UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA INGENIERÍA EN SISTEMAS COMPUTACIONALES

TEMA:

Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil

AUTOR:

GUERRA GUAMAN, VICTOR HUGO

Trabajo de titulación previo a la obtención del título de

INGENIERO EN SISTEMAS COMPUTACIONALES

TUTOR:

Ing. Toala Quimí, Edison, Mgs

Guayaquil, Ecuador

12 de Septiembre de 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por el **Guerra Guamán, Victor Hugo**, como requerimiento para la obtención del título de **Ingeniero en Sistemas Computacionales.**

Tutor:

_____
Ing. Edison José Toala Quimí, Mgs.

Director de la Carrera:

_____
Ing. Ana Isabel Camacho Coronel, Mgs.

Guayaquil, a los doce días del mes de septiembre del año 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA INGENIERÍA EN SISTEMAS COMPUTACIONALES

DECLARACIÓN DE RESPONSABILIDAD

Yo, Guerra Guamán, Víctor Hugo

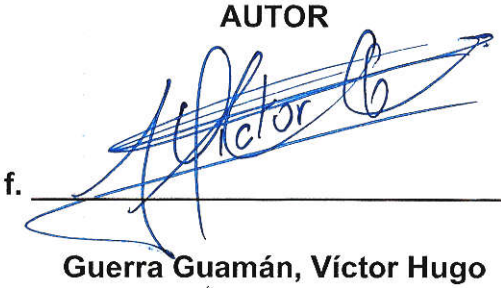
DECLARO QUE:

El Trabajo de Titulación, **Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil** previo a la obtención del título de Ingeniero en Sistemas Computacionales, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los (día) del mes de (mes) del año (año)

AUTOR



f. _____

Guerra Guamán, Víctor Hugo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA INGENIERÍA EN SISTEMAS COMPUTACIONALES

AUTORIZACIÓN

Yo, Guerra Guamán, Víctor Hugo

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 12 días del mes de Septiembre del año 2019

AUTOR:

f. _____

Guerra Guamán, Víctor Hugo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

REPORTE URKUND

URKUND

Documento	GUERRA VICTOR 20082019 (1).docx (D55121640)
Presentado	2019-08-29 21:39 (-05:00)
Presentado por	EDISON TOALA QUIMI (edison.toala@cu.ucsg.edu.ec)
Recibido	edison.toala.ucsg@analysis.urkund.com

1% de estas 39 páginas, se componen de texto presente en 4 fuentes.

TUTOR

f. _____

Ing. Edison José Toala Quimí, Mgs

AGRADECIMIENTO

En este proyecto, agradezco A Dios por siempre darme un día más de vida, a mis padres quienes me han apoyado en todo momento, al Ing. Edison Toala y al Ing. Gilberto Castro, quienes con su ayuda desinteresada, me brindaron información relevante, a mis amigos, que siempre han estado en las buenas y malas, agradezco a todos ellos que, de alguna u otra forma, me han ayudado a la culminación de este proyecto.

DEDICATORIA

Dedico este proyecto de titulación A Dios y a mis padres, A Dios porque siempre ha estado conmigo en todo momento, ayudándome, cuidándome y dándome fuerzas para seguir adelante, a mis padres, quienes me han brindado el estudio y valores, han sido pilares fundamentales en toda mi vida, depositándome toda su confianza ante cada reto que se ha cruzado en mi camino, gracias a ellos soy lo que soy ahora, los amo.

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

CARRERA INGENIERÍA EN SISTEMAS COMPUTACIONALES

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ing. Ana Isabel Camacho Coronel, Mgs

DIRECTORA DE CARRERA

f. _____

Ing. Vicente Adolfo Gallardo Posligua, Mgs.

COORDINADOR DEL ÁREA O DOCENTE DE LA CARRERA

f. _____

Ing. Galo Enrique Cornejo Gómez, Mgs.

OPONENTE

ÍNDICE GENERAL

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Se diseñó una infraestructura de red de datos funcional para el Centro de desarrollo de Software y Fábrica Iot con los recursos disponibles de la Facultad de Ingeniería, para el proceso se utilizaron varios equipos de comunicación tanto físicos como lógicos, el laboratorio está bajo estándares de cableado estructurado y de seguridad, mismos que se describieron para dar soporte a la solución. El proyecto se enfocó en la metodología cualitativa y no contiene tablas numéricas ni tabulaciones, sus métodos de recolección de datos permiten identificar todos los requerimientos dados por el usuario y de esta manera cumplir las necesidades. Para la implementación del laboratorio se utiliza un cableado de Cat 6 para tener una mejor frecuencia y será instalado en topología estrella bajo las estandarizaciones del cableado estructurado y por medidas de seguridad tiene instalado un firewall que va a contener 2 interfaces; una red WAN que permite la salida a internet y una red LAN donde se ha configurado el firewall con 5 interfaces virtuales donde cada una tiene diferentes configuraciones, una de esas interfaces estará configurada para dar señal de wifi. Además, en el laboratorio también se dispone de un software para monitoreo, con el cual se visualiza gráficamente el consumo de ancho de banda y los procesos de memoria de las computadoras. Finalmente se identificó, analizó, diseñó e implementó todos los requerimientos con los recursos disponibles de la sala de cómputo, dejando así una infraestructura de red de datos segura y funcional para el Centro de desarrollo y Fábrica de IoT.

Palabras Claves: (Infraestructura de datos, estándares cableado estructurado, interfaces virtuales, software de monitoreo)

ASTRACT

A functional data network infrastructure was designed for the Software Development Center and Factory Iot with the resources available from the Faculty of Engineering, for the process were used several communication equipment both physical and logical, the laboratory is under structured wiring and security standards, which were described to support the solution. The project focused on qualitative methodology and does not contain numerical tables or tabulations, its data collection methods allow to identify all the requirements given by the user and thus meet the needs. For the implementation of the laboratory a Cat 6 wiring is used to have a better frequency and it will be installed in star topology under the standardizations of the structured wiring and for security measures it has installed a firewall that is going to contain 2 interfaces; a WAN network that allows the exit to internet and a LAN network where the firewall has been configured with 5 virtual interfaces where each one has different configurations, one of those interfaces will be configured to give wifi signal. In addition, in the laboratory there is also a software for monitoring, with which the bandwidth consumption and the memory processes of the computers are graphically visualized. Finally, all the requirements were identified, analyzed, designed and implemented with the available resources of the computer room, thus leaving a secure and functional data network infrastructure for the IoT Development Center and Factory.

Keywords: (Data infrastructure, structured cabling standards, virtual interfaces, monitoring software)

INTRODUCCIÓN

En la actualidad a nivel mundial la mayoría de personas utilizan internet sea cual sea su propósito, el internet tiene un impacto sumamente fuerte en el ámbito laboral, conocimientos y ocio. La forma de que el internet llegue a sus destinos es por medio de una infraestructura de red, es la que permite a las personas tener conexión a cantidades extensas y diversas de información online

Las tendencias institucionales educativas en el ámbito de la comunicación digital, buscan brindar facilidades a los actores educativos determinando con anticipación sus necesidades de redes, actuales y futuras; respecto al aprovechamiento de recursos en cuanto a la multiplicidad de servicios de internet que se puede obtener con la asignación de direcciones públicas en equipo informático, considerando aspectos como: seguridad de información, ancho de banda, administración de usuarios y recursos de almacenamiento.

Los comportamientos de la infraestructura de red en las universidades del Ecuador cuentan con una seguridad total de la información que se maneja dentro de las mismas, por medio de esta infraestructura de red se ha podido realizar desarrollar programas y proyectos de investigación tecnológica o científica y abastecer las necesidades de los requerimientos de los estudiantes, la cual pretende colaborar a la sociedad.

La infraestructura de red en la Universidad Católica de Santiago de Guayaquil es una red privada, está diseñada para abastecer la señal de internet a todas las facultades, esta misma ayuda a los estudiantes a facilitar sus investigaciones.

La facultad de ingeniería de la universidad Católica de Santiago de Guayaquil, está creando su fábrica de software así como también la elaboración de sus productos IoT(Internet de las cosas) para lo cual, precisa de un diseño de red de estrella de modo que la operatividad de cada estación de trabajo sea independiente de otra; generando interdependencia del servicio de red en el momento de presentarse fallas técnica aleatoriamente.

En una estación de trabajo se necesita identificar las necesidades de sus requerimientos para su implementación, basados en la división de distintos segmentos de red, que separe ambientes de desarrollo, producción y pruebas estas pruebas implican conexiones a internet, para una problemática que se ha identificado que estos dispositivos van a soportar la fábrica de software y los productos IOT que no permiten la configuración de proxy.

CAPITULO I

EL PROBLEMA

Dentro del desarrollo de este capítulo se va a explicar sobre problemática identificada en el laboratorio de centro de desarrollo de software. Los planteamientos de los objetivos tanto generales como específicos se especificarán en este capítulo que tiene como fin cumplir el alcance de esta investigación.

Descripción del problema

La Facultad de Ingeniería tiene prevista la apertura de centro de desarrollo de software y laboratorio para IoT (Internet de las cosas) por lo cual es necesario implementar una red de datos bajo normas y estándares de infraestructura tecnológica que asegure el óptimo funcionamiento de sus servicios. El centro de desarrollo de software y laboratorio para IoT se encontrará ubicado en la sala de cómputo de la facultad de ingeniería.

En este sentido, se requiere la implementación tanto física como lógica de la infraestructura tecnológica, de acuerdo a los requerimientos operativos que se evidencien a lo largo de la investigación, así como a la aplicación de estándares y normativas de la industria y de seguridad vigentes; además, se considera necesario disponer de un sistema de monitoreo de la infraestructura implementada que muestre su disponibilidad, rendimiento y generación de alarmas en caso de presentar alguna afectación en sus servicios.

Los recursos de infraestructura de red con que actualmente cuenta la sala de cómputo de la Facultad de Ingeniería para la implementación del proyecto son limitados para lo cual habrá que maximizar su utilidad, asegurando la implementación de una infraestructura funcional, y que cumpla con las necesidades funcionales requeridas por la facultad.

Justificación del tema

La Facultad de Ingeniería busca proveer a sus estudiantes y docentes un área que disponga de los recursos tecnológicos necesarios para el desarrollo de sus actividades de carácter académicas, mediante la creación de un laboratorio de IoT

y de Fábrica de Software; por lo tanto, en respuesta ante este requerimiento, se precisa diseñar una infraestructura de red de datos.

Se considera que el desarrollo de la infraestructura de red sea de tipo LAN ya que se trabajará de manera segmentada y delimitado para un grupo de PC's.

El trabajo de titulación a desarrollarse responde a la línea de investigación establecida en la carrera Ingeniería en Sistemas computacionales, "Desarrollo de nuevos Productos y Servicios".

Alcance

Implementar la infraestructura de red para el laboratorio de IoT y el centro de desarrollo de software a nivel físico y lógico mediante la aplicación de los principales estándares y buenas prácticas de la industria, para este tipo de implementación.

Se considera posible que sea necesario implementar infraestructura para un ambiente de desarrollo para la creación de software, que permitirá el acceso total a las paginas necesarias para su creación, mientras que un ambiente de prueba podría ser configurado para restringir accesos a ciertas páginas de consumo masivo de datos y un ambiente de producción para ejecutar los softwares creados por los estudiantes que tendrán acceso total para su distribución.

Se realizará un análisis de las interfaces de monitoreo de red disponibles en el mercado, basadas en software libre y de libre distribución para realizar el monitoreo de la disponibilidad y del rendimiento de los equipos de la red de IOT y fábrica de software. Finalmente se diseñará y ejecutará un plan de pruebas que permitan garantizar el correcto funcionamiento de la infraestructura de red del laboratorio de IoT y del centro de desarrollo de software.

La ejecución de la implementación de la infraestructura de red será en el transcurso del periodo de UTE, que empieza desde el mes de mayo hasta el mes de septiembre y se realizará la implementación con los equipos existentes en el laboratorio de cómputo de la Facultad de Ingeniería.

Objetivos

En base al problema propuesto, se exponen los siguientes objetivos:

General

Diseñar e implementar la infraestructura de red para el centro de desarrollo de software y la fábrica para IoT de la facultad de ingeniería de la UCSG.

Específicos

- Identificar y analizar los requerimientos para la implementación de la infraestructura del centro de desarrollo de software y fábrica IoT; y, los recursos disponibles en el laboratorio de cómputo de la facultad de Ingeniería.
- Diseñar la propuesta de la solución integral de la infraestructura de datos para el centro de desarrollo de software y la fábrica IoT, con base en la disponibilidad de recursos del laboratorio de cómputo de la facultad de Ingeniería y a los estándares de la industria.
- Instalar y configurar la infraestructura de datos y seguridad con su correspondiente sistema de monitoreo.
- Realizar las pruebas de comunicación respectivas para validar el correcto funcionamiento de la infraestructura implementada.

Delimitación

La implementación de la infraestructura de red se llevará a cabo en la Universidad Católica de Santiago de Guayaquil en la Facultad de Ingeniería en el laboratorio de IoT y de Fábrica de Software, como una red funcional con los recursos de infraestructura disponible en el laboratorio.

Pregunta de investigación

Con respecto a la pregunta de investigación del trabajo de titulación parte de la problemática establecida y tiene como fin responderla en base a los objetivos establecidos.

¿Es posible implementar una red funcional con los recursos de infraestructura disponible en los laboratorios de cómputo de la facultad de ingeniería de la UCSG, así como la implementación de un sistema de monitoreo basado en software libre?

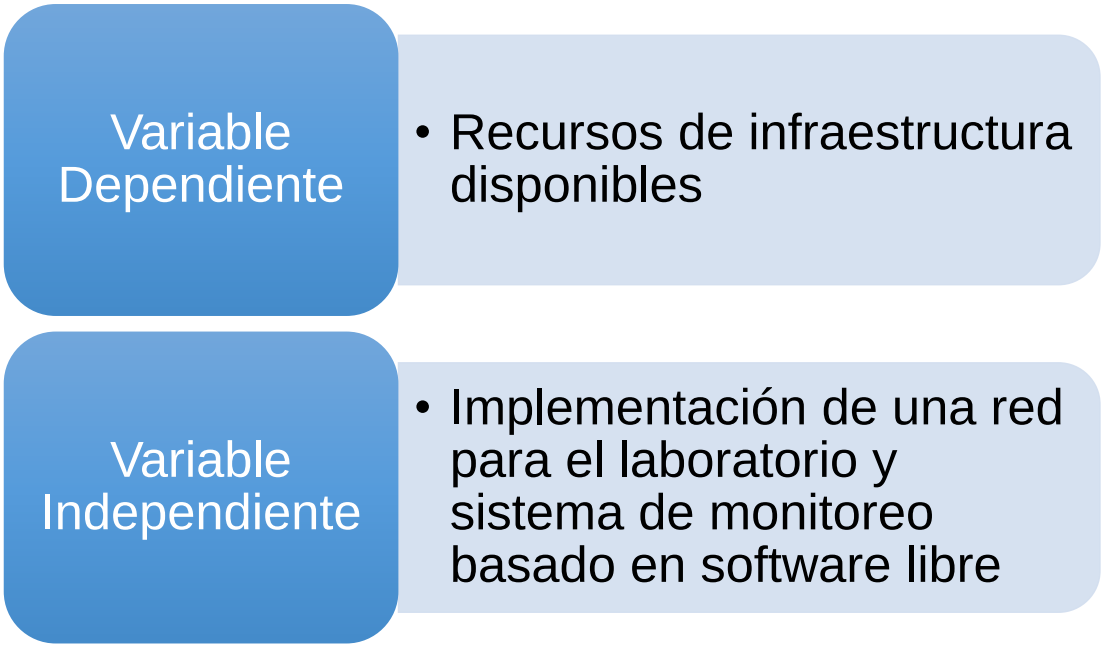


Figura 1: Variables

CAPITULO II

MARCO CONCEPTUAL

En este capítulo se explicará detalladamente la resolución del proyecto, se utilizará conceptos técnicos que ayudarán al desarrollo de este documento y así poder lograr un mejor entendimiento sobre el tema de titulación propuesto.

MARCO CONCEPTUAL

En el desarrollo del marco conceptual se describirán los principales conceptos o definiciones de los términos que se utilizarán durante el proceso de desarrollo e implementación del presente proyecto de titulación. Estos conceptos o términos se utilizarán para soportar el uso de los componentes lógicos y físicos de la solución propuesta.

REDES INFORMÁTICAS/NETWORKING

Una red informática respecto al autor Decarbo, (2014), aclara que:

"Las redes informáticas surgieron como una necesidad de interconectar diferentes computadoras de una empresa o institución para poder así compartir recursos y equipos específicos. Como tal, debemos pensar en un soporte físico que abarque el cableado, las placas necesarias para las computadoras, y un conjunto de programas que formen el Sistema Operativo de la Red. Se puede definir una red informática como un sistema de comunicación que conecta computadoras y otros equipos informáticos o dispositivos entre sí, con la finalidad de compartir información, recursos y por sobre todas las cosas, economiza el presupuesto de hardware y software."

Una red informática o también llamada red de computadoras o de ordenadores), es un conjunto de equipos (dispositivos o computadoras), que están conectados por medio de; cableado estructurado, señales u otro método para el transporte de datos, de manera que pueda compartir información, recursos y servicios, a cada una de los equipos conectados. La red informática

cuenta con varios tipos de red tales como: Red WAN, PAN, LAN, MAN, donde cada tipo de red está enfocada a diferentes áreas de trabajo y estas redes son desarrolladas bajo las siguientes topologías: Malla, Estrella, Árbol, Bus y Anillo.

Switchs

Básicamente un switch es un equipo de comunicación de datos que permite la interacción entre los dispositivos de una red local principalmente; sin embargo, en la actualidad la utilidad de los mismos no solo se circunscribe a nivel de redes locales, ni únicamente a la capa 2 de las capas OSI (Open System Interconection). De acuerdo a Iglesias (2019):

"Un switch es un dispositivo que sirve para conectar varios elementos dentro de una red. Estos pueden ser un PC, una impresora, una televisión, una consola o cualquier aparato que posea una tarjeta Ethernet o Wifi. Los switches se utilizan tanto en casa como en cualquier oficina donde es común tener al menos un switch por planta y permitir así la interconexión de diferentes equipos".

Figura 2 Switch. Tomado de Cisco SG250-10P - Switch Cisco Systems en LDLC (s. f.)

Complementando la descripción previamente dicha también es importante mencionar que los switches se clasifica en dos tipos administradores y no administradores. Con respecto a esto Cisco (2015a) menciona que los switch no administrables no necesitan de configuración, porque funcionan de forma automática y en su mayoría son utilizados para redes domésticas, mientras que los del tipo administrable brindan más

funciones configurables para la red, estos switch se pueden acoplar de forma remota o local para tener un control sobre el tráfico en el ancho de banda.

Switch Multicapa o Switch Capa 3

Es un dispositivo que opera hacienda uso de una tabla de direcciones MAC y la tabla de enrutamiento de un router, ofrece una mayor velocidad de transmisión, así mismo permite el control, el enrutamiento y comunicación entre-VLANS, en otras palabras, agrega funciones de conmutación y enrutamiento.

Características de los Switches

A continuación, veremos el funcionamiento y las principales características de los switchs

Tabla 1: Principales Características swichts

Características Generales

a. **Permiten la conexión de segmentos físico de red local (LAN)**	b. El primer puerto mayormente se lo utiliza para recibir la señal de la red
c. **Los switches son dispositivos que funcionan en la Capa 2 (Capa de Enlace) del modelo OSI**	d. Su función es interconectar dos o más segmentos de red en base a una dirección física de origen y destino.
e. **Las redes se conectan por medio de cables UTP**	f. Cuando reciben una señal cualquier puerto, la señal se comparte a los demás puertos

Nota: tomado de Vera & Martinez (2017)

Los switchs se puede utilizar e implementar en distintos escenarios ya sea para configurar

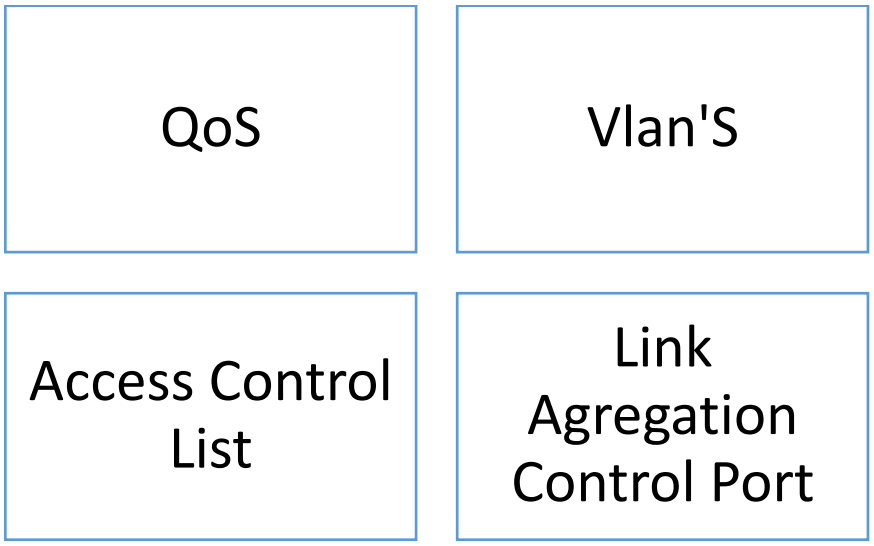


Figura 3: Elaborado por el autor (2019)

Una VLAN (Red de área local virtual), es una red de capa 2, que se encarga de unir una serie de dispositivos de una forma lógica creando particiones dentro una infraestructura de red, las cuales se configuran en un switch para ser controladas de una forma independiente; las VLANs ayudan a mejorar la flexibilidad en el control y cambios de la red.

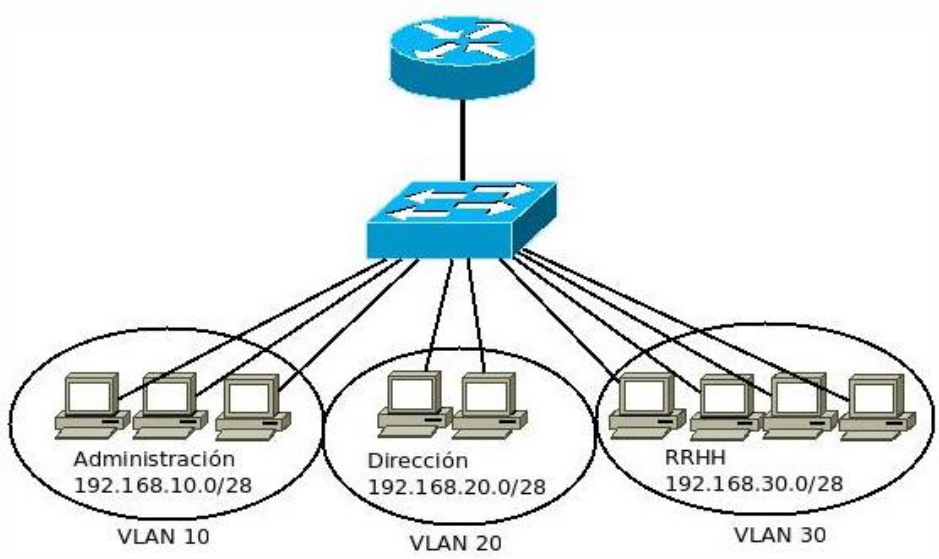


Figura 4: Ejemplo VLAN(«Introducción a las VLAN», 2010)

En la figura 4, se muestra las particiones de los dispositivos dentro de una misma red.

LACP (Link Agregation Control Port - Puerto de Control de Agregación de Enlaces): Forma parte de los estándares IEEE (802.3ad) el cuál es el encargado de crear varios puertos físicos que por medio de la creación de esos puertos lograrán integrar un único canal lógico, los LACP pueden utilizarse para proporcionar los EtherChannel en un ambiente de diferentes proveedores, estos mismos permiten hallar la configuración de ambos lados y se debe garantizar que sean compatibles para que el enlace EtherChannel pueda estar habilitado cuando sea necesario, IBM (2014) manifiesta que EtherChannel y LACP, son formas de agregar puertos de red los cuales van a permitir la incorporación de diversos adaptadores Ethernet.

Tabla 2 Diferencias entre la Agregación de enlaces IEEE 802.3ad y EtherChannel

EtherChannel	**Agregación de enlaces IEEE 802.3ad**
Requiere la configuración del conmutador.	Requiere la configuración del conmutador para el intercambio de unidad de datos del Protocolo de control de Agregación de enlaces (LACPDU).
Las pulsaciones no se intercambian entre el puerto del conmutador y el puerto del sistema adyacente.	Las pulsaciones (LACPDU) se intercambian durante el intervalo definido por el IEEE 802.3ad estándar. Las pulsaciones proporcionan protección adicional en caso de anomalía.

Nota: Tomado de (IBM, 2014a)

QoS o calidad de servicio asegura la fluidez del tráfico de red mediante diferentes mecanismos. De acuerdo a lo declarado por Cabello (2015) da a conocer que:

"QoS es el acrónimo de Quality of Service, o calidad de servicio, que establece diversos mecanismos destinados a asegurarnos la fluidez en el tráfico de la red. Para ello, lo que hace es dar prioridad al tráfico según el tipo de datos que transportan"

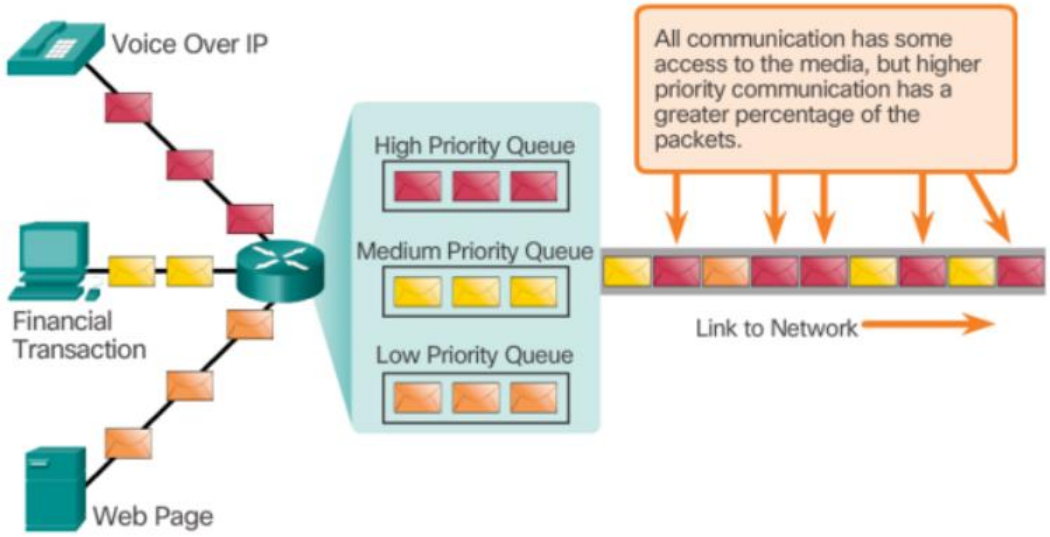


Figura 5: Ejemplo QoS. Elaborado por Salazar (2016)

En la figura 5, se muestra un ejemplo el tráfico de red y como QoS da prioridad a los datos de acuerdo a su orden de llegada, aplica el método FIFO (First in, first out – primero en entrar, primero en salir)

El control de acceso o ACL determina permisos de acceso y ayudan a controlar el tráfico de red, profundizando más en el tema Vera & Martinez (2017) puntualiza que:

"El control de Acceso es un concepto de seguridad usado para determinar permisos de acceso apropiados a un determinado objeto, en base a determinado criterio. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como Routers o Switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición" (p. 5).

