arquitectura de red TCP/IP, misma que sustentó la determinación de requerimientos, detección de errores, corrección de errores, pruebas y mantenimiento en el proceso de implementación del servidor Firewall-Proxy.

El análisis de la situación de la red universitaria permitió conocer la realidad actual de cada segmento de red, tomando en cuenta estos antecedentes se ha desarrollado el presente proyecto especificando parámetros de diseño en concordancia con la realidad de cada Facultad de la Universidad y precisando la implementación del servidor Firewall-Proxy en la Facultad de Ingeniería en Ciencias Aplicadas.

El estudio de requerimientos físicos mediante el dimensionamiento del hardware, el análisis de elección de un software considerando el estándar IEEE 29148, sustentó el diseño e implementación del servidor, de esta manera se documentó las características que se debe tomar en consideración para el buen funcionamiento del Firewall-Proxy.

La creación de subredes en la VLAN de laboratorios permitió gestionar de manera autónoma cada laboratorio, con lo cual se ha cumplido un objetivo específico dentro del

desarrollo del proyecto, controlando el acceso al servicio de internet así como la gestión de sitios web a los que se quiere acceder.

Las políticas y reglas asignadas al Firewall fueron definidas en base a las necesidades de cada Facultad, considerando el reglamento interno de uso de laboratorios y acorde con las políticas institucionales manejadas por el administrador de la red de datos, esto facilitó la asignación de reglas tanto de entrada, salida y enrutamiento en el servidor, así como la documentación de las políticas establecidas.

Se concluyó que la capacidad de la memoria cache que requiere un proxy está estrictamente relacionado con la disponibilidad de RAM en el equipo, la disponibilidad de espacio en el disco duro, el procesamiento interno del servidor y el tráfico generado por la red de datos. La cache, la cantidad de RAM y la cantidad de memoria en disco duro se calcularon en función al tráfico que genera la VLAN de los laboratorios, tomando como referencias el reporte generado por EXINDA, y el tamaño promedio de un objeto. El cálculo de estos parámetros permitió asignar la cantidad de memoria requerida por los procesos que ejecuta el proxy Squid.

El sistema se complementó con la implementación de una herramienta gráfica "Webmin", cuyo funcionamiento ha permitido interactuar con una interfaz web funcional y amigable para la administración del mismo, facilitando el uso y configuraciones de las herramientas de configuración y gestión.

Se implementó la herramienta "SARG" para la generación de reportes, la misma que capta información de la bitácora del proxy, esto permitió conocer el flujo de datos que los usuarios transportan por la red y los sitios web a los que se accede con frecuencia. Información que es considerable para tomar decisiones administrativas con el fin de optimizar el uso del servicio de internet.

5.2 Recomendaciones

Realizar el levantamiento de información antes de iniciar la implementación de un servicio, despeja dudas sobre el diseño del proyecto y permite obtener un producto final acorde a las necesidades.

Trabajar conjuntamente con los encargados de las áreas tecnológicas y cumplir con los procesos estipulados, para de esa manera, encaminarse en una ejecución del proyecto clara y confiable.

Es recomendable dimensionar el hardware acorde con las necesidades y funciones que este debe realizar, y considerar un estándar IEEE 29148 para la elección de un software, ya que de esta manera se podrá obtener una visión clara de que requerimientos son los necesarios, como se estructurará y que actores formarán parte del sistema.

Se recomienda documentar cada acción que se lleva a cabo en la implementación del servidor, ya que servirá de guía para esclarecer posibles problemas que puedan presentarse.

Operar herramientas gráficas ayuda a gestionar los procesos de configuración del sistema de manera rápida.

Para almacenar bloques más solicitados, el proxy hace uso de la RAM, por lo que se recomienda asignar la tercera parte de la capacidad ya que el sistema operativo realiza procesos internos y/o procesos pertenecientes a otras herramientas.

Se recomienda la asignación de memoria cache en disco duro entre un 50% a un máximo de 80% del espacio libre disponible, esto si no se ha hecho un análisis previo a la asignación de memoria.

Se sugiere que cuando se realicen cambios en la configuración se guarden y se apliquen los cambios y de ser necesario reiniciar los módulos de servicio para constatar que los cambios se han hecho correctamente y si han hecho efectivos.

Los parámetros de configuración son exclusiva responsabilidad del administrador del sistema, para evitar que personas ajenas a esta actividad modifiquen el mismo, se recomienda emplear un mecanismo de seguridad, CentOS cuenta con un procedimiento para el establecimiento y confirmación mediante autenticación de usuario y contraseña.

Bibliografía

Barabas, A. (2012). *SlidePlayer*. Recuperado el 18 de Septiembre de 2015, de http://slideplayer.es/slide/25780/#

Christian, B. G. (2011). *Desrrollo de unprototipo de solucion integral Web para la administracion de una red tipo SOHO bajo la plataforma GNU/Linux.* Quito.

Cisco Networking Academy. (2014). *Exploracion de las red.* Recuperado el 13 de agosto de 2015, de www.cisco.com

Cisco Networking Academy. (2015). Scaling Networks. Obtenido de http://www.cisco.edu.mn/CCNA_R&S_3_(Scaling%20Networks)/course/module4/index.html#4.0.1.1

Dueñas, J. B. (03 de 05 de 2016). *alcancelibre.org*. Obtenido de http://www.alcancelibre.org/staticpages/index.php/tabla-comparativa-distros-linux

Linux, C. (5 de Diciembre de 2016). *Gnu Colombia Linux*. Obtenido de http://www.linuxcolombia.com.co/?q=node/59

Lois, M. (2015 de 10 de 2015). *Como funciona un servidor proxy*. Obtenido de http://latiguillo01.pbworks.com/w/page/26678125/Como%20funciona%20un%20servidor%20proxy

Stallings, W. (2004). *Comunicaciones y Redes Computacionales* (7 ed. ed.). Pearso Educación.

Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de Computadoras* (5 ed. ed.). Pearso Educación.

Tomala, M. (21 de Febrero de 2011). *Las Redes MAN.* Recuperado el 7 de Septiembre de 2015, de http://www.monografias.com/trabajos84/redes-man/redes-man.shtml

Vallejo, R. (Productor). (2014). *Connecting Networks* [Película]. Obtenido de https://www.youtube.com/watch?v=HAlLCwa3fco

Trujano Soto, L. A., Gómez Pizaña, J. A., & Cerón Juárez, L. A. (2015). *Implementación de seguridad de red en capa 2 mediante vlan.*

Arévalo Galárraga, L. G., & Vaca Tello, G. A. (2010). *" Análisis, diseño e implementación de un software prototipo de firewall y servidor proxy multiplataforma con tecnología Java".*

Cholanco, N., & Anibal, J. (2009). Implementación de un proxy en plataforma linux para el control de transferencia de archivos con FTP, E-mail y Firewall para el laboratorio de software.

Cuauhtémoc, C. d. L. A. (2009). Desarrollo de cortafuegos de aplicación en modo transparente con software libre (GNULINUX) y evaluación de su desempeño con.

Esparza Morocho, J. P. (2013). *Implementación de un Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados.* QUITO/EPN/2013.

Ferrer Berbegal, M. (2006). Firewalls software: Estudio, instalación, configuración de escenarios y comparativa.

Izura, P. X. A. (2003). *IPTABLES: manual práctico*.

Laurencio, E. D., Gómez, R. M., Felipe, M. d. R. C., & Diaz, P. M. P. QoS en redes de área local.

Mazzari, G., & Monsalve Arteaga, C. (1998). Seguridad de redes de computadoras frente a internet, estudio diagnostico e implementación de firewalls.

Rosalba Ximena, C. T., & Verónica Marcela, Z. Y. (2008). Desarrollo y pruebas de Servidores de Firewall y Proxy en Linux Red Hat Enterprise 4.0 mediante máquinas virtuales (VMware).

Santana, T. B., Barredo, Y. L. A., Pavón, M. D., Bonachea, R. R., & Oduardo, E. L. Analizador de registros proxy para auditores Proxy Log Analyzer for auditors.

TEJEDA, C. G. M. (2002). Estudio, diseño e implementación de un Firewall.

GRAHAM, SHAW, IEEE 802.1Q VLAN Tutorial. En: http://www.microhowto.info/tutorials/802.1q.html#idm9120, [25 de Noviembre de 2015].

MEDINA, Jorge, Configurando una interfaz Ethernet como enlace VLAN trunk 802.1q en sistemas GNU/Linux. En: http://tuxjm.net/docs/Configurando_una_interfaz_Ethernet_como_enlace_VLAN_trunk_802.1q_en_sistemas_GNU_Linux/ [25 de Noviembre de 2015]

GARRON, Guillermo,Centos o Debian En: https://www.garron.me/es/gnu-linux/centos-vs-debian.html [26 de Noviembre de 2015]

RINCON DE LOS DESARROLLADORES, Acerca de Debian En: https://www.debian.org/intro/about#users [24 de Noviembre de 2015]

CENTOS PROJECT, Centos Linux En: https://www.centos.org/about/ [26 de Noviembre de 2015]

Glosario

802.11, es un estándar internacional que define las características de una red de área local inalámbrica

AP, Punto de Acceso; es un dispositivo que interconecta computadoras en una red.

DMZ, Zona desmilitarizada o red perimetral; es una zona segura que se ubica entre la red interna de una organización y una red externa

DSL, Es una tecnología que proporciona el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica.

Ethernet, es un estándar de transmisión de datos para redes de área local, con acceso al medio por detección de la onda portadora y con detección de colisiones

FTP, Protocolo de Transferencia de Archivos; protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

HDLC, sus siglas corresponden a control de enlace de datos de alto nivel, es un protocolo de comunicaciones de propósito general punto a punto

HTML, hace referencia al lenguaje de marcado para la elaboración de páginas web.

HTTP, protocolo de transferencia de hipertexto; protocolo de comunicación que permite las transferencias de información en la World Wide Web.

ICMP, protocolo de control y notificación de errores.

IP, Internet Protocol, es un protocolo de comunicación de datos digitales

IPv4, Protocolo de Internet versión 4; es la cuarta versión del Internet Protocol (IP).

ISO, Organización Internacional de Estandarización; es una federación de alcance mundial integrada por cuerpos de estandarización

LAN, Red de Área Local; por las siglas en inglés de Local Area Network

MAC, Media Access Control Identificador que poseen las tarjetas o dispositivos de red, este identificador es único a nivel mundial.

NAT, traducción de direcciones de red; mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

NFS, Network File System; utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local.

OSI, Open System Interconnection; es un lineamiento funcional para tareas de comunicaciones.

RS-232, Es un estándar para la conexión serial de señales de datos binarias entre un equipo terminal de datos y un equipo de terminación del circuito de datos.

Scheduler, Se refiere a programar procesos dentro de un período de tiempo constante, independientemente del número de procesos se están ejecutando en el sistema operativo

SMB, Server Message Block; es un protocolo de red que permite compartir archivos, impresoras, etc. entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows

SMTP, protocolo para transferencia simple de correo; es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

SSH, Intérprete de órdenes seguro, irve para acceder a máquinas remotas a través de una red.

TCP/IP, Conjunto de protocolos; es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos.

TCP, Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet.

Telnet, Telecomunication Network, es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente.

UDP, es un protocolo mínimo de nivel de transporte orientado a mensajes.

WAN, Red de Área amplia; por sus siglas en ingles Wide Área Network.

WLAN, Redes de Área Local Inalámbricas; pos sus siglas en ingles Wireless Local Area Network.

Anexo 1. Manual de Instalación de software.

El manual incluye los aspectos fundamentales para instalar las herramientas necesarias para la implementación del Firewall-Proxy.

1. Instalación Sistema Operativo CentOs 6.5

La distribución Linux más común que se utiliza para instalar un servidor es CentOS es una distribución de Linux que se basa en Red Hat Entrerprise Linux pero que es totalmente libre.

1.1. Modo de arranque de la instalación

Inserte el DVD de CentOs y espere unos 40 segundos para el inicio automático e ingrese la opción de instalación. Ver Figura 127.

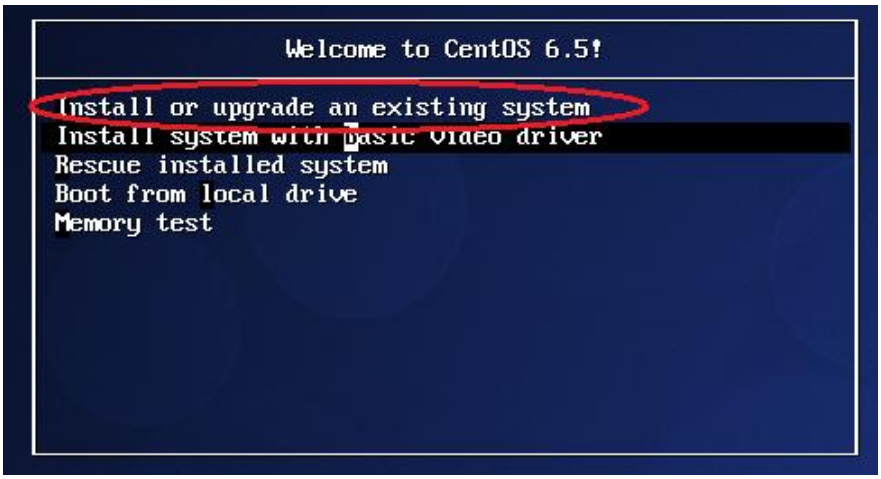


Figura 127. Modo de Arranque de instalación CentoOS 6.5.
Fuente: Servicio CentOS

1.2. Verificación del medio de instalación

Cuando inicia la instalación te solicita verificar el medio de instalación este proceso debe realizarse solo si es un servidor critico o si quieres tener la seguridad de que el DVD esté bien grabado y que todo se encuentre normal, si es un servidor de prueba

puedes omitir este paso seleccionando “Skip” y presionando “Enter”. Si deseas realizar la verificación del medio seleccionar “Ok” y presiona la tecla “Enter”.Ver Figura 128.

Figura 128. Disc Found- Verificación del medio de instalación
Fuente: Servicio CentOS

1.3. Pantalla de Bienvenida Instalación CentOS

Una vez que aparezca la pantalla de bienvenida de Centos hacer click sobre Next. Ver Figura 129.

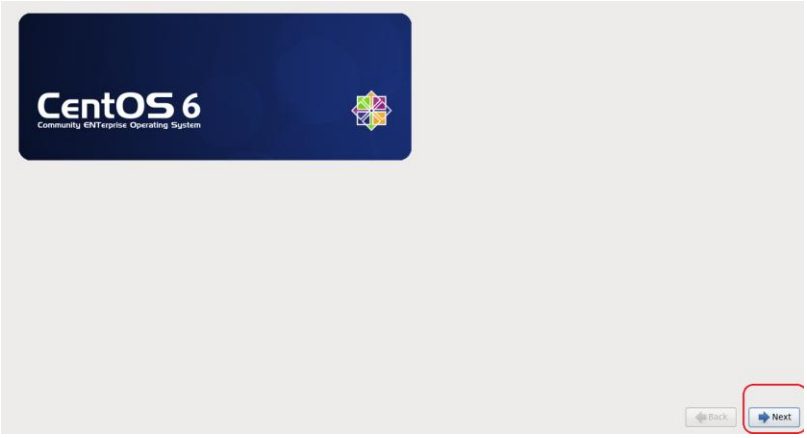


Figura 129. Pantalla Bienvenida CentOS.
Fuente: Servicio CentOS

1.4.Selección de Idioma en el proceso de Instalación CentOS.

Seleccionar idioma Spanish:Español para el proceso de instalación y hacer click sobre Next. Ver Figura 130.

