UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL+

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y PROTECCIÓN DE DATOS EN LA RED DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL.

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

LÍNEA DE INVESTIGACIÓN:

Hardware y Redes

AUTOR:
David Fernando Sánchez Cunalata

TUTOR:

Ing. David Omar Guevara Aulestia Mg.

Ambato - Ecuador

Junio, 2017

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"Implementación de un Sistema de Monitoreo y Protección de Datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.", del señor David Fernando Sánchez Cunalata, estudiante de la carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato

Ambato, Junio del 2017

EL TUTOR

Ing. David Omar Guevara Aulestia Mg.

AUTORÍA

El presente trabajo de investigación titulado: "Implementación de un Sistema de Monitoreo y Protección de Datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Junio del 2017

David Fernando Sánchez Cunalata

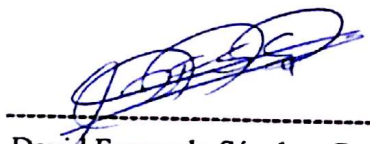
CC: 1804570511

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato junio, 2016



David Fernando Sánchez Cunalata
CC: 1804570511

APROBACIÓN COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes, Ing. Renato Urvina, Ing. Oswaldo Paredes, revisó y aprobó el Informe Final del trabajo de graduación titulado "Implementación de un Sistema de Monitoreo y Protección de Datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial", presentado por el señor David Fernando Sánchez Cunalata de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. Pilar Urrutia

PRESIDENTE DEL TRIBUNAL

Ing. Renato Urvina

DOCENTE CALIFICADOR

Ing. Oswaldo Paredes

DOCENTE CALIFICADOR

DEDICATORIA

A Dios por haberme permitido cumplir con este sueño. A mi Papá y Mamá por ser quienes me guiaron en todo el camino académico, les doy las gracias porque me han dado la vida, porque siempre me protegen, porque me cuidan y son mi ejemplo para seguir adelante, gracias papi y mami.

A mi esposa que por su apoyo incondicional, por su paciencia, por su comprensión, por su dedicación, por su fuerza, por su amor y por ser tal y como es, en realidad son tantas palabras que no me alcanza para describirlas y decirle lo mucho que la amo.

A mis hermanos, el agradecimiento eterno por ser mi apoyo y los amigos incondicionales, por estar en las buenas y malas, por los regaños que me sirvieron para ser un buen hombre y por estar siempre unidos como una gran familia.

David Fernando Sánchez Cunalata

AGRADECIMIENTO

A la Universidad Técnica de Ambato, por ser mí camino a la superación intelectual y profesional. Gracias infinitas a las autoridades de la Facultad de Ingenieria en Sistemas Electrónica e Industrial, gracias al Ing. David Omar Guevara Austelia para que este proyecto de investigación haya podido desarrollarse satisfactoriamente, gracias a los miembros del Tribunal de Grado quienes han confiado en el presente proyecto de investigación

David Fernando Sánchez Cunalata

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El propósito del presente trabajo de investigación es Implementar un Sistemas de Monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, con la finalidad de analizar y dar solución a los problemas planteados en la investigación, para mejorar el ancho de banda y cumplir a cabalidad la productividad operativa de la FISEI en beneficio de la comunidad Universitaria.

En la actualidad por los ataques al ancho de banda, la falla de los dispositivos y el descontrol de usuarios conectados a la red, ya que los APs tiene la capacidad física para gestionar 2048 direcciones MAC. Sin embargo, dado que el AP es un medio compartido, que funciona como un concentrador inalámbrico, el desempeño de cada usuario disminuye a medida que aumenta el número de usuarios en un AP individual. Idealmente, no más de 24 clientes deben asociarse con el AP, ya que el desempeño de procesamiento se reduce con cada cliente que se asocie con el mismo, por lo cual ha dado lugar a que se promueva la implementación de un Sistema de Monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial mejorando el control interno y externo, se recopiló información de los dispositivos de red y equipos de cómputo de los laboratorios y áreas administrativas, además se configuró los sistemas MUNIN, MRTG y CACTI para su monitoreo, los mismo que emiten alertas inmediatas de fallas en los distintos dispositivos de la red, así mismo, una vez realizado lo detallado, se procedió a realizar un cuadro comparativo para el análisis de los sistemas de monitoreo ya para finalizar el presente proyecto de investigación se implementó el sistemas IDS/IPS Suricata mitigando la problemática de ancho de banda como las actividades no autorizadas que provoquen la degradación en la red.

Palabras Claves: Implementación, sistema de monitoreo, protección de datos, red.

Glosario de términos y acrónimos

Switch: Es el dispositivo digital lógico de interconexión de equipos.
Servidor: Es una computadora central en un sistema de red que provee servicios a otras computadoras
SNMP: El Protocolo simple de administración de redes, facilita la administración de equipos en la red.
MIB: Base de Información Gestionada es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones.
WAP: Wireless Access Point
ICMP: Protocolo de Mensajes de Control de Internet
TCP: Protocolo de Control de Transmisión
UDP: User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas.
NMS: Sistema de Gestión de Red

INTRODUCCIÓN

En el mundo actual en que vivimos, con la tecnología avanzando segundo a segundo, con los ataques informáticos cada vez más invasivos; es necesario contar con sistemas de monitoreo y protección, tanto para hardware como para software; más aun cuando empresas públicas como privadas guardan sigilosamente la información que poseen.

Es por eso que se requiere la IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y PROTECCIÓN DE DATOS EN LA RED DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL para salvaguardar la pérdida de creación e innovación en los sistemas de información o perjuicios a nivel de datos.

En el CAPÍTULO 1: EL PROBLEMA.- Tema, Planteamiento del Problema, Delimitación, Justificación, Objetivo General y Objetivos Específicos.

En el CAPITULO 2: MARCO TEÓRICO.- Antecedentes Investigativos y Funadamentación Teórica.

En el CAPITULO 3: METODÓLOGIA.- Modalidad Básica de la Investigación, Recolección de la Información, Procesamiento y Análisis de Datos y Desarrollo del Proyecto.

En el CAPITULO 4: DESARROLLO DE LA PROPUESTA.- Datos Informativos, Análisis de Factibilidad, Ejecución de la Propuesta, Análisis de la Entrevista, Determinación de las Herramientas Utilizidas para el Monitoreo de la Red, Monitoreo la Red de Datos para detectar Fallos y Congestionamiento, Análisis de los Resultados del Monitoreo para identificar Actividad no Autorizada y Anomalías que Provoquen Degradación en la Red, Instauración de mecanismos de Control y protecicón de datos para mejorar el rendimientode la red e Instalación y Configuración de Suicata.

En el CAPITULO 5: CONCLUSIONES Y RECOMENDACIONES.- Conclusiones y Recomendaciones.

Bibliografía

Anexos.

CAPÍTULO 1

El Problema

1.1. Tema

Implementación de un Sistema de Monitoreo y Protección de Datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.2. Planteamiento del problema

A nivel mundial el congestionamiento de las redes y la seguridad informática se debe a la cantidad de usuarios conectados a Internet, ocasionando que se reduzca cada vez más la velocidad de ancho de banda de la red de datos.
Debido a la mayor cantidad de usuarios de Internet y al crecimiento de dispositivos en el mundo, ha llegado a ocasionar un tráfico global casi tres veces mayor que en los anteriores cinco años de acuerdo con la corporación Cisco Visual Networking Index Global Forecast and Service Adoption for 2013 to 2018, en la cual menciona un crecimiento del 25 % de congestionamiento en la red, por ejemplo en Europa más concretamente en España, el tráfico IP se multiplicó por 13 entre 2011 y 2016, existe 258 millones de dispositivos conectados (5,1 conexiones por habitante)[1].
Como se ha mencionado de acuerdo a los autores citados a nivel mundial, las repercusiones del congestionamiento de red, afectan el desempeño en instituciones públicas o privadas, ya sea en su comunicación de datos, amenazando su producción e inclinándose a una caída en el mercado.
Por otro lado en el estado Ecuatoriano, el Instituto Nacional de Estadísticas y Censos (INEC), ha determinado que la utilización de Internet según el área se la realiza desde teléfonos móviles y PCs ya que el uso de redes sociales es la mayor forma de comunicación que existe en la actualidad, teniendo así un 28.3 % de hogares a nivel nacional con acceso a Internet como lo demuestra los resultados de las encuestas de condición de vida realizados por el INEC del 2010 al 2013 cubriendo el área urbana, rural y nacional [2].
Cabe señalar que el congestionamiento en la red en el Estado Ecuatoriano se debe al retardo en la entrega de paquetes que se produce por el excedente de ancho de banda de salida teniendo así perdida o retraso en la transmisión de información, los cuales son ocasionados también por ataques de denegación de

servicio, de acuerdo con un informe Radware 2014 sobre Seguridad Global de Red y Aplicaciones, en el cual 51 % de los ataques DDoS son dirigidos a la red y el 49 % a las aplicaciones, de manera que un estudio realizado por GMS y Kaspersky, mencionan que los informáticos en Ecuador crecieron en un 360 % en el 2010 llegando al 2015 con un exceso de 580 % teniendo como perdida millones de dólares por delitos informáticos alcanzando 1.308 quebrantamientos en el País [2].

El congestionamiento de la red en la Universidad Técnica de Ambato en la Facultad de Sistemas, Electrónica e Industrial, se produce frecuentemente un exceso de ancho de banda con una capacidad de procesamiento bajo y una saturación de aproximadamente 20 % a un 40 % en horas pico, detectado por el programa de análisis llamado wireshare, sin permitir localizar en que zona y equipo de la red se ocasiona el problema.