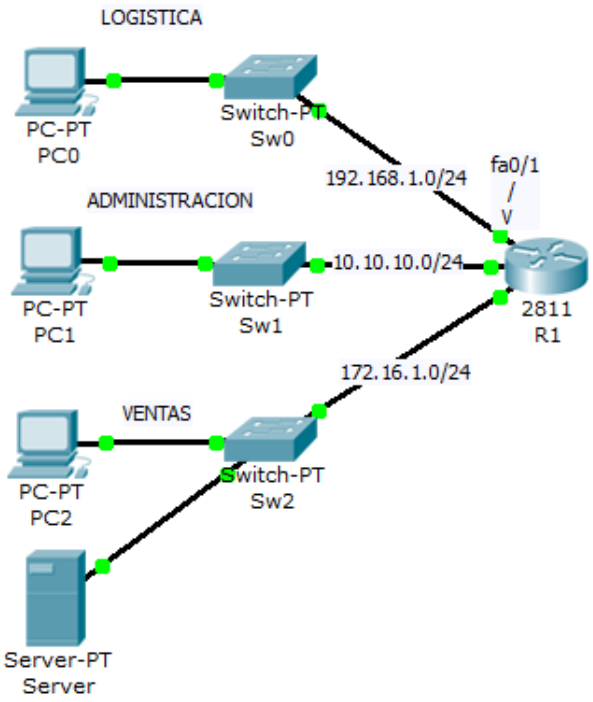


Figura 6: Ejemplo ACL. Elaborado por Rodrigo (2012)

En la figura 6, se muestra un ejemplo de cómo se maneja una lista de acceso dentro de una red, los paquetes son enviados desde el router a las respectivas áreas (Logística, Administración, Ventas) como se puede observar en la imagen.

Access Point

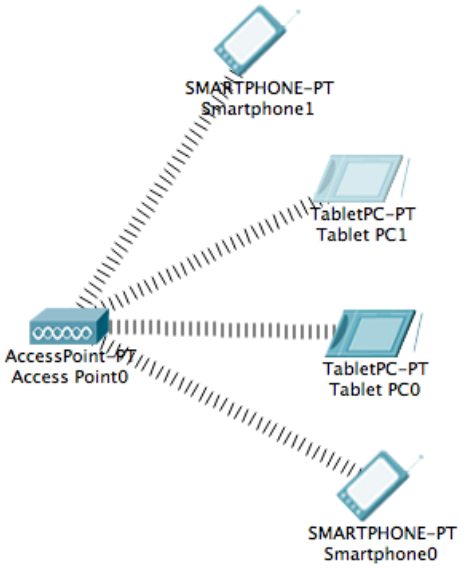
Se define como punto de acceso por sus siglas en ingles (Wireless Access Point), es un equipo de comunicación inalámbrico para formar una red inalámbrica, su conexión no necesita de cableado. Con respecto al autor Mesa (2016) aclara que un AP es:

"Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Habitualmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Diversos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red

donde los dispositivos cliente se administran a sí mismos sin la necesidad de un punto de acceso convirtiéndose en una red ad-hoc). Los puntos de acceso inalámbricos tienen direcciones IP determinadas, para poder ser configurados.”

Figura 7 Access Point. Elaborado por el autor (2019)

De acuerdo a las palabras expresadas por el autor el Access Point tiene



Son los encargados de transformar la red de forma inalámbrica, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

Router

Dispositivo que sirve para encaminar paquetes desde una red hacia otra, que funciona por medio de direcciones IP para conocer donde deben ser direccionados los paquetes de datos, a diferencia del switch el router es más inteligente; ya que cuenta con tablas de enrutamiento que funcionan como mapas donde tienen previsto la mejor ruta para poder llegar a la dirección de destino especificada, complementando este concepto Tadimety (2015) dice que:

"Un router es un dispositivo de red que reenvía paquetes de red desde una red interconectada a dispositivos de otra red, donde dos redes pueden conectarse mediante un enrutador.

Un router recopila y mantiene información sobre el paradero de todas las redes de su dominio. Este incluye las redes que están directamente conectadas a él, así como las que están indirectamente conectadas a él, siendo estas últimas accesible a través de otros routers intermedios.

El conocimiento o la visión general del router de todas las redes de su dominio le da la capacidad de actuar como una puerta de enlace entre redes.

Los datos que deben transferirse desde una estación de trabajo de origen o sistema final de destino de trabajo se dividen en segmentos más pequeños que luego se transmiten por separado en el interior dentro de paquetes de red.

Un paquete de red transporta como carga una pequeña parte de los datos totales que deben ser transportado entre dos dispositivos comunicados.

La parte que es transportada como carga por una red también se llama popularmente la carga útil de datos.

El trabajo del router es muy exigente ya que tiene que transferir datos cada vez que se realiza peticiones” (p.9).

Figura 8 Router. Tomada de Cisco (2015)

Concretando la descripción antes dicha un router es un dispositivo que por direcciones IP envía información a otros dispositivos de otra red; un router cuenta con componentes internos, en base a sus componentes Romero (2003), describe que cuenta con: RAM/DRAM, son tablas de enrutamiento donde se realiza script de configuración del router y se almacena la información, en la NVRAM se encuentran los archivos de configuración de inicio y se realiza las copias de respaldos, en la parte FLASH contiene la imagen del SO, permite actualizar su software y puede almacenar varias versiones, en ROM programa de arranque y memoria de lectura y como último Interfaces son conexiones a la red.

Esquemas de Enrutamiento

Tiene como finalidad compartir o intercambiar información de enrutamiento hacia distintas redes por medio de tablas, en cuanto se refiere Lucas (2015) dice que:

“Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento. Dicha información se usa para construir, crear y mantener las tablas de enrutamiento” (p.1).

Previa a la descripción de los protocolos de enrutamiento estáticos y dinámicos, según Petersen (2007) expresa que los protocolos de enrutamiento dinámico, comparten información dinámicamente, de forma

automática actualiza las tablas de enrutamiento cuando se cambia la topología y elige el mejor destino, esta configuración es mediante comandos IOS, en cuanto a los protocolos de enrutamiento estático Polo (2007) aclara que su configuración es de forma manual y sus cambios no son adaptables por sí solo, es por eso que el administrador de red es el encargado de gestionar las rutas y también las topologías en el caso de que tenga una actualización.

Paneles de conexión (Patch Panel):

Patch panel, es un organizador que estructura el cableado de red, consta de una regleta metálica que son instaladas en Racks(Bastidores). En su parte frontal cuenta con un número exacto de conectores y su parte posterior se utiliza para las conexiones de cable de red UTP (Unshield Twist Pair - Par trenzado sin blindaje). Su primordial tarea es agrupar el cableado rígido UTP en su parte trasera mismo que viene de la red local (LAN), mientras que la función de conectar la red con los switch o hubs, se efectúa es en su parte delantera. Con respecto al enunciado por Clark, Prairie, Kessler, & Heights (2003), expresan que:

"Las redes de área local y las conexiones de telecomunicaciones suelen utilizar paneles de conexión, especialmente en las instalaciones del cliente, para permitir una conexión cruzada rápida y conveniente entre los equipos de telecomunicaciones. El cable de comunicación de par trenzado se utiliza a menudo para conectar los dispositivos de telecomunicaciones a estos paneles de conexión, y cada cable incluye cuatro pares trenzados u ocho cables individuales en total."

De acuerdo a lo escrito anteriormente por los autores, un patch panel permite conectar varios elementos de telecomunicaciones mismos que van instalados en un rack, los cuales permiten instalar varios dispositivos de red. Fuentes Telleria & Lujan Apaza (2017) escriben que: los pacht panel permiten la circulación de datos por medio de conectores RJ45, los que definen la velocidad de transmisión, para que todo dispositivo que está conectada a la red trabaje bajo una misma velocidad.

Sistema De Cableado Estructurado

Es la infraestructura diseñada para transportar y soportar el ancho de banda en una construcción, permite una sencilla administración de reubicación de personas y equipos, sin llegar a ser necesario a realizar modificaciones en el sistema, ya que cuenta con un cableado único y completo. Velasco (2001) dice que:

"La infraestructura de un sistema de cableado estructurado debe ser capaz de soportar el incremento del ancho de banda requerido y de la velocidad de transmisión de las redes actuales y futuras, ello trae como consecuencia la incorporación de nuevas categorías de cableado que recojan las recomendaciones necesarias y la definición de nuevos parámetros, de forma que se garantice una recepción correcta de los datos enviados a través de un enlace".

Con respecto a lo citado, un buen sistema de cableado es el que garantiza una correcta distribución de datos, de tal forma que ayudará a compartir la señal dentro del laboratorio de IoT y centro de desarrollo de software. Por medio del cableado UTP también se permitirá amplificar la señal y así obtener una conectividad rápida y eficaz en el laboratorio, en tal virtud existen varios tipos de cableado UTP, los más utilizados en la actualidad son los de categoría 5e y 6. Donde Pérez (2005) menciona que:

"Categoría 5e (Enhanced-Extendida): Es una extensión de la norma que especifica la categoría 5. Esta categoría especifica requerimientos de parámetros más estrictos que la 100BaseT. La categoría 5e establece los límites mínimos de Pérdida de Retorno y el ELFEXT, que para la Cat.5 son sólo informativos. La cat.5e está regida por la norma ANSI/TIA/EIA-TSB-95 (The additional Transmission Performance Guildelines for 100 Ohm – 4-pair Categoría Cabling), estableciendo los métodos de prueba de los componentes de conexión a nivel de componentes y los métodos de prueba. Los parámetros que debe cumplir el UTP para encuadrarse dentro de la cat. 5e son: El Mapa de cableado, la Longitud de los segmentos, la Atenuación, el Retardo de Propagación, el Delay Skew, el NEXT y el ELFEXT (par a par y la Potencia suma) y la Pérdida de Retorno. El rango de frecuencias de trabajo es

extendido a 1 – 100 MHz. Con respecto a la Categoría 6 el autor expresa que; La norma del cableado de Categoría 6 lo específica para uso hasta 250 MHz. Esta categoría está siendo analizada por el ANSI/TIA/EIA TR-42.7.1 por el ISO/IEC/SC25WG3. La categoría 6 extiende el rango de frecuencias de trabajo a 250 MHz, especificando un mínimo de ACR a 200 MHz que es aproximadamente igual al mínimo ACR del Cat. 5 a 100 MHz. Los parámetros requeridos son iguales a los especificados por la Cat. 5e. En esta categoría, los conectores de 8 pines Jacks y Plug RJ45 deber estar diseñados como un par sintonizado o apareado para conseguir un alto nivel de desempeño en las pruebas de NEXT y FEXT. Si el usuario mezcla los conectores apareados, el enlace puede que no cumpla con los parámetros de la Cat 6. Constructivamente consiste de 4 pares de conductores de cobre de 0,50 a 0,53 mm con cubierta FED. La cubierta exterior es igual a la usada en las categorías 5 y 5e. Se toma extremado cuidado en el diseño y armado del mismo, manteniendo la uniformidad del trenzado" (p.16).

Haciendo una referencia de lo que expresa el autor el cableado de categoría 5e, es una extensión de la categoría 5, contiene planos de cableado, longitud de segmentos e implanta límites de pérdida de retorno. En tanto a la categoría 6, específica que son diseñados para sintonizar y obtener un nivel alto de trabajo en las pruebas NEXT y FEXT, además amplifica el rango de la frecuencia de trabajo a 250 MHz.

Protocolos De Comunicación

Es un conjunto de reglas, el cual puede transferir e intercambiar datos entre dos o más dispositivos dentro de una red, por medio de sus reglas definen su secuencia y sincronización del envío de datos, estableciendo así la forma correcta de transmitir esos datos y la forma de cómo deben procesarse. Dicho con palabras de Tolosa (2014), argumenta que:

"Un protocolo de comunicación está formado por un conjunto de reglas y formatos de mensajes establecidas a priori para que la comunicación entre el emisor y un receptor sea posible. Las reglas definen la forma en que deben de efectuarse las comunicaciones de las redes, incluyendo la temporización, la secuencia, la revisión y la corrección de errores" (p.4).

Tomando en cuenta lo que expresa Tolosa en el párrafo anterior, los protocolos de comunicación sirven para poder transferir datos, los cuales se acoplan a un conjunto de reglas para poder ser enviados dentro de una red, es por medio de los protocolos de comunicación obtendremos una correcta distribución de los paquetes de datos en el laboratorio de IoT y centro de desarrollo de software. Los protocolos de comunicación cuentan con diferentes tipos de configuración, tales como; TCP/IP, DHCP y SNMP.

Protocolo TCP

Con respecto al protocolo de red TCP, sus siglas significan “Protocolo de Control de Transmisión”, el mismo cuenta con una arquitectura basada en capas funciona y puede ser implementado en un entorno multinetwork, Cisco (2005), da a conocer:

“TCP es un protocolo de transporte orientado a la conexión que envía datos como un flujo de bytes no estructurado. Al usar números de secuencia y mensajes de acuse de recibo, TCP puede proporcionar un nodo de envío con información de entrega sobre paquetes transmitidos a un nodo de destino. Cuando los datos se han perdido en tránsito desde el origen hasta el destino, TCP puede retransmitir los datos hasta que se alcance una condición de tiempo de espera o hasta que se haya logrado una entrega exitosa. TCP también puede reconocer mensajes duplicados y los descartará adecuadamente. Si la computadora emisora está transmitiendo demasiado rápido para la computadora receptora, TCP puede emplear mecanismos de control de flujo para retardar la transferencia de datos. TCP también puede comunicar la información de entrega a los protocolos de capa superior y las aplicaciones que admite. Todas estas características hacen que TCP sea un protocolo de transporte confiable de extremo a extremo” (p.2).

Haciendo énfasis de la descripción previa realizada por Cisco, se puede destacar que el protocolo TCP es el encargado de transmitir datos, en el caso de que la información no llegue hasta su receptor, TCP vuelve a reenviar los datos con la finalidad de que estos datos lleguen a su destino, por todas sus cualidades dichas anteriormente, TCP es un protocolo de transmisión confiable de host a host.

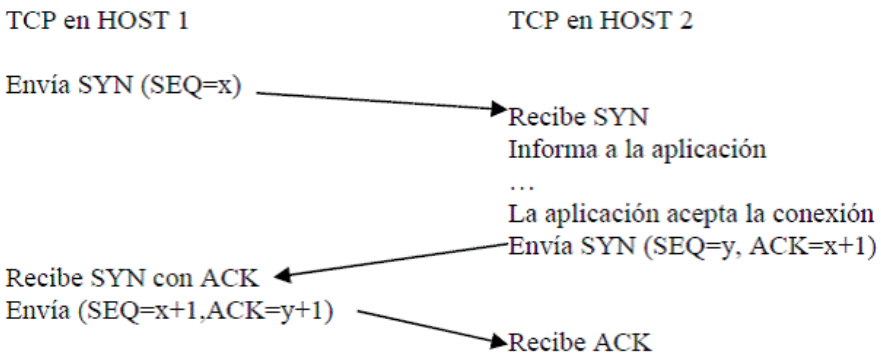


Figura 9: Intercambio de mensaje de inicio a fin de la conexión. Elaborador por Montañana,(s. f.)

Con base en el análisis de la figura 9, se puede visualizar que se realiza una interacción entre dos hosts (A y B), dentro de esa interacción se produce una comunicación en la cual se busca establecer una conexión entre ambos hosts, donde el host A informa una secuencia (x); el host B contesta con otro segmento y acepta la conexión e indica las sucesiones del sentido contrario (y), esto siempre se dará hasta que el TCP receptor decida aceptar la petición de conexión.

Protocolo IP

El protocolo IP (Protocolo Internet) provee un servicio de intercambio de información mediante la distribución de paquetes, su forma de transportar el flujo de datos es por medio de datagramas, durante su ejecución un datagrama puede ser dividido en varios fragmentos los cuales se pueden acoplar en el nuevo destino, Barcell (2014) agrega que:

"El protocolo IP es el encargado de etiquetar cada paquete de información con la dirección de la máquina origen y de destino apropiadas. Cada ordenador conectado a Internet tiene una dirección Internet (IP address) que es única y exclusiva y que lo distingue de cualquier otro ordenador perteneciente a Internet. El protocolo IP se encarga, por tanto de tomar los paquetes TCP, que contenían los segmentos de información, así como información adicional para reordenar y detectar errores en el destino, y les añade las direcciones IP de las máquinas origen y destino, generando un nuevo paquete IP que ya puede ser transmitido por la red" (p.2).

Como conclusión, IP es el encargado de llevar los datos desde su origen hasta su destino por medio de ello permite establecer una comunicación entre maquinas a través de la red.

Protocolo DHCP

DCHP (Dynamic Host Configuration Protocol - Protocolo de configuración de host dinámico), permite que cualquier equipo que esté conectado a la red pueda ser configurado de manera dinámica, el cual trabaja bajo el modelo Cliente – Servidor, mismo que es el encargado de asignar direcciones IP a las maquinas que estén conectadas a la red y transmitir datos. Nazareno (2012) describe que: DHCP configura las direcciones IP de forma automática. Cuando recibe la solicitud del cliente para una configuración IP, responde enviando los parámetros para que se auto-configuren los mismos.

El funcionamiento del protocolo DHCP:

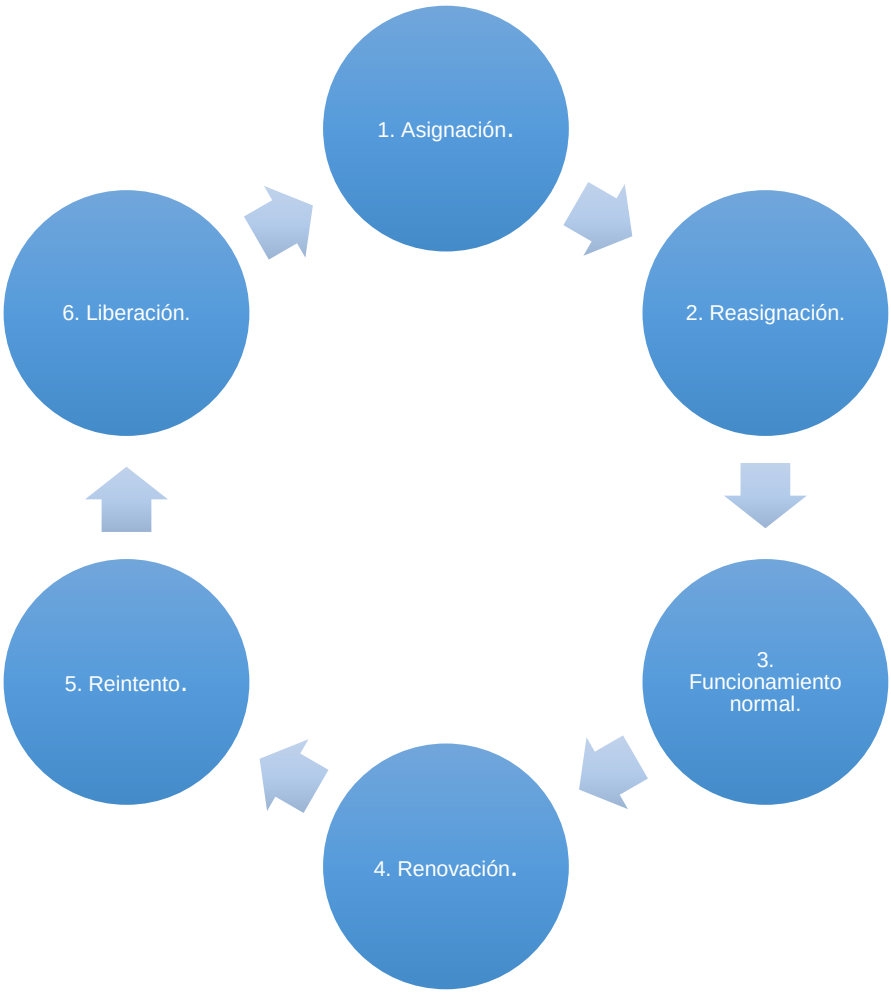


Figura 10 Funcionamiento del Protocolo DHCP elaborado por el autor (2019)

DHCP cumple con un ciclo de vida que posee las siguientes fases. Nazareno (2012) explica las 6 fases del DHCP

1. El cliente solicita la asignación de una dirección IP a un servidor.
2. El cliente ha recibido con anterioridad una dirección IP y, en un nuevo arranque, solicita al servidor la asignación de esa misma dirección IP. El proceso es similar al de la asignación pero más breve
3. El cliente utiliza la dirección IP asignada por el servidor

4. Cuando ha vencido un porcentaje del tiempo de asignación de la dirección IP2, el cliente solicita al servidor una renovación de la asignación.

5. Si la renovación no ha sido posible durante un cierto tiempo 3, el cliente intenta la renovación de la misma con otros servidores alternativos si existen, tomando como nueva IP la que le ofrezca cualquiera de estos servidores alternativos

6. El cliente puede liberar en cualquier momento la IP que le ha sido asignada informando al servidor de que ya no se va a utilizar esa dirección IP.

Por medio de un gráfico se explicará el proceso que efectúa el DHCP:

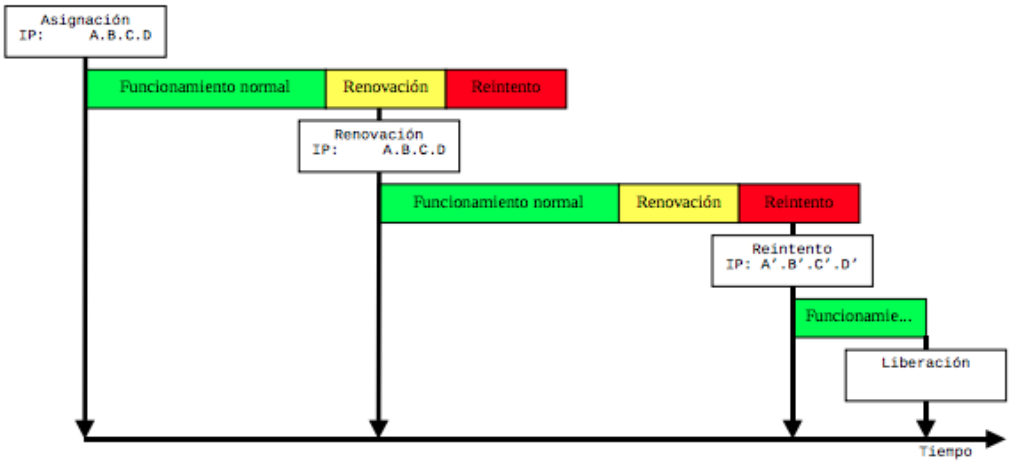


Figura 11 Funcionamiento de las Fases. Elaborado por (Nazareno, 2012)

En la figura 11, se muestra como cliente de DHCP le asignan una dirección IP del servidor, al finalizar tiempo de funcionamiento normal, se solicita una renovación, transcurrido otra vez el tiempo de funcionamiento normal, el cliente reintenta solicitar una nueva dirección IP a cualquier servidor DHCP. Como último punto después del funcionamiento normal de la fase anterior, si el cliente ya no desea hacer uso de la dirección IP, la puede liberar y culmina su funcionalidad en la red.

Protocolo SNMP

SNMP (Simple Network Management Protocol, Protocolo simple de administración de red), la Universidad Rey Juan Carlos (2013) sustenta que: la función primordial del SNMP es contar con un protocolo único el mismo que ayude administrar de una forma uniforme todos los dispositivos conectados en la red, de forma centralizada o distribuida en el caso de que sea necesario. De acuerdo al enunciado previamente mencionado del SNMP, es el encargado de administrar y monitorear los dispositivos de una red tales como: switch, routers, servidores, dispositivos móviles, etc. Por medio de su monitoreo se puede efectuar un control de velocidad de procesamiento, detectar el rendimiento y errores de la red, también se puede configurar alarmas que permitan enviar una señal cuando se produzca acontecimientos inusuales.

Por otra parte, en la base de datos MIB (Base de información de gestión) almacena la información que es gestionada por SNMP, por lo cual se puede distinguir los siguientes elementos:

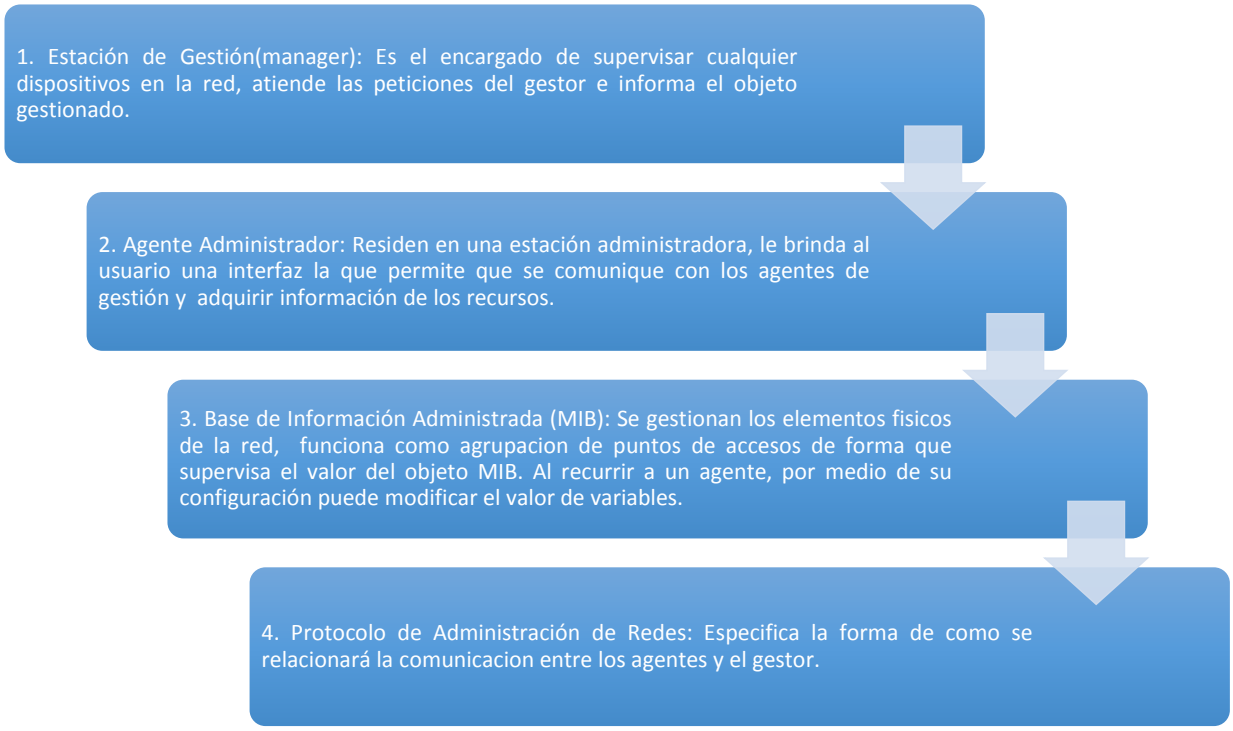


Figura 12 Elementos del SNMP. Elaborado por el autor (2019)

El protocolo SNMP permite gestionar el hardware a nivel de IP ejemplo; velocidades de interfaces, consumos interfaces, recursos de CPU utilizados, memoria, etc. En la figura 13 con respecto al proyecto explica la funcionabilidad del protocolo SNMP, indica que en la parte de estación de gestión de red, se encuentra el equipo, aplicativo o dispositivo que va a gestionado y controlado a través del protocolo SNMP, se establecerá la gestión de interfaces, de CPU y de memoria RAM (consumo) en el aplicativo de gestión, donde las transferencias de los valores las realizará por medio de la capa de transporte UDP, de tal forma que enviará y retornará valores, el equipo gestionado tiene que estar configurado por medio de un agente mismo que va de acuerdo al tipo de: versión, puertos y comunidad a la que pertenece y por la cual está siendo gestionado, todos los datos que recibe se almacenarán en MIB.