Figura 130. Idioma para instalación
Fuente: Servicio CentOS

1.5.Selección de distribución de Teclado

Selecciones el teclado apropiado para el sistema, puede ser latinoamericano, español o el del tipo de teclado que uses. Ver Figura 131. Seleccionamos español

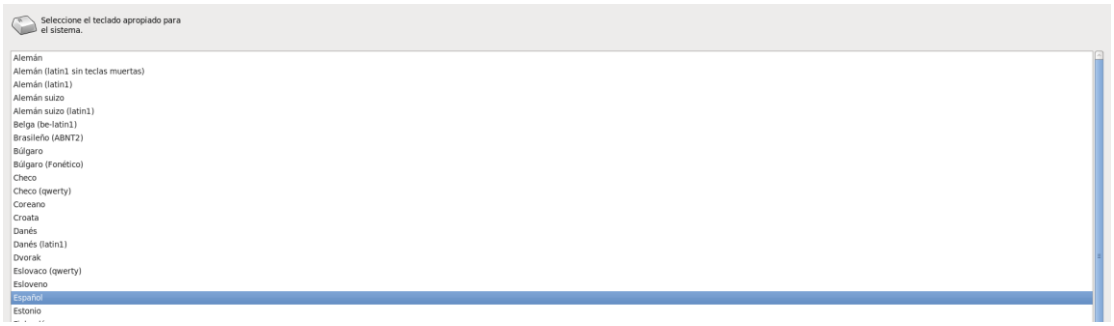


Figura 131. Idioma para el teclado
Fuente: Servicio CentOS

1.6. Selección de tipo de dispositivo

Seleccione el tipo de dispositivo que involucra la instalación. En nuestro caso disponemos solo de discos duros seleccione “Dispositivos de almacenamiento básico” y hacer click en siguiente. Ver Figura 132.

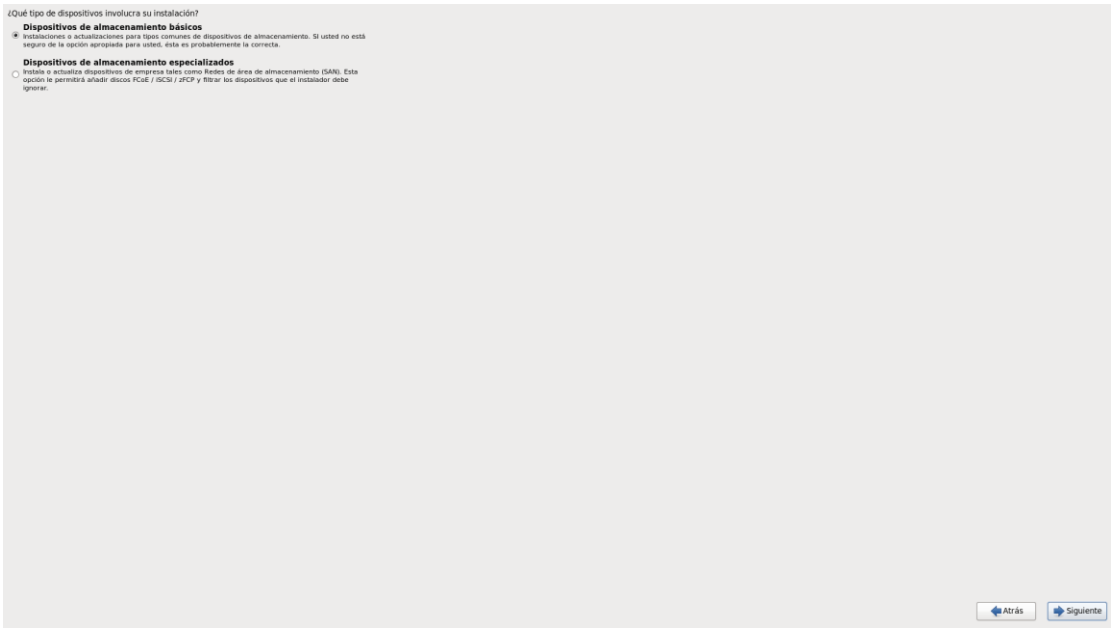


Figura 132.Tipo de dispositivo
Fuente: Servicio CentOS

1.7. Definición de nombre de host

Indica un nombre para tu servidor y también puedes configurar la o las interfaces de red aunque siempre recomiendo que se configuren hasta que el servidor esté operativo y solo hasta entonces conectar cualquier interfaz de red. Ver Figura 133.

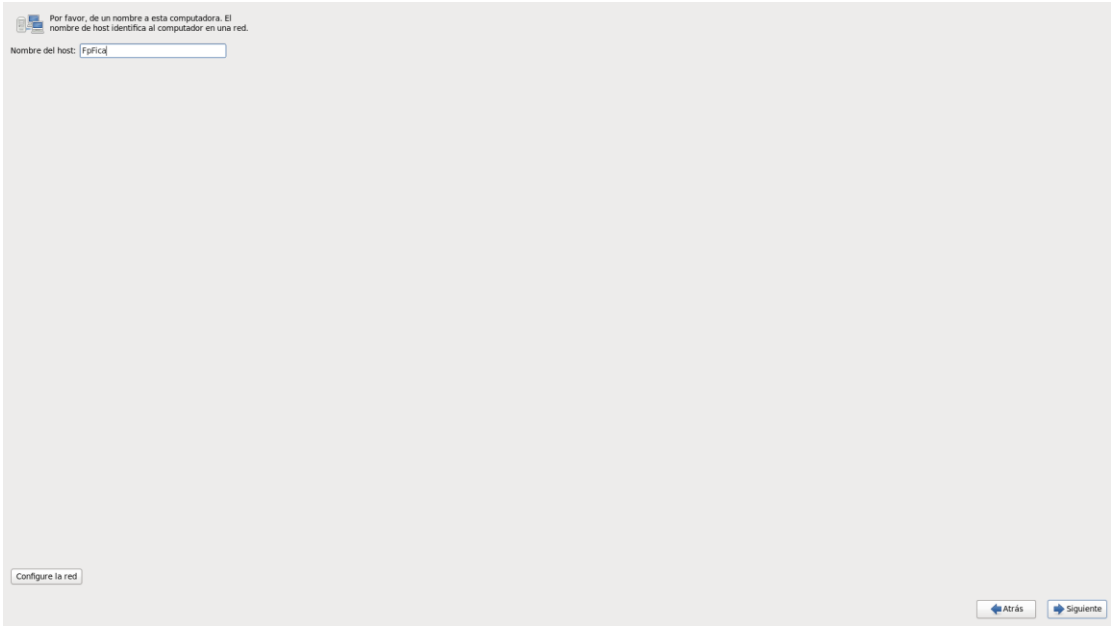


Figura 133. Nombre del host.
Fuente: Servicio CentOS

1.8. Selección de zona horaria

Seleccione la zona horaria que corresponda a su localidad haciendo clic sobre cualquier punto en el mapa. Ver Figura 134.

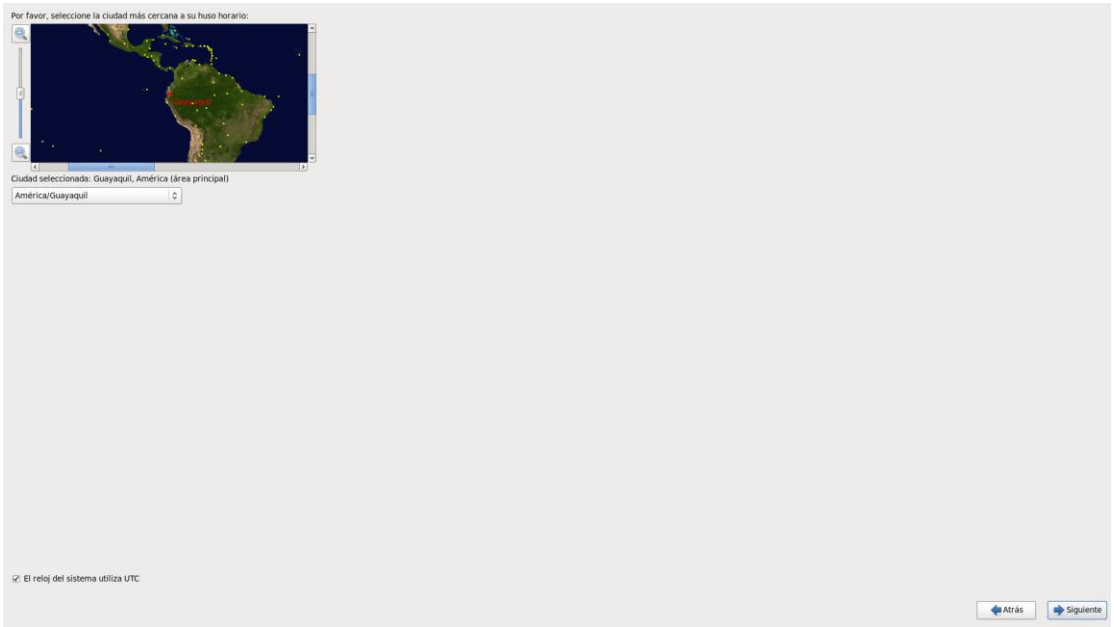


Figura 134. Zona horaria
Fuente: Servicio CentOS

1.9.Definición de contraseña para el usuario root

Defina y confirme la contraseña para root, cuenta que será utilizada para la administración del sistema. Al terminar haga clic sobre Siguiente. Ver Figura 135.

Figura 135. Contraseña para root
Fuente: Servicio CentOS

1.10. Tipo de instalación

Como nuestro servidor es dedicado hacer una tarea en la siguiente imagen seleccionamos usar todo el espacio, las particiones se crearan de forma automática. Luego dar click en siguiente. Ver Figura 136.

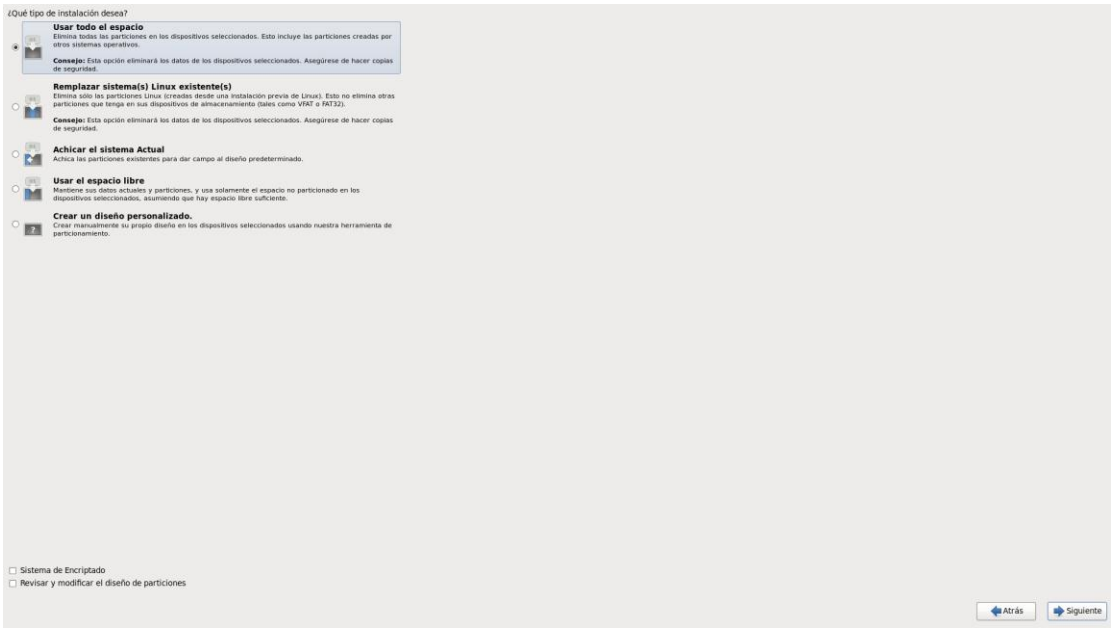


Figura 136. Tipo de instalación
Fuente: Servicio CentOS

Damos click sobre Escribir cambios al disco. Ver Figura 137.

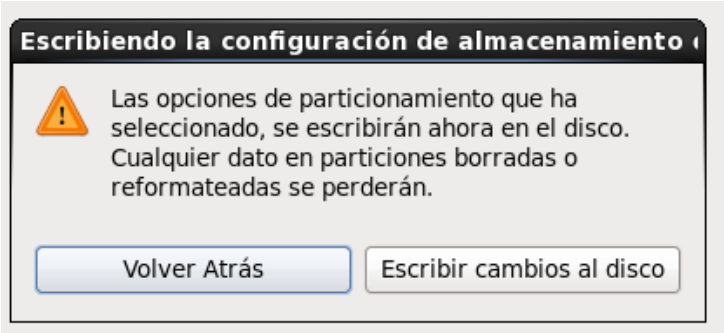


Figura 137. Aceptar cambios al disco
Fuente: Servicio CentOS

1.11. Tipo de conjunto de software

Elegir el tipo de instalación. Seleccionamos el tipo Desktop para facilitar la configuración de opciones de manera gráfica. Damos click en Siguiente. Ver Figura 138.

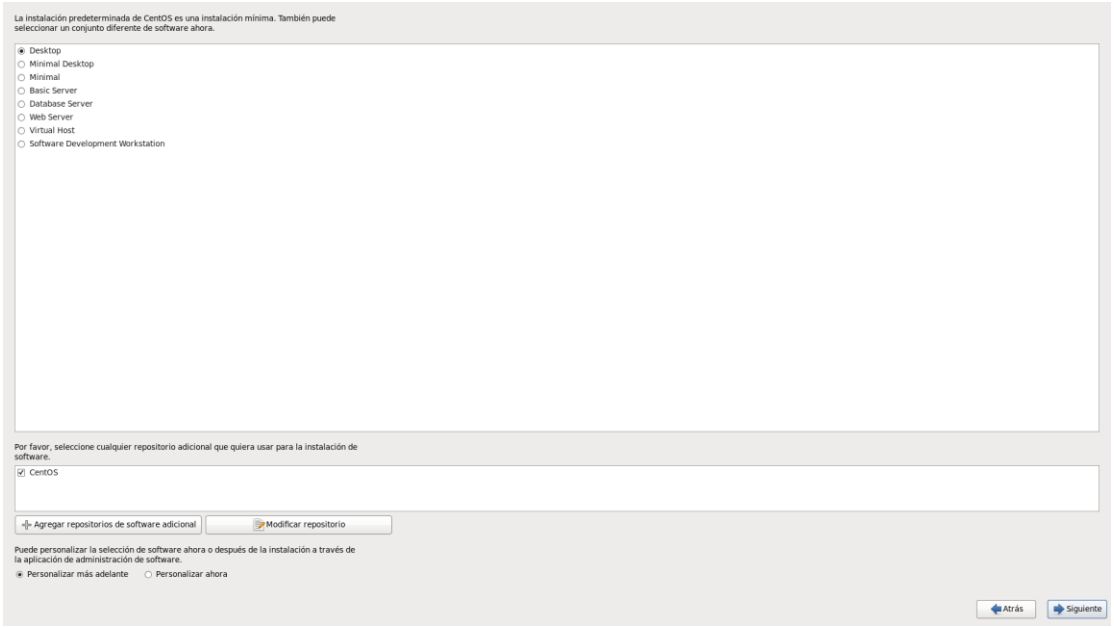


Figura 138. Tipo de instalación conjunto de software
Fuente: Servicio CentOS

1.12. Proceso de copia de paquetes

El proceso de instalación del sistema operativo iniciará como se muestra en la Figura 139.