El tráfico de las redes en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial ha ocasionado que el nivel de servicio de la infraestructura de TI baje, siendo lo más requerido para la institución por los que proveen de servicios tanto de personal administrativo, docente y estudiante.

1.3. Delimitación

- **Área Académica:** Hardware y Redes.
- **Línea de Investigación:** Tecnologías de la Información
- **Sub líneas de investigación:** Seguridad Computacional
- **Delimitación espacial:** Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- **Delimitación temporal:** La presente investigación se desarrolló en los 6 meses posteriores a la aprobación del proyecto por parte del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4. Justificación

La seguridad de los datos es una necesidad presente en toda institución, con el fin de resolver las limitaciones que en algunos casos presentan para el almacenamiento de la información, en estadísticas de seguridad de datos se muestran que hoy en día estas soluciones ya se han vuelto prácticamente indispensables en toda

organización, siendo obligatorio el uso de una buena solución de seguridad en la red y es ineludible el brindar estas soluciones con calidad, eficiencia y eficacia [2].
Con la elaboración del presente proyecto de investigación se pretende detectar y resolver fallos de congestionamiento existentes en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para mejorar el rendimiento y brindar un mejor servicio a los usuarios a través de la implementación de sistemas de monitoreo de tráfico y protección de datos, mejorando la calidad de servicio y precautelando su buen desempeño.
Con la implementación de sistemas de monitoreo y protección de datos, se pretenderá analizar el tráfico de red, en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato para conocer en qué intervalos de tiempo existe mayor carga de congestionamiento en la red; recalcando la importancia que pretende tener el presente proyecto de investigación al identificar actividades no autorizadas por la Institución provocando de forma directa la degradación en la red.
La necesidad que se evidenció como saturación de ancho de banda, los conflictos de IPs, las alertas de intrusos o virus, han provocando un colapso total de la red de datos en la facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, esto determina que se implemente un sistema de monitoreo y protección de la red de datos para visualizar en los software de control implementados en el proyecto de desarrollo cuyo aporte científico es detener intrusiones externas e internas a la facultad y generar alertas reales inmediatas de cualquier tipo de saturación posible indicando precisamente la falla.
Debido a que la facultad no cuenta con una red de datos física estructurada, lo que motivo investigar los lugares específicos en donde las mediciones de los problemas mencionados son reales con el propósito de que el usuario que lleva el monitoreo y control identifique rápidamente el problema y pueda llegar a mitigar a tiempo e impedir cualquier tipo de conflicto con los usuarios sin inconveniente de datos falsos.
Con el presente proyecto de investigación se contribuirá a los estudiantes, personal administrativo y autoridades de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato ya que con la implementación de un sistema de monitoreo y protección de datos se garantizará resolver los problemas ocasionados por los ataques a la red; del mismo modo se menciona que la implementación del presente proyecto de investigación es de posible realización como de aplicación efectiva para la protección de datos.

1.5. Objetivos

1.5.1. General

Implementar un Sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.5.2. Específicos

- Determinar las herramientas utilizadas para el monitoreo de la red.
- Monitorear la red de datos para detectar fallos y congestionamiento.
- Analizar los resultados del monitoreo para identificar actividad no autorizada y anomalías que provoquen degradación en la red.
- Establecer mecanismos de control y protección de datos para mejorar el rendimiento de la red.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Una vez examinadas las fuentes bibliográficas y repositorios disponibles en bibliotecas y sitios web especializados para el desarrollo de la investigación, se ha expuesto las más distintivas en el presente documento respecto a las variables del tema de investigación: La revisión realizada en el repositorio de la Universidad Técnica de Ambato en la Facultad de Ingeniería en Sistemas Electrónica e Industrial ha denotado la existencia de temas de investigación vinculantes al presente proyecto.

El trabajo de grado desarrollado por Franklin Edmundo Escobar Vega, proyecto con el tema "Sistema de análisis y control de red de datos & VoIP para el Gobierno Provincial de Tungurahua", el investigador determina a través de la conclusiones que no dispone de un buen control al momento de monitorear los equipos de TI ya que carece de información centralizada que provoca retardo en las redes de datos[3].

El autor mencionado en el párrafo anterior indica que los problemas más notables están localizados en la configuración de servidores, switch, routers, generando retardo en la red administrativa de la institución[3].

De las referencias citadas indica que la vulnerabilidad de la red radica en la falta de un sistema de control de monitoreo para identificar la problemática en hardware y software en un Data Center.

El investigador Luis Alberto Del Pozo Guevara en el trabajo de grado con el tema "Herramienta integrada de monitoreo de redes para soporte de estudios de disponibilidad" anuncia que con un monitoreo eficiente y minimizando el uso de aplicaciones no permitidas mejora el ancho de banda que ayude a manejar más eficientemente la comunicación. Dicho problema es crítico debido al desarrollo de la Internet, el mercado globalizado y crecimiento tecnológico de la empresas, más el gran volumen de información que fluye a través de estas, las organizaciones deben estar mejor preparadas para asegurar que la información que fluye a través de su red, así como sus aplicaciones, tengan una mayor disponibilidad y rendimiento frente aplicaciones no deseadas que pueden estar circulando por la

red[3].
De acuerdo al trabajo de graduación realizado por Silvana Judith Garcés Ulloa con el tema “Seguridad Informática para la red de datos en la Cooperativa de Ahorro y Crédito Unión Popular LTDA ”indica que los riesgos y vulnerabilidades analizados por los sistemas de monitoreo de red son presentados en informes, estadísticas las cuales son relevantes para conocer las inseguridades tales como equipos mal configurados, interconectados o posibles intrusos que dañen la red [4].
En la investigación de Martín R. Payero, de la Universidad de Palermo, Facultad de Ingeniería, Argentina con el tema “Administración de dispositivos Informáticos wireless orientado a Open Source” estipula que las tecnologías para el monitoreo de la infraestructura informática de cualquier organización, son fundamentales para poder administrar y resolver cualquier contingencia que suceda en la misma, siendo así las acciones resultantes permiten realizar prevención o corrección de contingencias, al contar con una buena implementación se puede tener un control más estricto sobre la red de información en la cual permite poder asegurar la disponibilidad y seguridad en los servicios en funcionamiento[5].

2.2. Fundamentación teórica

2.2.1. Hardware y Software de un Data Center

Servidor

En redes, un servidor es una computadora central en un sistema de red que provee servicios a otras computadoras.
En Internet, los servidores son los proveedores de todos sus servicios, incluyendo la WWW (las páginas web), el FTP, el correo electrónico, los grupos de noticias, aplicaciones web, etc.
Todos estos servicios y otros son provistos por una o más computadoras (servidores) conectadas a Internet, encargadas de recepcionar requerimientos. El servidor analizará el requerimiento, lo procesará y enviará un resultado.
Los típicos servidores son: servidor de base de datos, servidor de archivos, servidor de Email, servidor de impresión, servidor web, servidor de juegos, servidor de aplicaciones, servidor proxy, etc. Ver más abajo el cuadro con los distintos tipos de servidores [6].

Figura 1: Servidor

Punto de Acceso Inalámbrico (WAP o AP)

Puntos de acceso inalámbrico (WAP o AP: Wireless Access Point) son un transmisor y un receptor (transceptor de dispositivo) que se utiliza para señales de radio inalámbricas LAN (WLAN) a WAP es típicamente un dispositivo de red independiente con una antena, un transmisor y el adaptador incorporado. Los WAP utilizan el modo de red de infraestructura inalámbrica para proporcionar un punto de conexión entre las redes WLAN y una red LAN Ethernet cableada. Los WAP también suelen tener varios puertos que permiten una forma de ampliar la red para apoyar a los clientes adicionales [7].
Un WAP pueden funcionar como un puente que conecta una red con cables estándar para dispositivos inalámbricos o como transmisiones de datos a partir de un punto de acceso a otro[7].

Figura 2: Acceso Inalámbrico

Switch

Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un Switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El Switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los Switches permiten ahorrar dinero y aumentar la productividad [8].
Existen dos tipos básicos de Switches: administrados y no administrados.

- Los Switches no administrados funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar Switches no administrados.
- Los Switches administrados permiten su programación. Esto proporciona una gran flexibilidad porque el Switch se puede supervisar y ajustar de forma local o remota para proporcionarle control sobre el desplazamiento del tráfico en la red y quién tiene acceso a la misma.

Figura 3: Switch

Router

Un Router o encaminador es un dispositivo que permite la interconexión de redes al nivel de la capa de Red del Modelo de Referencia OSI.
El router permite físicamente interconectar las redes entre si, consiguiendo que a través de las interfaces entren y salgan los datos.
Así mismo el Router opera como receptor de la red encargándose así de redistribuirlo a todos los equipos que se encuentran conectados, siendo similar a la conexión de Internet con otra de área local[9].

Figura 4: Router

Cortafuegos o Firewall

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios [3].

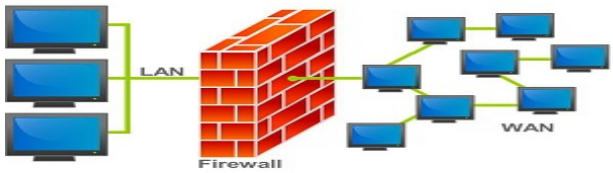


Figura 5: Firewall

La protección del firewall otorgada a un sistema de información automatizado para lograr los objetivos de preservar la integridad, la disponibilidad y la confidencialidad de los Recursos del sistema de información (incluye hardware, software, firmware, información / Datos y telecomunicaciones) [10].
Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada dato y si no cumplen con los requisitos de seguridad específicos estos son bloqueados.