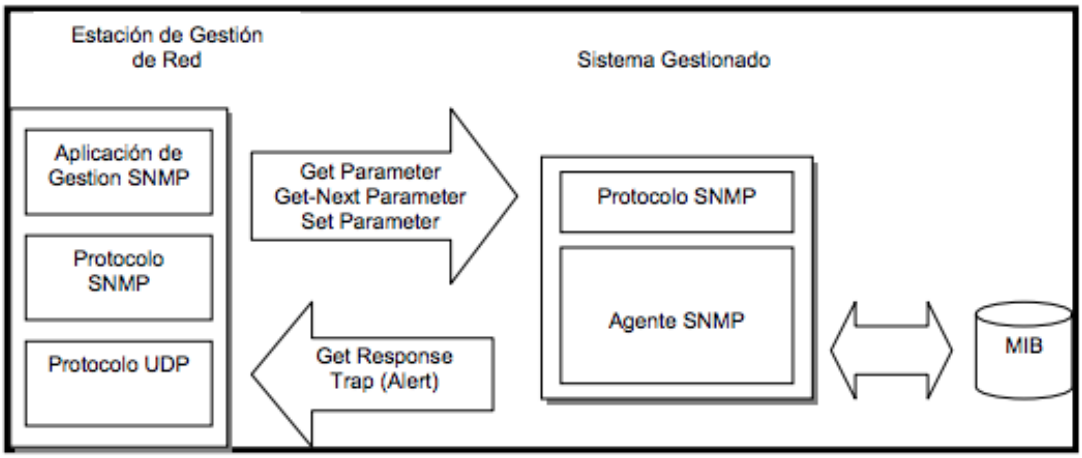


Figura 13 Elementos SNMP. Tomado de (SNMP.pdf, s. f.)

Comandos del protocolo SNMP:

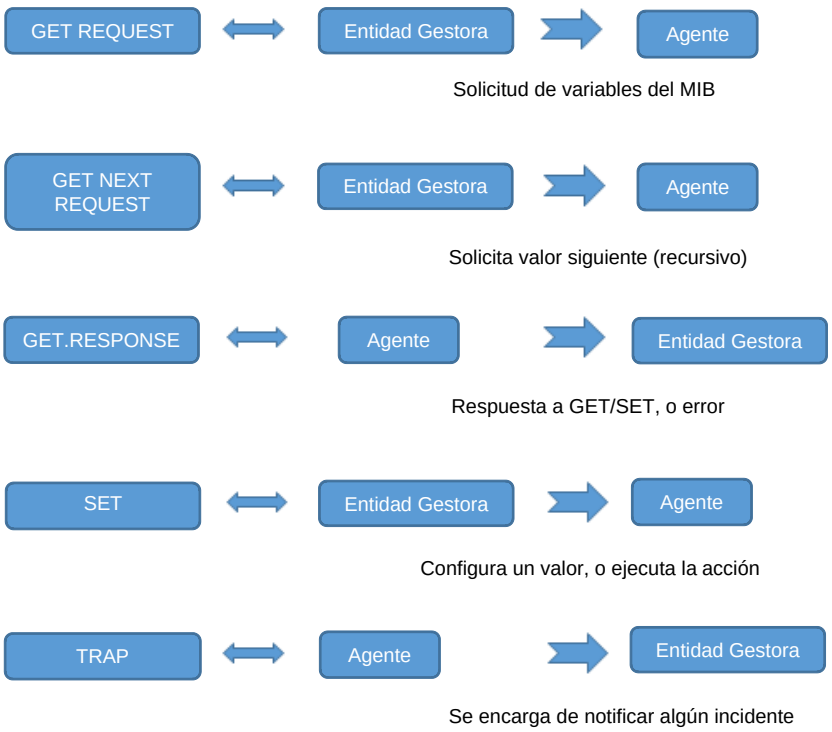


Figura 14 Comandos del protocolo SNMP. Elaborado por el autor (2019)

El protocolo SNMP, ha desarrollado algunas versiones, a continuación la Universidad Rey Juan Carlos (2013) menciona:

- SNMP v1. Año 1988. RFC 1065, 1066, 1067 Muy inseguro. Contraseñas transmitidas en texto claro
- SNMP v2. Año 1993. RFC 1441, 1452 Introduce GetBulkRequest Mejora la seguridad, pero resulta muy complicado y apenas se utiliza. En la práctica se sigue empleando una versión 2 simplificada (SNMP v2c, RFC 1901, 1908), que mantiene el envío de contraseñas en abierto
- SNMP v3. Año 2002. Incluye autenticación, confidencialidad e integridad. Rehace toda la notación, aunque mantiene funcionalidad.

En conclusión, se puede observar que la versión 3 es la más segura del protocolo SNMP, porque usa criptografía simétrica la cual permite tener una comunicación segura entre los dispositivos.

Firewall

Firewall (cortafuegos) forma parte de un equipo de red, su función primordial es bloquear y denegar acceso a redes que no estén autorizadas a la red o a un sistema y de paso también permite el acceso a las máquinas que cuenta con la autorización. El firewall es configurado para poder limitar, permitir, cifrar, descifrar y sobre todo proteger el tráfico que circula dentro de una red por medio de reglas, normas o políticas. Este sistema es mayormente utilizado para restringir el acceso a los usuarios que no estén autorizados de manera que no permitirá que ninguna red pública ingrese a la red LAN privada. El firewall también puede enmascarar las direcciones IP por medio de reglas de NAT, eso conlleva a que las direcciones IP privadas sean direcciones IP públicas, su propósito es limitar el acceso a la red LAN, bloqueo de puertos lo mismo que pueden vulnerables a escaneos o ataques. IBM (2014b).

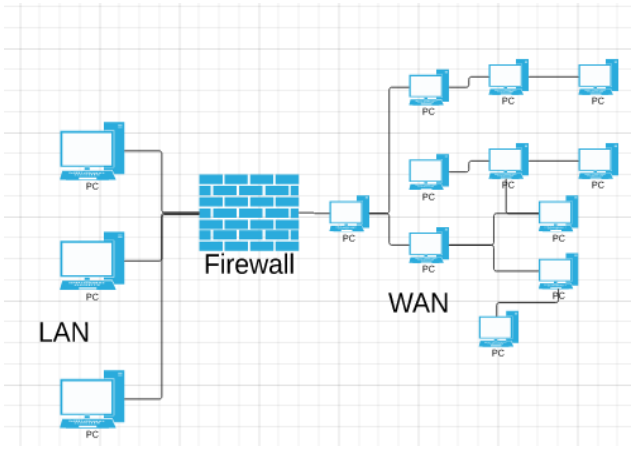


Figura 15 Ubicación Firewall. Elaborado por el autor (2019)

Estándares de Seguridad y Comunicación

Conjunto de medidas que permiten a las organizaciones mantener su información resguardada y protegida de manera que logren obtener la integridad y confidencialidad de los datos. En palabras de los autores Lanza & Sánchez (2015) plantean que los estándares de seguridad y comunicación son mecanismos encargados de garantizar un funcionamiento correcto a manera que previene fallos, logrando que la información y recursos sean accesibles y utilizados por lo que se prevenía.

Actualmente existen varios estándares para la seguridad de la información, pero en este proyecto de titulación se enfocará en los siguientes:

- Norma ISO 27001 (Gestión de seguridad de la información)
- Estándares del IEEE
- Estándares de cable estructurado (UTP)

Norma ISO 27001

La norma ISO 27001 con respecto al autor Álvarez (2017) argumenta que:

"El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente" (p.7).

De acuerdo con el autor Álvarez la norma ISO 27001: (International Organization for Standardization / Organización Internacional de Normalización), proporciona una metodología para lograr implementar el sistema de gestión de seguridad de la información (SGSI), que consiste en mantener una integridad, disponibilidad y confidencialidad de la información que contiene una organización, en los tres términos nombrados se establece la base que debe tener toda organización.

- Integridad: Mantiene con exactitud y fiabilidad la información y los métodos de procesos que se emplean dentro de una organización.
- Disponibilidad: Acceso a servicios y utilización de la información, cuando los usuarios lo requieran.
- Confidencialidad: Información que mantienen las organizaciones no a disposición de usuarios, entidades o personas no autorizada.

Para poder garantizar el buen funcionamiento de la seguridad de la información esta tiene que ser bien administrada, la cual se realizará mediante procesos sistemáticos o documentados, donde tiene que ser conocido por toda la organización, este es el proceso que compone la norma ISO 27001, la misma que puede ser implementada en cualquier tipo de organización, sea pequeña o grande, pública o privada, esta normativa también permite que una organización obtenga su certificación; significa que una entidad ha sido implementada bajo el cumplimiento de la norma ISO 27001 la cual se ha convertido a nivel mundial en la principal norma para la seguridad de la información, de tal forma que logra mantener los niveles de rentabilidad, competitividad y beneficios económicos.

Estándares Del IEEE

(Institute of Electrical and Electronic Engineers), pertenecen a unas de las más grandes asociaciones del mundo, la IEEE se encarga de elaborar normas para recomendar y guiar con respecto a su nivel de prescripción, su función principal es el uso de protocolos a seguir permitiendo el uso de estándares para una máxima compatibilidad y al mismo tiempo un sencillo manejo entre varios fabricantes.

La mayor parte de las redes locales están bajo la estandarización de la IEEE, el proyecto que emprendió la IEEE y lo denominaron proyecto 802, el mismo que contiene un conjunto de estándares. Este proyecto se divide en grupos de trabajo donde se identifican con un numero decimal, ejemplo 802.1, en la división del proyecto 802 se especificará todo sobre las diferentes tecnologías la red local.

El proyecto 802 está conformado con un total de 13 grupos de trabajo, a continuación, el autor Puentes (2015) explica cada uno de ellos:

Tabla 3 Estándares del IEEE

802.1	Establece los estándares de interconexión relacionados con la gestión de redes
802.2	Define el control de enlace lógico (LLC). El LLC es la parte superior de la capa enlace en las redes de área local. Asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación.
802.3	Es una especificación estándar sobre la que se monta Ethernet, un método de establecimiento de comunicaciones físicas a través de una red de área local o LAN.
802.4	El estándar token bus define esquemas de red de anchos debanda grandes, usados en la industria de manufactura. La idea es representar en forma lógica un anillo para transmisión por turno, aunque implementado en un bus. Esto porque cualquier ruptura del anillo hace que la red completa quede desactivada
802.5	Red de área local Token Bus: Este estándar define una red con topología de anillo la cual usa token (paquete de datos) para transmitir información a otra. En una estación de trabajo la cual envía un mensaje lo sitúa dentro de un token y lo direcciona específicamente aun destino, la estación destino copia el mensaje y lo envía a un token de regreso a la estación origen la cual borra el mensaje y pasa el token a la siguiente estación
802.6	El estándar MAN (Red de área metropolitana) Está diseñado para proveer servicios de datos, voz y vídeo Define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado Bus Dual de Cola Distribuid.
802.7	Grupo de Asesoría Técnica sobre banda ancha Este estándar fue desarrollado para las compañías del Internet del cable. Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes
802.8	Grupo de Asesoría Técnica sobre fibra óptica Especificación para redes de fibra óptica tipo Token Passing /FDDI. (Soporte a las estaciones de trabajo de alta velocidad)
802.9	Redes integradas para voz, datos y vídeo. Decimos Servicios integrados porque utiliza la misma infraestructura para muchos servicios que tradicionalmente

	requerían interfaces distintas (télex, voz, conmutación de circuitos, conmutación de paquetes...)
802.10	Seguridad de las redes. Este grupo está trabajando en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y encriptamiento
802.11	Red local inalámbrica, también conocido como Wi-Fi (El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capa física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.
802.12	Método de acceso de prioridad bajo demanda, el cable especificado es un par trenzado de 4 hilos de cobre utilizándose un concentrador central para controlar el acceso al cable. Las prioridades están disponibles para soportar la distribución en tiempo real de aplicaciones multimediales
802.13	No utilizado.

Nota: Tomado de Puentes (2015)

En lo expresado anteriormente por el autor Puentes, cada grupo de trabajo del proyecto 802 de la IEEE, explica los diferentes niveles de la tecnología de la red local (LAN), la que se acomoda más al presente proyecto es él estándar IEEE 802.3, ya que es donde se monta Ethernet, el mismo que permitirá establecer las comunicaciones físicas por medio de la red de área local. A continuación, la descripción del estándar enfocado al proyecto:

Estándar Ethernet 802.3

Este estándar está definido para una red LAN, y el cual servirá de base para la implementación de la red cableada dentro del laboratorio; como las características de cableado, señalización a nivel físico y los formatos de las tramas a nivel de la Capa de Enlace de datos. Este estándar comúnmente se toma como sinónimo de IEEE 802.3 pero muestra grandes diferencias en las tramas que trasmiten.

Otras características son: tecnología fácil de instalar, el coste de instalación es muy bajo, operan en distintos medios de transmisión como lo

es Coaxial, Par trenzado y Fibra Óptica, y por último sus velocidades han aumentado al pasar del tiempo de 10 Mbps a 10 Gbps.

Tabla 4: Trama Ethernet

Trama Ethernet					
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes
Preámbulo	Dirección de Destino	Dirección de Origen	Tipo	Datos	CRC

Nota: Elaborado por el autor (2019)

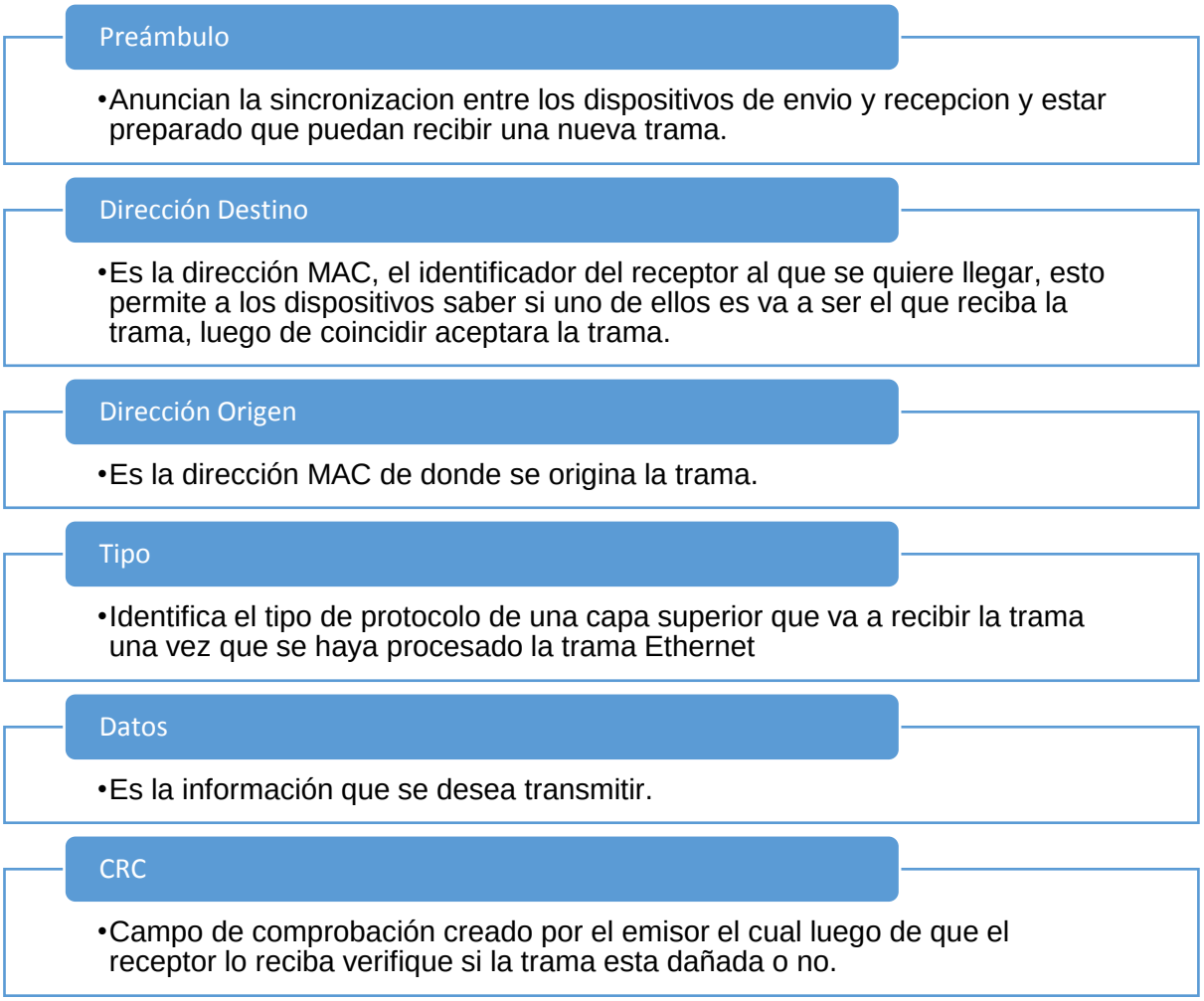


Figura 16: Trama Ethernet. Elaborado por el autor (2019)

El estándar Ethernet trabaja mediante la contienda CSMA/CD y permite verificar el medio antes de transmitir una trama. En este proceso:

1. Medio inactivo: puede trasmitir la trama.
2. Medio ocupado: retrasa la trasmisión de la trama.
3. Detección de Colisión: si detecta una colisión al momento que está trasmitiendo, volverá a retrasmitir la trama en un tiempo aleatorio.

Las redes LAN Ethernet se encuentran sometidas a muchas limitantes que pueden afectar a la transmisión de datos, ya que comparten el mismo medio físico, son propensas a interferencias electromagnéticas, ruido, atenuación y el tipo de dispositivo y dominio que compartirá con los demás elementos de la red. Es importante conocer los dos tipos de dominio que se mostraran a continuación:

- Dominio de Colisión: cuando 2 o más equipos comparten el mismo medio físico para transmitir, al momento de hacerlo puede existir colisión de datos. Dentro de los dispositivos que reducen el dominio de colisión son aquellos que operan en la Capa 2 del modelo OSI, como un Switch.
- Dominio de Broadcast: cuando 2 o más equipos comparten el mismo medio lógico de trasmisión lo cual hace que un paquete llegue a cada uno de esos equipos dentro del mismo dominio, generando saturación en la red. Dentro de los dispositivos que reducen el dominio de broadcast se encuentran los Router, los cuales operan en la Capa 3 del modelo OSI.

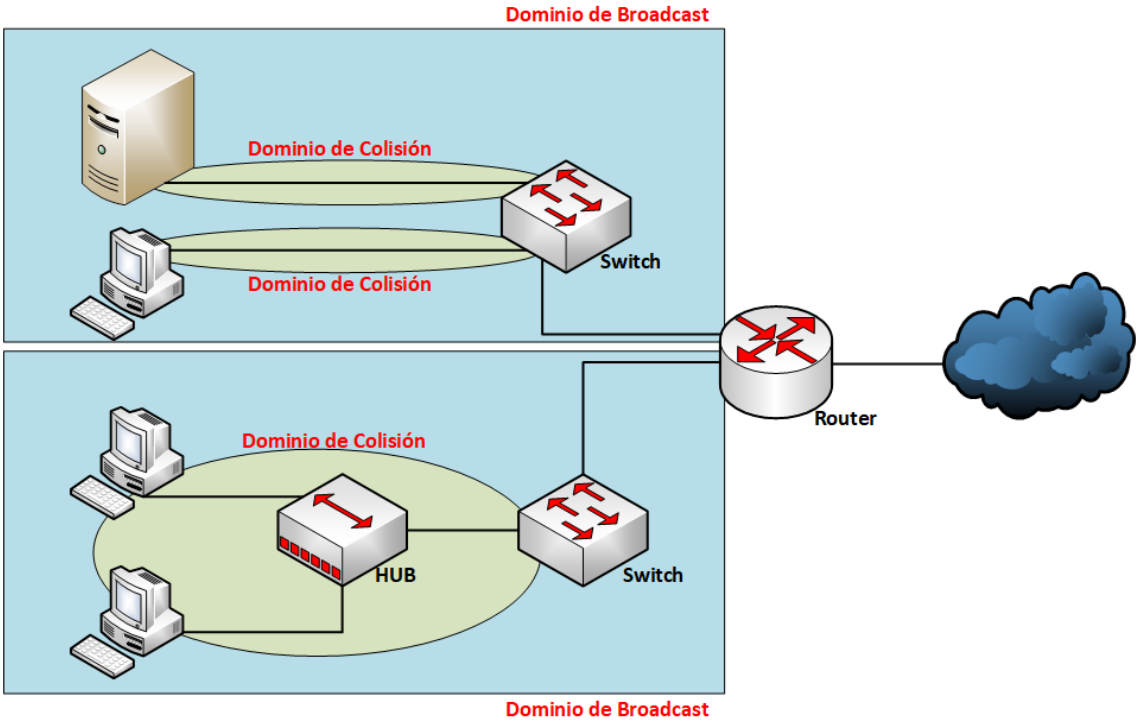


Figura 17 Dominio de Broadcast. Elaborado por el autor (2019)

Con las categorías de cableado mencionadas en el capítulo anterior, el estándar Ethernet incluye tres principales tecnologías de transmisión:

10 Mbps Ethernet para redes LAN sobre cable Coaxial

100 Mbps Ethernet (Fast Ethernet) para redes LAN sobre cable par trenzado

1000 Mbps Ethernet (Gigabit Ethernet) para redes LAN sobre cable par trenzado o fibra óptica

A continuación, se mencionan las versiones de tecnologías Ethernet que se acoplan a los alcances del proyecto:

Tabla 5 Características del Cable UTP

TIPO DE ETHERNET	ANCHO DE BANDA	TIPO DE CABLE	DUPLEX	DISTANCIA MÁXIMA
1000Base-T	1Gbps	UTP Cat 5e	Full	100 m
1000Base-TX	1Gbps	UTP Cat 6	Full	100 m
10GBase-T	10Gbps	UTP Cat 6e	Full	100 m

Nota: Elaborado por el autor (2019)

Estándares de cable estructurado (UTP)

Los estándares del cableado estructurado es la infraestructura que nos permite transportar a largo y ancho de una construcción algún tipo de señal, físicamente un sistema de cableado es una red completa y única, por tal razón su administración es de una manera muy sencilla. Para poder desarrollar un proyecto sea de instalaciones de equipos informáticos se debe regir bajo estándares, los cuales se describen a continuación y hacia dónde van enfocados.

Entre los estándares del cableado estructurado según Tropa (2013), se explica cuales son y en que están enfocados:

ANSI/TIA/EIA-568B: Esta norma define los principales conceptos de cableado estructurado, sus elementos, la topología, tipos de cables y tomas, distancias y pruebas de certificación

ANSI/TIA/EIA-569B: Esta norma define el área ocupada por los elementos de cableado estructurado, las dimensiones y tasa de ocupación de las rutas y demás información constructiva

ANSI/TIA/EIA-606A: Especifica técnicas y métodos para identificar y administrar la infraestructura de telecomunicaciones

TIA 942: Esta norma define infraestructura, la topología y los elementos para el proyecto de una data center

ANSI/TIA/EIA-570A: Esta norma se aplica a los sistemas de cableado y sus respectivos espacios y caminos a edificios residenciales multiusuarios y casas individuales.

Dentro del proyecto que se quiere implementar se tomó en cuenta, dos estándares que definen y se acoplan a los requerimientos para la red de datos del laboratorio.

El estándar ANSI/TIA/EIA-569 el cual se dio una breve explicación en el párrafo anterior; ha tenido varias versiones a lo largo de los años, llegando a la versión que entró en vigencia en el 2013 (ANSI/TIA/EIA-569-C

“Telecommunications Pathways and Spaces”), el cual indica y provee buenas prácticas para el diseño de las instalaciones de la infraestructura en un espacio.

El estándar define 3 conceptos que son fundamentales a considerar para un cableado estructurado, estos son:

- Las áreas, edificios o espacios se encuentran en constante remodelación y acondicionamiento, y es algo común ya que se contrate nuevo personal, y se cubren más áreas, por ende, éste estándar reconoce que existirán cambios, los mismos que están considerados dentro de las recomendaciones para poder ejecutar la canalización del cableado de telecomunicaciones.
- Los sistemas de telecomunicaciones que engloban distintas tecnologías y equipos de comunicaciones, constantemente están cambiando y evolucionando, por lo tanto el estándar contempla esto, y lo considera dentro de las recomendaciones independientemente de los tipos de tecnología y proveedores de los mismos.
- Y por último las telecomunicaciones no solo encierran voz y datos, los sistemas de telecomunicaciones incorporan todos aquellos sistemas que lleven información, tales como audio, video, alarma, seguridad, control ambiental.

El estándar identifica seis componentes para su infraestructura del sitio:

- Instalaciones de entrada
- Sala de equipos
- Canalización Back-bone
- Salas de Telecomunicaciones
- Canalización horizontales
- Áreas de trabajo

Para los alcances de este proyecto se tomarán en cuenta tres que serán implementados:

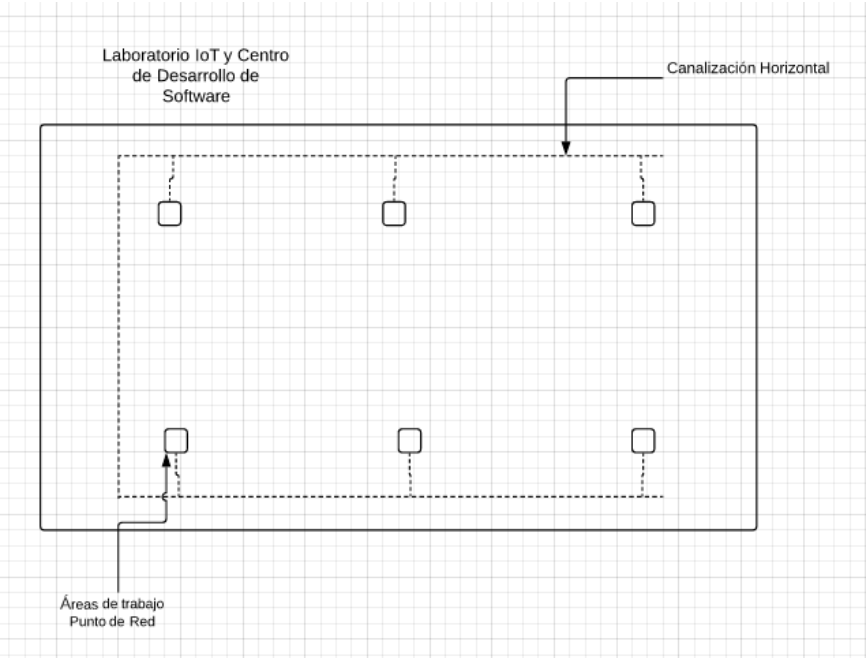
- Salas de telecomunicaciones: se las conoce como armarios de telecomunicaciones, es el espacio que permite la interconexión entre las áreas de trabaja y el Back-Bone, a partir de este punto el tendido de la canalización horizontal hacia las áreas de trabajo no debe superar los 90m.
- Canalizaciones horizontales: es el camino que tomaran los cables para vincular las salas de telecomunicaciones con las áreas de trabajo, las mismas que deben tener un diseño capaz de soportar los tipos de cables que serán utilizados y descritos más adelante en la norma TIA-568.