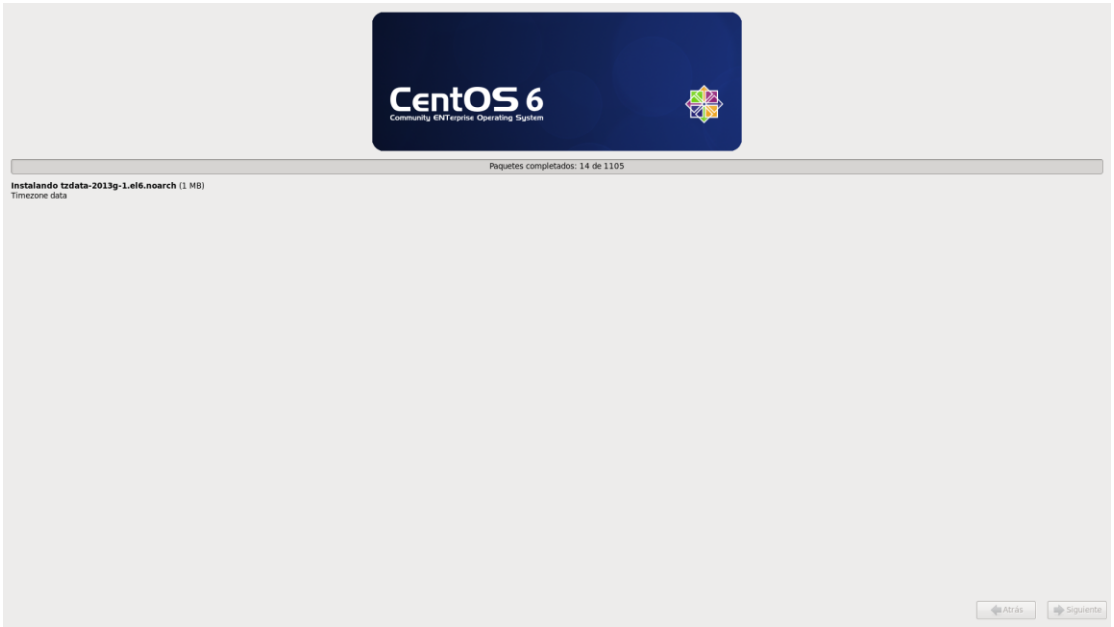


Figura 139. Instalación de paquetes CentOS.
Fuente: Servicio CentOS

1.13. Bienvenida al sistema

Luego del proceso de instalación, muestra la bienvenida al sistema operativo, presionamos sobre siguiente. Ver Figura 140.

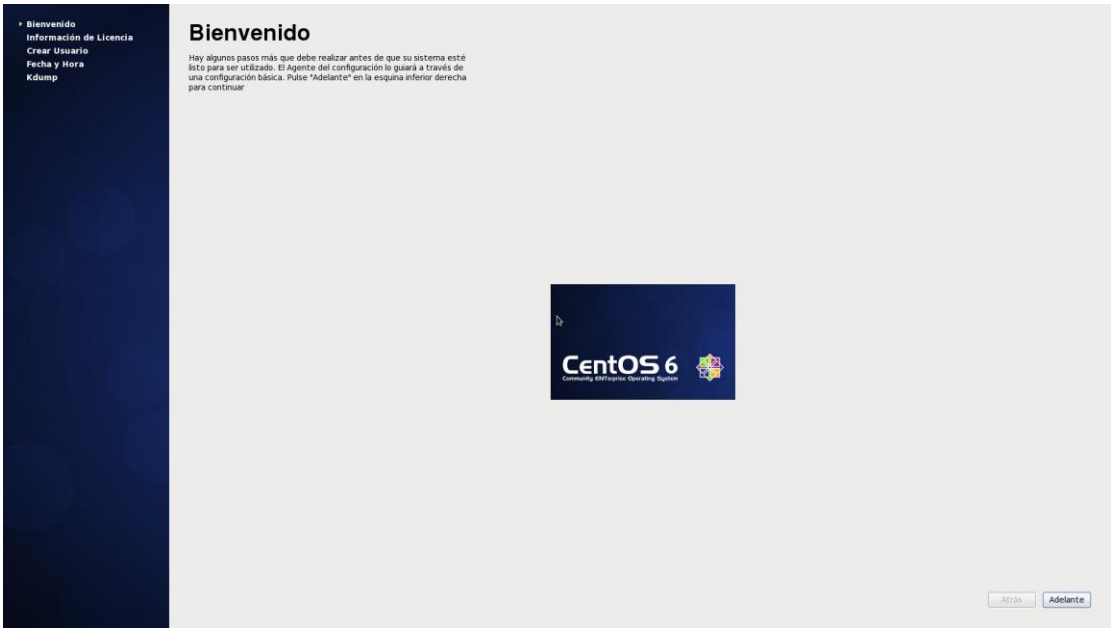


Figura 140. Bienvenida CentOS.
Fuente: Servicio CentOS

1.14. Información de licencia

Acordamos la información de licencia del producto y damos click sobre Siguiente. Ver Figura 141.

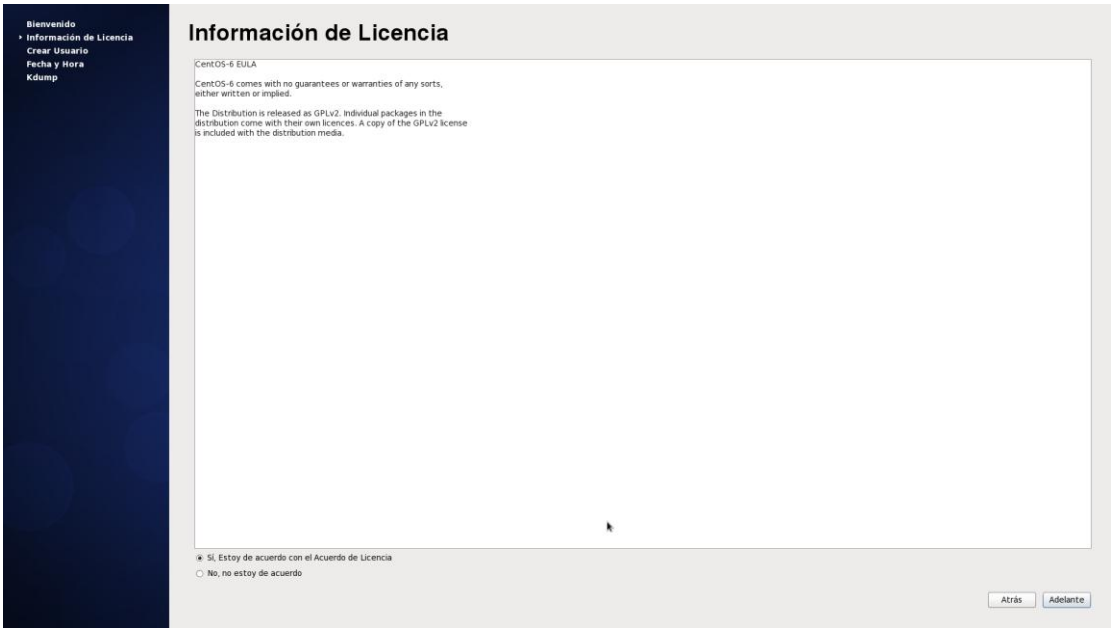


Figura 141. Información de Licencia.
Fuente: Servicio CentOS

1.15. Creación de usuarios.

Si deseamos creamos usuario caso contrario le damos click a Adelante. El mensaje que se muestra es información le damos click a Sí. Ver Figura142.

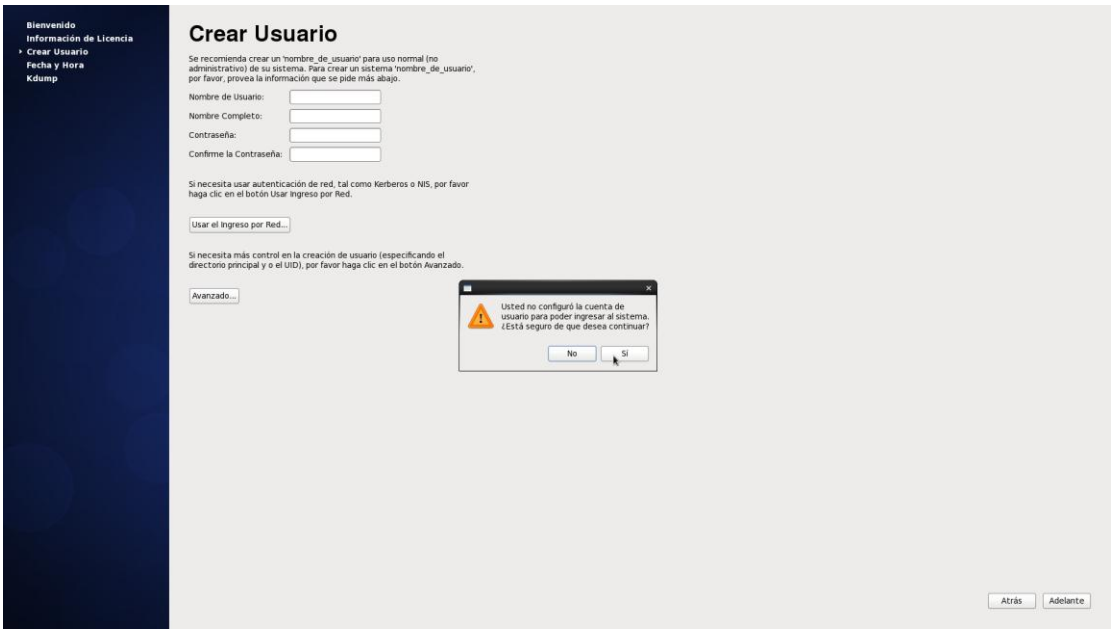


Figura 142. Crear Usuario.
Fuente: Servicio CentOS

1.16. Configuración fecha y hora

Configuramos Fecha y hora y seleccionamos los servidores NTP y le damos click a Adelante. Ver Figura 143.

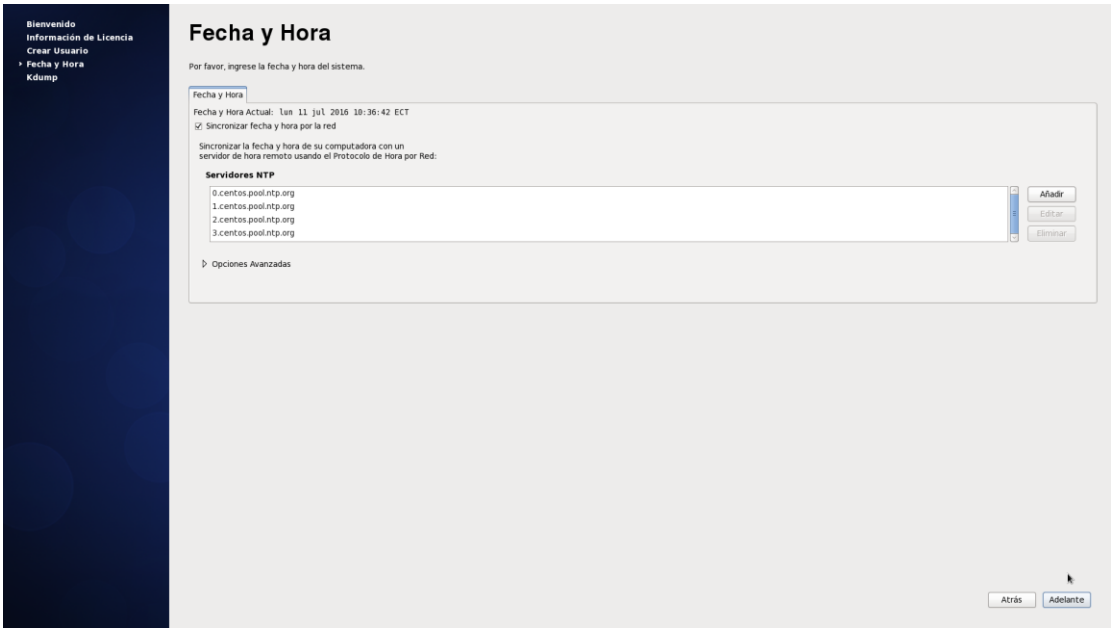


Figura 143. Fecha y hora.
Fuente: Servicio CentOS

1.17. Volcado de Fallos

La instalación se finaliza con el sistema de volcado de fallos Kdump. Damos click a Finalizar. El servidor se reiniciará. Ver Figura 144.

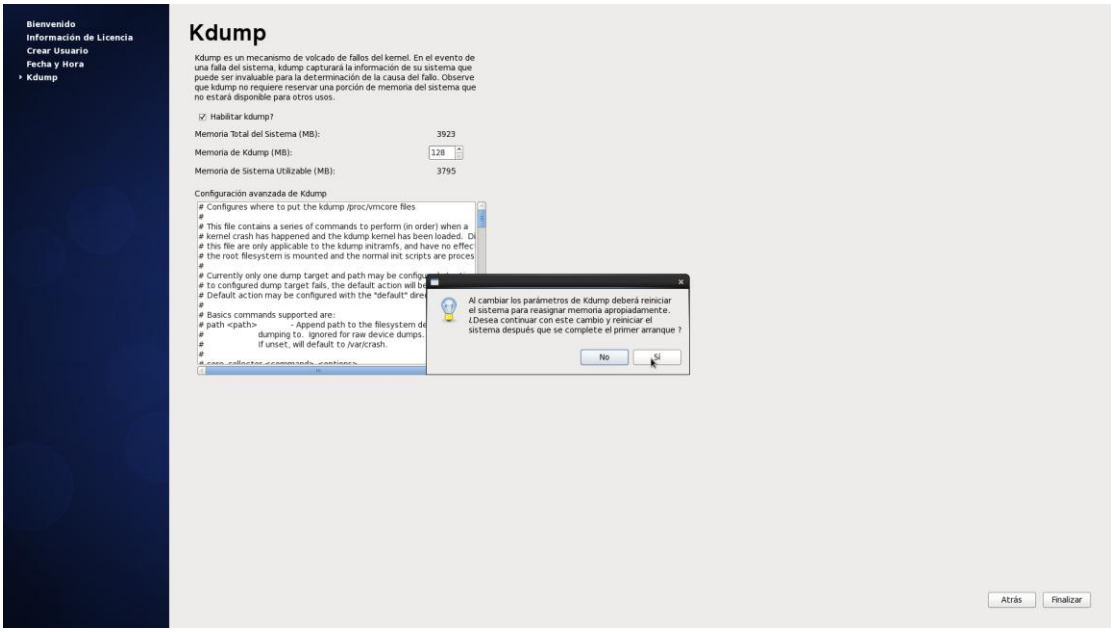


Figura 144. Kdump
Fuente: Servicio CentOS

2. Instalación SSH

La instalación del intérprete de órdenes seguro SSH se la realiza desde la línea de comandos de nuestro sistema operativo CentOS. Para ello nos dirigimos a Aplicaciones-Herramientas del sitema-Terminal. Ver Figura 145.

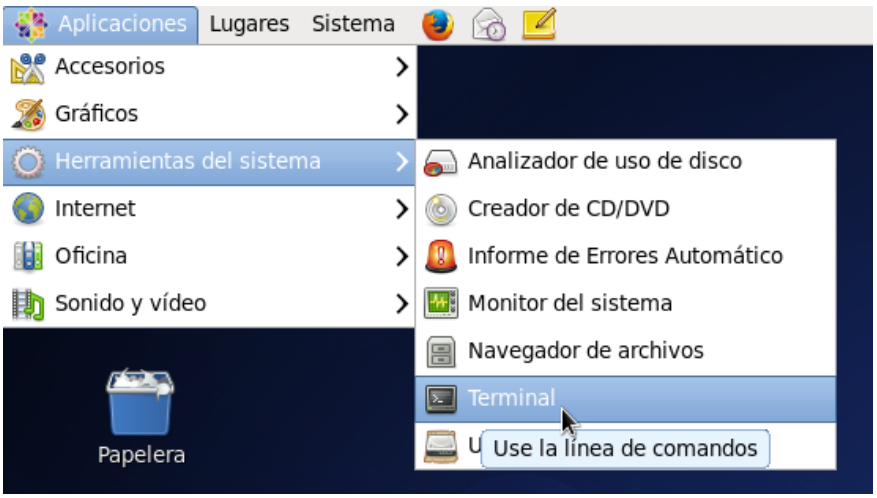


Figura 145. Abrir Terminal.
Fuente: Servicio CentOS

2.1. Busca instaladores SSH disponibles

Una vez abierto el terminal buscamos un servidor y cliente SSH disponible que se pueda instalar con el comando <<yum search openssh.server>> como se muestra en la Figura 146.

```
[root@FpFica ~]# yum search openssh.server
Complementos cargados:fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.cedia.org.ec
 * extras: mirror.cedia.org.ec
 * updates: mirror.cedia.org.ec
Aviso: No se ha encontrado ningún resultado para: openssh.server
No se ha encontrado ningún resultado
[root@FpFica ~]# yum search openssh
Complementos cargados:fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.cedia.org.ec
 * extras: mirror.cedia.org.ec
 * updates: mirror.cedia.org.ec
============================== N/S Matched: openssh ==============================
openssh-askpass.x86_64 : A passphrase dialog for OpenSSH and X
openssh.x86_64 : An open source implementation of SSH protocol versions 1 and 2
openssh-clients.x86_64 : An open source SSH client applications
openssh-ldap.x86_64 : A LDAP support for open source SSH server daemon
openssh-server.x86_64 : An open source SSH server daemon
```

Figura 146. Buscar paquete disponible SSH.
Fuente: Servicio CentOS

2.2. Instalación SSH

En la Figra 19 se puede observar los paquetes ssh disponibles. El paquete a instalarse es openssh-server.x86_64 y el paquete openssh-clients.x86_64 para ello ejecutamos el comando <<yum install openssh-server.x86_64 openssh-clients.x86_64>> y damos Enter. Ver Figura 20.

```
[root@FpFica ~]# yum install openssh-server.x86_64 openssh-clients.x86_64
```

Figura 147. Instalar SSH.
Fuente: Servicio CentOS

3. Instalar Proxy Squid

Para instalar el proxy squid se ejecuta el comando <<yum install squid>> como se muestra en la figura 148.