2.2.2. Monitoreo de Redes

El monitoreo de red describe el uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla vía correo electrónico u otras alarmas [11].
Los aplicativos de monitoreo del estado de red permiten, entre varias cosas:

- Revisar los signos vitales de la red en tiempo real.

Un sistema de monitoreo de red sirve para diagnosticar problemas y compilar estadísticas por la gestión y adaptación de la red.
Mientras un sistema de detección de intrusos monitorea una red de amenazas del exterior, un sistema de monitoreo de red monitorea la red de problemas debidos a servidores, conexiones de red u otros dispositivos sobrecargados y/o fuera de servicio.
Estado de respuesta de fallas, tal como cuando una conexión no puede ser establecida, está en tiempo muerto, o el documento o mensaje no puede ser recuperado, usualmente produce una acción del sistema de monitoreo. Estas

acciones varían: una alarma puede ser enviada al administrador del sistema, el sistema de failover automático puede ser activado para remover el servidor hasta que pueda ser reparado, reinicio del servicio, etc [11].
A continuación se describe sobre las guiás activas y pasivas de monitoreo y sus técnicas, de esta manera se crea una estrategia de monitoreo incluyendo la definición de métricas y la selección de las herramientas.
El monitoreo de una red abarca 4 fases [12]:

- Definición de la información de administración que se monitorea.
- Acceso a la información
- Diseño de políticas de administración.
- Procesamiento de la información.

Los tipos de monitoreo son [12]:

- Local.
- Remoto.
- Automático.
- Manual.

El monitoreo puede ser realizado en forma [12]:

- Continua
- Eventual

Objetivos del Monitoreo de Redes

- Identificar la Información a monitorear.
- Diseñar mecanismos para obtener la información necesaria.
- Utilizar la información obtenida dentro de las distintas áreas funcionales de la administración de red.
- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.
- Almacenar la información obtenida en Base de Información de gestión para su posterior análisis.
- Obtener conclusiones para resolver problemas concretos o bien para optimizar la utilización de la red[3].

Arquitectura de la Administración y Monitoreo de Redes

Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de la red, utilizan un software que le permite enviar mensajes de alerta cuando se detecta algún problema, al recibir estos mensajes las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, al cierre del sistema, y un proceso automático para la posible reparación del sistema.
Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ser ejecutada por un administrador de red [3].

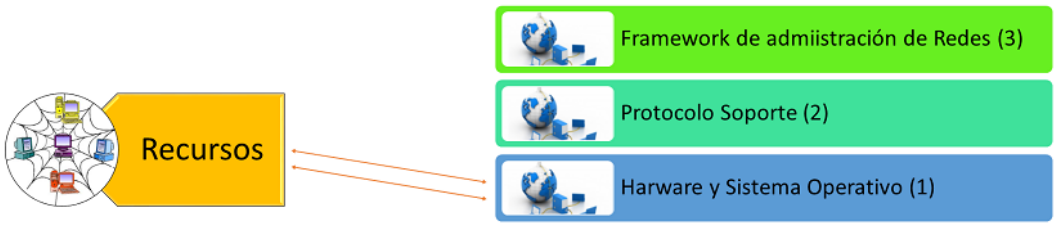


Figura 6: Arquitectura de Administración de redes

1. Hardware y el Sistema Operativo
2. Protocolo de soporte, en el cual incluye:
   - Capas por debajo de la capa de aplicación OSI, UDP/IP en Internet.
   - Protocolos de administración tales como SNMP, ICMP.
   - Conversión de diferentes protocolos y multi-protocolos que soporte protocolos heterogéneos.
3. Provee la base de varias aplicaciones de administración de redes [3]:
   - Funciones de agente y administración.
   - Funciones de administración de redes, tales como configuración y administración de falla.

2.2.3. Guía del Monitoreo

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan [13].

Monitoreo Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento en una red [13].

Técnicas del Monitoreo Activo

Basados en ICMP.

- Diagnosticar problemas en la red.
- Detectar retardo, pérdida de paquetes.
- Disponibilidad de host y redes

Basados en TCP.

- Tasa de transferencia.
- Diagnosticar problemas a nivel de aplicación

Basados en UDP.

- Pérdida de paquetes en un sentido (one-way)
- RTT (traceroute)

Monitoreo Pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para snmp, rmon y netflow. Este enfoque no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y para contabilizar su uso [14].

Técnicas de monitoreo pasivo

Solicitudes remotas

Mediante SNMP

- Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados traps que indican que un evento inusual se ha producido [14].

Otros métodos de acceso

- Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante para monitorear. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública, etc [14].

Captura de tráfico

- Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura.

- Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red [14].

2.2.4. Estrategia de monitoreo

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear así como las herramientas que se utilizarán para esta tarea y se detallaran más adelante [13]:

Aspecto a Monitorear

Uso de ancho de banda, consumo de CPU, de memoria, estado Físico de las conexiones, procesos, tipo de tráfico, alarmas, servicios (Web, base de datos), alcance de dispositivos a monitorear:

- Dispositivos de Interconección: ruteadores, switches, firewall,etc.

- Servidores: Proxy, DHCP y TCP/IP, DNS

- Red de Administración: monitoreo, logs, configuración.

Monitorear el rendimiento del sistema

La revisión de los sistemas a menudo incluye su vigilancia, lo que se denomina medición del desempeño de monitoreo de la red. Los productos para el desempeño de sistemas se han desarrollado para medir todos los componentes de un sistema de información computarizado, lo que abarca el hardware, software, bases de datos, telecomunicaciones y redes. Cuando se usan en forma correcta, estos productos permiten localizar de manera rápida y eficaz problemas reales o potenciales de la red.
El monitorizar el rendimiento del sistema se hace normalmente en respuesta a problemas de rendimiento. Bien sea que el sistema está corriendo muy lentamente, o los programas fallan en ejecutarse. En cualquiera de estos casos, la supervisión del rendimiento del sistema se realiza normalmente como el primer y el último paso de un proceso de tres pasos:

- Monitorizar para identificar la naturaleza y ámbito de la escasez de recursos que están causando los problemas de rendimiento.
- Se analizan los datos producidos a partir de la supervisión y se toma un curso de acción normalmente optimización del rendimiento o la adquisición de hardware adicional.
- Monitorizar para asegurarse de que se ha solucionado el problema de rendimiento[13].

Monitorear la capacidad del sistema

La supervisión de la capacidad del sistema se hace como parte de un programa continúo de planificación. La planificación de capacidad utiliza el monitoreo a largo plazo de los recursos del sistema para determinar las tasas de cambio en la utilización de los recursos del sistema. Una vez que se conocen estas tasas de cambio, se hace posible conducir una planificación a largo plazo más exacta con respecto a la adquisición de recursos adicionales.
La planificación de capacidades requiere un punto de vista a corto plazo o el uso incorrecto de recursos es de poco interés. En vez de esto, se recopilan los datos sobre un período de tiempo, haciendo posible categorizar la utilización de recursos en términos de los cambios en la carga de trabajo. En ambientes definidos de forma más limitada donde solamente corre una aplicación, es posible modelar el impacto

de la aplicación en los recursos del sistema. Esto se puede hacer con suficiente exactitud para determinar, por ejemplo, el impacto de cinco representantes de servicio al cliente ejecutando la aplicación de servicio al cliente durante la hora pico del día [13].

Monitoreo del Ancho de Banda

Es más complicado que la supervisión de otros recursos, la razón de esto se debe a las estadísticas de rendimiento tienden a estar basadas en dispositivos, mientras que la mayoría de los lugares en los que es importante el ancho de banda tienden a ser los buses que conectan dispositivos. En los casos donde más de un dispositivo comparte un bus común, puede encontrar estadísticas razonables para cada dispositivo, pero la carga que esos dispositivos colocan en el bus es mucho mayor.
Otro reto al monitorizar el ancho de banda es que pueden existir circunstancias donde las estadísticas para los dispositivos mismos no estén disponibles. Sin embargo, aun cuando no siempre tendrá disponibles estadísticas relacionadas al ancho de banda 100 % exactas, a menudo se encuentra información suficiente para hacer posible cierto nivel de análisis, particularmente cuando se toman en cuenta estadísticas relacionadas.
Algunas de las estadísticas más comunes relacionadas al ancho de banda son:

- Bytes recibidos/enviados: Las estadísticas de la interfaz de red proporcionan un indicativo de la utilización del ancho de banda de uno de los buses más visibles la red.

- Cuentas y tasas de interfaz: Estas estadísticas relacionadas a la red dan indicaciones de colisiones excesivas, errores de transmisión/recepción y más. Con el uso de estas estadísticas, es posible realizar un fragmento de resolución de problemas de la red antes de utilizar las herramientas de diagnóstico más comunes.

- Transferencias por segundo: Normalmente reunida por dispositivos de E/S(Entrada y Salida) en bloques, tales como discos y unidades de cinta de alto rendimiento, esta estadística es una buena forma de determinar si se está alcanzando el límite del ancho de banda de un dispositivo particular. Debido a su naturaleza electromecánica, las unidades de disco y de cinta solamente pueden realizar ciertas operaciones de E/S cada segundo; su rendimiento se ve afectado rápidamente a medida que se alcanza a este límite[13].