  Para este proyecto se realizarán canalizaciones con ductos perimetrales y hacer el tendido de cable horizontal hasta las áreas o puesto de trabajo.

  Las secciones de los ductos deben depender mucho del diámetro del cable que va a alojar, la cantidad de cables que pasaran por dichos ductos y el posible crecimiento que puede tener el área de trabajo, dejando el espacio necesario para cableado adicional.
- Áreas de trabajo: son los lugares donde ya se ubica el usuario final; escritorios, mesas, etc… aquellos sitios que requieres ser añadidos al sistema de telecomunicaciones.

  Comúnmente se recomienda prever como mínimo tres dispositivos por puesto o área de trabajo. En el siguiente capítulo se definirán la cantidad de dispositivos que habrá por área de trabajo

Figura 18: Canalización. Elaborado por el autor (2019)



El estándar **ANSI/TIA/EIA-568,** refiere a los requerimientos que se debe considerar en un sistema de cableado en una instalación, sin tomar en cuenta las aplicaciones para los cuales serán utilizados y los proveedores.

De la misma manera que el estándar anterior en su transcurso ha ido desarrollando varias versiones, llegando al último estándar publicado por la TIA es el ANSI/TIA/EIA-569-C el cual brinda recomendaciones de manera común o genérica a todo tipo de lugar donde se realice el cableado. Se encuentra conformado por cuatro partes:

ANSI/TIA/EIA 568-C-0: especifica un sistema de cableado genérico y permitir una planificación e instalación de un cableado estructurado en cualquier tipo de área o instalaciones independiente de los productos o los proveedores. Así mismo indica, como buena práctica, como se debe diseñar una estructura de cableado en una topología estrella y sus distintas nomenclaturas en cada una de las etapas o sub-sistemas de cableado.

Dentro del cableado es importante a considerar que la vida útil de un cableado es de 15 a 20 años, ya que las tecnologías constantemente cambian, es necesario establecer un tipo de cableado que pueda soportar las altas transmisiones de datos y sus anchos de banda, tanto para las actuales y futuras tecnologías.

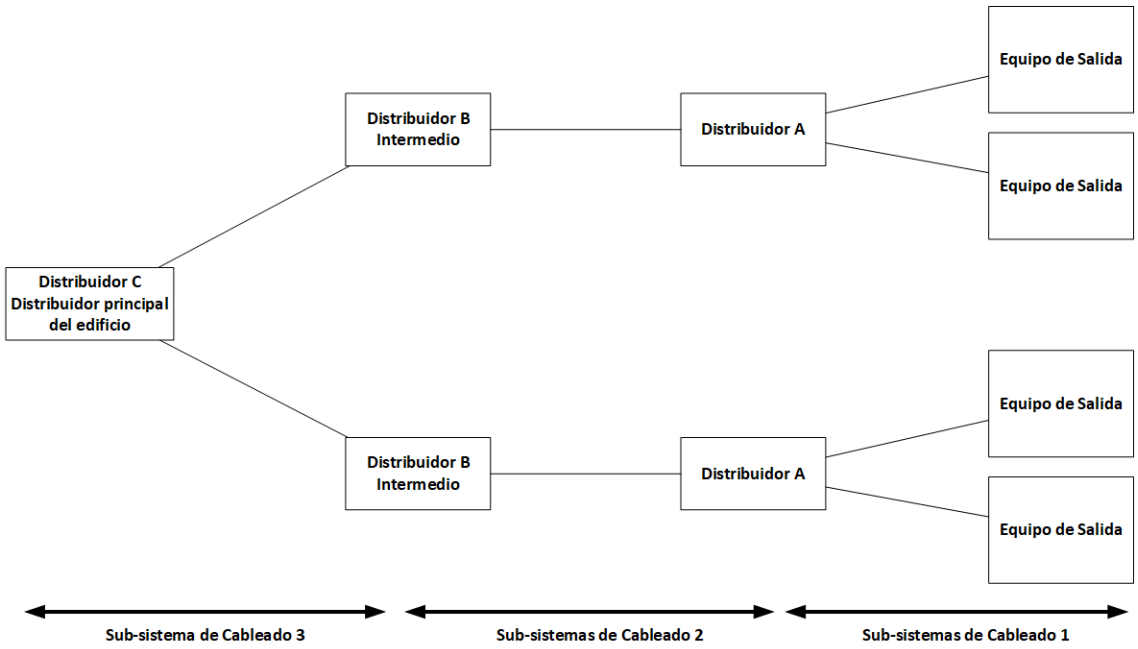


Figura 19: Distribución del cableado. Elaborado por el autor (2019)

- Sub-Sistemas 1: Es aquel cableado que se coloca entre las áreas de trabajo y el distribuidor A, en este proyecto es el laboratorio IoT y centro de desarrollo de software.
- Sub-Sistema 2: Es el cableado que conecta Distribución A con Distribución B, un nivel superior
- Sub-Sistema 3: Aquel que conecta con el distribuidor principal del edificio con las demás.
- Distribuidor A: Aquella sala o panel donde se conectarán todos los puestos de trabajo
- Distribuidor B: Ofrece la interconexión entre la Distribución principal con las de distribuciones de área de trabajo. En caso de que la estructura de cableado sea pequeña y no exista la Distribución A, las áreas de trabajo se conectaran directamente al Distribuidor B.
- Distribuidor C o Distribuidor principal del edificio: Donde está concentrada todas las conexiones que permiten la comunicación de todo el cableado tendido en un edificio o espacio.
- Equipos de salida: lugar donde se encuentran los puestos, puntos de trabajo o equipos finales.

ANSI/TIA/EIA 568-C-1: Brinda información referente a la planificación, instalación y verificación del cableado estructurado para las áreas.

Dentro de este estándar se forma de componentes funcionales, los cuales serán explicados en una tabla que relaciona el concepto del estándar TIA-568-C-0:

Tabla 6 Características Estándar TIA-568-C-0

Nomenclaturas TIA 568-C-0	Nomenclaturas TIA 568-C-1
Distribuidor C	Distribuidor Central de Cableado
Distribuidor B	Distribuidores Secundarios de Cableado
Distribuidor A	Distribuidores Horizontales de Cableado
Cableado de Sub-sistema 1	Cableado Horizontal a puestos de trabajo
Cableado de Sub-sistema 2	Interconexiones Cableadas entre áreas de trabajo
Cableado de Sub-sistema 3	Interconexiones Cableadas de Back-bone
Equipos de salida	Salida de Telecomunicaciones

Nota: Elaborado por el autor (2019)

En este proyecto solo se implementará a partir del distribuidor de cableado horizontal; el cual se encuentra dentro del armario o sala de telecomunicaciones lo que permitirá la interconexión entre las áreas de trabajo. Esta parte del cableado incluye lo siguiente:

- Cables de distribución horizontal

- Conectores en las áreas de trabajo
- Terminaciones de cableado horizontal
- Patch-cords dentro del rack vertical o sala de telecomunicaciones

El tendido de cableado de distribución horizontal no debe ser mayor a 90 metros y seguir una topología tipo estrella donde el terminal central se encuentra en el rack vertical que se encuentra ubicado en la habitación de los servidores.

Las terminaciones de cableado horizontal deben estar directamente conectadas al panel de interconexión (Patch-panel) que se encuentra en el rack vertical.

Los Patch-cord que se utilizan para conectar las áreas de trabajos a los equipos finales, y desde el rack vertical no debe ser mayor a 10 metros, se recomienda que cada Patch-cord sea menor a 5 metros y que la suma total del tendido de cable horizontal con los Patch-cord sea un máximo de 100 metros.

Cada área de trabaja debe mantener un mínimo de 2 conectores de comunicaciones, comúnmente uno de ellos es para la transmisión de voz y otra para la trasmisión de datos, o ya sea según la cantidad de dispositivos (Voz y/o Datos) que se desee implementar. Dependiendo de la tecnología para el servicio de voz se puede utilizar cable UTP, así mismo para la transmisión de datos se debe utilizar cable UTP categoría 5e o superior.

Las terminaciones en las áreas de trabajo deben usar conectores en “Jack” de 8 pares los cuales permiten dos tipos de conexiones T568A y T568B, las cuales permiten tener un orden y estándar de cómo será el cableado horizontal y sus conexiones.

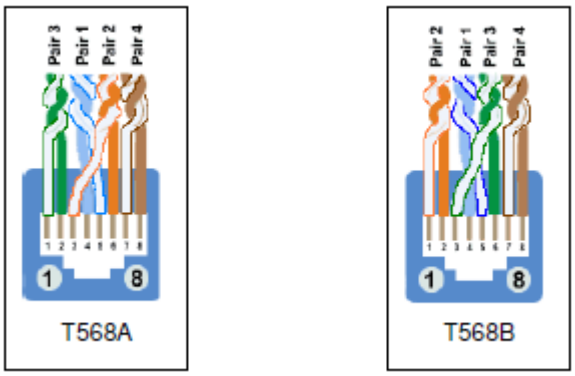


Figura 20: Hilos en un cable UTP. Tomado de Dr. Joskowic,(2013)

ANSI/TIA/EIA 568-C-2: Especifica los requerimientos de los cables par trenzado, sus componentes y parámetros de transmisión.

Este estándar y reconoce las siguientes categorías de cables:

Tabla 7 Categoría del Cable

	Cat 5e	Cat 6	Cat 6A
Tasa Máxima de Transmisión de datos	1000 Mbps	10 Gbps	10 Gbps
Frecuencia Máxima	100 Mhz	250 Mhz	500 Mhz
Distancia Teórica	100 mts	100 mts	100 mts
Distancia Máxima a la Máxima Tasa de Transmisión	50 mts	55 mts	

Nota: Elaborado por el autor (2019)

Existían categorías inferiores que ya quedaron obsoletas por ende no se las reconoce en este estándar.

Los cables que se utilizan para el tendido horizontal deben ser de 4 pares trenzados únicamente y el código de colores deben ser los siguientes:

Tabla 8 Construcción del Cableado

Par 1	Blanco Azul	Azul
Par 2	Blanco Naranja	Naranja
Par 3	Blanco Verde	Verde
Par 4	Blanco Café	Café

Nota: Elaborado por el autor (2019)

ANSI/TIA/EIA-606A: Este estándar define 4 clases diferentes para su administración, ya sea por su tamaño o características de la infraestructura del edificio que vaya a ser administrado.

Clase 1: Esta clase detalla los requerimientos de administración para una construcción, que contenga solo una sala de equipo y menos de 100 usuarios.

Se detalla los identificadores que utiliza la clase 1 para la administración, según Castro (2015) explica cuales son:

- Espacio de Telecomunicaciones (TS)
- Identificador Cableado Horizontal
- Barra Principal de Puesta a Tierra (TMGB)
- Barra de Puesta a Tierra (TGB)

Clase 2: La administración de la infraestructura es cuando hay más de una sala de cómputo y más de 100 usuarios.

Identificadores para la administración de la infraestructura de la clase 2, según Castro (2015) explica cuales son:

- Identificadores requeridos en la Clase 1
- Identificador del cableado vertical backbone
- Identificador del cable o fibra óptica
- Identificador de la ubicación del corta fuegos (firestopping)

Clase 3: Su administración de la infraestructura es para múltiples edificios y para más de 1000 usuarios.

Identificadores que se utiliza para su administración de la infraestructura según Castro (2015) dice que son:

- Identificadores requeridos en la Clase 2
- Identificador de Edificio
- Identificador del Backbone de Campus o Fibra Óptica

Clase 4: Detalla una infraestructura con varios sitios o campus

Identificadores requeridos para su administración, según Castro (2015) dice que son:

- Los identificadores requeridos en la Clase 3
- Identificador de Campus o Sitio

CAPÍTULO III METODOLOGÍA DE LA INVESTIGACIÓN

Para el desarrollo del proyecto, se utilizará la metodología cualitativa, como mencionan Rodríguez-Gómez, Gil-Flores, & Garcia-Jimenez (1996):

“Estudia la realidad en su contexto natural, tal y como sucede, intentando sacar sentido de, o interpretar los fenómenos de acuerdo con los significados que tienen para las personas implicadas. La investigación cualitativa implica la utilización y recogida de una gran variedad de materiales—entrevista, experiencia personal, historias de vida, observaciones, textos históricos, imágenes, sonidos – que describen la rutina y las situaciones problemáticas y los significados en la vida de las personas” (Pag, 32).

La metodología cualitativa es la que se ajusta más al proyecto de implementación de la infraestructura de red de datos para el laboratorio de IoT y centro de desarrollo de software, ya que al utilizar sus herramientas permitir el levantamiento de información, procesos, hechos o estructuras, las cuales no requieren de medición y tabulaciones numéricas.

Tipo de investigación: La investigación cualitativa se clasifica en: descriptiva e interpretativa. De acuerdo con las necesidades del proyecto, se utilizará la investigación descriptiva, misma que con sus mecanismos de la observación y la entrevista, facilitará conseguir resultados que beneficien a la realización de esta investigación sin llegar a deducir o admitir posición alguna en relación al evento descrito.

En base al estudio teórico y documental, se analizarán varios conceptos y modelos de información valida. Una ayuda adicional, representó la búsqueda, observación y análisis los datos secundarios obtenidos por otros investigadores o proyectos similares, relacionado al cableado estructurado de una infraestructura de red. Esta información se recopiló en base a papers, portales web, revistas científicas, libros y documentos impresos.

El primordial objetivo de esta investigación es, crear un diseño de una infraestructura de red para el laboratorio de IoT y centro de desarrollo de

software, para lo cual, se utilizará la investigación aplicada, según Vargas Cordero (2009) explica que:

"La investigación aplicada, entendida como la utilización de los conocimientos en la práctica, para aplicarlos en provecho de los grupos que participan en esos procesos y en la sociedad en general, además del bagaje de nuevos conocimientos que enriquecen la disciplina. Al respecto, en las ciencias puras y la investigación básica se busca indagar cómo funcionan las cosas para un uso posterior, mientras en las ciencias prácticas la investigación aplicada tiene como propósito hacer un uso inmediato del conocimiento existente"

Esta metodología de investigación permitirá dar solución a los problemas prácticos del diseño de la infraestructura de red del proyecto.

Técnicas e instrumentos de recolección de datos

Existen muchas técnicas e instrumentos de recolección de datos que ayudan a resolver inconvenientes que se presentan en los proyectos, en la siguiente tabla 4, que se indicarán las técnicas e instrumentos a utilizarse:

Tabla 9: Técnicas e instrumentos para recolección de datos

DISEÑO	TÉCNICAS	INSTRUMENTOS
Diseño Documental	Análisis documental	Normativas y estándares del cableado estructurado UTP.
Diseño de Campo	Entrevista	Estructura de entrevista / Grabadora.
	Observación	Fotografías, visita, formulario de observación.

Nota: Elaborado por el autor (2019)

A continuación, en la Tabla 5, se mostrará los campos de la persona seleccionada que con sus conocimientos ayudará a la resolución de la

problemática del proyecto con la utilización de formatos de entrevista y formulario de observación.

Tabla 10: Entrevistado

TITULO/ MAESTRÍA	DEPARTAMENTO	TIEMPO DE TRABAJO	CARGO	EXPERIENCIA
Si	Profesores tiempo completo	18 años	Tiempo Completo	Conocimiento total del tema

Elaborado: por el autor (2019)

Para el levantamiento de información del laboratorio de IoT y centro de desarrollo de software se emplearon los siguientes instrumentos:

- Entrevista
- Observación de Campo

La aplicación del instrumento de la entrevista permite conocer información y datos que son conocidos de manera directa por los expertos vinculados a los laboratorios de la Facultad de Ingeniería, expertos que conocen y dominan la temática de redes informáticas, tecnología e infraestructura de datos, con títulos profesionales de cuarto nivel, vinculados a la cátedra de redes en esta misma facultad. Consecuentemente, se puede inferir que los profesionales expertos tienen amplia experiencia en este tipo de temática, considerados además como parte de los docentes tutores de trabajos de investigación y de grado de la Universidad.

Las indagaciones realizadas utilizando los instrumentos de recolección de datos fueron orientadas a las necesidades propias del área y pensando en la aplicación de las mejores prácticas para implementar un laboratorio, el mismo que tenga un diseño de infraestructura de red de datos, cableado, conexión a internet, almacenamiento en la nube, conexión mediante VPN,

seguridad, acceso mediante Wireless, varios ambientes de pruebas, conexión remota y sobre todo un monitoreo sobre el consumo de ancho de banda de las maquinas.

El cumplimiento de las normativas es un aspecto importante que es considerado y analizado en el desarrollo del presente trabajo de investigación.

El propósito de la aplicación del instrumento para la recolección de datos es importante para entender y comprender la necesidad de los usuarios en la implementación de una solución de infraestructura en el laboratorio IoT y centro de desarrollo de software, es por eso que el instrumento de entrevista consideró preguntas abiertas de manera que permitió conocer los diferentes requerimientos y con ello conocer los tipos de equipamientos que se utilizarían como por ejemplo las características de las computadoras personales que se van a necesitar, el tipo de sistema operativo sobre el que operarán, el tipo de seguridad se deberá implementarse, la información que se guardará en los equipos y la forma de almacenamiento idónea.

Para la implementación del laboratorio IoT y centro de desarrollo de software se debe considerar que debe tener incluido esquemas de seguridad para que toda la información contenida dentro del laboratorio sea confidencial y no expuestas a ataques o amenazas, la información que se elabore en este laboratorio y salga a distribución tendrá un almacenamiento en la nube, de esa forma al momento de mostrar el aplicativo el usuario tendrán que conectarse al servidor que se encuentra la nube, los equipos que se instalarán tendrán que estar ubicados estratégicamente para que de esa forma se pueda ganar espacio y comodidad. El laboratorio dispondrá de cableado estructurado de tipo UTP Cat6 el mismo que va a permitir la conexión a los equipos de comunicación y por medio de ellos tener acceso a la red de Internet, también se pretende tener un contabilizador de datos para todas las máquinas existentes en el laboratorio y de manera que permita chequear el consumo de ancho de banda, también se dispondrá de un acceso remoto para que los usuarios puedan trabajar desde cualquier lugar y desempeñar eficientemente sus tareas de programación desde el lugar en que se

encuentre, se brindará a sus usuarios una conexión inalámbrica (Wireless) de manera que el estudiante tenga lo necesario para crear y desarrollar aplicativos informáticos, toda la implementación descrita anteriormente sobre el laboratorio IoT y centro de desarrollo de software se la realizará con los recursos que cuenta la Facultad de Ingeniería y en la parte lógica se utilizará software libre dejando de esta manera un laboratorio con una infraestructura actualizada de red de datos.

Con respecto al párrafo anterior el laboratorio contará con 5 ambientes los mismos que se describirán a continuación:

- Ambiente de Producción
- Ambiente de Pruebas
- Ambiente de Desarrollo
- Ambiente de Monitoreo
- Ambiente Access Point

El ambiente de producción se implementará definiendo una Vlan con identificación 100, la misma que tendrá las reglas de firewall que fueron sugeridas por el usuario, seguridad en bloqueo de páginas de ocio (redes sociales, juegos, entretenimiento), ICMP, acceso a servicio FTP para que toda información se guarde directamente en la nube y se le asignará un IP estática a las computadoras que estarán en este ambiente.

El ambiente de pruebas se implementará con la Vlan 200, esta vlan tendrá las reglas de firewall que fueron sugeridas por el usuario, seguridad en bloqueo de páginas de ocio (redes sociales, juegos, entretenimiento), ICMP y se le asignará un IP estática a las computadoras que estarán en este ambiente.

El ambiente de desarrollo se va a implementar sobre la Vlan 300, la misma que tendrá las reglas de firewall que pidió el usuario, en la parte de bloqueo de páginas, las máquinas que estarán en este ambiente tendrán acceso a video tutoriales ya que en este ambiente se van a desarrollar software y por tal motivo algunas explicaciones de código se encuentran en formato de video de tal manera esta vlan tiene excepciones en la parte de

bloqueo de páginas y por último se les asignará una IP estática a las computadoras que corresponderán a este ambiente.

El ambiente de monitoreo corresponderá a la Vlan 400, esta vlan tendrá las reglas de firewall diferente a las demás vlans ya que en la computadora que estará en este ambiente se le instalará un software el mismo que permitirá controlar el ancho de banda, también dispondrá seguridad en bloqueo de páginas de ocio, como esta vlan va a controlar el tráfico de red se asignó una IP al switch el mismo que va a permitir el monitoreo de las demás vlans y la computadora que estará en este ambiente se le asignará una IP estática.

El ambiente Access Point, pertenecerá a la interfaz de la Vlan 500, las reglas de firewall para esta vlan son las que sugirió el usuario, las mismas se describirá en la propuesta del proyecto, por seguridad se bloqueará páginas de ocio (redes sociales, juegos, entretenimiento), tendrá servicio FTP, filtrado de MAC, portal cautivo y esta vlan tendrá activado el DHCP server para asigne una IP aleatoriamente a los dispositivos que se conecten al AP, los dispositivos que estarán conectados al AP tendrán un tiempo limitado de conexión luego de que pase el tiempo tiene volverse a conectar.

Método de observación

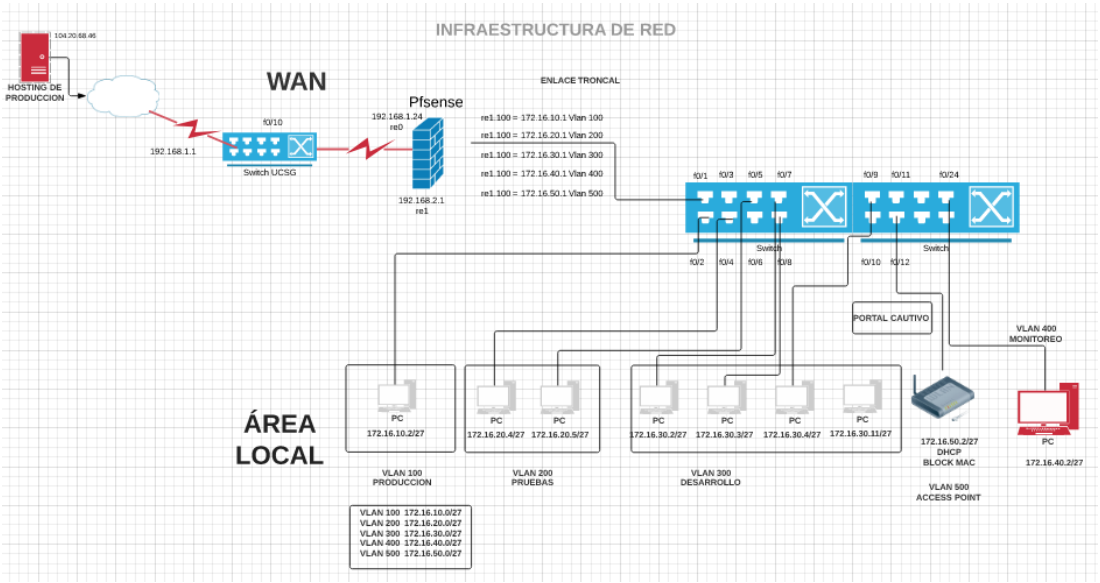
Aplicando el método de observación se pudo evidenciar en el lugar donde se implementará el laboratorio IoT y centro de desarrollo de software, no todas las computadoras están en óptimas condiciones y las que funcionaban no contaban con algún tipo de seguridad tanto físico como lógico, además se pudo observar que no se cuenta con acceso a internet, así como tampoco se dispone de un servicio de acceso inalámbrico; se pudo evidenciar novedades menores tales como el estado de las canaletas PVC que estaban totalmente sueltas y el cable que pase por ahí no está bien sujetado, no dispone de sillas ergonómicas para la comodidad de los usuarios; sin embargo, el laboratorio si dispone de un ambiente climatizado con aire acondicionado que favorece al buen desempeño de los equipos informáticos.

CAPÍTULO IV PROPUESTA TECNOLÓGICA

Introducción

Una vez que se detectó las necesidades del usuario por medio del levamiento de información efectuado en el Capítulo III, la finalidad de este Capítulo, es la implementación de la infraestructura de red de datos del laboratorio Iot y centro de desarrollo de software de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil teniendo en cuenta que se ha cumplido con todos los objetivos propuesto al principio de este proyecto. Es así, que, para la implementación de este proyecto, se compone de dos partes que son: El diseño del cableado y la configuración de la red:

Figura 21 Diseño de Red. Elaborado por el autor (2019)



En lo que se refiere al diseño del cableado, es de forma horizontal y vertical basadas en las normativas TIA/EIA 568-C y TIA/EIA 569-C. Antes de elegir el cable a utilizarse se realizará un cuadro comparativo entre los más utilizados en el medio.

Comparación del cable UTP Cat5e, Cat6, Cat6a:

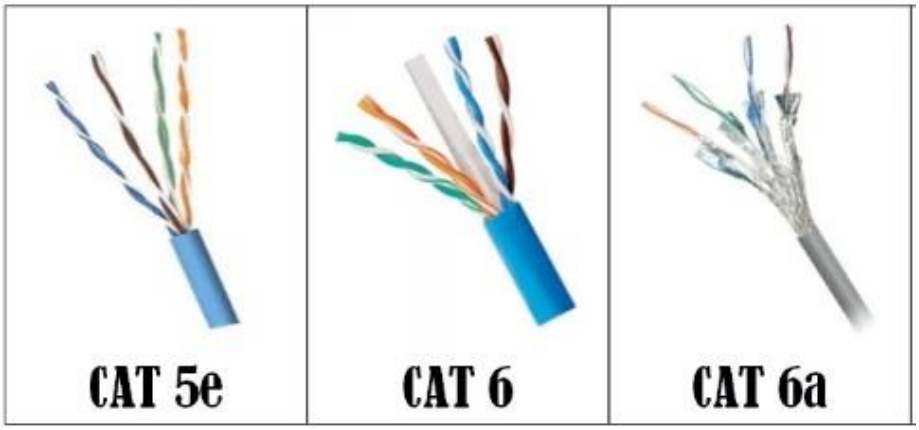


Figura 22 Tipos de Cable UTP. Elaborado por (Telectrónica, 2018)

Velocidad	1000Mbps	1000Mbps	1000Mbps
Frecuencia	100Mhz	250MHz	500 MHZ
Distancia	100 m	100 m	100 m
Retraso	45 ns	45ns	45 ns
Perdida de retorno (min. A 100 MHz)	20.1 dB	20.1 dB	8 dB

Tabla 11 Cuadro Comparativo del Cableado Cat 5e, Cat6 y Cat 6ª. elaborado por el autor (2019)

Con respecto al cuadro comparativo entre las dieferentes categoría de cableado más utilizado hoy en dia que son: Cat 5e, Cat 6 y Cat 6ª; los tres tipos de cableado disponen de una velocidad de 1000 Mbps, la distancia de longitud máxima permitida de los tres es de 100m y en lo que respecta a sus frecuencia cada categoria tiene una frecuencia diferente, las tres categorías estan basadas en la Norma EIA/TIA-568-B.