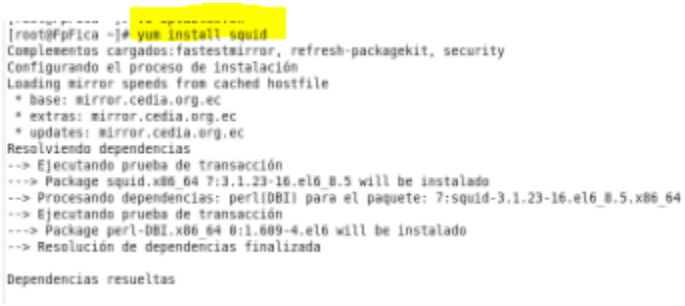


Figura 148. Instalar Squid.
Fuente: Servicio CentOS

Al final de la instalación de Squid se muestra un mensaje “Listo”. Como se puede apreciar en la Figura 149.

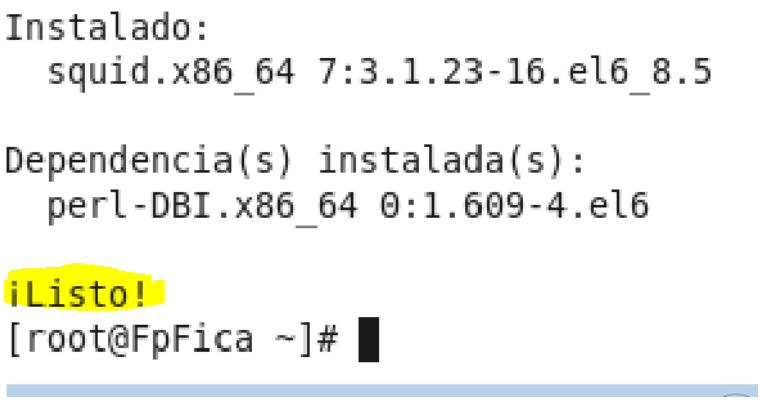


Figura 149. Finalización de instalación de Squid.
Fuente: Servicio CentOS

4. Instalación herramienta de reportes SARG.

Sarg es una herramienta para la generación de reportes a partir de las bitácoras de Squid. Permite ver con detalle la actividad de todos los equipos y/o usuarios dentro de la red de área local, registrada en la bitácora de Squid.

4.1. Instalación servidor http

Para instalar la herramienta SARG tenemos que en primera instancia instalar un servidor http. Para ello ejecutamos el comando <<yum install httpd>> como se muestra en la Figura 23.

```
[root@FpFica ~]# yum install httpd
Complementos cargados:fastestmirror, refresh-packagekit, security
Configurando el proceso de instalación
```

Figura 150. Instalación servidor http
Fuente: Servicio CentOS

4.2.Instalación paquete SARG

En segunda instancia instalamos el paquete SARG con el comando <<yum install sarg>>. Ver figura 151.

```
[root@FpFica ~]# yum install sarg
Complementos cargados:fastestmirror, refresh-packagekit, security
Configurando el proceso de instalación
Loading mirror speeds from cached hostfile
```

Figura 151. Comando de Instalación SARG.
Fuente: Servicio CentOS

La figura 152 nos muestra el mensaje de que SARG ha sido instalado correctamente.

```
Está de acuerdo [s/N]:s
Ejecutando el rpm_check_debug
Ejecutando prueba de transacción
La prueba de transacción ha sido exitosa
Ejecutando transacción
  Instalando    : libXpm-3.5.10-2.el6.x86_64                              1/3
  Instalando    : gd-2.0.35-17.el6.x86_64                                 2/3
  Instalando    : sarg-2.3.10-1.el6.x86_64                                3/3
  Verifying     : gd-2.0.35-17.el6.x86_64                                 1/3
  Verifying     : sarg-2.3.10-1.el6.x86_64                                2/3
  Verifying     : libXpm-3.5.10-2.el6.x86_64                              3/3

Instalado:
  sarg.x86_64 0:2.3.10-1.el6

Dependencia(s) instalada(s):
  gd.x86_64 0:2.0.35-17.el6          libXpm.x86_64 0:3.5.10-2.el6

¡Listo!
```

Figura 152. . Mensaje de confirmación de instalación SARG.
Fuente: Servicio CentOS

5. Instalación Webmin

Webmin es una herramienta de configuración de sistemas accesible vía web.

5.1. Creación archivo Webmin

Para la instalación de Webmin haremos uso de un repositorio para ello generamos un archivo con el comando <<vi /etc/yum.repos.d/webmin.repo >> como se muestra en la figura 26.

```
[root@FpFica ~]# vi /etc/yum.repos.d/webmin.repo
```

Figura 153. Creación archivo de repositorio Webmin
Fuente: Servicio CentOS

En el archivo antes creado debe contener lo siguiente:

[Webmin]

name=Webmin Distribution Neutral

#baseurl=http://download.webmin.com/download/yum

mirrorlist=http://download.webmin.com/download/yum/mirrorlist

enabled=1

El contenido del archivo se puede apreciar en la Figura 154.

```
[Webmin]
name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
~
~
~
~
~
```

Figura 154. Contenido archivo /etc/yum.repos.d/webmin.repo.
Fuente: Servicio CentOS

5.2. Resolviendo Dependencias

Como siguiente paso se resuelven las dependencias con el comando <<wget http://www.webmin.com/jcameron-key.asc>> como se muestra en la Figura 155.

```
[root@FpFica ~]# wget http://www.webmin.com/jcameron-key.asc
--2016-07-25 17:03:47--  http://www.webmin.com/jcameron-key.asc
Resolviendo www.webmin.com... 216.34.181.97
Connecting to www.webmin.com|216.34.181.97|:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1320 (1,3K) [text/plain]
Saving to: `jcameron-key.asc'

100%[======================================>] 1.320       --.-K/s   in 0s

2016-07-25 17:03:47 (166 MB/s) - `jcameron-key.asc' saved [1320/1320]

[root@FpFica ~]#
```

Figura 155. Comando para resolver dependencias Webmin.
Fuente: Servicio CentOS

Importamos la firma digital con el comando <<rpm --import jcameron-key.asc>> como se muestra en la Figura 156.

```
[root@FpFica ~]# rpm --import jcameron-key.asc
[root@FpFica ~]#
```

Figura 156. Impartar firma digital Webmin.
Fuente: Servicio CentOS

5.3. Instalación de paquete Webmin

Instalar Webmin con el comando <<yum install webmin>> como se muestra en la Figura 157.

```
[root@FpFica ~]# yum install webmin
Complementos cargados:fastestmirror, refresh-packagekit, security
Configurando el proceso de instalación
Loading mirror speeds from cached hostfile
 * base: mirror.cedia.org.ec
 * extras: mirror.cedia.org.ec
 * updates: mirror.cedia.org.ec
Webmin                                                  | 1.0 kB     00:00
Webmin/primary                                          |  32 kB     00:00
Webmin                                                               253/253
Resolviendo dependencias
```

Figura 157. Comando para instalar Webmin
Fuente: Servicio CentOS

Anexo 2. Manual de Configuración de Software.

La configuración que aquí se presenta hace referencia al diseño previo ya establecido en el proyecto de implementación de un Servidor Firewall-Proxy para la Facultad de Ingeniería en Ciencias Aplicadas.

1. Configuración de interfaces de red.

1.1. Soporte para configuración de VLANs.

El soporte necesario para configurar VLANs se incluye junto con el paquete iproute, el cual se incluye en la instalación predeterminada, pues se trata de un paquete obligatorio e indispensable para el sistema.

Editar el archivo /etc/sysconfig/network mediante el comando <vi /etc/sysconfig/network>

Añadir el siguiente parámetro para activar el soporte para VLAN, mismo que permitirá que posteriormente cargue automáticamente el módulo 8021q del núcleo de Linux. Ver Figura 158.

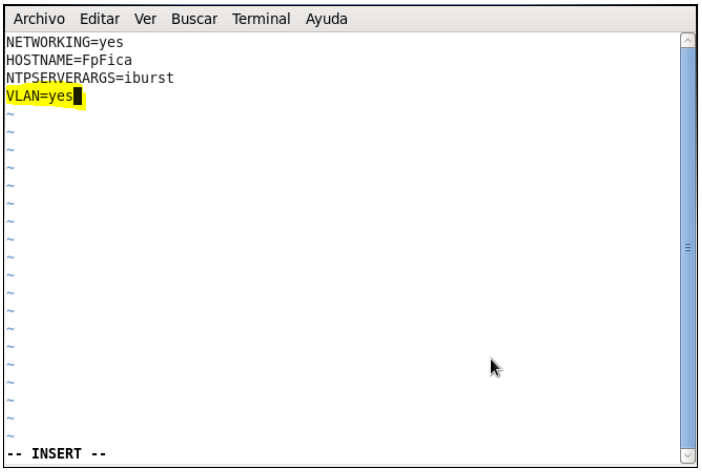


Figura 158. Archivo de configuración VLAN 82.1q Linux
Fuente: Servicio CentOS

1.2. Creación interfaces de red virtuales.

Para la implementación de interfaces de red virtuales se lo puedes hacer mediante la creación de archivos (scripts) o usando la herramienta de interfaz gráfica webmin.

1.2.1. Configuración de interfaces de red mediante la creación de archivos.

Mediante el comando <<ifconfig>> verificamos la interfaz de red que disponemos en este caso el nombre de la tarjeta de red es eth0 de la cual se van a derivar las interfaces de red virtuales. Ver Figura 2.

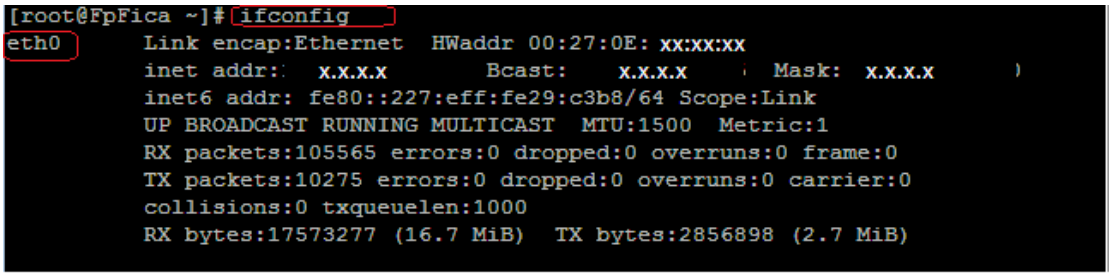


Figura 159. Interfaz de red disponible en el equipo
Fuente: Servicio CentOS

Para que los dispositivos de VLANs sean permanentes, es necesario crear, dentro del directorio /etc/sysconfig/network-scripts, los archivos de configuración de interfaz, siguiendo el siguiente formato: icfg-DISPOSITIVO:ID-VLAN.

En nuestro caso crearemos las interfaces virtuales que harán de puertas de enlace para cada laboratorio.

Para ello ejecutamos el siguiente comando para crear los archivos << vi /etc/sysconfig/network-scripts/ifcfg-eth0:64>> y cada uno de los archivos debe tener los siguientes parámetros.

NAME=""

BOOTPROTO=none
NM_CONTROLLED=no
MACADDR=""
IPV6INIT=no
DEVICE=eth0:64
NETMASK=255.255.255.192
MTU=""
BROADCAST=172.17.40.127
ONPARENT=yes
IPADDR=172.17.40.65
NETWORK=172.17.40.64
ONBOOT=yes

Para la primera interfaz virtual quedaría como se muestra en la Figura 160.

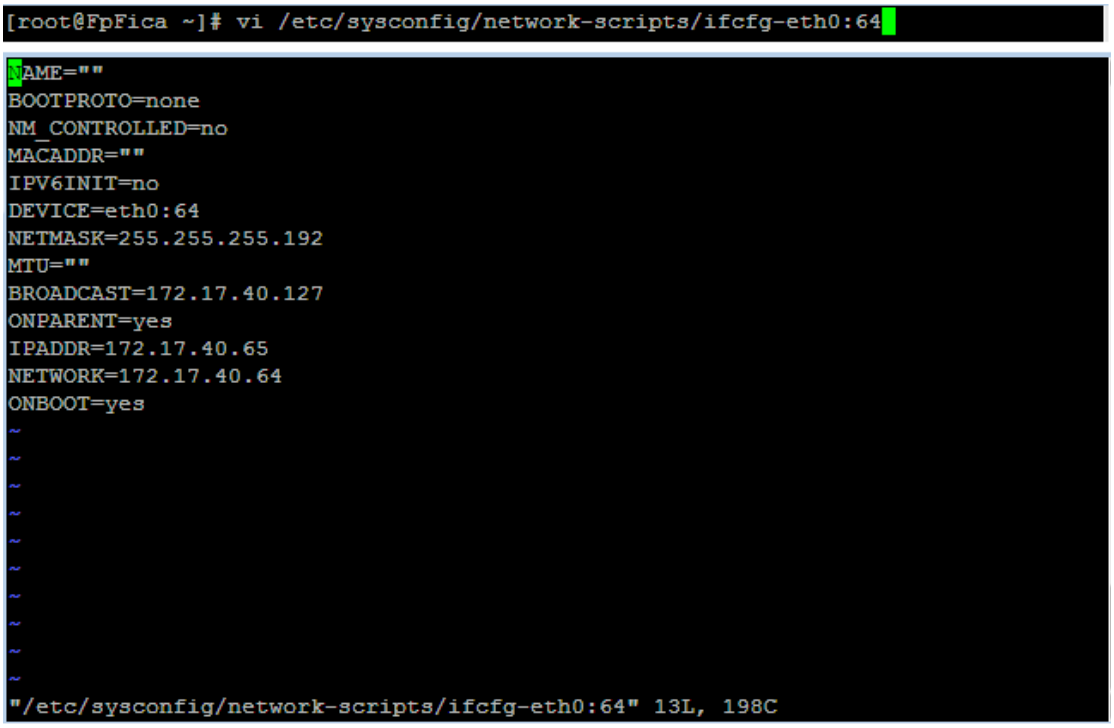


Figura 160. Configuración Interfaz de red Virtual eth0:64
Fuente: Servicio CentOS

La segunda interfaz de red se configura como se muestra en la Figura 161.