Monitorear la Memoria

Esta área es donde se puede encontrar gran cantidad de estadísticas de rendimiento en la utilización de la memoria. Al identificar una degradación en el desempeño de los servidores, los sospechos mas comunes son el CPU, la memoria y el disco duro.
Es aquí donde tiene lugar la mayoría del trabajo de un administrador de sistemas con la administración de recursos, ya que al momento de identificar una degradación en el rendimiento del servidor, los primeros elementos a investigar son la CPU, la memoria, y el disco.

Monitorear el Almacenamiento

El monitoreo del almacenamiento normalmente tiene lugar en dos niveles diferentes: monitorizar insuficiente espacio en disco y monitorizar problemas de rendimiento relacionados con el almacenamiento. La razón de esto es que es posible tener problemas en un área y en otra no. Por ejemplo, es posible causar que a la unidad de disco se le acabe el espacio sin causar ningún tipo de problemas relacionados al rendimiento.
De la misma manera, es posible tener una unidad de disco que tiene 99 % de espacio libre, pero que se ha puesto más allá de sus límites en términos de rendimiento. Las estadísticas siguientes son útiles para supervisar el almacenamiento:

- Espacio libre: es probablemente el recurso que todos los administradores de sistemas vigilan más de cerca, sería raro el administrador que no verifica el espacio [13].

Monitoreo de la Red

El uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla, vía correo electrónico u otras alarmas. Los aplicativos de monitoreo del estado de red permiten, entre varias cosas:

- Revisar los signos vitales de la red en tiempo real. Mientras un sistema de detección de intrusos monitorea una red de amenazas del exterior, un sistema de monitoreo de red monitorea la red de problemas debidos a servidores, conexiones de red u otros dispositivos sobrecargados y/o fuera de servicio[13].

ALERTA	SIGNIFICADO
WARNING	El servicio tiene valores superiores al valor percibido como aceptable.
CRITICAL	El servicio tiene valores superiores o iguales valor percibido como crítico.
DOWN	El host en cuestión no tiene conectividad a la red
RECOVERY	El host en cuestión ha recuperado la conectividad a la red
UP	El host en cuestión tiene conectividad a la red
FLAPING START	El servicio está oscilando entre estados
FLAPING STOP	El servicio a dejado de oscilar entre estados

Figura 7: Alertas y su significado

Alarmas

Las alarmas son eventos con comportamiento inusual, en donde las más comunes reportan cuando el estado operacional cambia. Existen diferentes tipos de alarmas en patrones previamente definidos en nuestras métricas, son valores máximos conocidos como umbrales.
El servidor que envía las notificaciones cuando algo anormal sucede con los dispositivos o con algún servicio como un Linux, Centos, Windows u otros estas notificaciones serán enviadas hacia el administrador de red vía E-mail, usando la herramienta mailx, Postfix u otro en comunicación con un servidor smtp externo como por ejemplo Gmail, Hotmail, Yahoo [15].
Las alarmas técnicas emiten los equipos y ayudan para una mejor verificación, entre las más comunes:

Ventajas del Monitoreo de la Red

- El monitoreo de la red puede indicar la presencia de troyanos o virus, ya que pueden inducir trafico excesivo y ser una brecha de seguridad.
- Se puede ver si la velocidad hacia o desde el Internet se está aprovechando, si es la suficiente, si se necesite subir el ancho de banda.
- Se puede ver, si ciertos usuarios tienen malos hábitos de navegación como paginas eróticas, de seguridad, hackers, redes sociales, etc.
- Se puede hacer bitácoras de trafico de red para ver si cuando insertas una nueva tecnología o servicio el tráfico de la red sube o baja, es decir si es más optimizado o ahora el diseño es más pobre o tiene impacto[13].

Análisis de Tráfico

Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos que envíen información mediante RMON (Remote Network Monitoring - Norma basada en SNMP para informar diversas condiciones de red. RMON tiene 10 grupos diferentes de administración que proporciona información detallada sobre una red.) o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

Flujos

También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con:

- La misma IP origen y destino
- El mismo puerto TCP origen y destino
- El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing).

2.2.5. Elementos involucrados en la Administración y Monitoreo de Red

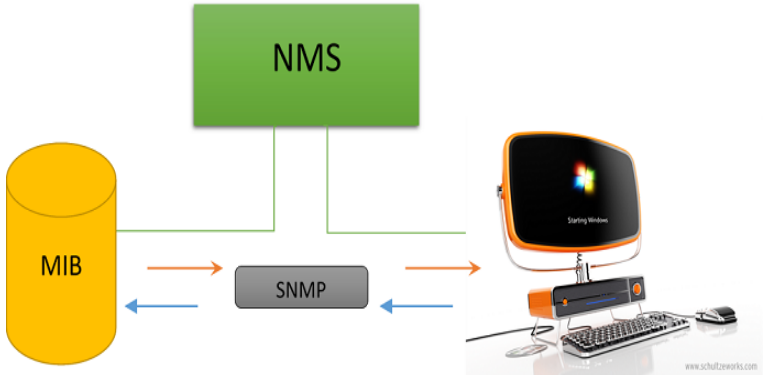


Figura 8: Componentes de la Administración y monitoreo de red

En donde:

- MIB (Base de Información Gestionada o del Ingles Management Information Base) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones.
- NMS (Sistema de Gestión de Red o del Ingles Network Management System) que es una combinación de hardware y software utilizado para controlar y administrar una red de ordenadores o redes.
- SNMP (Protocolo Simple de Administración de Red o del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento[3].

2.2.6. SNMP (Simple Network Management Protocol - Protocolo Simple De Administración De Red)

El Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) es un protocolo ubicado en la capa siete del modelo OSI, facilita la administración de los equipos en la red, permitiendo a los administradores supervisar, encontrar y resolver problemas de una manera mucho más fácil y cómoda. El protocolo SNMP se ha convertido en un estándar de gestión de red sobresaliente y la mayoría de los equipos de interconexión (switches, routers, hubs, puentes) dispositivos de encaminamiento, estaciones de trabajo y PCs ofrecen agentes SNMP para ser gestionados.

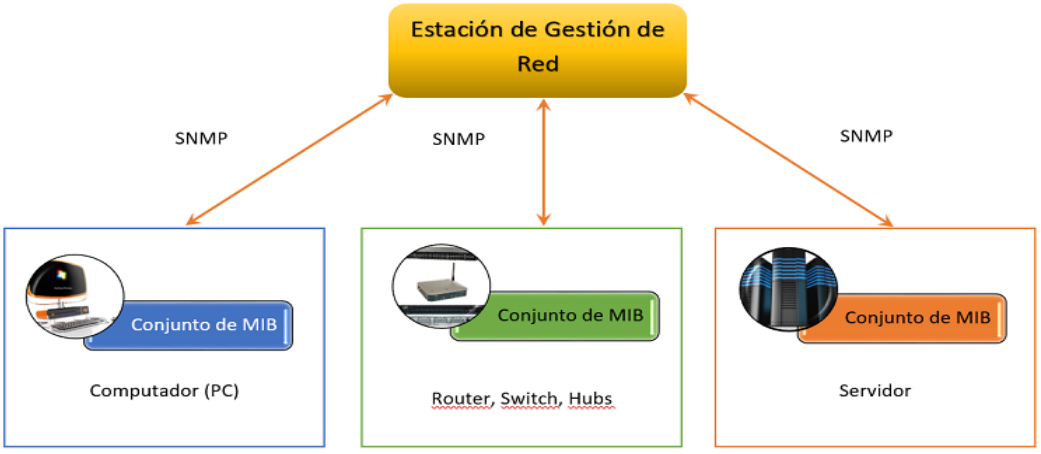


Figura 9: Arquitectura del modelo SNMP

SNMP proporciona un método de administración de hosts de redes como switch, puentes, enrutadores y equipos de servidor o estaciones de trabajo desde un equipo central donde se ejecuta software de administración de redes. SNMP realiza servicios de administración mediante una arquitectura distribuida de sistemas de administración y agentes. Puesto que la administración de redes es fundamental para la administración de recursos y auditoría [3].
El SNMP se ha convertido en un estándar de gestión de red sobresaliente y la mayoría de los equipos de interconexión (switches, routers, hubs, puentes) dispositivos de encaminamiento, estaciones de trabajo y PCs ofrecen agentes SNMP para ser gestionados [12].
Se implementa fácilmente y consume un tiempo moderado del procesador y de recursos de red. Basado en paquetes UDP, es decir, es un protocolo "no orientado a la conexión". Cabe destacar que el protocolo sencillo de administración de redes (SNMP) es un protocolo de administración de red estándar utilizado en Internet. Un posible modelo de SNMP puede ser el que a continuación se muestra, allí se administran cuatro componentes:

- Nodos de administración
- Estaciones administradas
- Información de administración
- Un protocolo de administración