El cable más utilizado e instalado actualmente es el cable de Cat 6, ya que posee una mejora de velocidad con respecto al tráfico de red y mantiene un costo aceptable, es por eso que para la implementacion del cableado estructurado del laboratorio se utilizará el cableado Cat 6.

El cableado a utilizar en este diseño, es el par trenzado de tipo UTP Cat6, que tiene un diámetro exterior de 7.1 mm (0.71 cm – 0.27 plg), el cual es aceptado por la normativa ANSI/TIA/EIA 568B.2, además este cable posee otras características las cuales son:

- Alta compatibilidad electromagnética
- Buen desempeño ante interferencias.
- Es muy utilizado en laboratorios informáticos, instituciones educativas, etc.
- Avalado por estándares ISO11801, TIA/EIA 568 B y CENELEC 50173

Los lineamientos o requisitos que se deben tomar en cuenta para el diseño del cableado de red son los siguientes:

- Uso de canaletas de PVC en base de la normativa TIA/EIA 569-C para la distribución del cable de red hacia las máquinas.
- Cada cable será etiquetado para tener una rápida identificación al momento de su implementación, una vez concluido con su recorrido, se etiquetarán bajo el estándar ANSI/TIA/EIA/606-B.
- El cableado debe ser direccionado al momento que se saque del carrete con el propósito de comprobar su rendimiento
- Durante el recorrido de los cables no debe existir ningún tipo de obstáculos, y serán sujetados por medio de correas plásticas para que el cable este distribuido de una mejor forma.
- El rack a utilizarse es de forma aérea, en el cual se colocarán el switch y el pacth panel, por seguridad o cambios de mejora se dejará 2 m de cable para facilitar el trabajo.
- En la distribución del cableado se debe colocar los puntos de jack’s necesarios para llevar la señal a las máquinas.

Configuración de Red

De acuerdo con las necesidades que dio a conocer el usuario en la entrevista, uno de sus requerimientos que indicó fue que la infraestructura de red de datos tenga seguridad, por lo tanto, se realizó una investigación de medidas de seguridad para la infraestructura de la red de datos. A continuación, se describirá algunas medidas de seguridad más usadas:

- Firewall: Controla los servicios que se encuentra expuestos en la red, de tal forma que termina bloqueándolos o restringiéndoles el acceso a los puertos.
- Antivirus: Son programa creados para la prevención, bloqueo y eliminación de archivos que puede perjudicar la funcionalidad de la máquina.
- Sistema de prevención de intrusos: Controla el acceso en una red, protegiendo a todos los sistemas que se encuentren dentro de la red de ataques o amenazas externas.
- Proxy: Es un dispositivo o programa que permite la conexión entre un dispositivo y otro, entonces por medio del proxy la información va primero al dispositivo intermedio y este se comunica al dispositivo de destino, quedando claro que el dispositivo de destino nunca va a tener una conexión directa entre el primero y último.
- Red privada virtual(VPN): Es utilizada para conectar una o más computadoras a una red privada ya sea desde casa u oficina utilizando internet, por medio de las VPN podemos conectarnos de forma segura y remota ya que estas mismas aplica una capa de cifrado y autentificación a la ruta para proteger el tráfico de red.

Como conclusión y de acuerdo a los requerimientos del usuario la medida de seguridad y a la que más se ajusta a las necesidades es el Firewall o cortafuego.

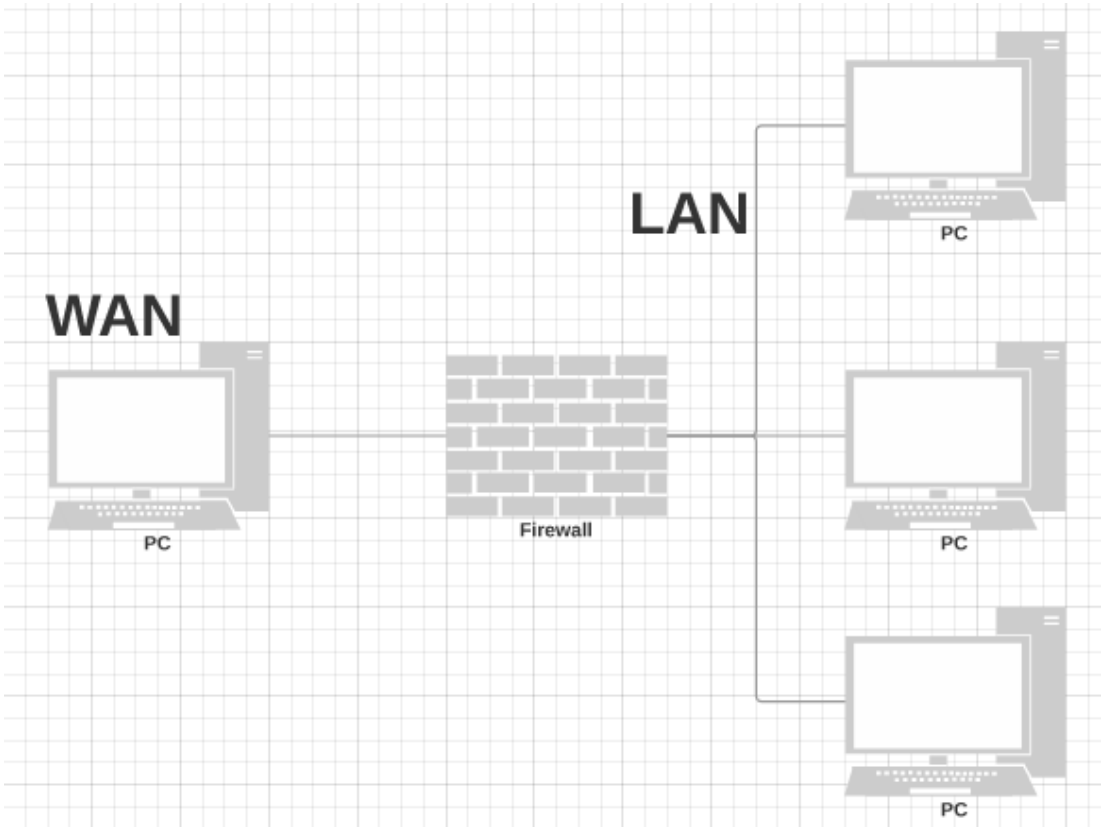


Figura 23 Firewall. Elaborado por el autor (2019)

En la figura 23, represento como va a estar organizada la red, se tendrá dos interfaces; red WAN y red LAN. Por medio del firewall se va a poder restringir, detectar y prevenir los accesos no autorizados a nuestra red LAN, también ayudará a proteger los dispositivos y equipos que se encontraran dentro del laboratorio a implementar.

Existen dos tipos de firewall de: software y hardware. Actualmente para tener una mayor seguridad es necesario implementar los dos tipos. De acuerdo con los recursos que posee la Facultad de Ingeniería se utilizara para este proyecto el firewall de software libre, por tal razón se investigó varios tipos de firewalls de software entre los que están:

Cuadro comparativo de Firewalls de Software:

	Comodo Firewall	PfSense	FortiGate
Sistema operativo	Windows	Linux	Linux
Precio	Free	Free	Free
Calificaciones	Fácil de configurar, administrar y de usar, tiene una calidad de soporte de 8.2 de 10	Fácil de configurar por medio de una interfaz web, administrar y de usar, tiene una calidad de soporte de 8.3 de 10	Fácil de configurar, administrar y de usar, tiene una calidad de soporte de 8.5 de 10
Características de Administración	Contiene gestión de políticas, realiza registro e informes y Gateway de aplicación	Contiene gestión de políticas, realiza registro e informes y Gateway de aplicación y sesiones concurrentes	Contiene gestión de políticas, realiza registro e informes y Gateway de aplicación y sesiones concurrentes
Funcionabilidad	Trabaja con VPN, filtrado de URL	Trabaja con VPN, creación de interfaces, antivirus, filtrado de URL y vlans	Trabaja con VPN, antivirus, filtrado de URL
Vigilancia	• Balanceo de carga • Análisis continuo	• Balanceo de carga • Análisis continuo • Prevención de intrusos	• Balanceo de carga • Análisis continuo • Prevención de intrusos • Detección de intrusos

		• Detección de intrusos • Bloqueo de intrusos	
Industrias	Es utilizado en negocios pequeños menos de 50 empleados.	Es utilizado en negocios pequeños y medios.	Es utilizado para negocios pequeños, medios y grandes.

Tabla 12 Cuadro Comparativo Firewall. Elaborado por el autor (2019)

Previo a la comparación los firewall de software más utilizados, se concluyó que Pfsense es el producto que más se ajusta a las necesidades de los laboratorios. Este firewall está basado en FreeBSD (es un sistema totalmente libre no requiere pago alguno), el sistema operativo que utiliza Pfsense es Linux mismo que al estar instalado en este SO permitirá mantener una mayor seguridad, la configuración de este firewall se la puede realizar mediante consola o interfaz web, su administración es fácil y obtuvo un 8.3 sobre 10 en su calidad de soporte. Unas de sus características en la administración es que gestiona las políticas y realiza un registro o informe de sesiones concurrentes, este firewall es considerado uno de los mejores del mundo ya que posee packet filter (filtro de paquetes) el cual permite filtrar el trafico TCP/Ip, controla el ancho de banda y lo gráfica, permite la configuración VPN, creación de interfaces, creación de portal cautivo, URL etc. También muestra el status y diagnósticos ya sea de la maquina o de las interfaces virtuales y VPN creadas. En su seguridad este firewall posee un análisis continuo, detecta y bloquea a personas no autorizadas, contiene una lista muy grande de paquetes que permiten expandir de una forma muy fácil todas las funcionabilidades y no compromete la seguridad de la red o sistema, con respecto a su utilización está considerado para industrias o empresas pequeñas y medias.

Explicación de la configuración de la red de datos en Pfsense

1. Instalación del Firewall Pfsense

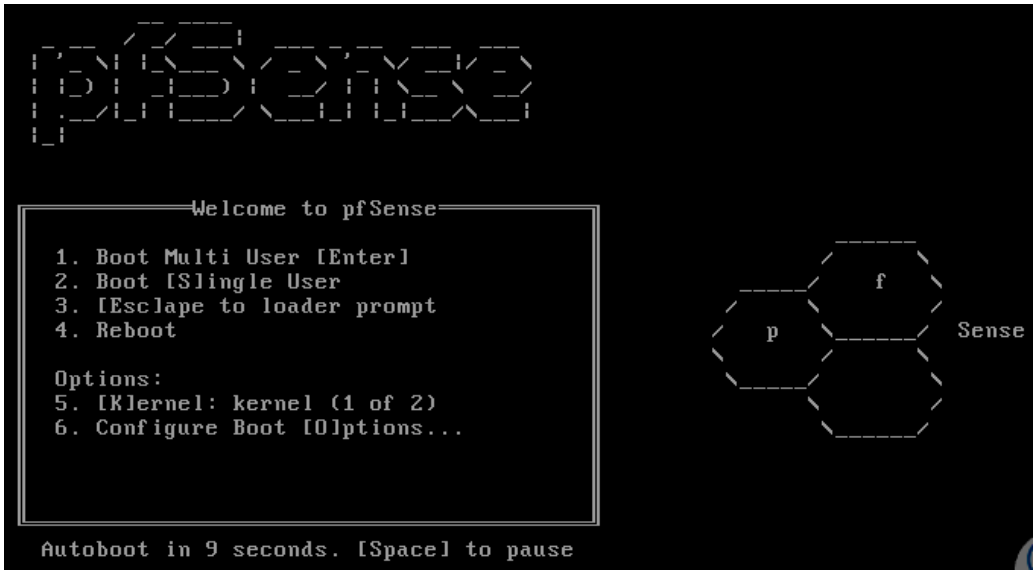


Figura 24 Instalación Firewall Pfsense. Elaborado por el autor (2019)

Luego de instalación del firewall, automáticamente aparecerá la siguiente pantalla donde se reconocerá las interfaces de red que tiene el servidor y se debe seleccionar cual será la red WAN y red LAN

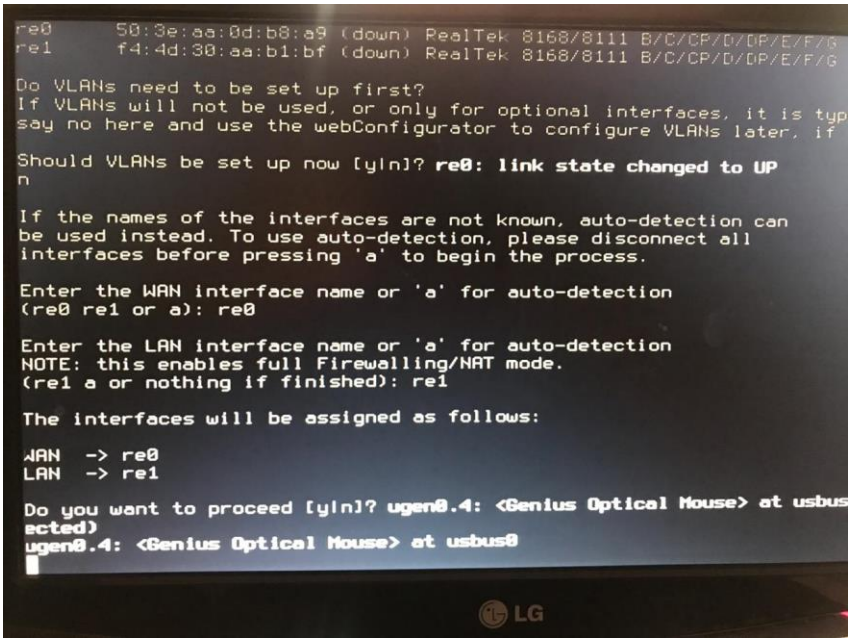


Figura 25 Configuración de Interfaces. Elaborado por el autor (2019)

El firewall por default asignará una IP para la red WAN y LAN.

Pero para la red WAN se tiene configurado DHCP cliente porque espera a que se le asigne una IP, en cambio para la red LAN se da por defecto una IP estática como se muestra a continuación:

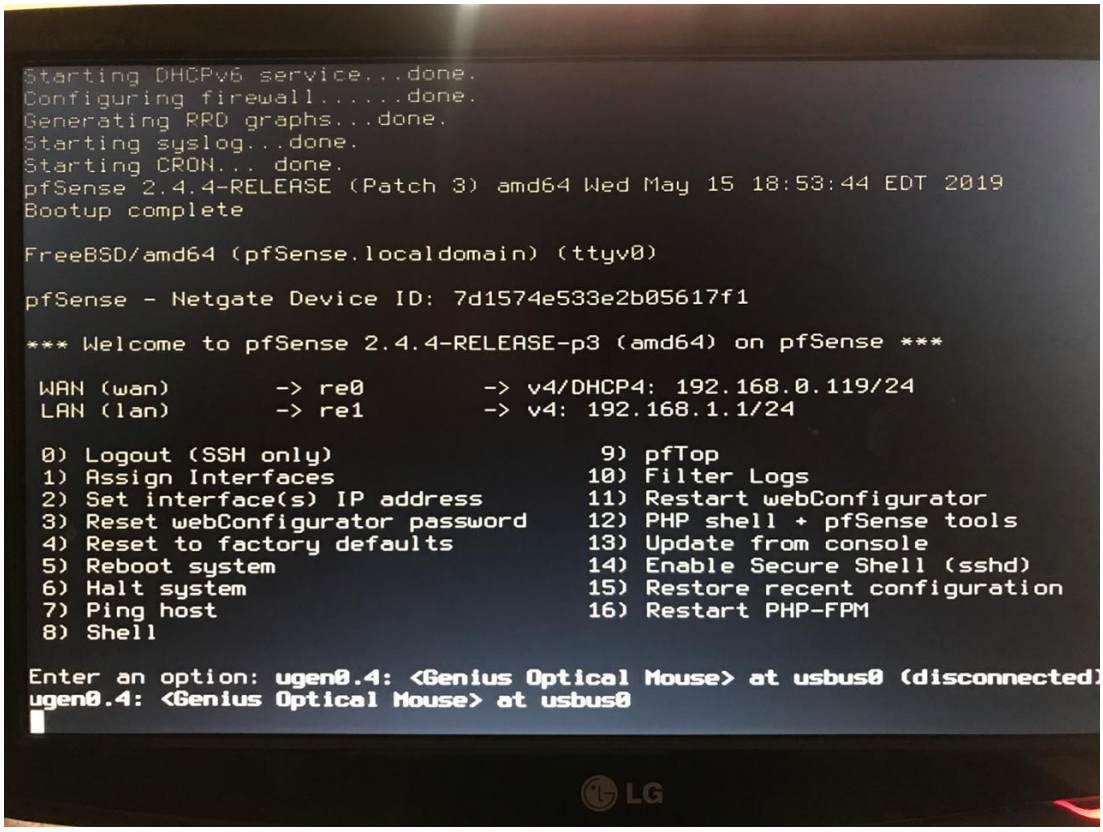


Figura 26 Asignación de IP. Elaborado por el autor (2019)

Ingresar a la IP de la red LAN y se re dirige a un explorador web para su configuración.

Login con el usuario y contraseña que nos da Pfsense por defecto, que sería:

User: admin

Pass: pfsense

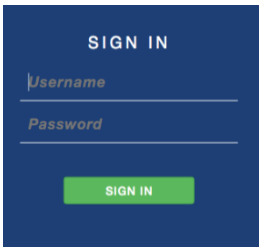


Figura 27 Login Firewall. Elaborado por el autor (2019)

La primera configuración dentro del Pfsense es asignar a la red WAN la IP y el puerto por el cual se va a acceder al Pfsense

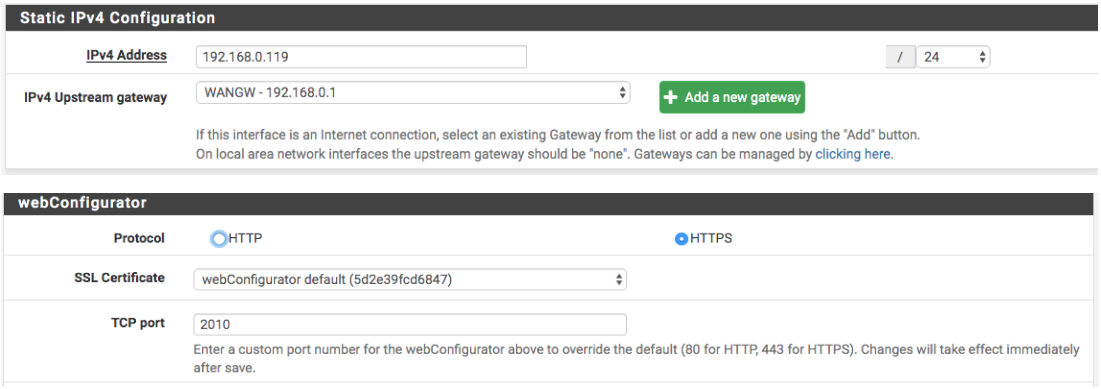


Figura 28 IP WAN y puerto. Elaborado por el autor (2019)

CREACIÓN Y CONFIGURACIÓN DE VLANS Y ENRUTAMIENTO ENTRE VLANS

Luego de asignar la IP y puerto, se crean y se configuran los siguientes ambientes en Pfsense, para aplicar los requerimientos identificados al aplicar las herramientas de investigación:

- VLAN100: PRODUCCION
- VLAN200: PRUEBAS
- VLAN300: DESARROLLO
- VLAN400: MONITOREO

- VLAN500: ACCESS POINT

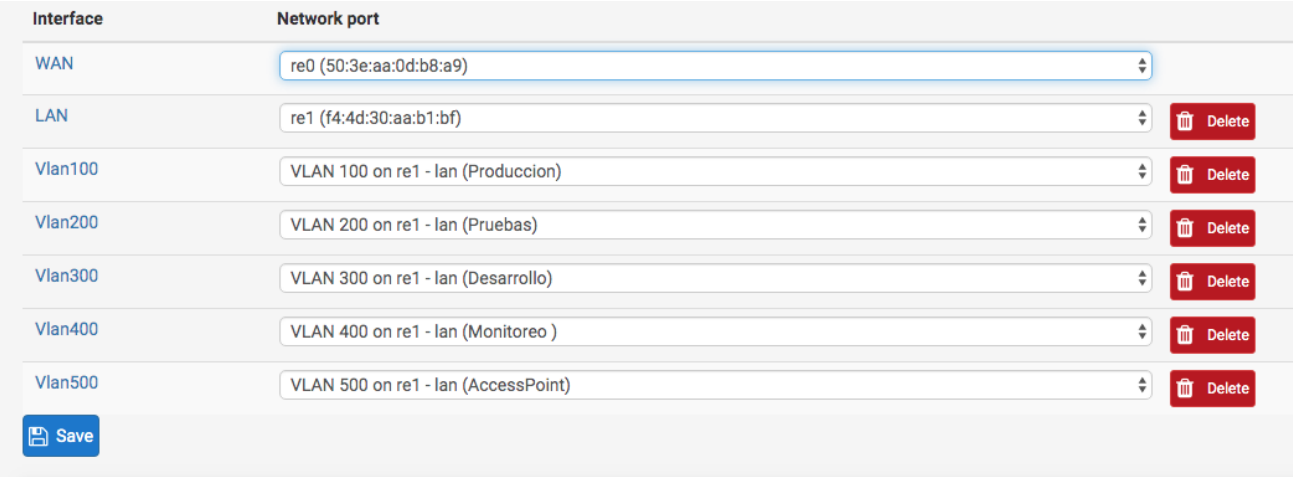


Figura 29 Vlan's Creadas. Elaborado por el autor (2019)

Una vez creadas las interfaces virtuales en el Pfsense, se asigna una IP para cada Vlan.

- Vlan 100= 172.16.10.1 Ambiente de Producción
- Vlan 200= 172.16.20.1 Ambiente de Pruebas
- Vlan 300= 172.16.30.1 Ambiente de Desarrollo
- Vlan 400= 172.16.40.1 Ambiente de Monitoreo
- Vlan 500= 172.16.50.1 Access Point

Las mismas tendrán mascará 27 y cuya función será de indicar a los dispositivos a que parte de la dirección IP es su identificador de red, también incluida la subred.

Cabe indicar que, en la VLANS de Producción, Pruebas, Desarrollo y Monitoreo esta desactivado DHCP Server por el motivo que las asignaciones de IP a las maquinas serán de forma estática y en la VLAN Access Point está activado el DHCP Server, mismo que servirá para que de forma dinámica se le asigne una IP a los dispositivos que se conecten.

Luego de asignar las IP a las VLANs se procederá a la configuración del Switch donde se creará la mismas VLANs que tiene Pfsense, pero asignándole un puerto en el Switch, como se puede apreciar a continuación:

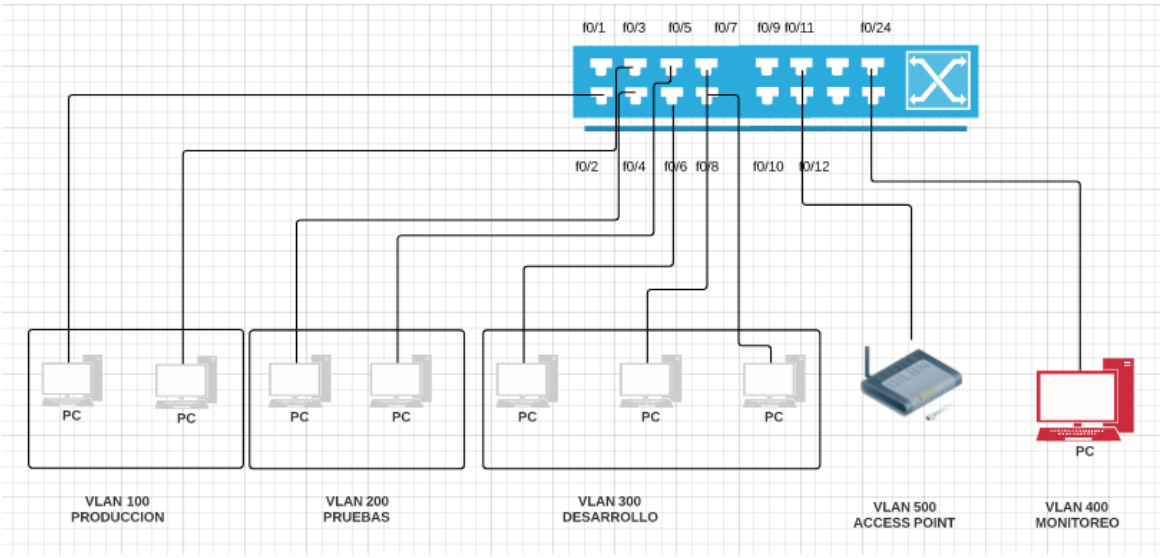


Figura 30 Distribución de Vlan's. Elaborado por el autor (2019)

Creación de Vlans y asignación de las interfaces.

SW1>enable

SW1#show vlan //Comprobar si existe VLANs creadas

SW1#configure terminal //Modo privilegiado

SW1(config)#vlan 100 // Crear la VLAN 100

SW1(config-vlan)#name Produccion // Asignamos un nombre

SW1(config-vlan)#exit //Salir

Asignar un puerto a una VLAN

SW1(config)#interface f0/2 //Entrar al modo de configuración de interface

SW1(config-if)#switchport mode access // Paso del tráfico de una vlan en especifico

SW1(config-if)#switchport access vlan 100 // Se asigna la interface a la VLAN 100

SW1(config-if)#no shutdown // Inicializa la interfaz del Switch

SW1(config-if)#do write // Guarda toda la configuración

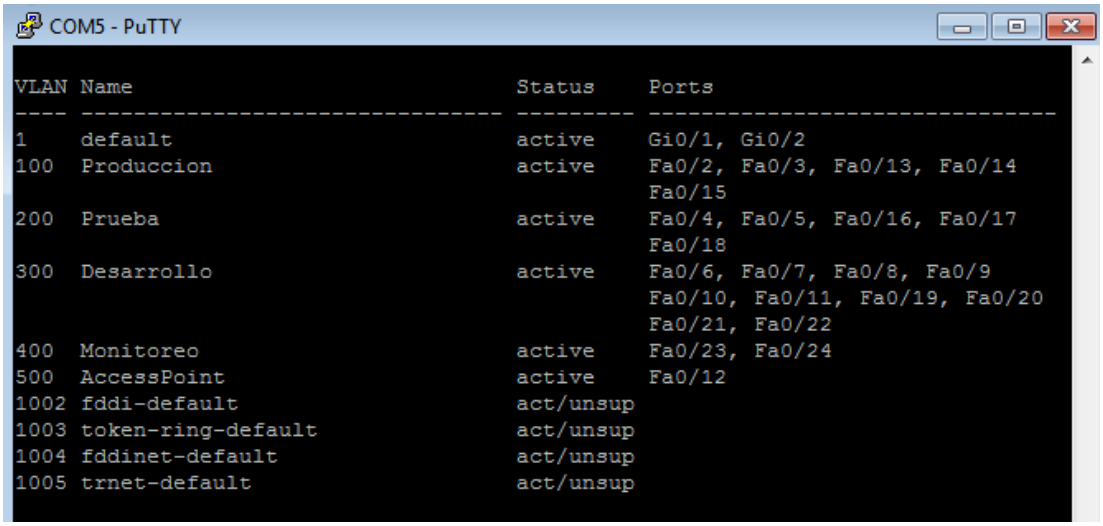
SW1(config-if)#exit // Salir del modo de configuración

SW1(config)#exit

En la parte de enrutamiento el firewall Pfsense por defecto crea el enrutamiento entre las VLANs

Con respecto a la configuración del Switch está distribuido de la siguiente manera:

Figura 31 Interfaces asignada a las Vlan's. Elaborado por el autor (2019)



De tal forma que solo se utilizarán las siguientes interfaces:

- f0/1: Enlace Troncal
- f0/2: Vlan 100 (Producción)
- f0/3: Vlan 100 (Producción)
- f0/4: Vlan 200 (Pruebas)
- f0/5: Vlan 200 (Pruebas)
- f0/6: Vlan 300 (Desarrollo)
- f0/7: Vlan 300 (Desarrollo)
- f0/8: Vlan 300 (Desarrollo)
- f0/9: Vlan 300 (Desarrollo)
- f0/11: Vlan 500 (Access Point)
- f0/24: Vlan 400 (Monitoreo Server)

- f0/23: Vlan 400 (Monitoreo)

Los puertos no nombrados anteriormente, estarán disponibles en caso de que se quiera añadir más computadoras a las diferentes VLANs.