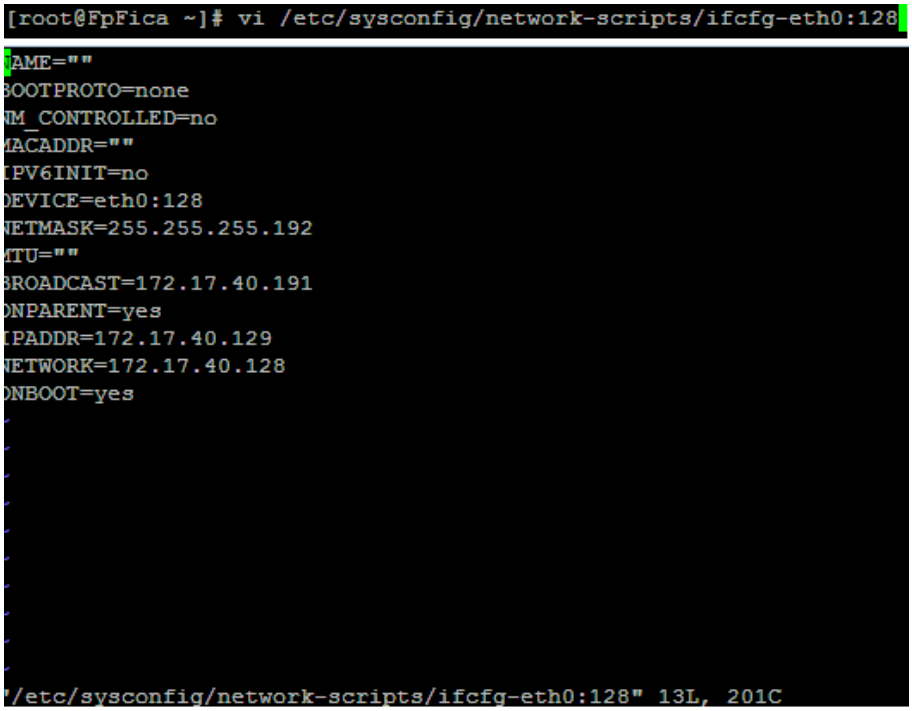


Figura 161. Configuración Interfaz de red Virtual eth0:128
Fuente: Servicio CentOS

La tercera interfaz de red se configura como se muestra en la Figura 162.

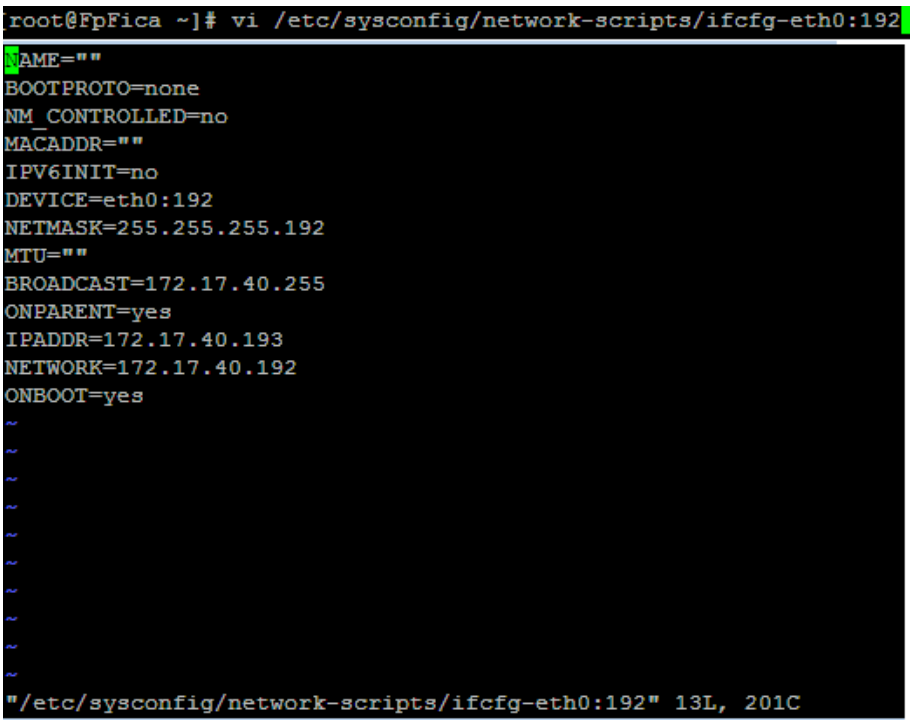


Figura 162.Configuración Interfaz de red Virtual eth0:192
Fuente: Servicio CentOS

La cuarta interfaz de red se configura como se muestra en la Figura 163.

```
[root@FpFica ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0:410
BOOTPROTO=none
NAME=""
MACADDR=""
NM_CONTROLLED=no
IPV6INIT=no
DEVICE=eth0:410
NETMASK=255.255.255.192
MTU=""
ONPARENT=yes
BROADCAST=172.17.41.255
IPADDR=172.17.41.1
NETWORK=172.17.41.0
ONBOOT=yes
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/network-scripts/ifcfg-eth0:410" 13L, 197C
```

Figura 163.Configuración Interfaz de red Virtual eth0:410
Fuente: Servicio CentOS

La quinta interfaz de red se configura como se muestra en la Figura 164.

```
[root@FpFica ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0:4164
BOOTPROTO=none
NAME=""
MACADDR=""
NM_CONTROLLED=no
IPV6INIT=no
DEVICE=eth0:4164
NETMASK=255.255.255.192
MTU=""
ONPARENT=yes
BROADCAST=172.17.41.255
IPADDR=172.17.41.65
NETWORK=172.17.41.64
ONBOOT=yes
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/network-scripts/ifcfg-eth0:4164" 13L, 200C
```

Figura 164. Configuración Interfaz de red Virtual eth0:4164
Fuente: Servicio CentOS

La sexta interfaz de red se configura como se muestra en la Figura 165.

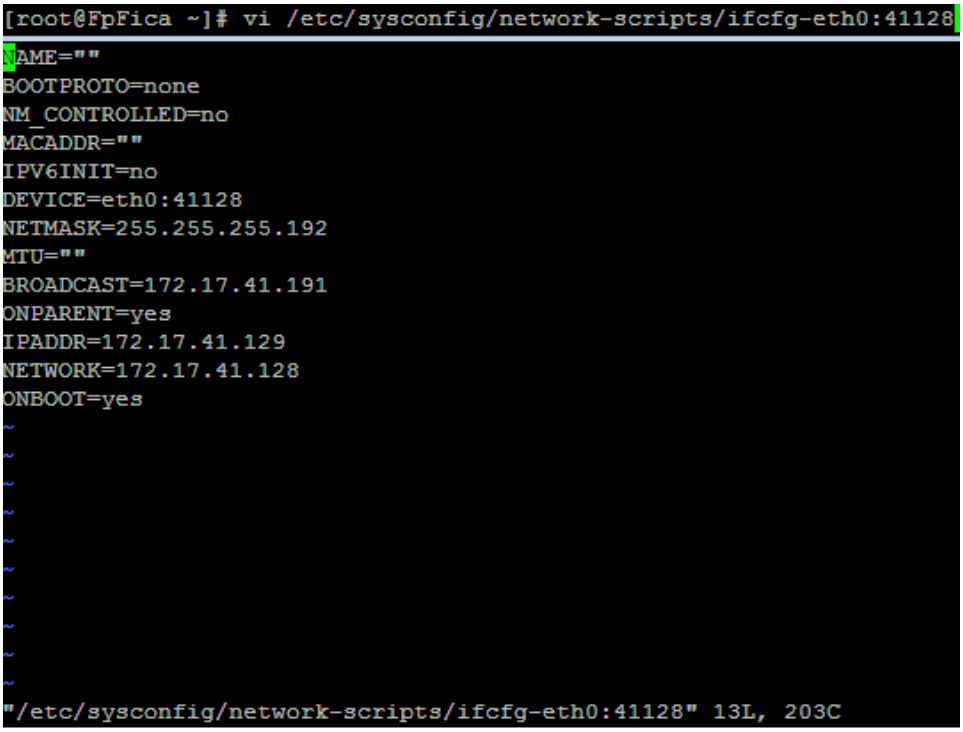


Figura 165.Configuración Interfaz de red Virtual eth0:41128

La séptima interfaz de red se configura como se muestra en la Figura 166.

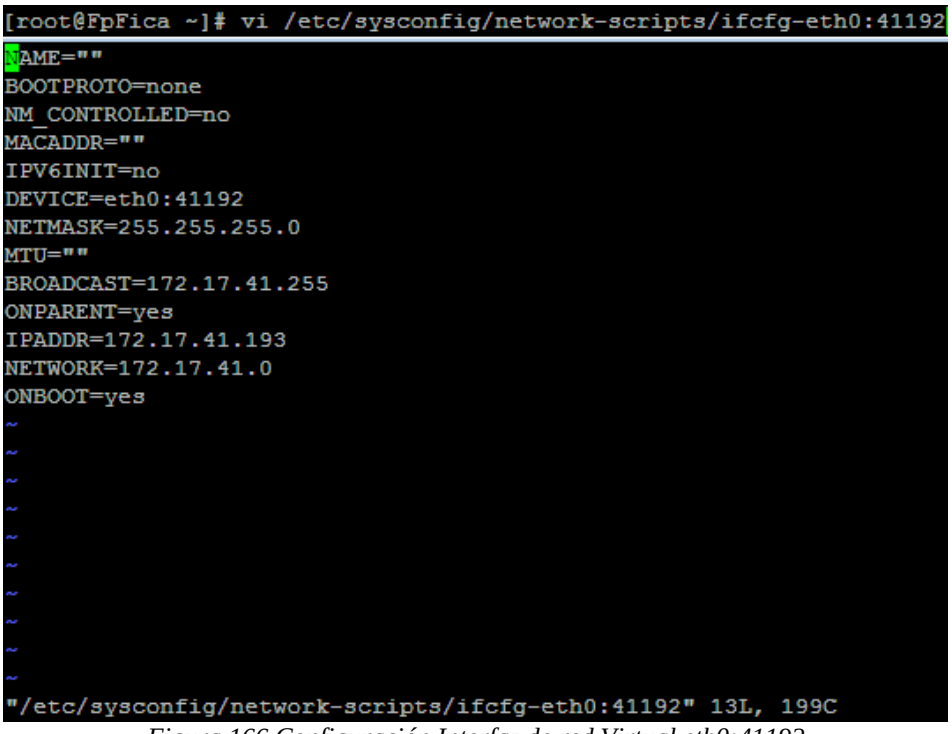


Figura 166.Configuración Interfaz de red Virtual eth0:41192
Fuente: Servicio CentOS

La interfaz de red física eth0 se configura como se muestra en la Figura 167. En algunos casos el fichero ya está creado y tiene el nombre ifcfg-eth0.

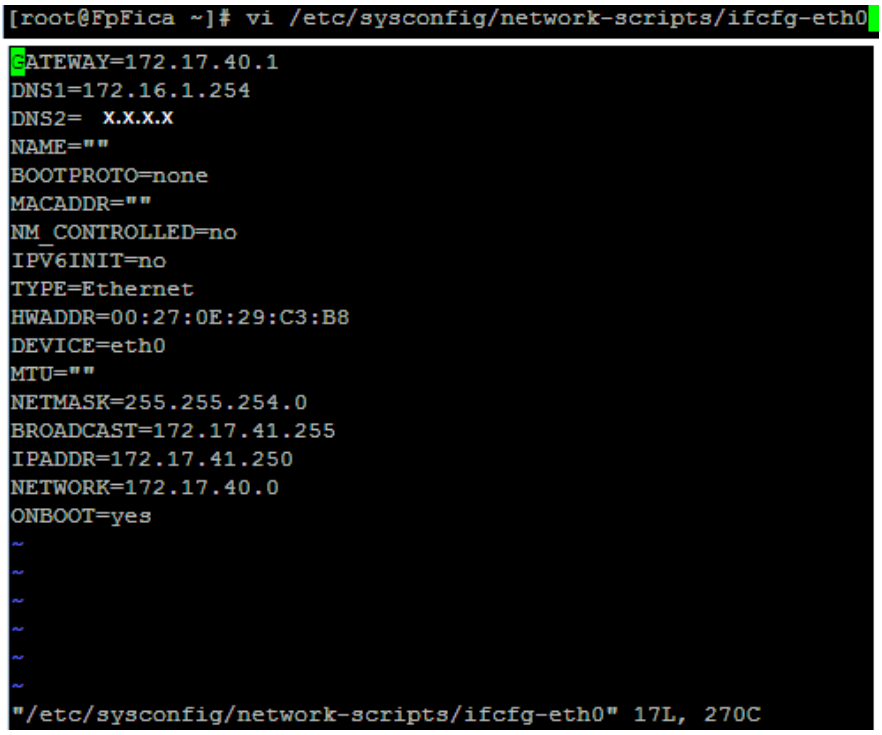


Figura 167.Configuración Interfaz de red Física eth0
Fuente: Servicio CentOS

Se verifica la creación de los archivos mediante el comando << ls /etc/sysconfig/network-scripts/>>, como se muestra en la Figura 168.

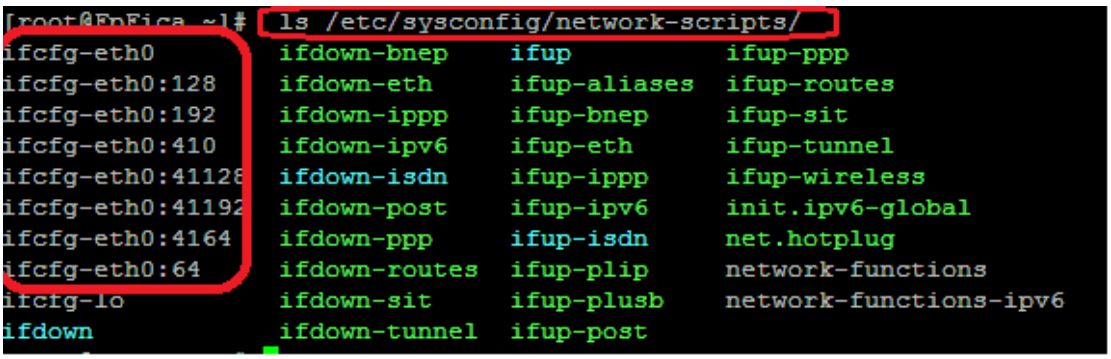


Figura 168. Lista de archivos de configuración de Interfaces de Red.
Fuente: Servicio CentOS

Se recomienda reiniciar el servicio mediante el comando << service network restart>> como se muestra en la Figura 169, para que los cambias sean efectivos.

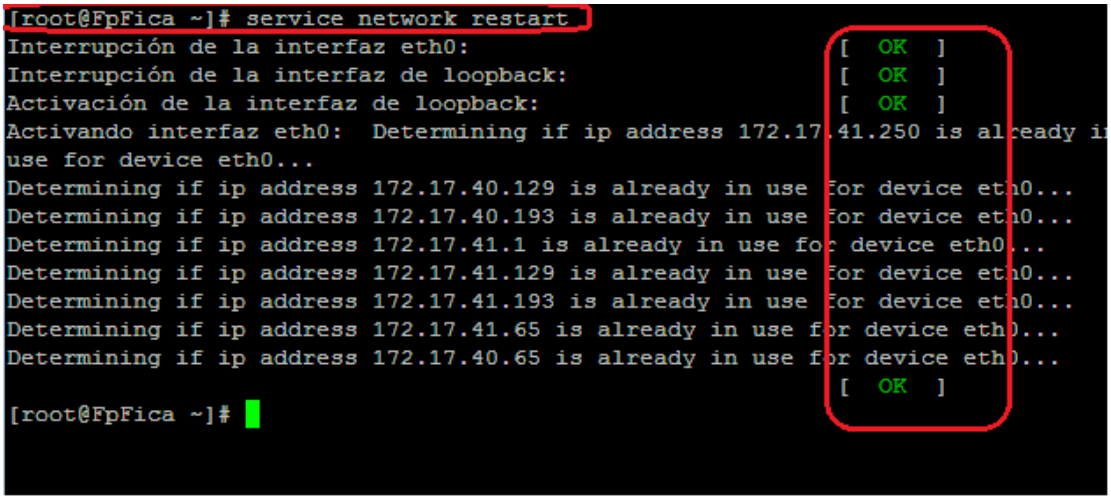


Figura 169.Reinicio de servicio de red..
Fuente: Servicio CentOS

1.2.2. Configuración de interfaces de red mediante Webmin.

Otra forma de configurar las interfaces de red es mediante la herramienta Webmin, (para permitir conexión a nuestro webmin habilitamos en la configuración de nuestro Firewall, ver sección configuración Firewall), para ello ingresamos a la administración por medio de un navegador de internet en este caso se usa Chrome. Escribimos en la barra de direcciones la dirección ip de nuestro servidor y el puerto por el cual se comunica Webmin por defecto es el 10000. Ver figura 170.