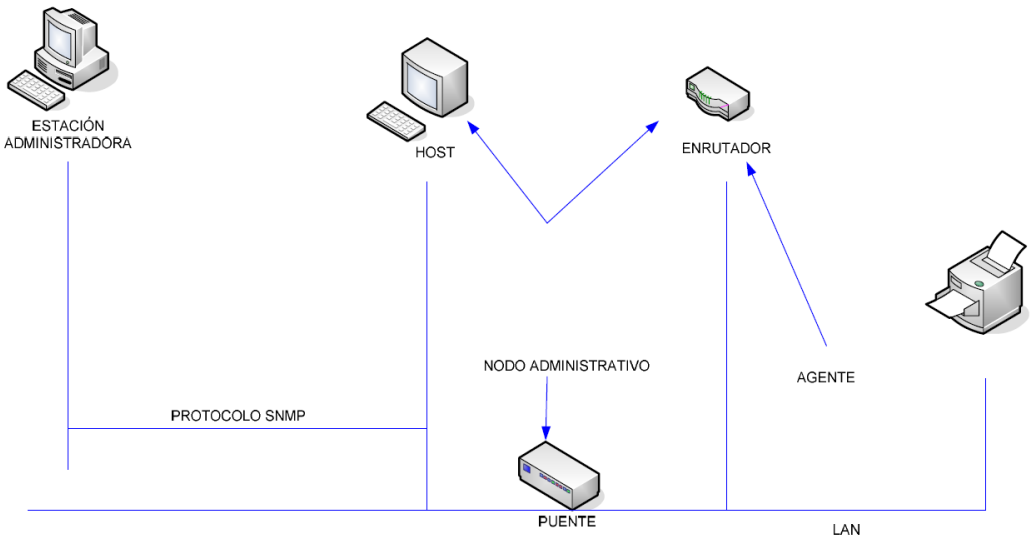


Tabla 1: Proceso de Administración

Los nodos administradores pueden ser enrutadores, host, puentes, impresoras u otros dispositivos capaces de comunicar información de estado al mundo exterior. El protocolo SNMP describe la información precisa y exacta de cada tipo de agente que tiene que administrar y el formato con que este le proporciona los datos; pero lo más importante es la definición de quien tiene que llevar el registro y como se comunica la información [12].
Cuando se refiere a objetos y/o al conjunto de todos los posibles objetos de una red, estos se dan en la estructura de datos llamados MIB, lo que hace realmente es que cada dispositivo administrado por el SNMP, mantiene una o más variables que describen su estado, y estas variables son llamadas Objetos; cada uno tiene un modo de acceso, solo lectura o solo escritura por que la mayor parte de los SNMP consiste en un tipo de comunicación de Consulta-Respuesta.
Cuando existen sucesos no planeados (las líneas pueden desactivarse y levantarse de nuevo) y ocasionan congestión en la red, cada uno de los sucesos significativos son definidos en un modulo MIB, e inmediatamente lo informa a las estaciones administradoras, llamado Interrupción SNMP, que indica lo ocurrido y es responsabilidad de la estación administradora, emitir consultas para informarse de los detalles.
El agente en SNMP es el equivalente a un servidor en Internet, esto quiere decir que un agente SNMP es un sistema que responde a cierta solicitud sobre el estado y condición de la red, desde una estación cliente o estación administrativa [12].
SNMP puede utilizarse para:

- Configurar dispositivos remotos.
- La información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración.
- Supervisar el rendimiento de la red.
- Puede hacer un seguimiento de la velocidad de procesamiento y el rendimiento de la red, y recopilar información acerca de las transmisiones de datos.
- Detectar errores en la red o accesos inadecuados.
- Puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos.
- Cuando se dispara una alarma, el dispositivo envía un mensaje de suceso al sistema de administración. Entre las causas más frecuentes de alarma se

incluye el cierre y reinicio de un dispositivo, un error de un vínculo detectado en un enrutador y un acceso inadecuado.

- Auditar el uso de la red.
- Puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario, y los tipos de uso de servicios y dispositivos de la red [3].

2.2.7. Comandos básicos SNMP

Se utiliza 4 comandos SNMP básicos:

- READ
- WRITE
- TRAP
- Operaciones de recorrido (Traversal Operations).

1. El comando READ es utilizado por un NMS (Network Management Station) para supervisar los dispositivos gestionados o (MD). El NMS examina diferentes variables que son mantenidas por los MD.
2. El comando WRITE es utilizado por un NMS para controlar los MD. El NMS cambia los valores de las variables almacenadas dentro de los Managed Devices
3. El comando TRAP es utilizado por los Managed Devices para reportar eventos de forma asíncrona a los Network Management Systems (NMS). Cuando cierto tipo de eventos ocurren, un MD envía un TRAP hacia el NMS.
4. Las operaciones de recorrido o Traversal Operations son utilizadas por los NMS para determinar cuáles variables son soportadas por los MD y obtener secuencialmente información en una tabla de variables, tal como un routing table[16].

2.2.8. Versiones de SNMP

El protocolo SNMP ha ido avanzando a medida que han surgido las necesidades, principalmente de seguridad. Aunque SNMP es un protocolo flexible, extensible a gran tipo de redes, es un protocolo simple y difícil de implementar por eso fue adquiriendo avances para mejorar su funcionamiento. Su primera versión fue [12]:

SNMP v1

Esta versión fue muy simple y utiliza como método la autenticación basada en comunidades. Se define por arquitectura, física (gestor-agente), en la seguridad introduce el cifrado con clave pública y firma digital. La forma sencilla de autenticarse en esta versión por el método de comunidades son tipos de mensaje como: get, get-next , get-response , set-request y trap no tiene ninguna seguridad implementada [3].

- Fue diseñado a mediados de los 80.
- Lograr una solución temporal hasta la llegada de protocolos de gestión de red con mejores diseños y más completos.
- Se basa en el intercambio de información de red a través de mensajes (PDU's).
- No era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo.

Ventajas

- Es un estándar de mercado
- Simple y fácil de usar

Desventajas

- Limitaciones en el mecanismo de la obtención de información
- Limitaciones de las capacidades de modelado de datos [12]

SNMP v2

Esta versión contiene mejoras en cuanto a SNMP v1, ha mejorado en los tipos de datos y operaciones, pero sigue quedando corto en cuanto a seguridad [3].

- Definida en 1993 y revisado en 1995
- Añade mecanismos de seguridad.
- Mayor detalle en la definición de las variables.
- Se añaden estructuras de la tabla de datos para facilitar el manejo de los datos.

- No fue más que un parche, es más hubo innovaciones como los mecanismos de seguridad que se quedaron en pura teoría, no se llegaron a implementar.

Ventajas:

- Admite mecanismos de seguridad como la autentificación y el cifrado
- Permite la comunicación entre estaciones de gestión.

Desventajas

- Su incompatibilidad con la versión SNMP y la mayor complejidad añadida a las plataformas están desestimando su futura implementación.

SNMP v3

Ofrece autenticidad e integridad utilizando claves de usuarios y mensajes con huellas digitales también ha mejorado en la privacidad al cifrar los mensajes y valida temporalmente sincronizando relojes y una ventana de 150 segundos con chequeo de secuencia.

- Desarrollado en 1998.
- A esta versión se le agregan los mecanismos de seguridad que no se llegaron a implementar en la versión anterior, los cuales son:

Integridad del Mensaje: asegura que el paquete no haya sido violado durante la transmisión.
Autenticación: determina que el mensaje proviene de una fuente válida.
Encriptación: encripta el contenido de un paquete como forma de prevención[3].

Ventajas:

- - Las áreas a las que SNMPv3 va enfocado son primordialmente mejorar la seguridad y la administración respecto a SNMPv2.

Desventajas:

- Aún no es muy conocido y poco implementado [12].

Proceso de envió de un Mensaje SNMP

El envío de mensajes SNMP se realiza por medio del siguiente proceso:

- Transmisión
  - Se construye UDP
  - Se involucra el servicio de autenticación con la dirección de transporte.
  - Se construye el mensaje SNMP
  - Se codifica
- Recepción
  - Comprobación sintáctica
  - Verificación de la versión utilizada
  - Autentificación, Verifica si falla
  - Proceso de petición
- Mensaje SNMP
  - Mensaje SNMP <---------->Datagrama UDP
  - Disminuye el procesado de mensajes y complejidad del agente.

IMPORTANTE: Por el puerto 161 UDP son recibidos los mensajes SNMP y los Traps por el puerto 162.

Mensajes enviados por SNMP

Get Request: Solicita uno a mas atributos de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado). Get Next Request: Solicita el siguiente atributo de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).
Get Bulk Request: Presente en SNMP v2, solicita un amplio conjunto de valores en vez de ir solicitando uno por uno. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).
Set Request: Actualiza uno o varios atributos de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado).
Set Next Request: Actualiza el siguiente atributo de un objeto. Es transmitido por el NMS (o nodo administrador) y recibido agente (o nodo administrado).
Get Response: Devuelve los atributos solicitados. Es transmitido por el agente (o nodo administrado) y recibido por el NMS (o nodo administrador).

Trap: informa de fallos en el agente (como perdida de la comunicación, caída de un servicio, problemas con la interfaz, etc). Es transmitido por el agente (o nodo administrado) y recibido por el NMS (o nodo administrador).
Inform Request: Describe la base local de información de gestión MIB para intercambiar información de nodos administradores entre sí. Es trasmitido por el NMS (o nodo administrador) y recibido por el agente (o nodo administrado) [12].