Configuración de Políticas de Firewall

Crear una política en Pfsense

En la barra de menú que dispone este firewall, dar clic en la opción de Firewall, luego dar clic en Rules

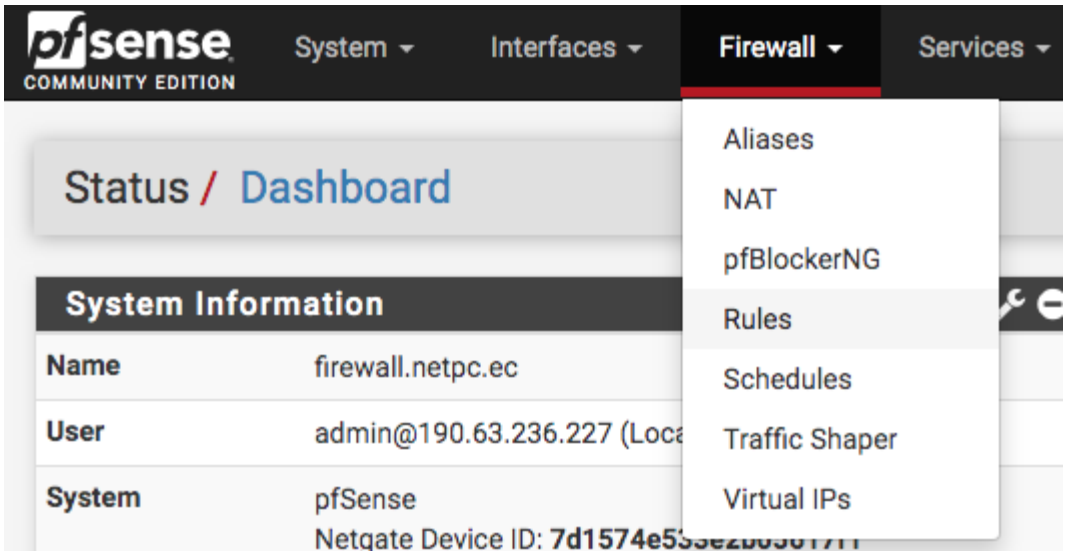
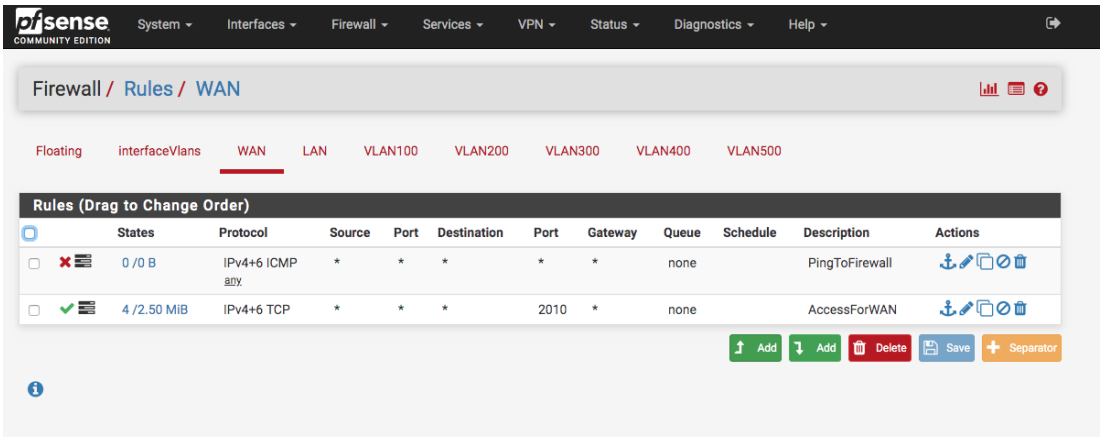


Figura 32 Agregar Regla de Firewall. Elaborado por el autor (2019)

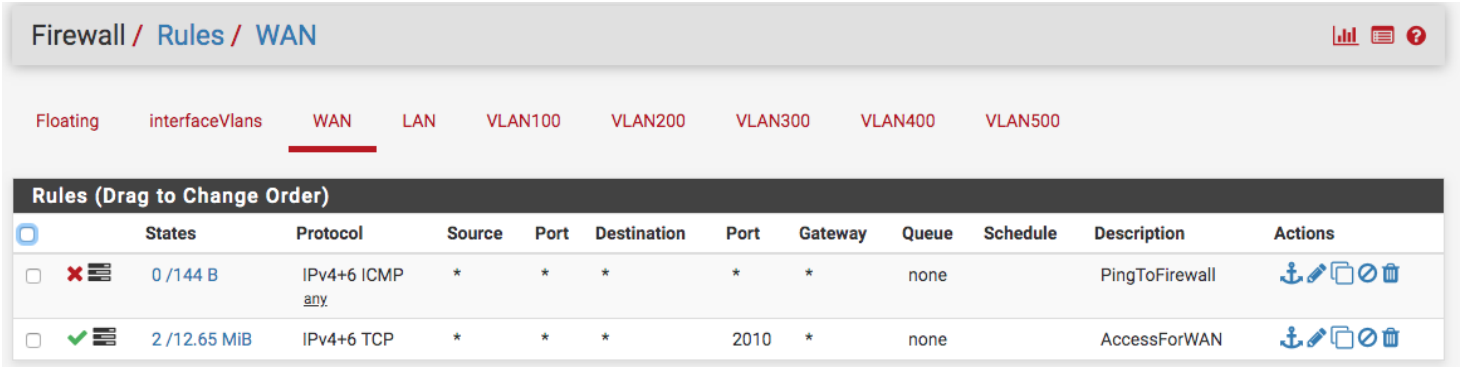
Escoger la interfaz a la que se va a asignar una regla, dentro de la interfaz escogida dar clic en la opción add para añadir una nueva regla.



Previo a la explicación de cómo agregar una regla en el firewall, continuamos con la configuración de las interfaces virtuales que contiene el Pfsense, donde se definirá y se agregará diferentes reglas para cada interfaz.

Interfaz WAN

Figura 33 Reglas Interfaz WAN. Elaborado por el autor (2019)

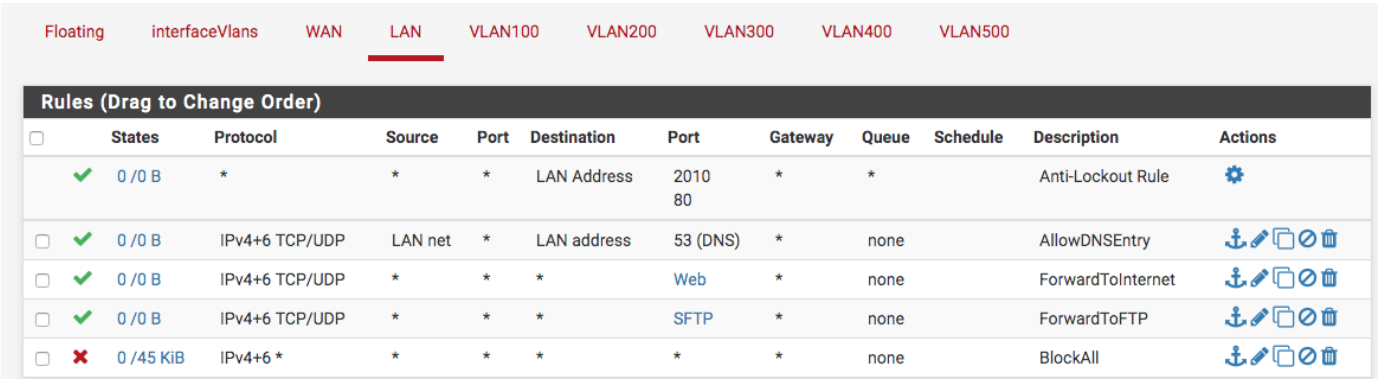


Regla 1: No permite hacer ping al firewall

Regla 2: Acceso a Pfsense por medio del puerto 2010

Interfaz LAN

Figura 34 Reglas Interfaz LAN. Elaborado por el autor (2019)



Regla 1: Esta regla la da por defecto el Pfsense, e indica que todo tráfico que tenga como destino la IP de la LAN del Pfsense hacia el puerto 2010 y 80 sea permitido por defecto.

Regla 2: Permite que solo los protocolos TCP/UDP envíen paquetes DNS que tenga origen desde LAN net y tenga como destino LAN address, quiere decir que traduce los nombres de la red y permite conocer la Ip de la maquina donde se está alojando el dominio al que queremos acceder.

Regla 3: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, sea desde cualquier origen a cualquier destino de la red LAN, permitirá todo lo que es trafico web.

Regla 5: Permite transferencia SFTP y FTP, los puertos incluidos son (20, 21, 22).

Regla 6: Lo demás que no esté considerado en estas las reglas establecidas anteriormente estará bloqueado.

LAN Net: Es todo el segmento de red de la interfaz.

LAN Address: Es la IP que tiene asignada la interfaz dentro del Firewall Pfsense.

Interfaz VLAN 100

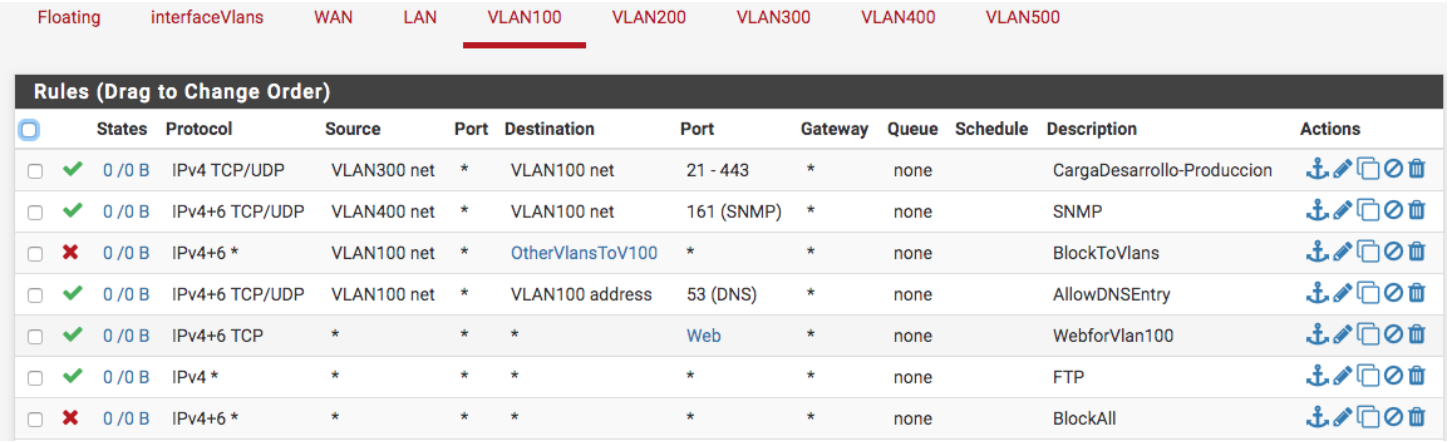


Figura 35 Reglas Interfaz Vlan100. Elaborado por el autor (2019)

Las reglas que se asignó en la interfaz de la VLAN 100 son las siguientes:

Regla 1: Permite protocolos TCP/UPD que tenga como origen la VLAN 300 y tenga como destino la VlLAN 100 y sea desde el puerto 21 hasta 443, permitirá la carga de archivos.

Regla 2: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, que su origen sea la VLAN 400 y su destino sea la VLAN 100 y que aceda por el puerto 161 (SNMP), será permitido.

Regla 3: No permite ping entre las VLANs a excepción de la VLAN 300 a la VLAN 100.

Regla 4: Permite que solo los protocolos TCP/UDP envíen paquetes DNS que tenga origen desde VLAN 100 net y tenga como destino VLAN 100 address, quiere decir que traduce los nombres de la red y permite conocer la Ip de la maquina donde se está alojando el dominio al que queremos acceder.

Regla 5: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, sea desde cualquier origen a cualquier destino de la red LAN, permitirá todo lo que es trafico web.

Regla 6: Permite transferencia SFTP y FTP, los puertos incluidos son (20, 21, 22).

Regla 7: Lo demás que no esté considerado en estas las reglas establecidas anteriormente estará bloqueado.

Interfaz VLAN 200

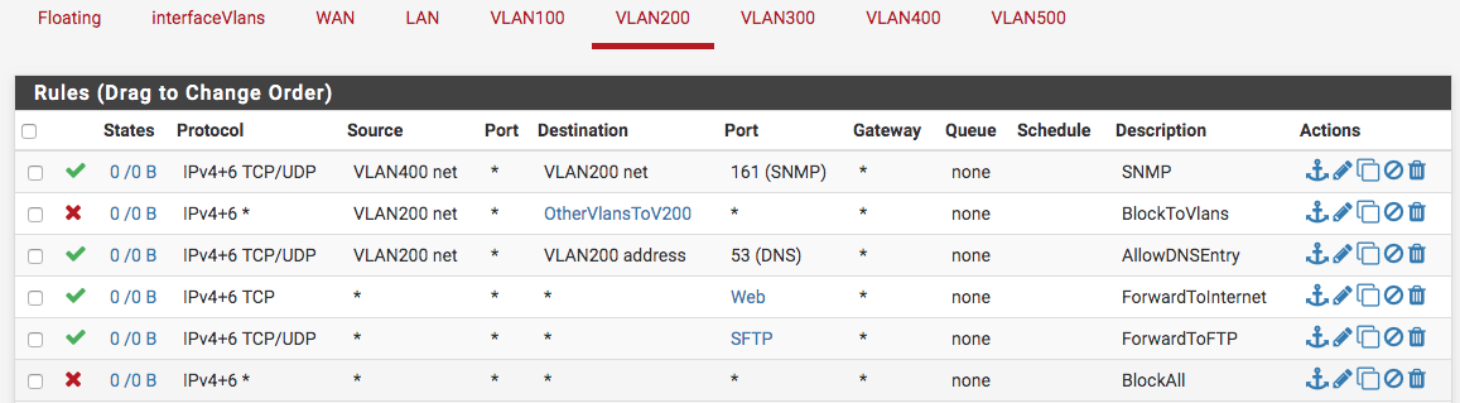


Figura 36 Reglas Interfaz Vlan200. Elaborado por el autor (2019)

Las reglas que se asignó en la interfaz de la VLAN 200 son las siguientes:

Regla 1: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, que su origen sea la VLAN 400 y su destino sea la VLAN 200 y que aceda por el puerto 161 (SNMP), será permitido.

Regla 2: No permite ping entre las demás VLANs.

Regla 3: Permite que solo los protocolos TCP/UDP envíen paquetes DNS que tenga origen desde VLAN 200 net y tenga como destino VLAN 200 address, quiere decir que traduce los nombres de la red y permite conocer la Ip de la maquina donde se está alojando el dominio al que queremos acceder.

Regla 4: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, sea desde cualquier origen a cualquier destino de la red LAN, permitirá todo lo que es trafico web.

Regla 5: Permite transferencia SFTP y FTP, los puertos incluidos son (20, 21, 22).

Regla 6: Lo demás que no esté considerado en estas las reglas establecidas anteriormente estará bloqueado.

Interfaz VLAN 300

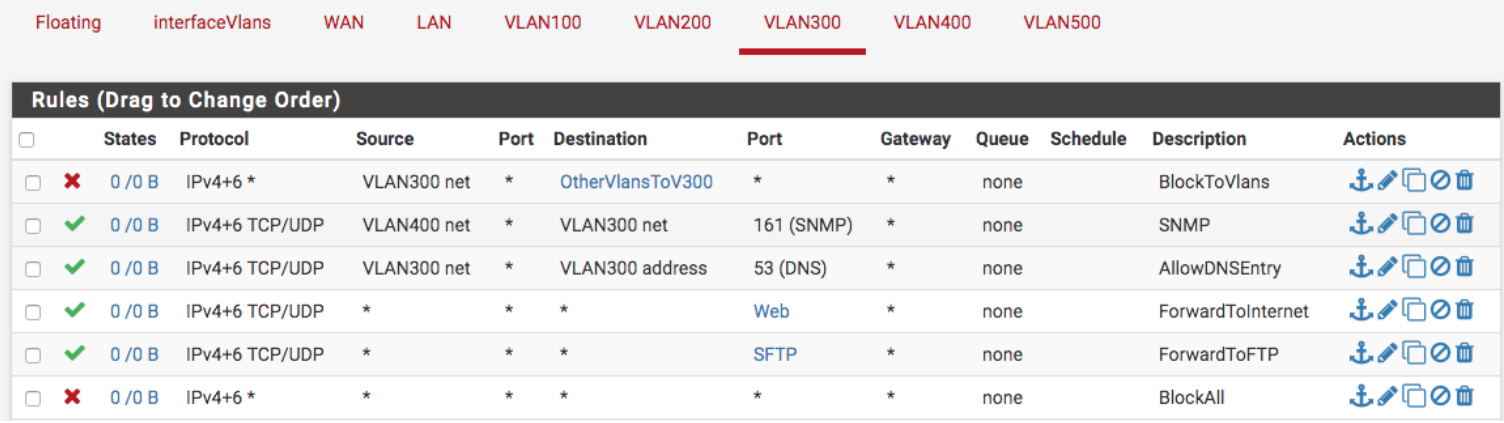


Figura 37 Reglas Interfaz Vlan300. Elaborado por el autor (2019)

Las reglas que se asignó en la interfaz de la VLAN 300 son las siguientes:

Regla 1: No permite ping entre las demás VLANs.

Regla 2: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, que su origen sea la VLAN 400 y su destino sea la VLAN 300 y que aceda por el puerto 161 (SNMP), será permitido.

Regla 3: Permite que solo los protocolos TCP/UDP envíen paquetes DNS que tenga origen desde VLAN 300 net y tenga como destino VLAN 300 address, quiere decir que traduce los nombres de la red y permite conocer la Ip de la maquina donde se está alojando el dominio al que queremos acceder.

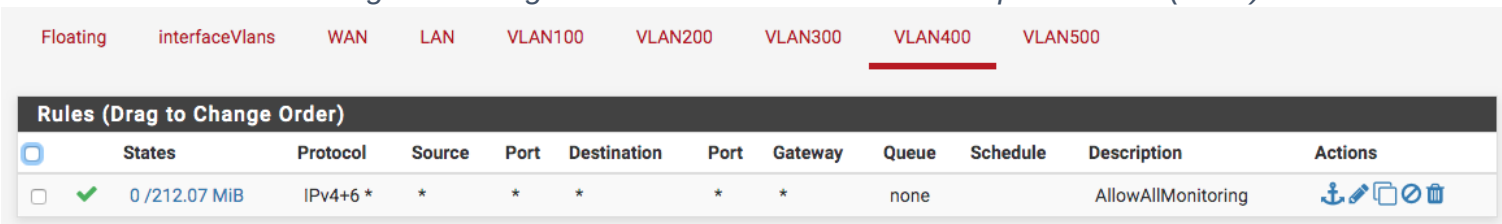
Regla 4: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, sea desde cualquier origen a cualquier destino de la red LAN, permitirá todo lo que es trafico web.

Regla 5: Permite transferencia SFTP y FTP, los puertos incluidos son (20, 21, 22).

Regla 6: Lo demás que no esté considerado en estas las reglas establecidas anteriormente estará bloqueado.

Interfaz VLAN 400

Figura 38 Reglas Interfaz Vlan400. Elaborado por el autor (2019)

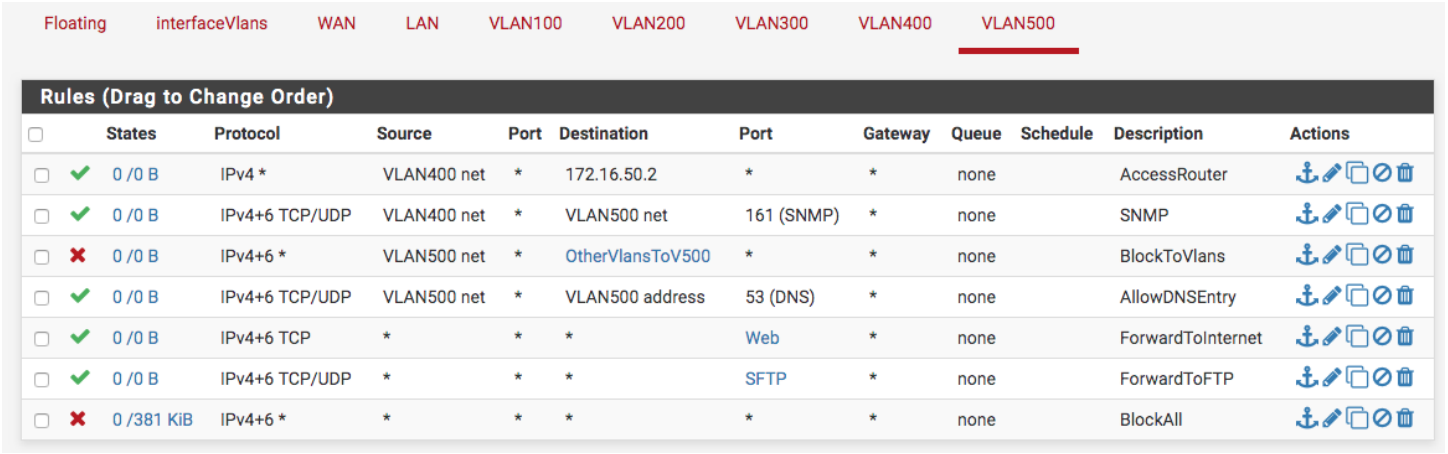


Las reglas que se asignó en la interfaz de la VLAN 100 son las siguientes:

Regla 1: Solo los protocolo Ipv4 e Ipv6 tiene acceso total, desde cualquier origen a cualquier destino y sea por cualquier puerto, el motivo de esta regla es porque este firewall bloquea todo por default, entonces se añade una regla donde permita el paso y de tal forma monitorear todo el tráfico.

Interfaz VLAN 500

Figura 39 Reglas Interfaz Vlan500. Elaborado por el autor (2019)



Las reglas que se asignó en la interfaz de la VLAN 100 son las siguientes:

Regla 1: Permite que todo protocolo IPv4, que tenga su origen desde la VLAN 400 y su destino se la IP 172.16.50.2, por cualquier puerto sea permitido, esta regla es para el acceso del router.

Regla 2: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, que su origen sea la VLAN 400 y su destino sea la VLAN 500 y que aceda por el puerto 161 (SNMP), será permitido.

Regla 3: No permite ping entre las demás VLANs.

Regla 4: Permite que solo los protocolos TCP/UDP envíen paquetes DNS que tenga origen desde VLAN 500 net y tenga como destino VLAN 500 address, quiere decir que traduce los nombres de la red y permite conocer la Ip de la maquina donde se está alojando el dominio al que queremos acceder.

Regla 5: Permite que solo los protocolos Ipv4 e Ipv6 que estén bajo la capa de transporte TCP/UDP, sea desde cualquier origen a cualquier destino de la red LAN, permitirá todo lo que es trafico web.

Regla 6: Permite transferencia SFTP y FTP, los puertos incluidos son (20, 21, 22).

Regla 7: Lo demás que no esté considerado en estas las reglas establecidas anteriormente estará bloqueado.

BLOQUEO DE PÁGINAS DE ENTRETENIMIENTO, REDES SOCIALES, JUEGOS Y PÁGINAS PARA ADULTOS

Luego de aplicar las reglas de firewall a cada interfaz de VLAN se procedió a la descargar de paquetes complementarios del Firewall Pfsense para poder bloquear páginas de entretenimiento, juegos, pornografía, videos y musica, los paquetes descargados son los siguientes:

- Snort
- Squid
- Squid Guard
- pfBlockerNG

Se aplicó estos 3 filtros de seguridad para esta infraestructura de red de datos, mismas que me permitieron bloquear de forma general y detallada páginas que no son útiles al momento de desarrollar un software (páginas de ocio). La configuración de cada filtro de seguridad se describirá a continuación:

Primer Filtro: SNORT

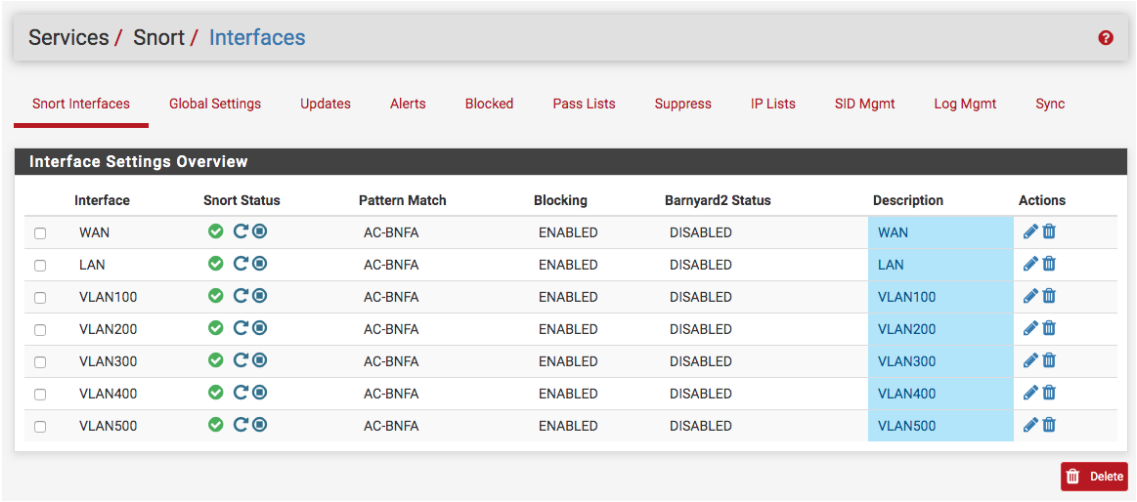


Figura 40 Servicio Snort. Elaborado por el autor (2019)

Este filtro nos sirve para la detección de intrusos, mismo que cuenta con la capacidad de crear reglas que permitirá definir patrones que se van a utilizar al momento de monitorear el sistema, por la cantidad de reglas y filtros que tiene predefinido hace que su instalación y configuración sea lo más ajustable a lo necesitado, es por eso que por medio de consola se puede ver en tiempo real lo que sucede en la red y en todo el tráfico, gracias a las reglas y filtrado que se procedió a configurar a todas las interfaces del Pfsense, se obtuvo el bloqueo de páginas de: entretenimiento, videos, juegos, pornografías y ocio, llegando a tener un control total de las interfaces del firewall.