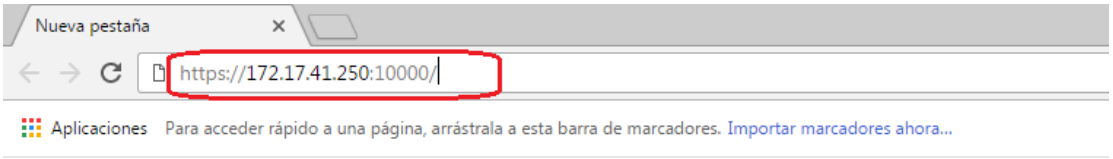


Figura 170. .Acceso a Webmin
Fuente: Servicio CentOS

Se debe autenticar como usuario root. Ver Figura 171.

Figura 171. Login Webmin
Fuente: Servicio Webmin

La pantalla de inicio de Webmin se puede apreciar en la Figura 172.

Figura 172.Pantalla de inicio Webmin
Fuente: Servicio Webmin

Para configurar las interfaces de red dirigirse a: Red-Configuración de red-Interfaces de Red. Ver Figura 173.

Figura 173.Direccion Configuración Interfaces de Red Webmin
Fuente: Servicio Webmin

Una vez en la dirección de configuraciones de red nos despliega en la pantalla las interfaces de red con las que cuenta el sistema como se muestra en la Figura 174.

Figura 174. Interfaces de Red disponibles en el sistema
Fuente: Servicio Webmin

Seleccionamos la interfaz de red eth0 dando click sobre ella y nos despliega una pantalla donde configuraremos según los parámetros necesarios. Para nuestro sistema nos quedara como nos muestra en la Figura 175. Damos a Salvar y Aplicar

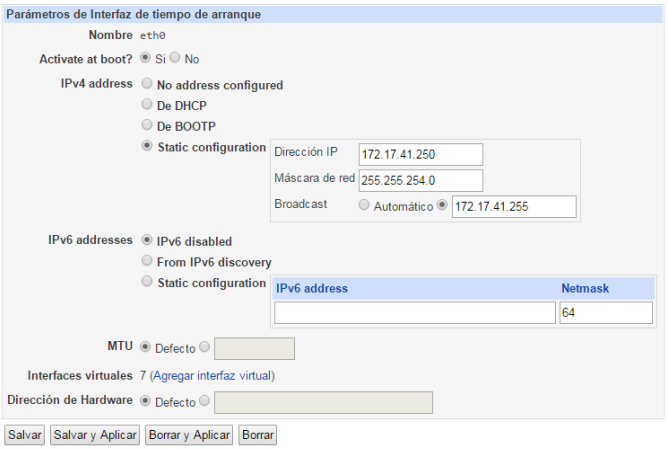


Figura 175. Configuración Interfaz de Red Física Webmin
Fuente: Servicio Webmin

Para configurar las interfaces de red Virtuales damos click sobre la interfaz eth0 y nos dirigimos hacia “Agregar Interfaz Virtual” como se muestra en la Figura 176.

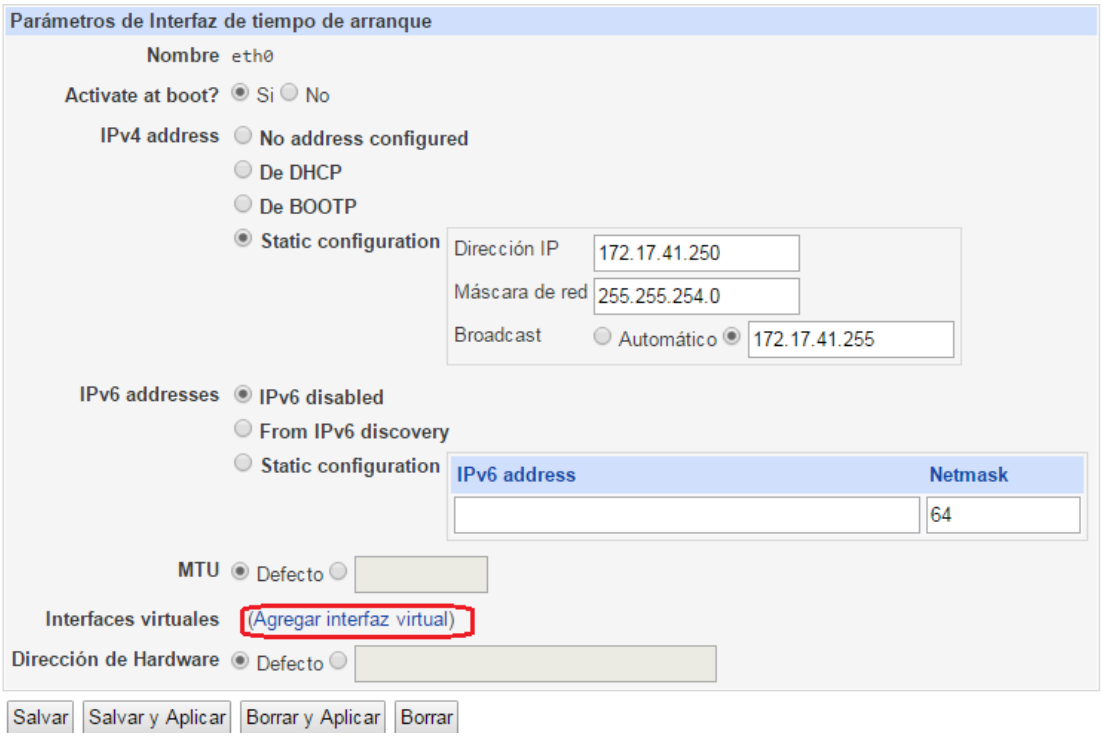


Figura 176. Agregar Interfaz Virtual Webmin
Fuente: Servicio Webmin

Los parámetros que llenamos son los de dirección Nombre, Dirección IP y Mascara de red, como se muestra en la Figura 177. Le damos a Crear y Aplicar.

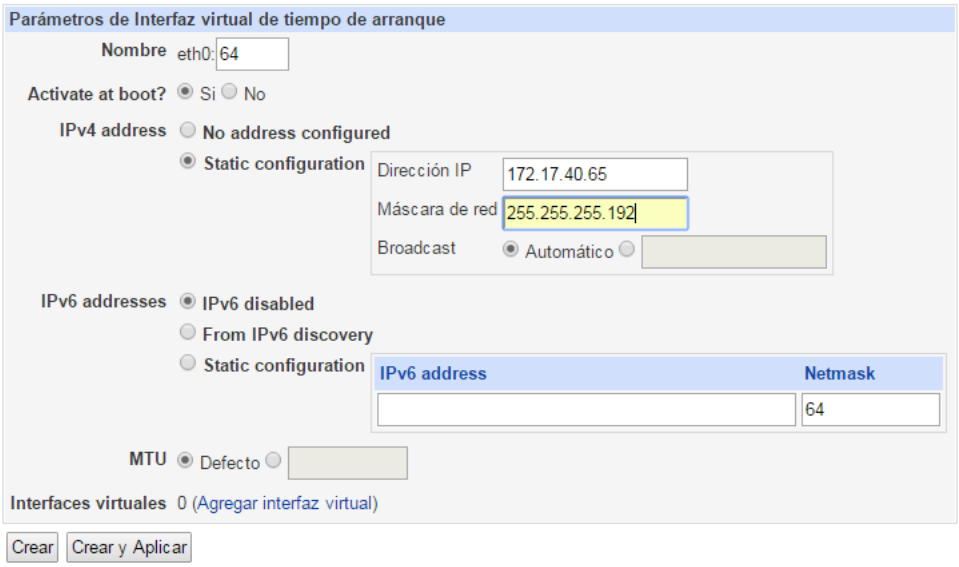


Figura 177. Agregar Primera Interfaz Virtual Webmin
Fuente: Servicio Webmin

El proceso se repite hasta crear las 7 interfaces de red virtuales como se muestra en la Figura 178.

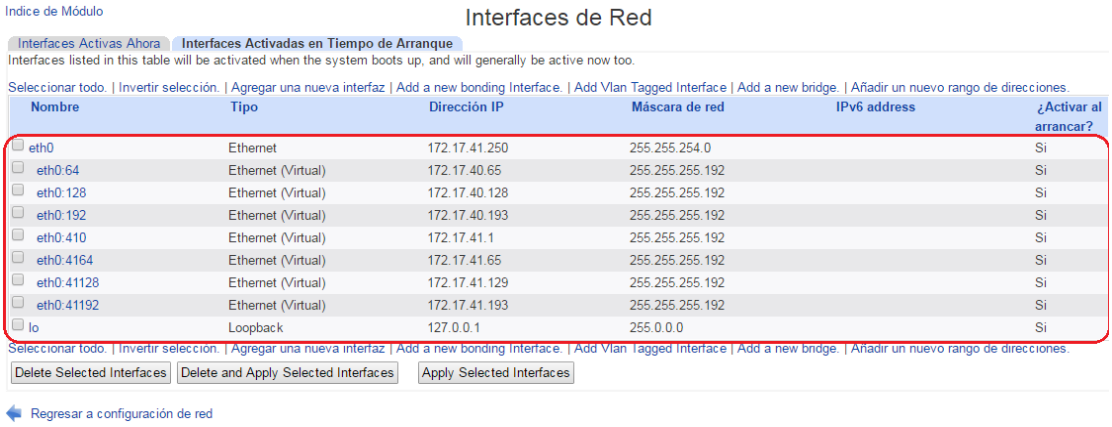


Figura 178. Interfaces de red Virtuales creadas- Webmin
Fuente: Servicio Webmin

2. Configuración Firewall.

Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

2.1. Creación archivo iptables3.sh

Para la configuración de Firewall de nuestro sistema Haremos uso de netfilter mediante iptables.

Para ello crearemos un script con la extensión .sh. Lo llamaremos iptables3.sh donde se ejecutarán las instrucciones de iptables. Ver Figura 179.

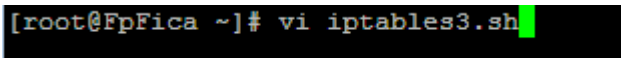


Figura 179. Creación de Archivo para Script iptables
Fuente: Servicio Webmin

2.2. Configuración inicial Script Shell

El archivo debe contener el siguiente contenido.

- Enlace a la actual configuracion shell del sistema
- Saludo a la afición (echo)
- Borrado de las reglas aplicadas actualmente (flush)
- Habilitar el forward de nuestro sistema
- Aplicación de políticas por defecto para INPUT, OUPUT, FORWARD

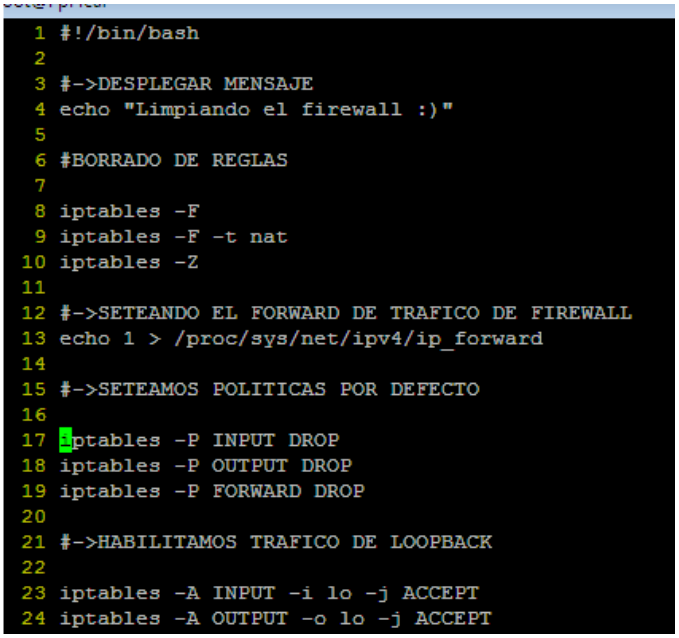
Los parámetros de configuración inicial se muestran en la Figura 180.

```
#!/bin/bash

#->DESPLEGAR MENSAJE
echo "Limpiando el firewall :)"

#BORRADO DE REGLAS

iptables -F
iptables -F -t nat
iptables -Z

#->SETEANDO EL FORWARD DE TRAFICO DE FIREWALL
echo 1 > /proc/sys/net/ipv4/ip_forward

#->SETEAMOS POLITICAS POR DEFECTO

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Figura 180. Configuración Inicial Script Shell iptables
Fuente: Servicio Terminal Centos

2.3. Habilitar Tráfico de loopback

La habilitación de tráfico de loopback permite acelerar posesos internos del sistema operativo. Para habilitar el tráfico de loopback se asignan las sentencias como se muestra en la Figura 181 en las líneas 23 y 24.



```
#!/bin/bash

#->DESPLEGAR MENSAJE
echo "Limpiando el firewall :)"

#BORRADO DE REGLAS

iptables -F
iptables -F -t nat
iptables -Z

#->SETEANDO EL FORWARD DE TRAFICO DE FIREWALL
echo 1 > /proc/sys/net/ipv4/ip_forward

#->SETEAMOS POLITICAS POR DEFECTO

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#->HABILITAMOS TRAFICO DE LOOPBACK

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Figura 181. Habilitar tráfico de loopback
Fuente: Servicio Terminal Centos

2.4. Manejo de estado de conexiones

Una de las características de importancia que está construida por encima del framework de netfilter es el seguimiento de conexiones (connection tracking). El seguimiento de conexiones le permite al núcleo llevar cuenta de todas las conexiones o sesiones lógicas de red y de este modo relacionar todos los paquetes que pueden llegar a formar parte de esa conexión. Esto nos permite disminuir el número de instrucciones que se deben establecer.

El seguimiento de conexiones clasifica cada paquete en uno de cuatro estados:

- NEW (nuevo)

Intentando crear una conexión nueva.

- ESTABLISHED (establecido)

Parte de una conexión ya existente.

- RELATED (relacionado)

Relacionada, aunque no realmente parte de una conexión existente.

- INVALID (inválido)

No es parte de una conexión existente e incapaz de crear una conexión nueva.

El manejo de estado de conexiones se puede apreciar en la Figura 182 en las líneas 34,35 y 36.

```
25
26
27
28
29          #--->MANEJO DE ESTADOS DE CONEXIONES
30
31 #->HABILITAR TODAS LOS CONEXIONES ESTABLECIDAS Y RELACIONADAS
32
33
34 iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
35 iptables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT
36 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
37
```

Figura 182. Manejo de estado de Conexiones
Fuente: Servicio Terminal Centos

2.4. Variables de entorno

Las variables de entorno es el conjunto de variables que forman parte del entorno operativo de nuestro script. Nuestras variables, las cuales vamos a utilizar, son los segmentos de red.

Las variables de entorno definidas se pueden apreciar en la Figura 183 en las líneas de la 43 a la 50.

```
41 #->VARIABLES DE ENTORNO
42
43 SUBREDLAB1="172.17.40.64/26"
44 SUBREDLAB2="172.17.40.128/26"
45 SUBREDLAB3="172.17.40.192/26"
46 SUBREDLAB4="172.17.41.0/26"
47 SUBREDLAB5="172.17.41.64/26"
48 SUBREDLAB6="172.17.41.128"
49 SUBREDLAB7="172.17.41.192"
50 SUBREDLABS="172.17.40.0/23"
```

Figura 183. Variables de Entorno
Fuente: Servicio Terminal Centos

2.5. Reglas Input.

Las reglas input se aplican a los paquetes que entran a nuestra máquina, quiere decir las que tienen ip destino nuestro equipo.

Las reglas input definidas se pueden apreciar en la Figura 184.