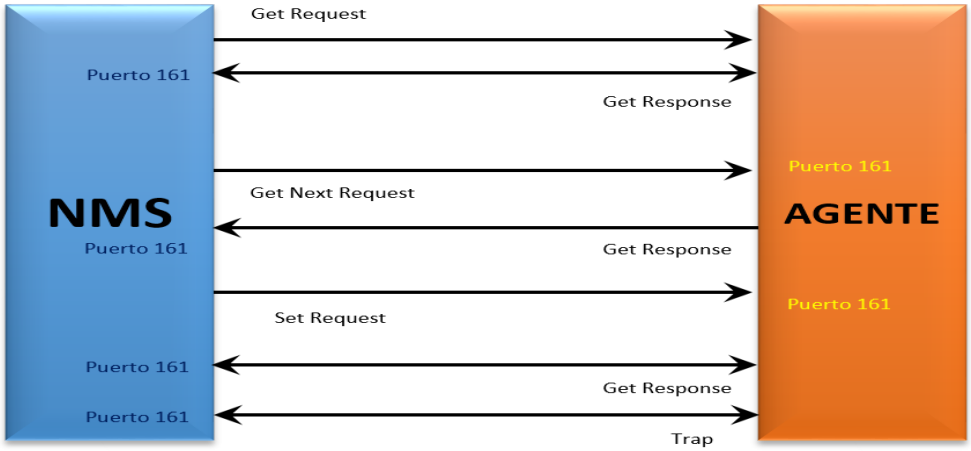


Figura 10: Distribución del Mensaje SNMP

El NMS envía un mensaje Get Request solicitando el atributo de un objeto, el Agente devuelve un Get Response con los atributos solicitados, luego el NMS envía un Get Next Request solicitando el siguiente atributo del objeto, el agente a su vez responde de nuevo con un Get Response, el NMS envía un Set Request para actualizar los atributos de un objeto, el agente le envía un Get Response [12].

2.2.9. Base de información de gestión (MIB)

Un MIB define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información que la MIB incluye el número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad entre otros.
Así también se puede decir que es una base de datos de objetos administrados que son accesibles por el agente y manipulados vía SNMP para lograr la administración de la red, es una información jerárquica estructurada en forma de árbol de todos los dispositivos gestionados en una red [3].

Estructura de una MIB

Los objetos que se guardan en las MIB tienen un identificador único. Este identificador de objetos se llama (OID) es una secuencia de números enteros no son negativos y están separados por puntos que sale de un árbol estandarizado mundialmente conformado por ramas y nodos.

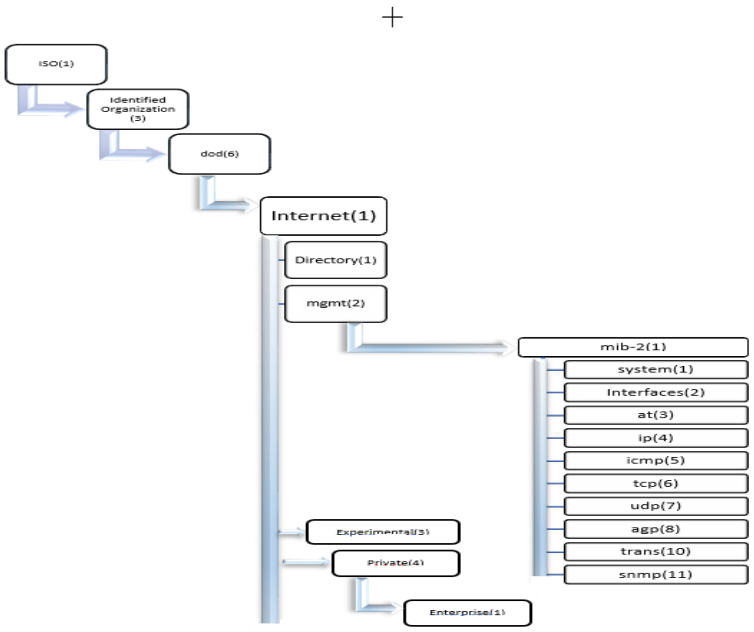


Figura 11: Estructura de una MIB

Tiene 8 niveles de registro que son:

GRUPO	VARIABLE	SIGNIFICADO
System (sys)	sysUpTime	Tiempo desde el último arranque.
Interfaces (intf)	ifNumber	
Interfaces (intf)	ifInErrors	Número de paquetes entrantes en los que el agente ha encontrado error.
Addess Traslation (add trs)		Address Traslation (add trs)
Internet Protocol (ip)	ipInReceives	
Internet Control Message (icmp)	icmpInEchos	Número de solicitudes ICMP recibidas.
Transmision Control Protocol (tcp)	tcpInSegs	Número de paquetes TCP recibidos
User Datagram Protocol (udp)	udpInDatagrams	Número de datagramas UDP recibidos.

Tabla 2: Niveles de Registro de una MIB

Las MIB están escritas utilizando la sintaxis ASN.1. Esta es utilizada para descubrir estructuras de datos que se definen para guardar la información de gestión. Las reglas de codificación básicas (BER), es la codificación utilizada para la transmisión de información escrita en sintaxis ASN.1 a otras aplicaciones

mediante una sintaxis que define y permite definir el formato de cómo se van a enviar los datos.
En el ASN.1 se definen tres tipos de objetos:

1. Tipos (Types)---->define nuevas estructuras de datos y comienzan en mayúsculas.

2. Valores (Values)----->son variables de un tipo y se escriben en minúsculas.

3. Macros---->usados para cambiar la gramática y son escritas en mayúsculas.

Especificaciones de la Base de Información de Gestión (MIB)

La MIB define tanto los objetos de la red operados por el protocolo de administración de red, como las operaciones que pueden aplicarse a cada objeto. La MIB no incluye información de administración para las aplicaciones Telnet, FTP o SMTP, debido a los inconvenientes que se presentan al instrumentar aplicaciones de este tipo para la MIB por parte de las compañías fabricantes. Para definir una variable u objeto para la MIB es necesario especificar lo siguiente:
Sintaxis: Especifica el tipo de variable o valor entero, etc.
Acceso: Especifica el tipo de permiso como: Leer, leer y escribir, escribir, no accesible.
Estado: Define si la variable es obligatoria u opcional.
Descripción: Describe textualmente a la variable.

Grupos de la Base de Información de Gestión (MIB)

La MIB-1 define 126 objetos de administración, divididos en los siguientes grupos:

- Grupo de Sistemas

Usado para registrar información del sistema, por ejemplo: Compañía fabricante del sistema. Tipo de software. Tiempo que el sistema ha estado operando.

- Grupo de Interfaces

Registra la información genérica acerca de cada interfaz de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broatcast enviados, MTU(Maximum Transmission Unit) del dispositivo, etc.

- Grupo de traducción de dirección

Comprende las relaciones entre direcciones IP y direcciones específicas de la red de deben soportar, como la tabla ARP(Address Resolution Protocol), que relaciona direcciones IP con direcciones físicas de la red LAN.

- Grupo IP Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc. También contiene información de variables de control que permite a las aplicaciones remotas ajustar el TTL (Time To Live) de omisión de IP y manipular las tablas de ruteo de IP.

- Grupo TCP

Este incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activa como dirección IP, puerto o estado actual.

- Grupo ICMP Y UDP

Lo mismo que el grupo IP y TCP.

- Grupo EGP

Este grupo se requieren sistemas (ruteadores) que soporten EGP (Protocolo de Gateway o Salida Exterior)[3].

2.2.10. Tráfico de redes

El tráfico de redes es una expresión usada para describir todas las comunicaciones existentes de datos en un ordenador o una red informática en un punto dado.
Durante los etapas de alto tráfico de una red informática o computadora puede reducir la velocidad y atascarse si no es adecuada para la carga. En algunos casos, la demasía de tráfico puede impedir que los dispositivos de red u ordenador deje de funcionar.
El tráfico que se vive en una red se puede vigilar mediante la adopción de los tiempos de respuesta global de todos los principales puntos de acceso, como todos los routers primarios y servidores en una red, los tiempos de respuesta son indicadores de la cantidad de carga que se está notando en ese dispositivo.
Sitios como Informes o estadísticas de tráfico de Internet muestran como la congestión afecta la comunicación de toda la Internet por el control de los tiempos de respuesta de los puntos más importantes en Internet.

Principales causas del tráfico de redes

La congestión puede estar causada por problemas en los canales de datos, los cuales pueden ser físicos o lógicos. Los problemas físicos son más fáciles de corregir, ya que puede ser el cambio del medio de transmisión o un ajuste a los conectores de los elementos de la red, pero los problemas lógicos son aquellos que se presentan internamente en los dispositivos de red, por ejemplo el mal dimensionamiento de los buffers en los enrutadores, lo cual hace que se descarten paquetes.
El ancho de banda o la administración del ancho de banda es otro factor que contribuye a la congestión, ya que este es el recurso más sensible de las redes de datos. Es por este recurso donde se presentan flujos aleatorios que dependen de las diferentes aplicaciones ejecutadas en la red. Si los flujos son grandes y el ancho de banda pequeño, el descarte de los paquetes aumenta; si la situación es a la inversa, los paquetes descartados serán menores. Por consiguiente, la asignación de ancho de banda es una de las técnicas más poderosas para hacerle frente a la congestión; sin embargo, el ancho de banda es un recurso limitado, que en las redes de datos se traduce en costos de implementación.

Análisis del tráfico de redes:

Las tecnologías de transmisión de datos a través de redes de computadores son el eje central del funcionamiento de un entorno informático que presta servicios de tipo cliente/servidor. Un excelente desempeño de la red trae como consecuencia un aumento de la productividad informática.
El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o la de mantenimiento al cableado estructurado y las interfaces de red pueden causar la decadencia del desempeño de la red.
Por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos de red (switch, routers), podemos ofrecer una solución óptima para depurar y optimizar el funcionamiento de la red[17].