Segundo Filtro: Squid & SquidGuard

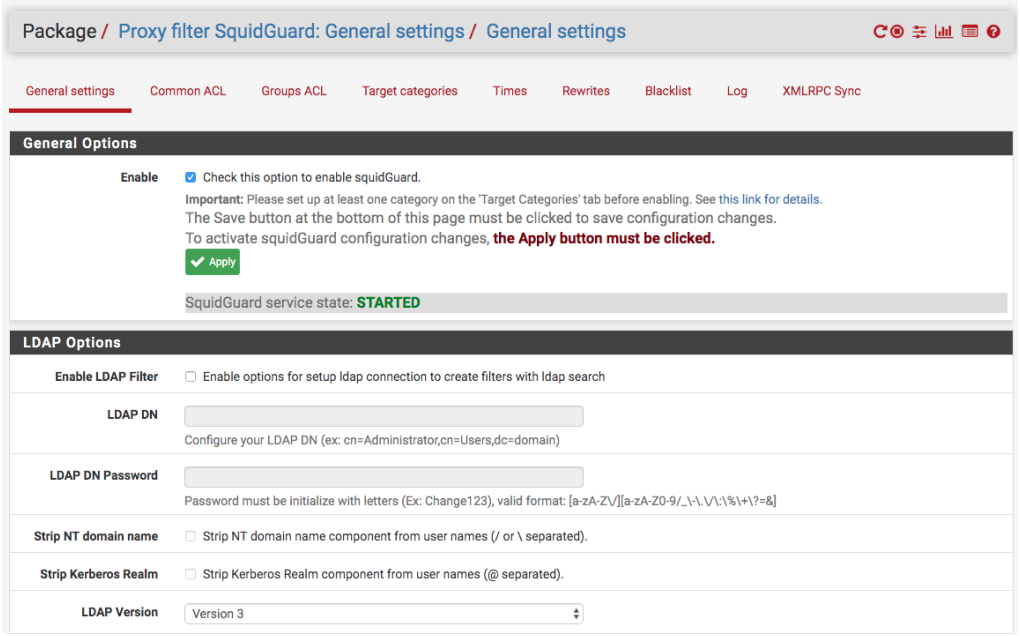


Figura 41 Servicio Squid & Squid Guard. Elaborado por el autor (2019)

Por medio de este filtro se ha creado un Blacklists (lista negra) de sitios web para permitir o denegar accesos a los usuarios que estén en el laboratorio IoT y Centro de desarrollo de software, es por eso SquidGuard es el encargado de redireccionar y filtrar Sitios Web utilizando la interfaz estándar del Squid, este filtro esta aplicado a todas las interfaces Vlans pero con distintas reglas, ya que el objetivo de cada interfaz es diferente.

Tercer Filtro: pfBlockerNG

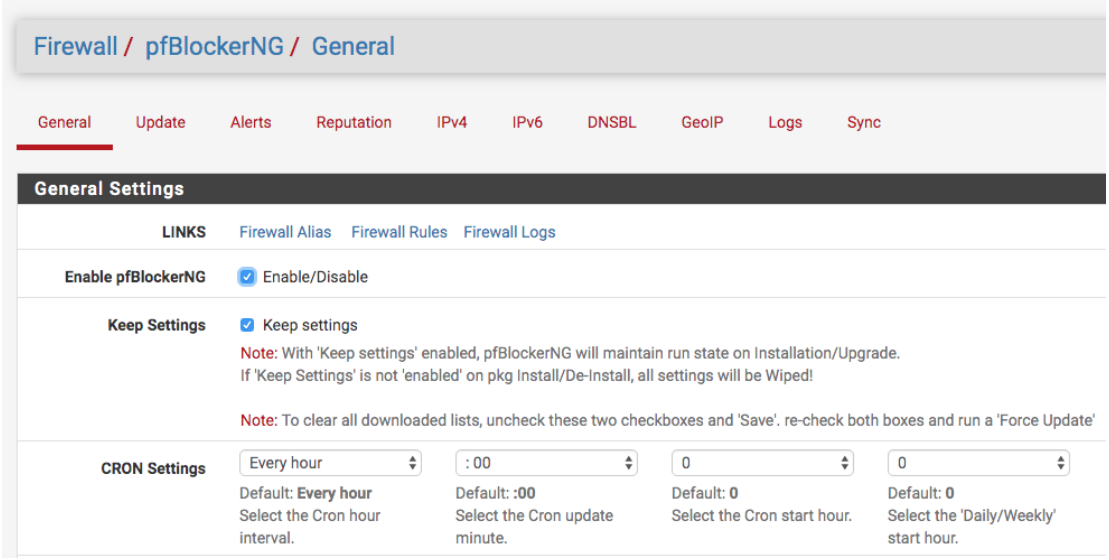


Figura 42 Servicio PfblockerNG. Elaborado por el autor (2019)

PfblockerNG permitió gestionar listas de direcciones IP misma que permitirá crear reglas en el firewall para poder permitir o denegar tráfico de red en las interfaces de Pfsense, la fortaleza de este filtrado reside en el uso de listas, las mismas que van a permitir bloquear rangos de IP tales como: malware, Spammers, spyware, botnets, y/o bloques de direcciones IP de países potencialmente peligrosos.

A continuación, los enlaces de listas negra que se descargó para el bloqueo de rango de Pfsense:

- Emerging Threats.
- The CINS Score.
- Malware Domain List.
- Malc0de.
- Spamhaus.
- Open BL.

Software de Monitoreo

	Cacti	Pandora	PRGT
Sistema Operativo	Linux, Windows, Solaris	Linux, Windows, Solaris, MacOs	Linux
Software	Free	Free	Pagado
Representación de monitoreo	Gráficos, estados y alertas	FMS, estados, gráficos	Estados, FMS, gráficos, alertas, mapas
Comunicación	Equipos de comunicación, CPU	Equipos de comunicación, CPU	Equipos de comunicación, CPU, dispositivos, laptops
Protocolo	SNMP	SNMP	SNMP
Administración	Portal Web	Aplicación	Aplicación
Industrias	Pequeñas	Medias y Grandes	Pequeñas, Medias y Grandes

Tabla 13 Comparación de Software de monitoreo. Elaborado por el autor (2019)

Con respecto a la comparación del software de monitoreo se eligió CACTI, porque puede ser instalada en Windows o Linux, se instaló en el sistema operativo Linux para una mayor seguridad, es un software libre, representa de manera gráfica el consumo de red y de memoria, trabaja bajo

el protocolo SNMP, su configuración es mediante una interfaz web, misma que facilita su administración y este software está enfocado para empresas pequeñas.

CACTI es un sistema de monitoreo con el que se puede monitorear todos los dispositivos en tiempo real ejemplo (CPU, servidores, conmutadores, routers, etc). Este software es muy potente ya que permite controlar el estado de la red, también tiene un recolector de datos y un sistema de creación de gráficos y plantillas, CACTI está diseñado en php y utiliza MySql para almacenar la información de los datos recogidos, para la comunicación de los diferentes equipos este sistema utiliza el protocolo SNMP, el mismo que permite el intercambio de información entre los dispositivos y deja el acceso para que los administradores puedan controlar el uso de la red.

Esquema de monitoreo CACTI

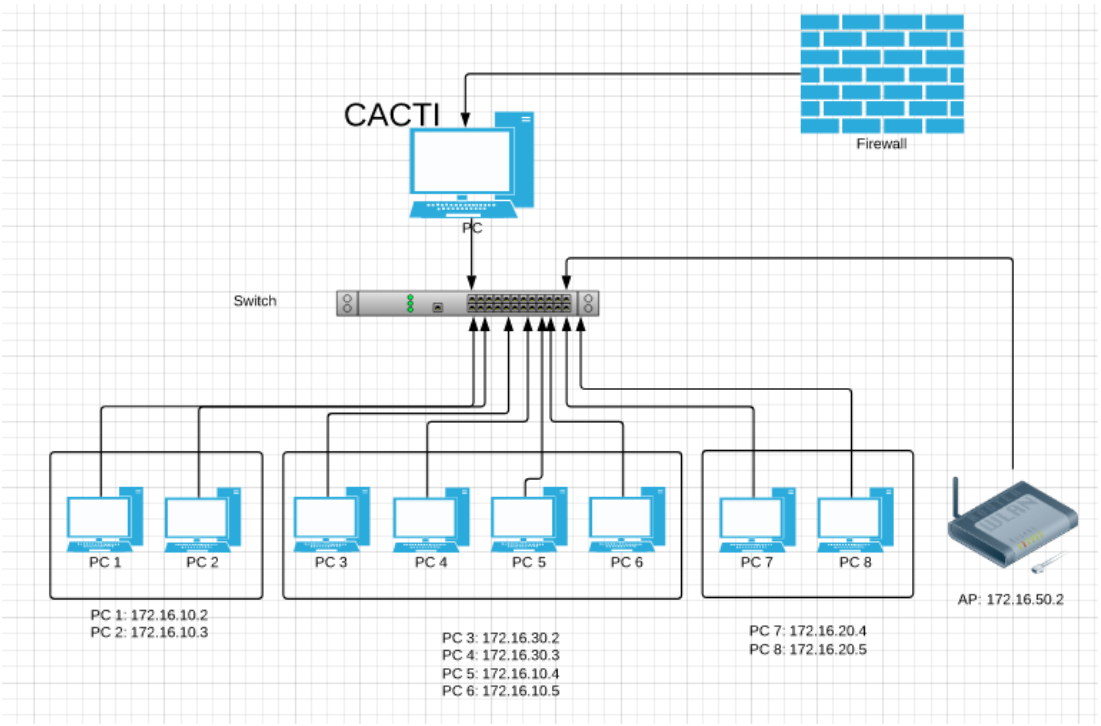


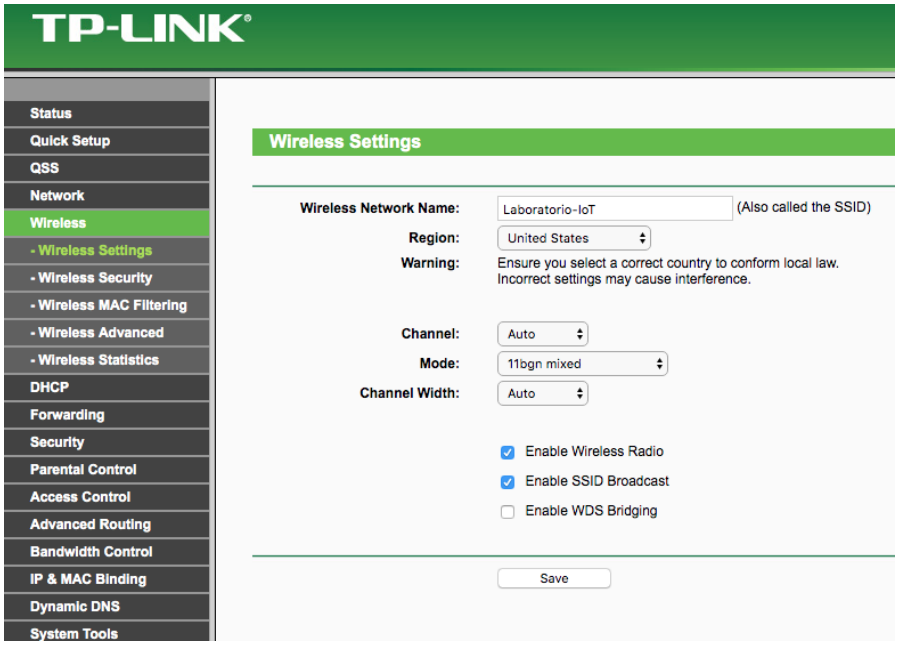
Figura 43 Monitoreo Cacti. Elaborado por el autor (2019)

A continuación, se explica la funcionalidad de CACTI, esta herramienta se encargará de ofrecer un análisis completo de la red, el software de monitoreo estará conectado al firewall, de tal forma que para la identificación de los dispositivos y equipos de comunicación que estén bajo la red LAN del firewall se debe activar el protocolo SNMP, mismo que permitirá enviar y recibir datos.

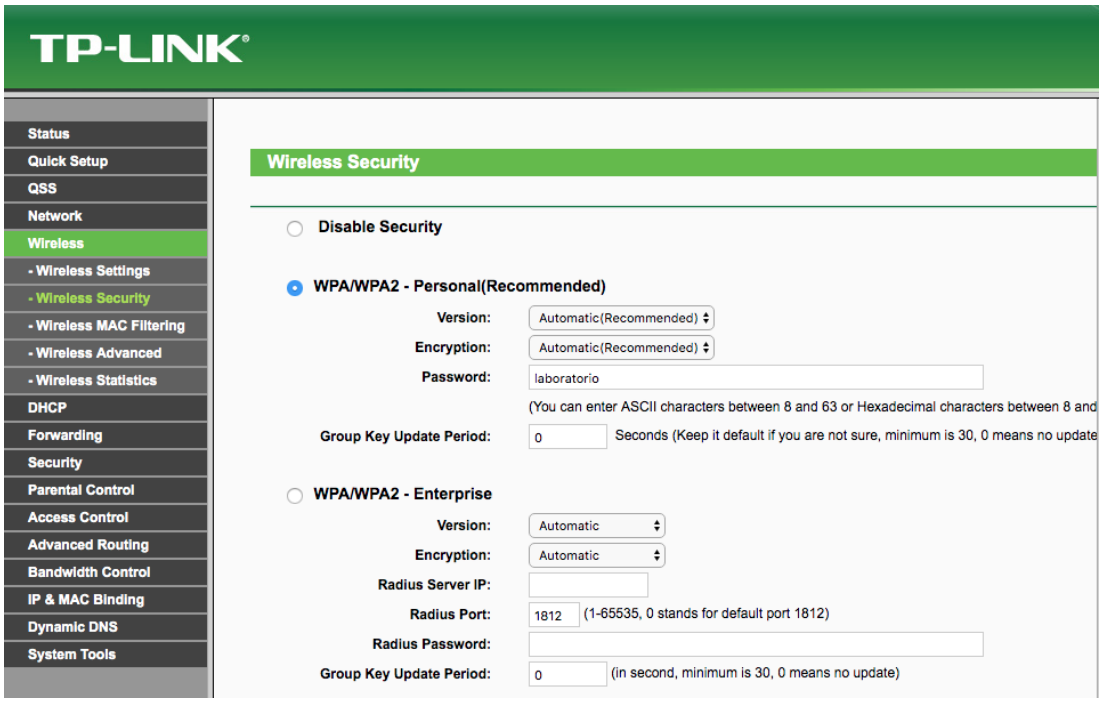
CACTI se encargará de efectuar informes de consumo de red y de memoria sobre todos los dispositivos y equipos, de manera que con los datos almacenados este software de monitoreo graficará el consumo y estado de los equipos.

Configuración del Access Point

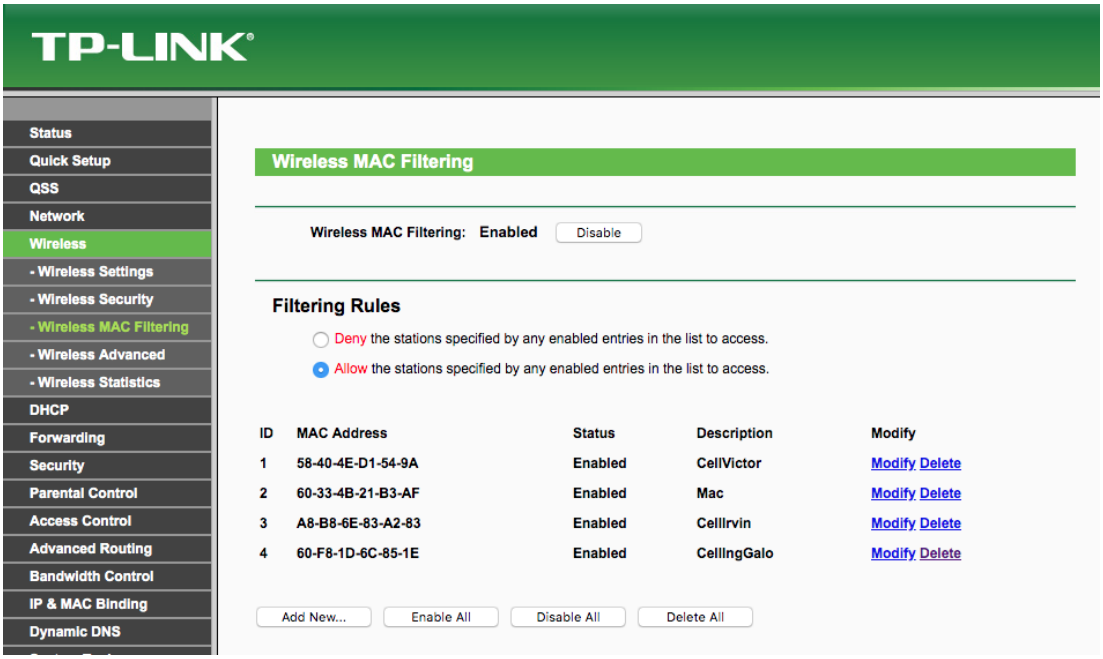
Para la configuración del Access Point Tp-link 150 Mbps, Ingresar a wireless settings, asignar el nombre la red de wifi “Laboratorio-IoT”



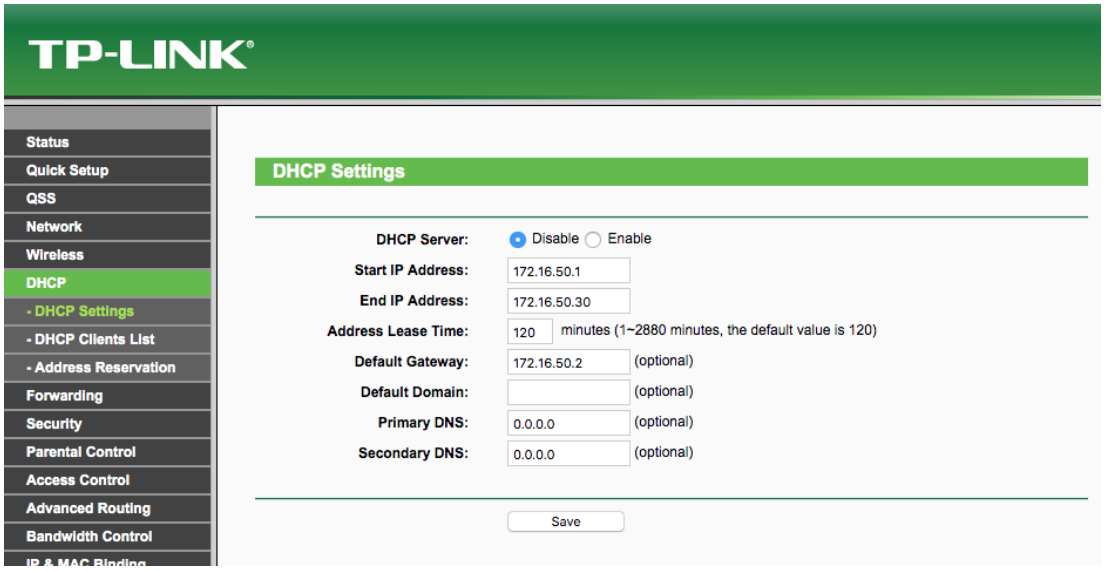
En la opción de Wireless security, Seleccionar la opción de red personal y agregar contraseña para el ingreso a la red.



En wireless MAC Filtering, está activado el filtrado de MAC, mismo que permitirá acceder equipos registrados.

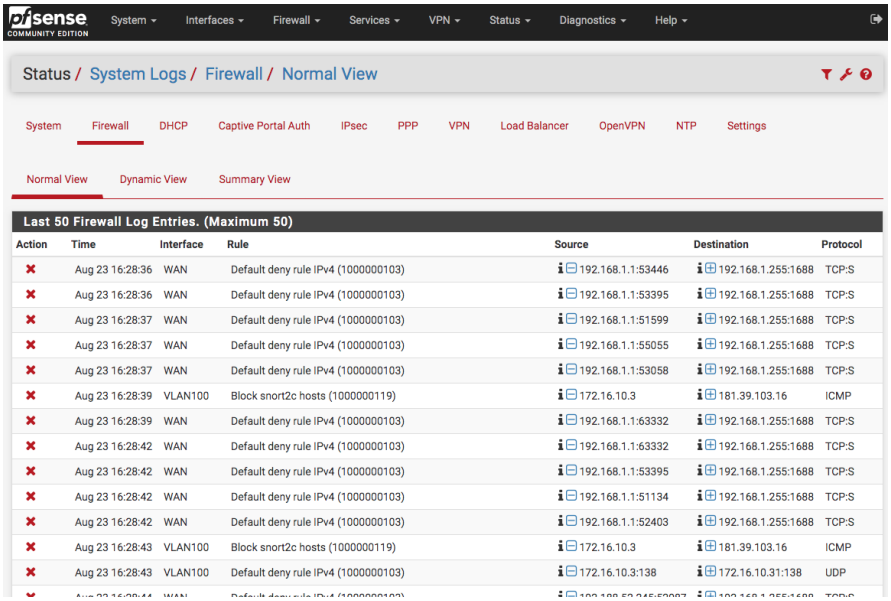


En la configuración del DHCP se ingresó el rango de direcciones, de tal forma los dispositivos que se conecte, el Access Point automáticamente tendrán una IP del rango de la interfaz del AP



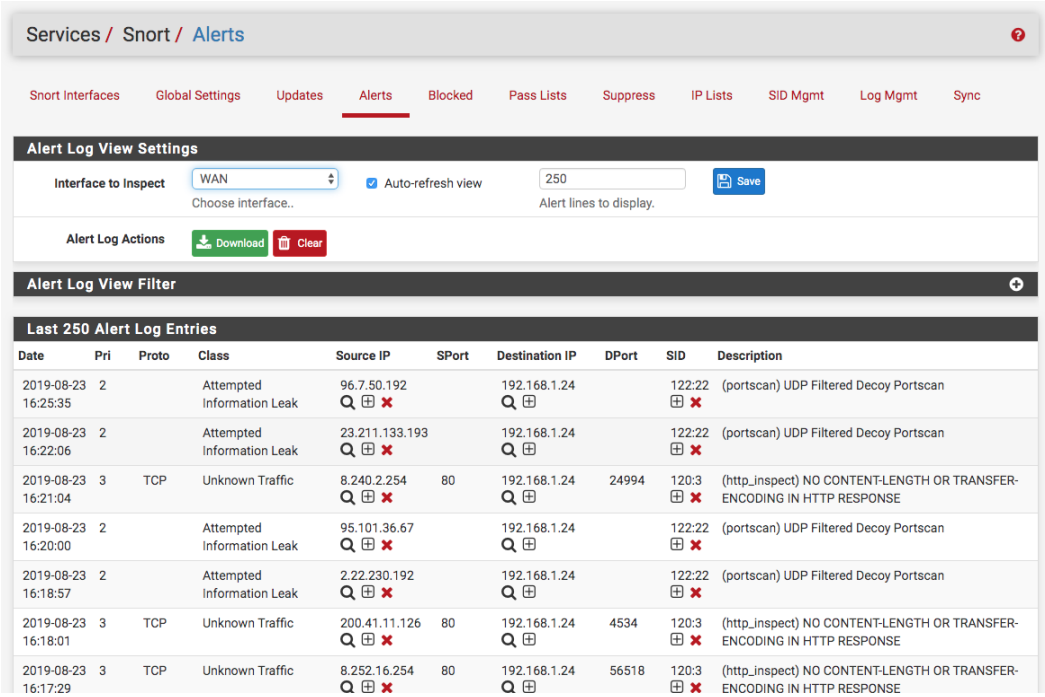
Pruebas de Servicios

1. Firewall
   a. El firewall bloquea todo lo que no esté considerado en las reglas añadidas en las interfaces y permite solo el paso de lo considerado. Logs Firewall

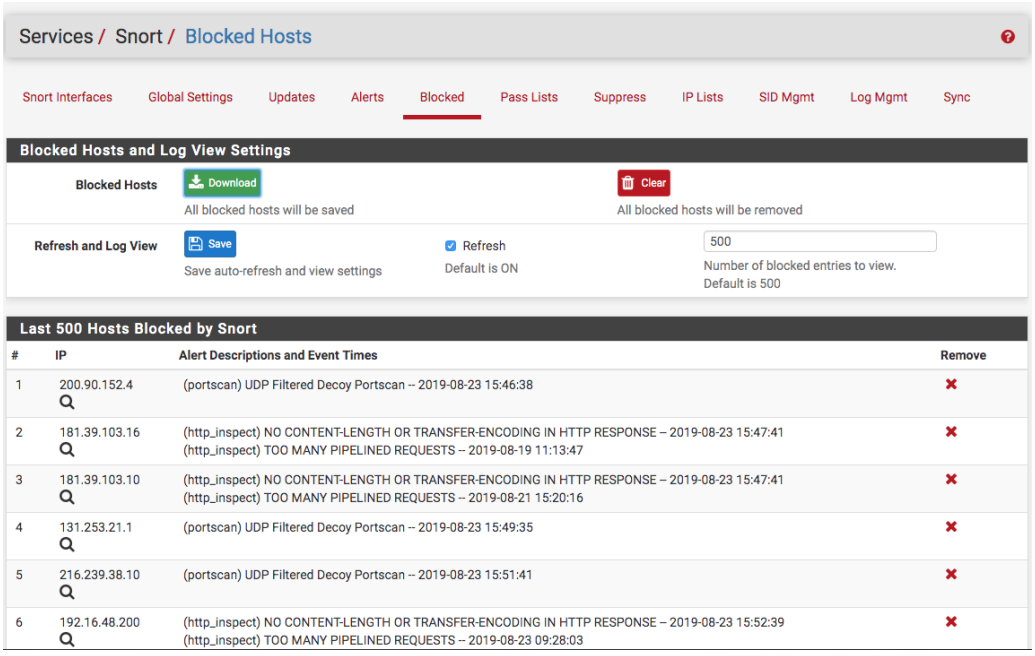


   b. Por medio de Snort que es un IDS (sistema de detención de intruso), se puede observar lo logs de las alertas y bloqueos que realiza a cada una de las interfaces del firewall, esta opción permite descargar informes tanto de las alertas como de los bloqueos.