- La línea 55 se acepta el tráfico con destino al puerto 22 SSH.
- La línea 58 acepta el tráfico con destino a nuestra herramienta grafica Webmin puerto 10000.
- La línea 61 acepta conexiones con el protocolo ICMP.
- Las Líneas 64, 65, 66 y 67 son las configuraciones para habilitar tráfico a nuestro proxy.
- Las Líneas 70 y 71 permite tráfico entrante del servidor DNS.
- La línea 75 deniega todo tipo de acceso de una botnet a nuestro equipo.

```
52          ##--->REGLAS INPUT <---##
53
54 #->Habilitamos la admin del firewall via SSH puerto 22
55 iptables -A INPUT -p tcp --dport 22 -j ACCEPT
56
57 #->Habilitamos acceso al servidor via webmin puerto 10000
58 iptables -A INPUT -p tcp --dport 10000 -j ACCEPT
59
60 #->Habilitamos trafico icmp
61 iptables -A INPUT -s $SUBREDLABS -p icmp -j ACCEPT
62
63 #->Habilitamos acceso al servidor proxy puerto 3128
64 iptables -A INPUT  -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
65 iptables -A INPUT -p udp -m state --state NEW --dport 80 -j ACCEPT
66 iptables -A INPUT -p tcp -m state --state NEW --dport 80 -j ACCEPT
67 iptables -A INPUT -s $SUBREDLABS -p tcp --dport 3128 -j ACCEPT
68
69 #->Habilitamos acceso a servidor DNS puerto 53
70 iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
71 iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
72
73 # DENEGAMOS ACCESO ABOTNET
74
75 iptables -A INPUT -s $SUBREDLABS -d 113.105.144.172/32 -j DROP
```

Figura 184. Reglas Input
Fuente: Servicio Terminal Centos

2.6. Reglas Forward.

Las reglas forwad se aplican a paquetes que pasan por nuestro equipo pero que no tiene destino ni origen nuestro servidor.

Las reglas forward asignadas en la Figura 185 permiten el tráfico hacia los recursos compartidos de Windows.

```
77          ##--->REGLAS FORWARD <---#
78
79 #->Habilitamos acceso forward a recursos compartidos (archivos) windows
80 iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 139 -j ACCEPT
81 iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 445 -j ACCEPT
82 iptables -A FORWARD -s $SUBREDLABS -p udp --dport 137 -j ACCEPT
83 iptables -A FORWARD -s $SUBREDLABS -p udp --dport 138 -j ACCEPT
```

Figura 185. Reglas Forward
Fuente: Servicio Terminal Centos

Para ejecutar el archivo y las instrucciones del firewall se ejecuta el comando <<sh iptales3.sh>> como se muestra en la Figura 186.

```
[root@FpFica ~]# sh iptables3.sh
Limpiando el firewall :)
[root@FpFica ~]#
```

Figura 186. Ejecutar Script iptables
Fuente: Servicio Terminal Centos

3. Configuración Proxy Squid.

Para configurar los parámetros de squid hacemos uso de nuestra herramienta webmin para ello nos dirigimos a: Un-used Modules-Squid - Servidor Proxy, como se muestra en la Figura 187.

Figura 187. Dirección del módulo Squid
Fuente: Servicio webmin

3.1. Puertos y trabajo en Red

Seleccionamos la Opción Puertos y Trabajo en Red donde definimos que puerto utilizara el servidor proxy la y la dirección IP. Lo parámetros configurados se muestran en la figura 188.

El puerto que usa squid es el 3128 Una vez configurado le damos a Salvar.

Figura 188. Puertos y trabajo en Red.
Fuente: Servicio webmin

3.2. Opciones de Cache

Esta opción se utiliza para establecer que tamaño se desea que utilice Squid para almacenamiento de caché en el disco duro. De modo predeterminado Squid utilizará el formato ufs para crear en el directorio /var/spool/squid un caché de 100 MB, dividido en jerarquías de 16 directorios subordinados, hasta 256 niveles cada uno.

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se consumirá menos el ancho de banda.

El formato de cache ufs puede llegar a bloquear el proceso principal de Squid en operaciones de entrada/salida sobre el sistema de archivos cuando hay muchos clientes conectados. Para evitar que esto ocurra, se recomienda utilizar ufs asíncrono, que utiliza

el mismo formato de ufs, pero funciona de manera asincrónica, consiguiéndo un mejor desempeño.

La configuración de cache se muestra en la Figura 189.

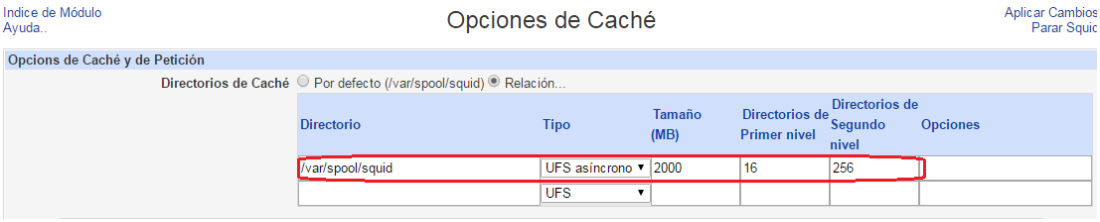


Figura 189. Opciones de Cache.
Fuente: Servicio webmin

3.3. Opciones de Memoria.

Límite de uso de memoria se utiliza para definir el tamaño máximo de los objetos en el caché. Se recomienda establecerla en escenarios con alta carga de trabajo, puesto que permite evitar desperdiciar recursos de sistema almacenando en el caché objetos de gran tamaño que probablemente sólo sean aprovechados por unos pocos usuarios, optimizando el uso del caché con objetos pequeños que de otro modo generarían una gran cantidad de peticiones hacia las redes públicas.

Es posible realizar una limpieza automática del caché de Squid cuando éste llegue a cierta capacidad. La opción “Marca de Bajamar de Disco” establece el porcentaje a partir del cual se comenzará a limpiar el cache. La opción “Marca de Pleamar de Disco” establece el porcentaje a partir del cual se comenzará a limpiar de manera agresiva el cache.

Los valores recomendados y establecidos se muestran en la Figura 190.

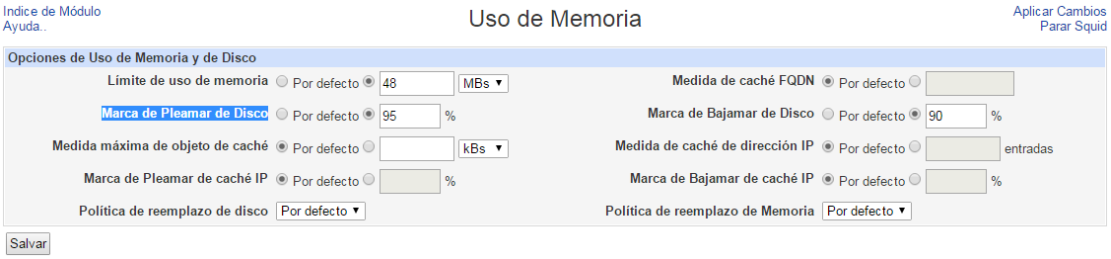


Figura 190. Opciones de Memoria.
Fuente: Servicio Webmin

3.4. Listas de control de Acceso

Para poder controlar el tráfico de los clientes hacia Internet, es necesario establecer Listas de Control de Acceso que definan una red. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

3.4.1. Dirección de Cliente

Si se desea establecer una lista de control de acceso que abarque a toda la red o subred local, basta con definir la IP correspondiente a la red y la máscara de la sub-red.

Para ello nos dirigimos a control de Acceso. Ver Figura 191

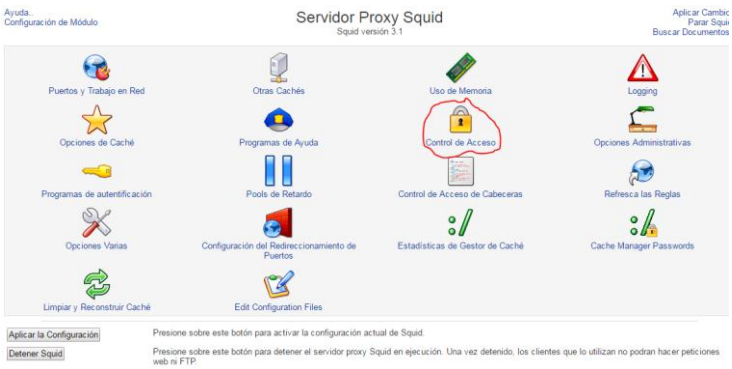


Figura 191. Dirección del cliente.
Fuente: Servicio Webmin

Seleccionamos la pestaña Listas de Control de Acceso Ver Figura 192.

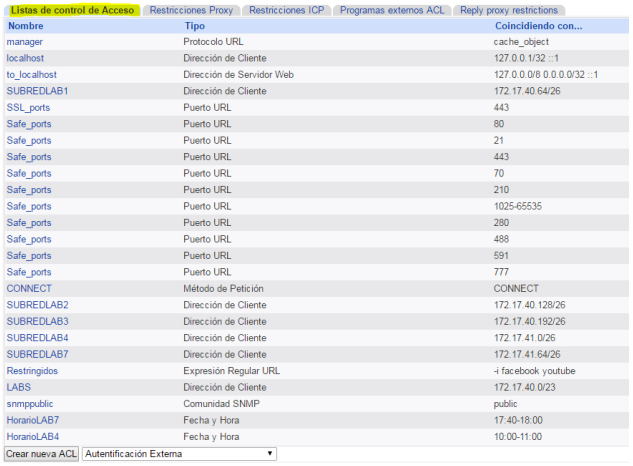


Figura 192. Lista de Control de Acceso.
Fuente: Servicio Webmin

En la parte inferior se encuentra un submenú donde nos permite crear las ACL para definir las subredes seleccionamos “Dirección de cliente” y definimos la primera subred. Ver Figura 193.

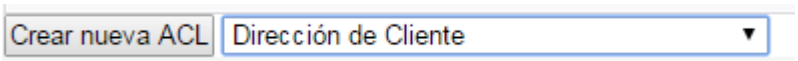


Figura 193. Crear lista de Control de Acceso.
Fuente: Servicio Webmin

Especificamos la dirección de red y la máscara de red y le damos a salvar. Ver Figura 194.

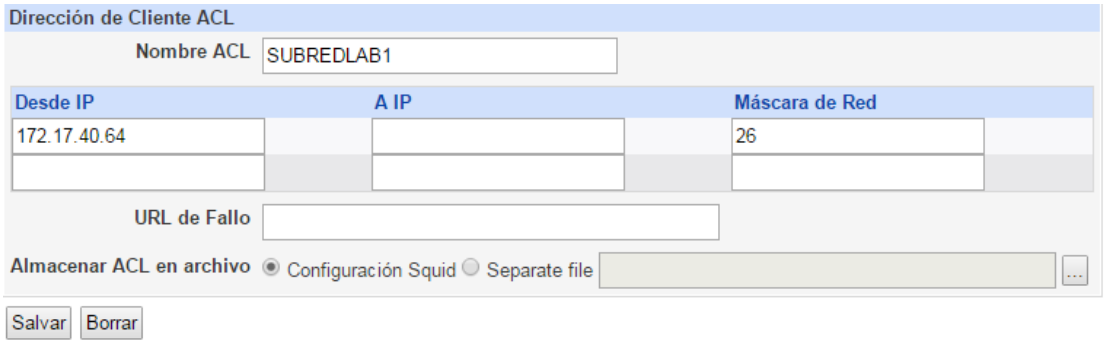


Figura 194. Crear lista de Control de Acceso-Cliente.
Fuente: Servicio Webmin

Se debe crear listas de acceso con todas las direcciones de clientes que contengan las subredes de laboratorios. Ver Figura 195.

Nombre	Tipo	Coincidiendo con...
manager	Protocolo URL	cache_object
localhost	Dirección de Cliente	127.0.0.1/32 ::1
to_localhost	Dirección de Servidor Web	127.0.0.0/8 0.0.0.0/32 ::1
SUBREDLAB1	Dirección de Cliente	172.17.40.64/26
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	591
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT
SUBREDLAB2	Dirección de Cliente	172.17.40.128/26
SUBREDLAB3	Dirección de Cliente	172.17.40.192/26
SUBREDLAB4	Dirección de Cliente	172.17.41.0/26
SUBREDLAB7	Dirección de Cliente	172.17.41.64/26
Restringidos	Expresión Regular URL	-i facebook youtube
LABS	Dirección de Cliente	172.17.40.0/23

Figura 195. Crear lista de Control de Acceso.
Fuente: Servicio Webmin

3.4.2. Expresión Regular

Para definir una lista de páginas web nos dirigimos al submenú crear nueva ACL "Expresión Regular URL". Ver Figura 196.

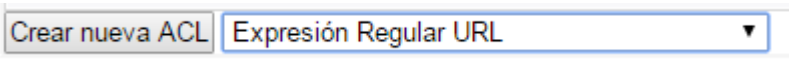


Figura 196. Expresión Regular URL.
Fuente: Servicio Webmin

En la Figura 197 se puede ver la forma de especificar las expresiones que se usan o la dirección completa de una página web. Especificadas los nombres de páginas web damos a Salvar. En este caso asignamos las páginas web de Facebook y YouTube.

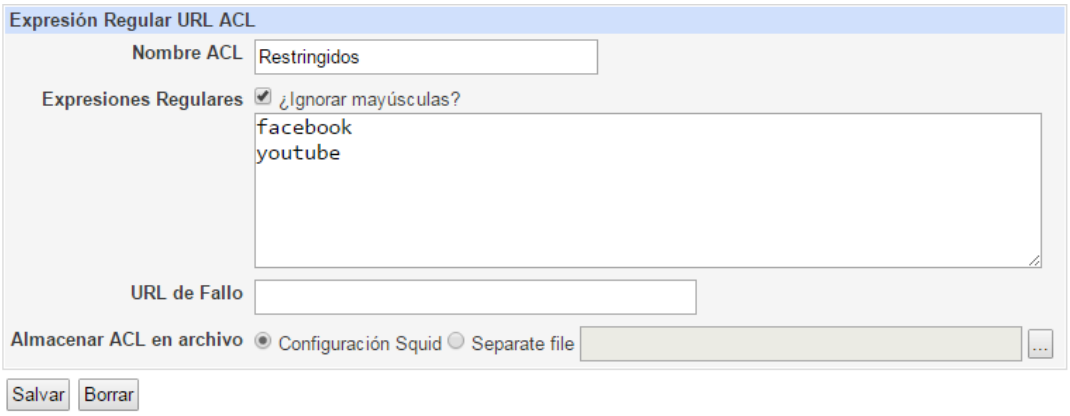


Figura 197. Expresión Regular URL-Configuración.
Fuente: Servicio Webmin

3.4.3 Fecha y Hora

Para configurar una ACL que contenga un horario en el submenu crear ACL seleccionamos Fecha y Hora, como se muestra en la Figrua 198.

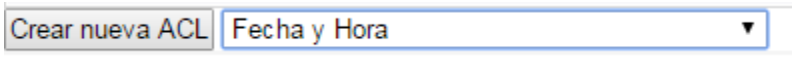


Figura 198. ACL Fecha y Hora.
Fuente: Servicio Webmin

Para el ejemplo creamos una ACL que defina un horario de 17:40 a 18:00, como se muestra en la Figura 199.

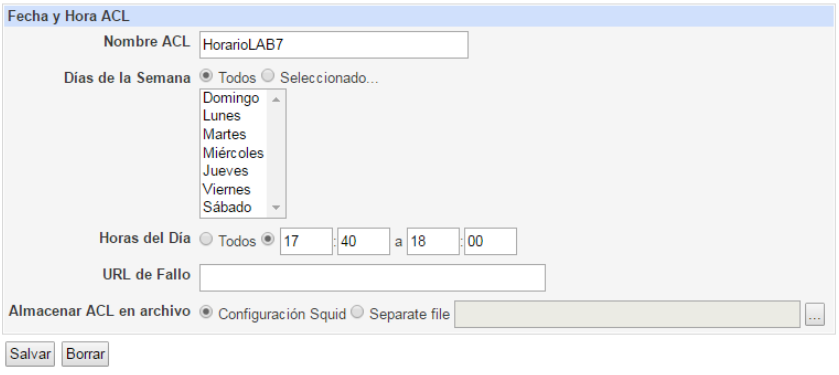


Figura 199. Configuración-ACL Fecha y Hora.
Fuente: Servicio Webmin

3.5 Restricciones Proxy

Las restricciones del proxy definen si se permite o deniega acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Estas Restricciones se ejecutan de manera, estructurada quiere decir que el cumplimiento de las mismas es en orden de acuerdo a la lista. Se ejecuta la que este primero.

Para acceder a estas opciones seleccionamos la pestaña Control de Acceso. Ver Figura 200.

Figura 200. Menú Restricciones Proxy.
Fuente: Servicio Webmin

3.5.1 Añadir Restricción Proxy

Para añadir una restricción damos click a "Añadir restricción proxy" y configuramos la restricción de forma adecuada a nuestro objetivo.