Herramientas de monitoreo de redes

Algunas herramientas se encuentran disponibles solo para la medición del tráfico de red. Algunas de estas herramientas miden el tráfico de red por sniffing y otros como: SNMP, WMI o agentes locales para la medida del uso de ancho de banda en equipos individuales y routers. Sin embargo, este último no detecta el tipo de

tráfico, otra opción son los appliances los cuales generalmente se ubican entre la LAN y la WAN o un router de Internet, así de esta manera todos los paquetes entrantes y salientes de la red pasarán a través de estos equipos. En la mayoría de casos los appliance operan como un bridge en la red lo cual los hace indetectables por los usuarios.
Generalmente las herramientas de medición del tráfico de red tienes las siguientes funciones y características:

- Interfaz de usuario: web, gráfica, consola
- Gráficos en tiempo real

Clasificación del Tráfico

La clasificación del tráfico, es un elemento que establece importantes tareas en la administración de la red, tales como: priorización del flujo, que según consiste en determinar la importancia de la aplicación según la obtención o utilización de los recursos; control del tráfico, (permite controlar la máxima tasa de transferencia dentro o fuera de la red), categorización de las aplicaciones, categorización del volumen de tráfico, planeación de la capacidad y aprovisionamiento del enrutamiento [18].
Los operadores distinguen a menudo tres tipos amplios de tráfico de red: Sensible, Mejor-Esfuerzo, e indeseado.

Tráfico sensible

El tráfico sensible es el tráfico del cual el operador tiene una expectativa de entregar a tiempo. Esto incluye VoIP, juegos en línea, video conferencia, y web browsing. Los esquemas se adaptan generalmente de una manera tal que la calidad de servicio de estas aplicaciones seleccionadas se garantice, o por lo menos se dan prioridad sobre otras clases de tráfico. Esto se puede lograr por la ausencia de formar para esta clase del tráfico, o dando prioridad a tráfico sensible sobre otras clases [17].

Tráfico de Mejor-Esfuerzo

El tráfico de Mejor-Esfuerzo es el resto de las clases de tráfico no-perjudicial. Éste es el tráfico que el ISP juzga como no sensible a la métrica de la calidad de servicio (inquietud, pérdida del paquete, estado latente). Un ejemplo típico sería el uso de programas peer to peer y del Email [17].

Tráfico Indeseado

Esta categoría se limita generalmente a la entrega del Spam y del tráfico creado por los gusanos, los botnets, y otros ataques malévolos. En algunas redes, esta definición puede incluir el tráfico tal como VoIP non-local (por ejemplo, Skype) o el vídeo streaming. En estos casos, los esquemas de la gestión de tránsito identifican y bloquean este tráfico enteramente, o seriamente obstaculizando su operación[17].

Software Propietario

Es aquel programa informático en el cual los usuarios tienen limitadas las posibilidades de usarlo y algunas restricciones como, copiarlo, modificarlo y compartirlo además su código fuente no está disponible o el acceso a éste se encuentra restringido. Es decir que cualquiera que tenga acceso a este programa no puede redistribuirlo por los derechos del autor que se otorga al creador del programa o empresa que lo publica, para poder acceder al código fuente y hacerle mejoras se necesita una autorización previa del autor por lo que al publicar estas mejoras sigue perteneciendo el software al propietario original con todos sus derechos.

Software Libre

El software respeta la libertad de los usuarios y la comunidad, es decir que los usuarios tienen la libertad de copiar, modificar, estudiar, distribuir y mejorar el software, con estas libertades el programador controla lo que hace el programa no el programa al usuario.
Un programa se considera software libre si cumplen las cuatro libertades esenciales:

1. Libertad de ejecutar el programa para cualquier propósito.
2. Libertad de estudiar cómo funciona el programa y cambiarlo para que haga lo que quiera (el acceso al código fuente es una condición necesaria).
3. Libertad de redistribuir copias para ayudar a su prójimo.
4. Libertad de distribuir copias de sus versiones modificadas a terceros (permite a la comunidad beneficiarse de las mejoras)[15].

Seguridad Informática

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos. consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización [19].

IDS

Sistemas de detección de intrusos, son sistemas que consiste en analizar las bitácoras de los sistemas en investigación de patrones de comportamiento o sucesos que puedan considerarse susceptibles, sobre la base de la información con la que han sido anticipadamente sustentados[20].

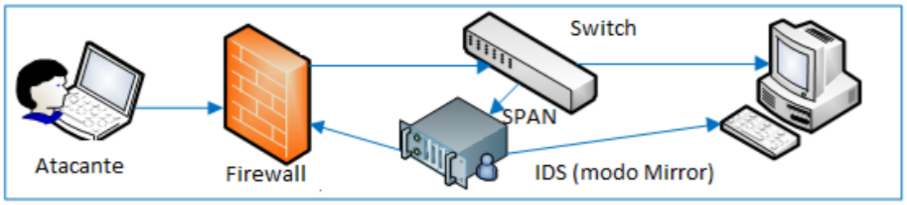


Figura 12: Sistema de Detección de Intrusos (IDS)

Funcionamiento de un IDS

El funcionamiento de esta herramienta se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes mal formados, etc. El IDS no sólo analiza que tipo de tráfico es, sino que también revisa el contenido y su comportamiento [21].

Tipos de IDS

Sistemas de detección de intrusiones en el host (HIDS):

El principio de funcionamiento de una HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades.

El HIDS intenta detectar tales modificaciones en el equipo afectando, y hacer un reporte de sus conclusiones [21].

Sistema de detección de intrusiones de red (NIDS):

Es basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando todo el tráfico de la red [21].

IPS

Es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos [21].

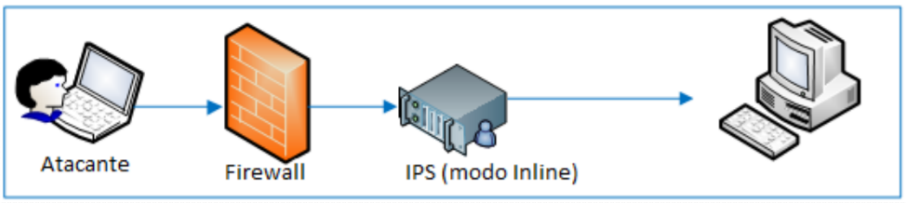


Figura 13: Sistema de Prevención de Intrusos

Características de un IPS

- El IPS se sitúa en línea dentro de la red IPS y no sólo escucha pasivamente a la red como un IDS (tradicionalmente colocado como un rastreador de puertos en la red).
- El IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes en modo nativo (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos, el bloqueo de un intruso, etc [21].

Funcionamiento

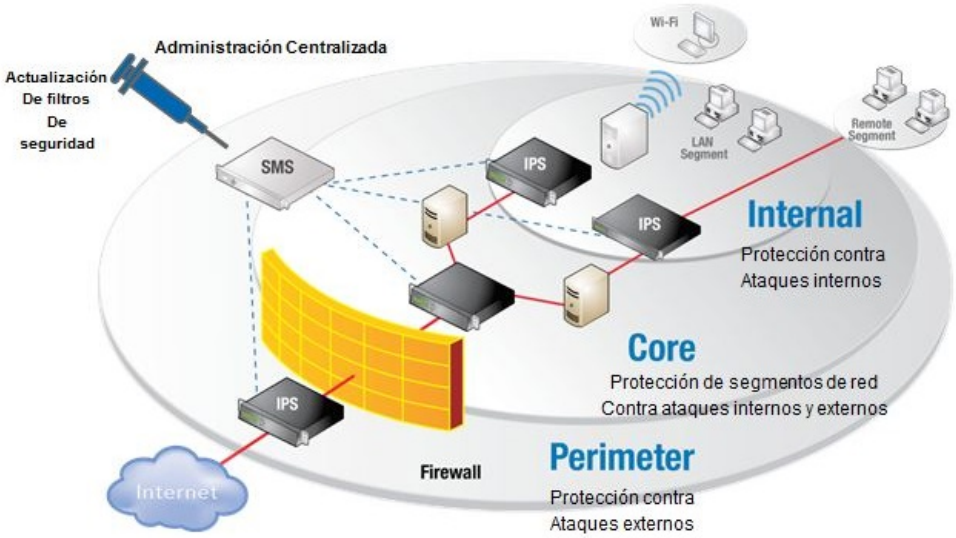


Figura 14: Funcionamiento de un IPS

Categorización del IPS para detectar el tráfico malicioso

El IPS se categoriza por lo siguiente [21]:

- Detección basada en firmas: como lo hace un antivirus.
- Detección basada en políticas: el IPS requiere que se declaren muy específicamente las políticas de seguridad.
- Detección basada en anomalías: en función con el patrón de comportamiento normal de tráfico.
- Detección honey pot (jarra de miel): funciona usando un equipo que se configura para que llame la atención de los hackers .

Diferencias entre IDS/IPS

	IPS	**IDS**
	Inline, Bloque Automático	**Mirror, Alertas para analistas**
Estabilidad de la red	Caída del sistema es catastrófica para la red	Caída del sistema quita información al analista de red. No es algo crítico
Desempeño	Requiere mayor capacidad de procesamiento. Puede producir cuellos de botella.	La falla de procesamiento puede ser compensada con buffers de mucha memoria. Nunca producirá cuellos de botella.
Precisión de Falsos Positivos	Produce bloqueos de paquetes. Problemas con aplicaciones.	Carga trabajo innecesaria para el analista en busca de falsas alarmas.
Precisión de Falsos Negativos	Paquetes maliciosos entran a la red. No es tan crítico como en el caso de los IDS.	Ataques resultan totalmente invisibles y pueden volver a ocurrir. Pérdida de información para el analista.