ALERTAS

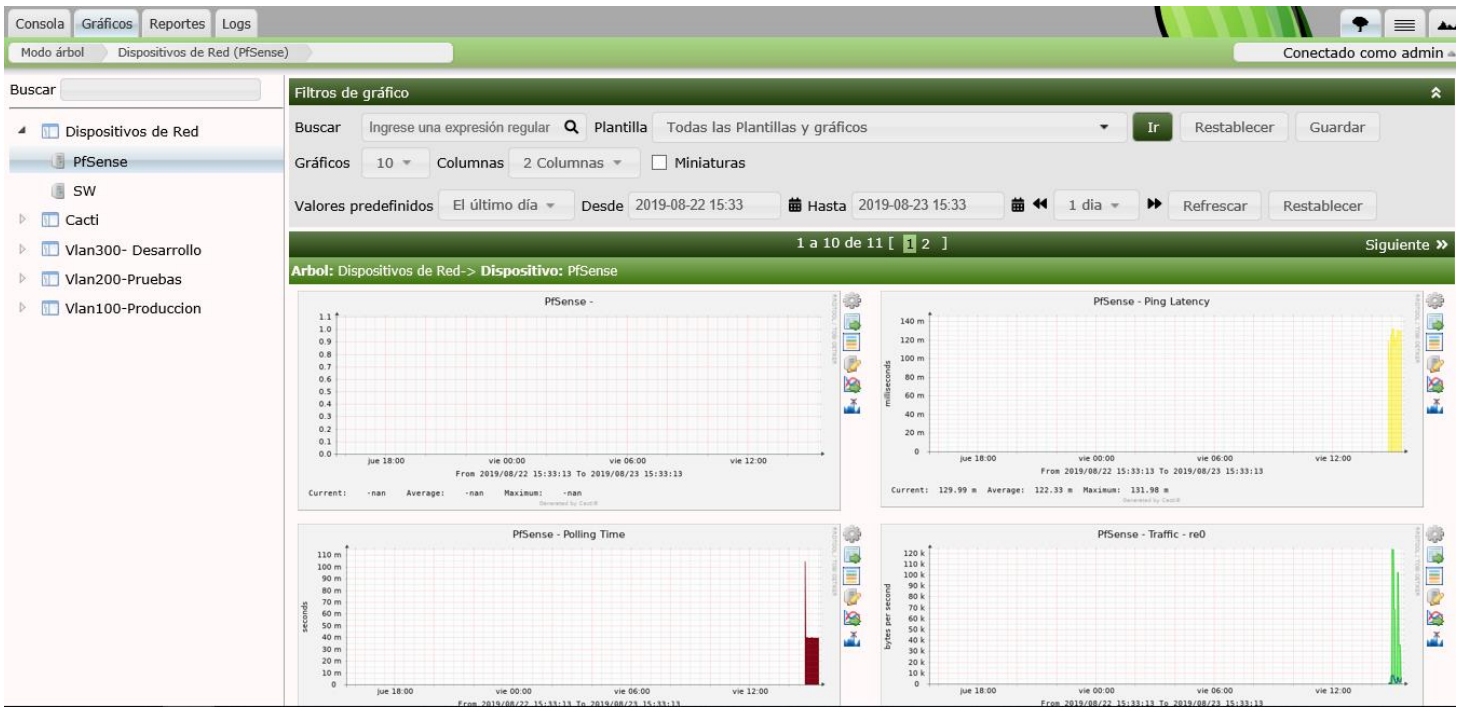


BLOQUEO



2. Monitoreo

   Pruebas de Paso de tráfico de red, gráficos del consumo de ancho de banda de todos los dispositivos conectados.



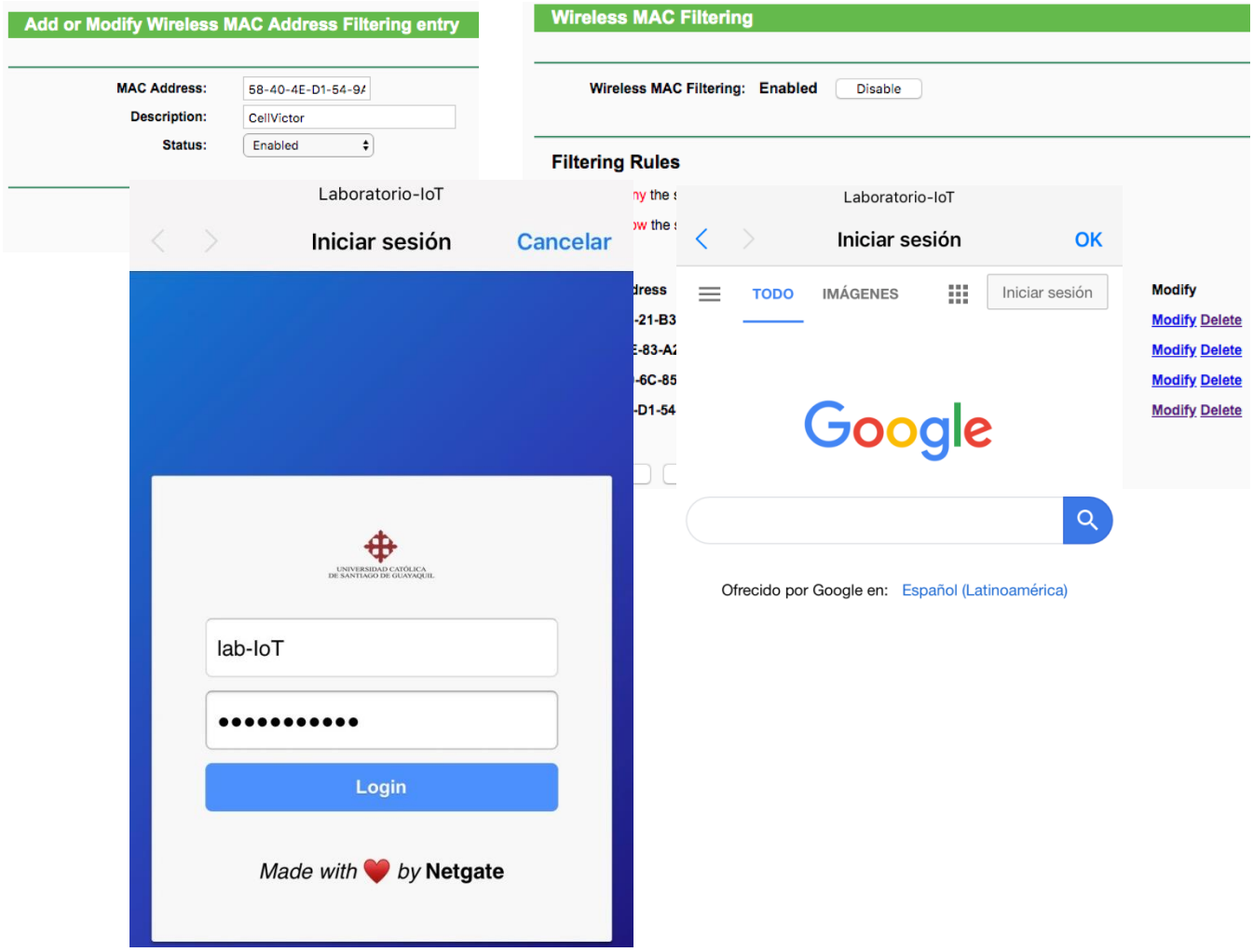
Interfaces Virtuales Activas.

Access Point

Pruebas de filtrado de MAC, misma que permitió pasar al portal cautivo y luego de logonearse poder navegar

a. Prueba sin tener registrada la MAC del dispositivo o equipo, no dejará conectarse a la red.

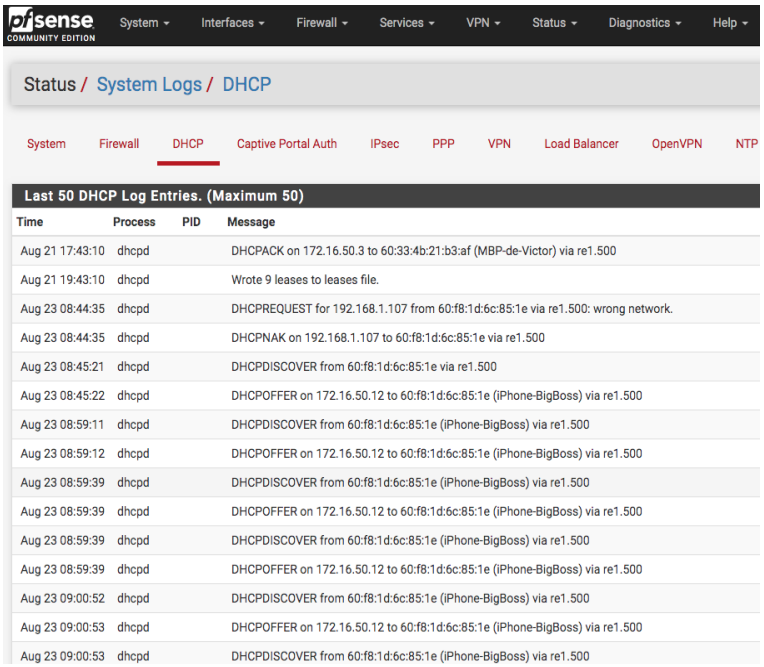
b. Registrar la MAC del dispositivo y con una pequeña descripción.



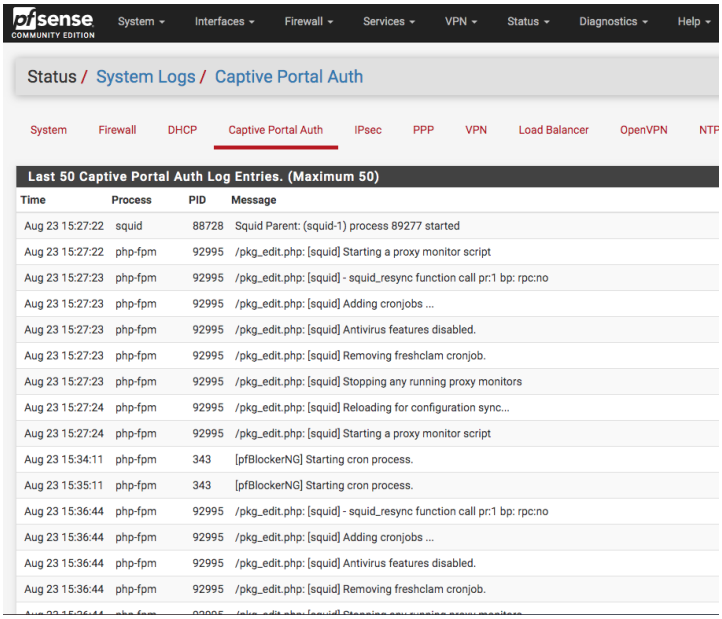
c. Registrada la MAC del dispositivo, acceder a la red de wifi e ingresar la contraseña, se dirigirá al portal cautivo, donde solo los usuarios registrados en el firewall podrán acceder y navegar.

d. El firewall por defecto detecta la conexiones de los dispositivos y los muestra en los logs del portal cautivo y DHCP

DHCP-Usuarios conectados en el interfaz de Access Point



Portal-Cautivo

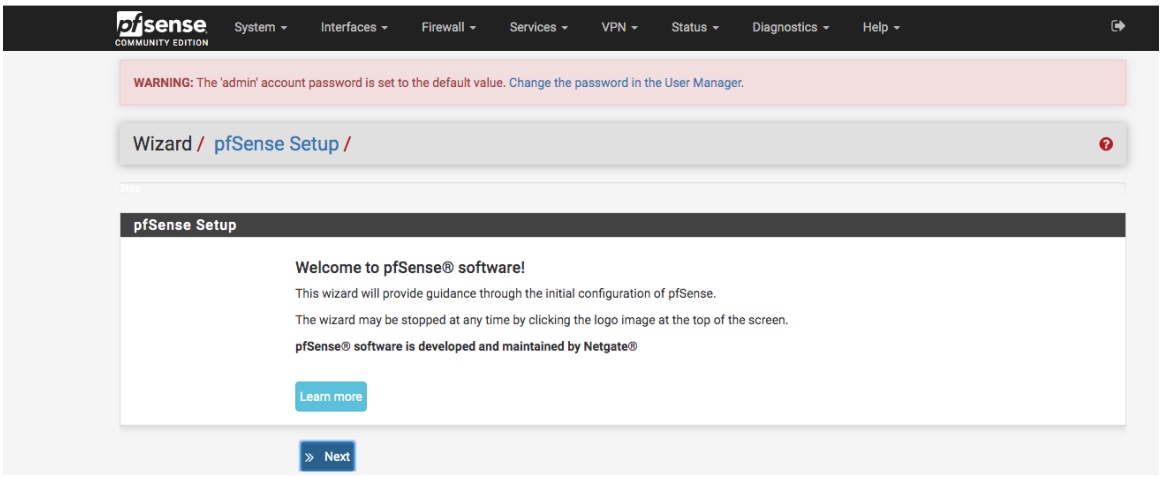


ANEXOS

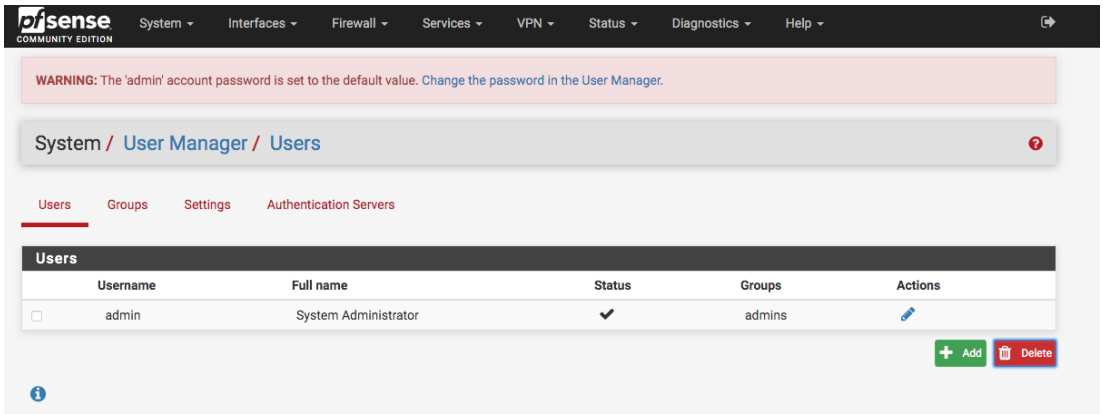
Como buenas practicas:

Lo primero en configurar una vez dentro del Pfsense, es cambiar la clave del administrador ya que por default nos da una y si no se la cambia cualquier persona podría entrar a nuestro Pfsense, entonces se configura el usuario administrador, se cambia la clave y se otorga total acceso al Pfsense. Cambio de clave del administrador, dar clic en system, luego en user manager

Se abrirá otra pantalla donde se debe dar clic en modificar, es el icono de un



lápiz.



Se procede a cambiar la clave y dar clic en guardar, al momento de recargar nuevamente la página tendremos que logonearnos con la nueva contraseña y de ahí si continuar con las siguientes configuraciones en nuestro Pfsense.

CONCLUSIONES

Por medio de los instrumentos aplicados en el proceso de recolección de datos se pudo evidenciar la ausencia de un correcto cableado, la deficiencia en equipos informáticos, la falta de internet y falta de esquemas de seguridad, cuyo análisis permitió definir la implementación de un cableado estructurado bajo los principales estándares, la implementación de esquemas de seguridad para restringir accesos y la instalación de software para el monitoreo y seguimiento de control.

La propuesta de la solución contiene un esquema de infraestructura de red de datos utilizando los recursos disponibles en la sala de cómputo, cuyo diseño contiene una red LAN donde se implementa varias interfaces virtuales que permiten distribuir las computadoras en ambientes distintos facilitando la administración, y también se diseñó una red WAN destinada para la salida a internet y al hosting, dejando así un diseño funcional que está bajo las normativas y estándares de la industria.

Se instaló un firewall que permite la creación de reglas para el control de acceso y el software CACTI para el monitoreo del consumo de recursos, que fue el producto mejor evaluado en el proceso comparativo del presente trabajo de titulación.

Las pruebas se realizaron de manera controlada a las interfaces WAN, LAN y VLANs (virtuales), aplicando las reglas de seguridad configuradas en el firewall definidas en el presente trabajo de titulación, de esta manera se aseguró una buena comunicación y funcionalidad de la infraestructura de red datos del Centro de desarrollo y Fábrica de IoT.

RECOMENDACIONES

Se sugiere adquirir el servicio de hosting basado en la nube mismo que permitirá tener un mayor control administrativo.

Se sugiere la implementación de una VPN para permitir acceso remoto seguro vía internet a los distintos servicios implementados en la red.

Para asegurar la alta disponibilidad y continuidad del servicio se sugiere la instalación de UPS que brinde redundancia eléctrica para el servidor de producción especialmente.

Mantenimiento de hardware para prolongar la vida útil de los equipos.

Se recomienda realizar respaldos de las configuraciones del firewall cada vez que se agregue una nueva política

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, C. (2017). *Implementacion iso 27001*. 115.

Barcell, M. F. (2014). *DEPARTAMENTO DE INGENIERÍA INFORMÁTICA*. 25.

Cabello, C. (2015, septiembre 11). Qué es el QoS y por qué es importante para tu red local. Recuperado 30 de mayo de 2019, de Nobbot website: https://www.nobbot.com/tecnologia/mi-conexion/que-es-el-qos-y-por-que-es-importante-para-tu-red-local/

Castro, V. M. R. (2015). Cableado estructurado norma ANSI/TIA/EIA-606-A. Recuperado 25 de junio de 2019, de http://www.ingeplus.net/2-uncategorised/188-cableado-estructurado-norma-ansi-tia-eia-606-a

Cisco. (2005). *Información general de TCP/IP*. 8. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13769-5.pdf

Cisco. (2015a). *Lo que usted necesita saber sobre routers y switches*. *1*, 5. Recuperado de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

Cisco. (2015b). Routers. Recuperado 30 de mayo de 2019, de Cisco website: https://www.cisco.com/c/es_es/products/routers/index.html

Cisco SG250-10P - Switch Cisco Systems en LDLC.com. (s. f.). Recuperado 28 de mayo de 2019, de https://www.ldlc.com/es-es/ficha/PB00212583.html

Clark, G. P., Prairie, E., Kessler, B. S., & Heights, G. (2003). *(54) TELECOMMUNICATIONS PATCH PANEL*. 35.

Decarbo, M. (2014). Texto-denwa-comunicaciones-convergentes—Módulo—4-redes.pdf—MODULO 4 Redes Informticas Objetivos Especficos Analizar los tipos de redes informticas. *Course Hero*, 75. Recuperado de https://www.coursehero.com/file/33805935/texto-denwa-comunicaciones-convergentes-m%C3%B3dulo-4-redespdf/

Dr. Joskowicz, J. (2013). *Cableado Estructurado* (Universidad de la Republica). Recuperado de https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructura

do.pdf

Fuentes Telleria, R., & Lujan Apaza, J. J. (2017). DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO DE TELECOMUNICACIONES «CONSTRUCCIÓN BLOQUE NUEVO HOSPITAL MATERNO INFANTIL D.10 DE LA CIUDAD DE COCHABAMBA» PARA LA EMPRESA I.S.T. BOLIVIA. *Journal Boliviano de Ciencias*, 22. Recuperado de http://www.revistasbolivianas.org.bo/scielo.php?script=sci_abstract&pid=&lng=es&nrm=iso&tlng=

IBM. (2014a, octubre 24). EtherChannel y Agregación de enlaces IEEE 802.3ad. Recuperado 10 de junio de 2019, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/etherchannel_intro.htm

IBM. (2014b, octubre 24). Función NAT de enmascaramiento (ocultación). Recuperado 10 de agosto de 2019, de www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_72/rzajb/rzajbrzajb4bhidenat.htm

Iglesias, P. A. L. S. (2019). El switch: Cómo funciona y diferencias con otros dispositivos. Recuperado 28 de mayo de 2019, de Aboutespanol website: https://www.aboutespanol.com/que-es-un-switch-841388

Introducción a las VLAN. (2010). Recuperado 30 de mayo de 2019, de https://www.mikroways.net/2010/01/18/introduccion-a-las-vlan/

Lanza, J., & Sánchez, L. (2015). *Seguridad en Redes de Comunicación. Tema I. Introducción a la Seguridad en Redes de Comunicación*. 73. Recuperado de https://ocw.unican.es/pluginfile.php/307/course/section/250/tema_01.pdf

Lucas, L. M. G. (2015). *PROTOCOLOS DE ENRUTAMIENTO*. 5.

Mesa, V. S. A. (2016). *IMPLEMENTACIÓN DE UNA RED WLAN QUE PERMITA EL ACCESO A LA INTERNET, A LAS PCS DE TODAS LAS AULAS DE LA ESCUELA FISCAL MIXTA "JOSÉ MARÍA VARGAS" UBICADA EN EL BARRIO DE SANTO DOMINGO DE CONOCOTO*. 103. Recuperado de https://bibdigital.epn.edu.ec/bitstream/15000/14300/1/CD-6764.pdf

Montañana, R. (s. f.). TEMA 5: EL NIVEL DE RED. Recuperado 7 de junio de 2019, de http://www.aulawiki.info/redes/T9_nivel-transporte.htm

Nazareno, G. (2012). *Introducción al servicio DHCP*. 7. Recuperado de http://informatica.gonzalonazareno.org/plataforma/pluginfile.php/4367/mod_resource/content/1/pres_dhcp.pdf

Pérez, P. (2005). *ARQUITECTURA DE REDES*. 20. Recuperado de http://www1.frm.utn.edu.ar/medidase2/varios/parametros_redes1.pdf

Petersen, E. H. (2007). *Capitulo 3 Introduccion a los Protocolos de Enrutamiento Cisco*. Recuperado de https://www.academia.edu/11856621/Capitulo_3_Introduccion_a_los_Protocolos_de_Enrutamiento_Cisco

Polo, J. (2007). *Enrutamiento Estático*. 43. Recuperado de http://giret.ufps.edu.co/cisco/descargas/Presentaciones/Modulo2_capitulo2.pdf

Puentes, R. (2015). *IEEE*. 18. Recuperado de https://www.academia.edu/8396032/IEEE

Rodrigo. (2012, agosto 9). Configuración de Access-List extendida. Recuperado 30 de mayo de 2019, de Todo sobre Packet Tracer website: https://todopacketracer.com/2012/08/09/configuracion-de-access-list-estandar/

Rodríguez-Gómez, G., Gil-Flores, J., & Garcia-Jimenez, E. (1996). *Metodología de la investigación cualitativa / Gregorio Rodríguez Goméz, Javier Gil Flores, Eduardo García Jiménez.*

Romero, M. (2003). *Ingeniería de Protocolos Curso 2002/2003*. 28. Recuperado de https://www.aprendaredes.com/downloads/manual-routers.pdf

Salazar, G. (2016, septiembre 30). Fundamentos de QoS - Calidad de Servicio en Capa 2 y Capa 3. Recuperado 28 de mayo de 2019, de https://community.cisco.com/t5/blogs-routing-y-switching/fundamentos-de-qos-calidad-de-servicio-en-capa-2-y-capa-3/ba-p/3103715

SNMP.pdf. (s. f.). Recuperado de https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/SNMP.pdf

Tadimety, P. R. (2015). *OSPF: A Network Routing Protocol*. 150. Recuperado de https://link.springer.com/search?query=OSPF%3A+A+Network+Routing+Protocol&facet-discipline=%22Computer+Science%22

Telectrónica. (2018, junio 22). ▷ Cable Categoría 8: Que es y cuáles son sus características. Recuperado 11 de julio de 2019, de Telectrónika website: https://telectronika.com/articulos/ti/categoria-8/

Tolosa, G. (2014). *Protocolos y Modelo OSI*. 32. Recuperado de http://www.tyr.unlu.edu.ar/pub/02-ProtocolosOSI.pdf

Tropa. (2013, octubre 23). CABLEADO ESTRUCTURADO: Estandares Del Cable

Estructurado. Recuperado 24 de junio de 2019, de CABLEADO ESTRUCTURADO website: https://espsistem.blogspot.com/2013/10/estandares-del-cable-estructurado.html

Universidad Rey Juan Carlos. (2013). Simple Network Management Protocol. *Departamento de Sistemas Telematicos y Computacion (GSyC)*, 16. Recuperado de https://gsyc.urjc.es/~mortuno/lagrs/07-snmp.pdf

Vargas Cordero, Z. R. (2009). La Investigación aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación*, *33*(1), 155. https://doi.org/10.15517/revedu.v33i1.538

Velasco, M. I. D. (2001). Sistemas de cableado estructurado: Normalización y parámetros. *Mundo electrónico*, (316), 36-42. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=132187

Vera, L., & Martinez, O. (2017). *Switches Principales Características y Aplicaciones*. 26.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Guerra Guamán, Victor Hugo**, con C.C: # **0923567994** autor/a del: **Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil,** previo a la obtención del título de **Ingeniería en sistemas computacionales** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 12 de septiembre de 2019

f. _____
Nombre: **Guerra Guamán, Victor Hugo**
C.C: **0923567994**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil.		
AUTOR(ES)	Guerra Guamán, Victor Hugo		
REVISOR(ES)/TUTOR(ES)	Ing. Toala Quimí, Edison, Mgs		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Ingeniería		
CARRERA:	Ingeniería en sistemas computacionales		
TITULO OBTENIDO:	Ingeniería en sistemas computacionales		
FECHA DE PUBLICACIÓN:	12 de septiembre de 2019	**No. DE PÁGINAS:**	112
ÁREAS TEMÁTICAS:	Tecnología, sistemas de información		
PALABRAS CLAVES/ KEYWORDS:	Infraestructura de datos, estándares cableado estructurado, interfaces virtuales, software de monitoreo.		

RESUMEN/ABSTRACT (150-250 palabras): Se diseñó una infraestructura de red de datos funcional para el Centro de desarrollo de Software y Fábrica Iot con los recursos disponibles de la Facultad de Ingeniería, para el proceso se utilizaron varios equipos de comunicación tanto físicos como lógicos, el laboratorio está bajo estándares de cableado estructurado y de seguridad, mismos que se describieron para dar soporte a la solución. El proyecto se enfocó en la metodología cualitativa y no contiene tablas numéricas ni tabulaciones, sus métodos de recolección de datos permiten identificar todos los requerimientos dados por el usuario y de esta manera cumplir las necesidades. Para la implementación del laboratorio se utiliza un cableado de Cat 6 para tener una mejor frecuencia y será instalado en topología estrella bajo las estandarizaciones del cableado estructurado y por medidas de seguridad tiene instalado un firewall que va a contener 2 interfaces; una red WAN que permite la salida a internet y una red LAN donde se ha configurado el firewall con 5 interfaces virtuales donde cada una tiene diferentes configuraciones, una de esas interfaces estará configurada para dar señal de wifi. Además, en el laboratorio también se dispone de un software para monitoreo, con el cual se visualiza gráficamente el consumo de ancho de banda y los procesos de memoria de las computadoras. Finalmente se identificó, analizó, diseñó e implementó todos los requerimientos con los recursos disponibles de la sala de cómputo, dejando así una infraestructura de red de datos segura y funcional para el Centro de desarrollo y Fábrica de IoT.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593993009595	E-mail: guerravit_09@hotmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Ing. Edison José Toala Quimí, Mgs	
	Teléfono: +59342202763	
	E-mail: edison.toala@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	