En el ejemplo la restricción se ejecuta a la ACL "SUBREDLAB7" que tenga acceso a internet en el horario que cumpla la ACL"HorarioLAB7" antes creados.

La configuración al objetivo se aprecia en la Figura 201.

Es necesario mencionar que es una restricción que va a permitir para ello se selecciona la Acción "permitir" y a su vez se seleccionan las ACL coincidentes que se requieren presionando la tecla ctrl.

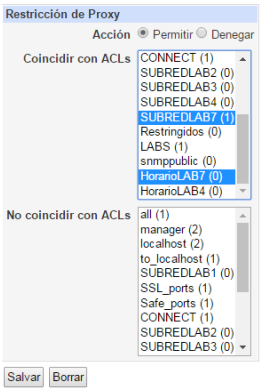


Figura 201. Restricción Proxy.
Fuente: Servicio Webmin

La restricción se muestra en la Figura 202. Para que los cambios sean efectivos dar click en Aplicar Cambios.

Figura 202. Restricción Proxy LAB7.
Fuente: Servicio Webmin

4. Análisis de Squid SARG.

Para acceder a la configuración del analizador de Squid nos dirigimos al menú Servidores y seleccionamos la pestaña "Generador de Informes de Análisis de Squid" como se muestra en la Figura 203.

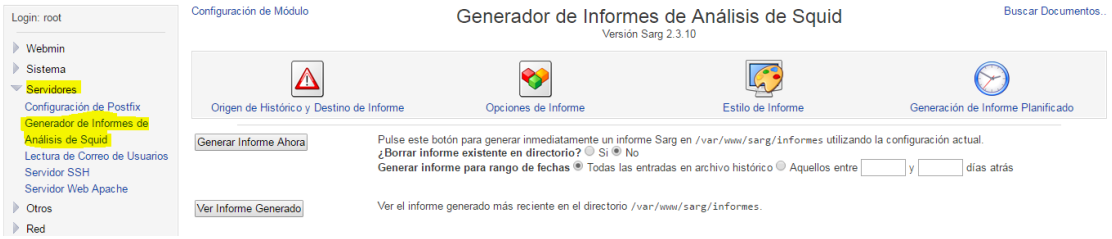


Figura 203. Menú SARG.
Fuente: Servicio Webmin

4.1. Origen de Histórico y Destino de Informe.

Verifique en la opción "Origen de Histórico y Destino de Informe" la ruta del archivo de registro, directorio donde almacenar los informes y número de reportes a almacenar. La configuración debe quedar como se muestra en la Figura 204.

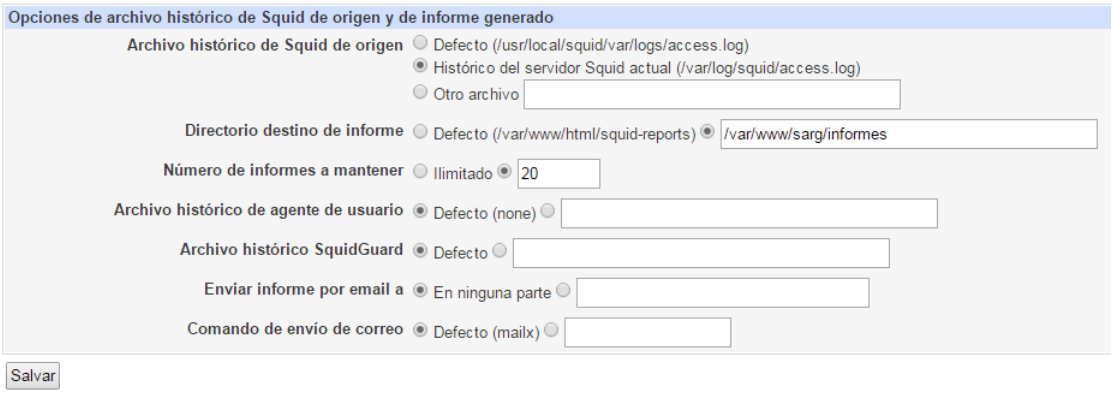


Figura 204. Origen de Histórico y Destino de Informe.
Fuente: Servicio Webmin

4.2. Generación de Informe Planificado

Para la generación de un informe podemos generarlo en el momento dando click a "Generar informe Ahora" o realizarlo de manera planificada. Ver Figura 205.

Figura 205. Generar Informe.
Fuente: Servicio Webmin

En nuestro ejemplo vamos a planificar la generación de informe todos los días de todas las semanas y todos los meses. El informe se generara a cada hora en un rango de 9am a 8pm.

La configuración se muestra en la Figura 206.

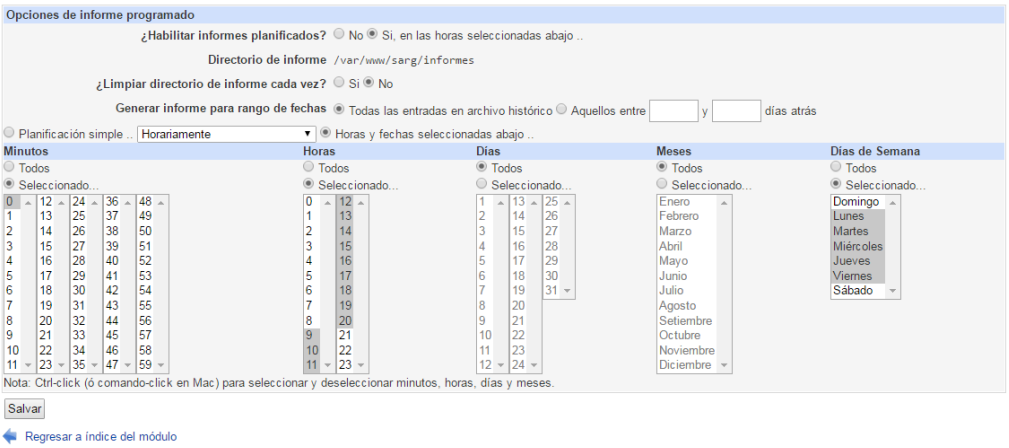


Figura 206. Informe Planificado.
Fuente: Servicio Webmin

4.3. Visualizar informes

Para visualizar los informes generados basta con dar Click en "Ver informe Generado", como se muestra en la Figura 207.

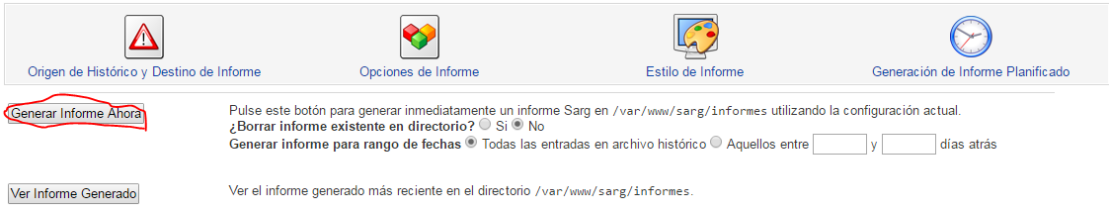


Figura 207. Ver Informe Generado.
Fuente: Servicio Webmin

Los informes se presentan en una lista siendo el final el más actual como se muestra en la Figura 208.

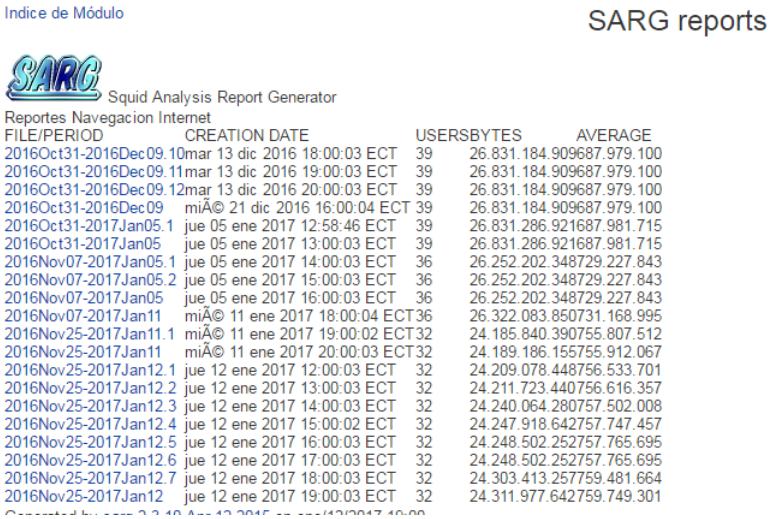


Figura 208. Lista de informes.
Fuente: Servicio Webmin

Al dar click sobre un informe se puede observar las diferentes opciones Ver Figura 209.

Reportes Navegacion Internet
Period: 2016 nov 25—2017 ene 12
Sort: bytes, reverse
Top users
Top sites
Sites & Users
Downloads
Denied accesses

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1	172.17.41.111	10.255	3.343.627.709	13,75%	0,22%	99,78%	37:01:19	133.279.832	3,61%
2	172.17.41.67	2.117	3.110.407.016	12,79%	0,04%	99,96%	14:47:36	53.256.514	1,44%
3	172.17.41.117	11.119	2.950.199.235	12,13%	0,72%	99,28%	143:33:32	516.812.464	14,00%
4	172.17.41.105	5.023	2.377.036.804	9,78%	0,33%	99,67%	65:06:54	234.414.473	6,35%
5	172.17.41.116	10.305	2.202.219.678	9,06%	0,55%	99,45%	137:32:37	495.157.837	13,41%
6	172.17.41.118	3.600	1.924.307.208	7,92%	0,63%	99,37%	47:10:12	169.812.657	4,60%
7	172.17.41.123	2.698	1.692.273.954	6,96%	0,33%	99,67%	32:59:19	118.759.954	3,22%
8	172.17.41.66	13.252	1.278.165.970	5,26%	1,38%	98,62%	189:40:54	682.854.600	18,49%
9	172.17.41.125	8.550	1.055.561.442	4,34%	0,68%	99,32%	54:07:56	194.876.805	5,28%
10	172.17.41.119	632	896.916.222	3,69%	0,11%	99,89%	07:31:55	27.115.055	0,73%
11	172.17.41.120	9.106	857.594.746	3,53%	0,77%	99,23%	52:42:49	189.769.678	5,14%
12	172.17.41.121	8.117	586.081.445	2,41%	1,50%	98,50%	20:03:37	72.217.327	1,96%
13	172.17.41.112	5.623	552.503.081	2,27%	2,00%	98,00%	51:25:17	185.117.494	5,01%
14	172.17.41.107	7.691	417.042.419	1,72%	0,80%	99,20%	20:14:41	72.881.695	1,97%
15	172.17.41.114	7.371	401.962.065	1,65%	3,95%	96,05%	20:30:06	73.806.527	2,00%
16	172.17.41.126	3.955	240.171.315	0,99%	1,13%	98,87%	41:28:31	149.311.383	4,04%
17	172.17.41.122	6.543	224.085.754	0,92%	2,77%	97,23%	40:59:41	147.581.880	4,00%
18	172.17.41.106	5.765	180.485.316	0,74%	3,75%	96,25%	37:59:04	136.744.418	3,70%
19	172.17.40.59	2.464	8.173.181	0,03%	97,06%	2,94%	02:55:20	10.520.380	0,28%
20	172.17.40.57	2.403	7.313.918	0,03%	96,86%	3,14%	02:29:36	8.976.098	0,24%
21	172.17.41.124	753	4.144.107	0,02%	15,99%	84,01%	03:27:42	12.462.404	0,34%
22	172.17.41.235	242	742.298	0,00%	88,56%	11,44%	01:13:06	4.386.101	0,12%
23	172.17.41.140	116	348.594	0,00%	95,33%	4,67%	00:15:23	923.919	0,03%
24	172.17.41.203	75	242.065	0,00%	83,41%	16,59%	00:12:33	753.172	0,02%
25	172.17.40.55	56	171.406	0,00%	95,74%	4,26%	00:05:48	348.844	0,01%
26	172.17.41.204	26	72.839	0,00%	100,00%	0,00%	00:00:00	0	0,00%
27	172.17.40.58	15	45.774	0,00%	100,00%	0,00%	00:00:00	0	0,00%
28	172.17.41.250	11	38.621	0,00%	100,00%	0,00%	00:00:00	0	0,00%
29	172.17.41.150	9	31.615	0,00%	100,00%	0,00%	00:00:00	0	0,00%
30	172.17.41.183	2	6.981	0,00%	100,00%	0,00%	00:00:00	53	0,00%
31	172.17.40.63	1	4.696	0,00%	100,00%	0,00%	00:00:00	0	0,00%
32	172.17.41.216	1	168	0,00%	0,00%	100,00%	00:00:22	22.001	0,00%
	TOTAL	127.896	24.311.977.642		0,71%	99,29%	1025:36:03	3.692.163.565	
	AVERAGE	3.996	759.749.301				32:03:00	115.380.111	

Figura 209. Reportes Navegación a Internet.
Fuente: Servicio Webmin

Anexo 3. Modelo Encuesta realizada a jefes de laboratorios de cómputo.

UNIVERSIDAD TECNICA DEL NORTE
FACULAD DE INGENIERIA EN CIENCIAS APLICADAS
CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACIÓN

La presente encuesta tiene como objetivo obtener datos que generen una idea clara para detallar políticas de seguridad a implementar en el diseño de un firewall-proxy, que servirá como alternativa para disminuir tráfico prescindible en la red de datos de la facultad.

Marque con una X las opciones

1. **¿Cuenta con un sistema que impida tráfico malicioso que se genera por el uso de los equipos en los laboratorios?**

Si	
No	

2. **¿Gestiona el acceso a Internet relacionado con sitios web maliciosos?**

Si	
No	

3. **¿De la siguiente lista que tipo de sitios web restringiría?**

Relacionados con Pornografía	
Relacionados con virus Informáticos	
Relacionado con Malware	
Otros	

Si eligió otros mencione a continuación los sitios

---

4. **¿Evitaría las actualizaciones Automáticas de Windows?**

Si	
No	

5. **¿Registra la actividad de los usuarios de los equipos de cómputo de los laboratorios?**

Si	
No	

6. **¿Restringiría el acceso al servicio de internet, si en algún horario se lo requiere?**

Si	
No	

7. **En los horarios que no se usan los laboratorios ¿evitaría generar tráfico en la red?**

Si	
No	

8. **De la siguiente lista qué servicios ofrece Los Laboratorios de cómputo**

Acceso a recursos compartidos en Windows	
Acceso a recursos compartidos Linux	
Acceso a servidores de Bases de Datos	
Acceso a servidor HTTP	
Otro	

Si maneja otro tipo de Servicios mencione a continuación

---

9. **En qué medida esta Ud. Interesado en gestionar el acceso al servicio de Internet de los Laboratorios**

Totalmente interesado	
Interesado	
No está interesado	

10. ¿En qué horarios se utilizan los Laboratorios?

	LAB1					LAB2					LAB3					LAB4					LA	
	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M

Anexo 4. Monitoreo de CPU Switch de distribución Fica.

Sin Proxy	Con Proxy
CPU utilization :: 18%/0%; CPU utilization :: 18%/0%; CPU utilization :: 13%/0%; CPU utilization :: 13%/0%; CPU utilization :: 17%/0%; CPU utilization :: 17%/0%; CPU utilization :: 17%/0%; CPU utilization :: 19%/0%; CPU utilization :: 19%/0%; CPU utilization :: 19%/0%; CPU utilization :: 19%/0%; CPU utilization :: 19%/0%; CPU utilization :: 14%/0%; CPU utilization :: 30%/0%; CPU utilization :: 30%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 19%/0%; CPU utilization :: 19%/0%; CPU utilization :: 30%/0%;	CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 15%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 16%/0%; CPU utilization :: 18%/0%; CPU utilization :: 14%/0%; CPU utilization :: 18%/0%; CPU utilization :: 14%/0%; CPU utilization :: 20%/0%; CPU utilization :: 14%/0%; CPU utilization :: 20%/0%; CPU utilization :: 15%/0%; CPU utilization :: 19%/0%; CPU utilization :: 19%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 14%/0%; CPU utilization :: 15%/0%; CPU utilization :: 19%/0%;