Tabla 3: Diferencias entre IDS/IPS

SURICATA

Suricata es una herramienta gratuita y de código libre que se ha desarrollado para controlar el tráfico de red y su principal objetivo es que rastree o busque los eventos de seguridad que pueden indicar un ataque o posible intrusión en un servidor o en algún equipo de la red.

Descripción y características de Suricata

Suricata es el nombre de un proyecto de software libre para un motor Sistema de Detección y Prevención de Intrusos o de manera abreviada IDS/IPS; fue desarrollado por la comunidad de OISF (Open Information Security Foundation). Entre algunas características de Suricata, las más representativas son las siguientes [22]:

- Multi-theading son multiples hilos de ejecución que permite realizar varios procesos a la vez.

- Estadísticas de Rendimiento
- Detección de Protocolos automáticos
- Fast IP Matching
- IP Reputation
- Graphic Cards Acceleration

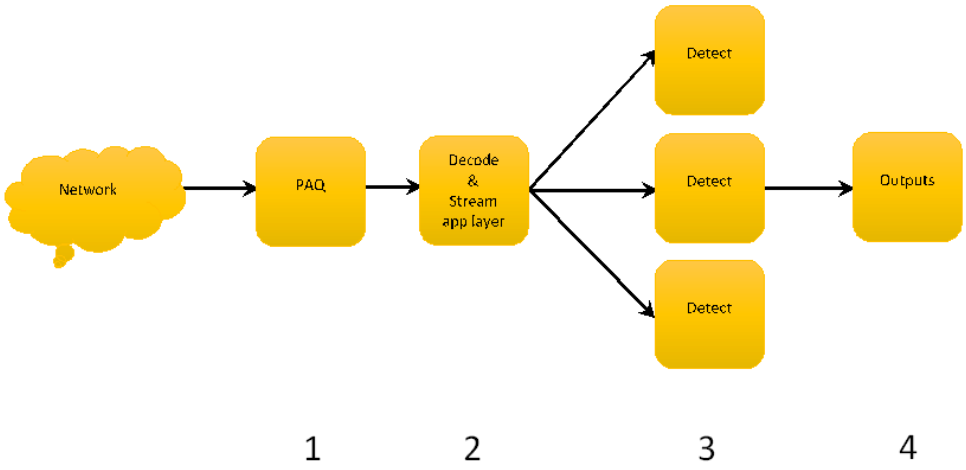


Figura 15: Proceso de los 4 módulos Multihilos en Suricata

En la figura 2.13 se muestra el procesamiento de un paquete y los módulos de suricata que intervienen [22]:

- PAQ se refiere a la adquisición de paquetes.
- Decode se refiere a la decodificación de paquetes.
- Stream app Layer realiza el seguimiento del flujo y reconstrucción.
- Detect, compara firmas y Output procesa todos los eventos y alertas.

2.3 Propuesta de Solución

Implementar un Sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de forma correcta que permita dar solución al problema generado en la Institución, alternativa que protegerá los datos informáticos y permitirá la satisfacción del personal administrativo, docentes y estudiantes permitiendo desarrollar de mejor forma sus actividades en la red informática.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la investigación

La realización de la presente investigación se basará en la investigación de campo la cual analiza el problema partiendo de hechos reales, para la obtención de información y requerimientos que evidencien los objetivos, la aplicación de esta modalidad de investigación ha sido considerada debido a la necesidad de concurrir a la fuente misma del problema, investigación que será realizada en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial en la carrera de Ingeniería en Sistemas Computacionales Informáticos de la Universidad Técnica de Ambato infraestructura destinada para la realización del trabajo de investigación.
Modalidad Bibliográfica o Documental: Se realizará mediante la utilización de libros e Internet, papers, publicaciones, proyectos de investigación; a través de la cual se obtendrá información que ayude en todo lo que concierne al desarrollo de la fundamentación teórica en la cual se basó la presente investigación y que fueron de ayuda y soporte para el investigador.
Modalidad aplicada: Se realizará al aplicar los conocimientos adquiridos a lo largo de la carrera universitaria para la elaboración y ejecución del presente proyecto de investigación.

3.2. Recolección de información

Para la recolección de la información sobre el análisis de la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la ciudad de Ambato, se determina el uso de Internet y la guía del tutor para el análisis de la parte técnica. Además se considera de suma importancia para la recolección de información del presente proyecto de investigación realizar entrevistas al ex Administrador de redes Ingeniero Eduardo Chaso, de la misma forma a la actual administradora de redes Ingeniera Cristina Frutos ya que los mencionados han palpado de forma directa el problema que pretende dar solución.

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Solucionar el congestionamiento del ancho de banda de la red de la FISEI.
2. ¿De qué personas u objetos?	Al ex administrador de redes y actual administradora de redes de la FISEI
3. ¿Sobre qué aspectos?	Implementación de un Sistema de Monitoreo y Protección de Datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
4. ¿Quién? ¿Quiénes?	El investigador
5. ¿Cuándo?	Abril 2015 - Diciembre 2016
6. ¿Dónde?	Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
7. ¿Cuántas veces?	Las que la investigación requiera
8. ¿Qué técnicas de recolección?	Con instrumento como guía de entrevista
9. ¿Con qué?	Mediante la técnica la entrevista mediante cuestionario guía de entrevista
10. ¿En qué situación?	En el horario de actividades normales

Tabla 4: Información recolectada

3.3. Procesamiento y análisis de datos

El procesamiento de la información pretende ser analizado de forma eficiente mediante la recolección de información o conocimientos brindados por parte de los involucrados en el proceso de la entrevista, del mismo modo la revisión del análisis de la red de la información recogida.
Una vez recolectado los datos se procederá a su respectivo análisis obteniendo resultados satisfactorios los cuales serán de gran importancia para la formulación de la propuesta. Los datos serán analizados y procesados en relación al problema para poder establecer las respectivas conclusiones asegurando que los datos sean lo más reales posibles.

3.4. Desarrollo del Proyecto

- Determinar las herramientas utilizadas para el monitoreo de la red.
- Monitorear la red de datos para detectar fallos y congestionamiento.
- Analizar los resultados del monitoreo para identificar actividad no autorizada y anomalías que provoquen degradación en la red.

- Establecer mecanismos de control y protección de datos para mejorar el rendimiento de la red.

CAPÍTULO 4

Desarrollo de la propuesta

4.1. Datos Informativos

4.1.1. Tema de la Propuesta

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y PROTECCIÓN DE DATOS EN LA RED DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL."

4.1.2. Institución Ejecutora

- Institución Educativa: Universidad Técnica de Ambato
- Nombre de la Institución: Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Tipo de Organización: Pública
- Departamento: Administración de Redes y Sistemas

4.1.3. Beneficiarios

Universidad Técnica de Ambato, Facultad de Ingeniería en Sistemas, Electrónica e Industrial, estudiantes, profesores y personal administrativo de la Institución.

4.1.4. Ubicación

- Provincia: Tungurahua
- Cantón: Ambato
- Dirección: Av. Los Chasquis y Río Payamino
- Teléfono: 03 2415288

4.1.5. Equipo Responsable

- Tutor: Ing. David Omar Guevara Aulestia.
- Investigador: David Fernando Sánchez Cunalata

4.2. Análisis de Factibilidad

Con el propósito de poder establecer de forma cualitativa la factibilidad de la aplicación del presente proyecto de investigación se determinará las circunstancias actuales de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, se buscará la forma más idónea para precautelar la información de la FISEI mediante una evaluación de cada una de ellas, para lo cual se realizará un análisis y posteriormente se procederá a determinar su grado de conveniencia para el proyecto, considerando de manera especial sus principales ventajas.

4.2.1. Factibilidad Institucional

La factibilidad institucional de implementar un sistema de monitoreo y protección de intrusos a la red de la FISEI dando solución al problema detectado en la red del presente proyecto de investigación posee la factibilidad ya que la misma necesita dar con una solución al problema detectado en la red en el ancho de banda y proteger la red, entonces se establece un análisis de la infraestructura informática de la facultad, analizando los dispositivos que se puedan encontrar, sus configuraciones y funciones dentro de la red de datos, es decir la institución permitirá y consolidará las condiciones necesarias para que el proyecto sea instalado con total apoyo para la protección de datos concernientes a la institución y que permita su instalación en beneficio de la misma.
Implementar un Sistema de Monitoreo y Protección de datos en la red de la FISEI ya que serán de gran utilidad para precautelar las actividades realizadas en la red como registrar el tráfico y precautelar las comprobaciones de rendimiento de Ethernet y que estas poseen beneficio para la Facultad ya que buscará la protección y cuidado para y en beneficio directo de los Docentes, Estudiantes y Administrativos.

4.2.2. Factibilidad Operativa

En la Facultad de Ingeniería en Sistemas Electrónica e Industrial se ha evidenciado que se dispone con la infraestructura física y equipos tecnológicos, para la aplicación del proyecto como base de la investigación. Cabe añadir que

las autoridades de la Facultad muestran interés hacia la presente propuesta de investigación con la responsabilidad directa del investigador.
La FISEI dispone de equipos tecnológicos de primer nivel los cuales permitirán el buen desarrollo del presente proyecto, los equipos necesarios para el buen desenvolvimiento del proyecto son: Servidores, Switch, Routers, entre otros. Cabe mencionar que los aparatos tecnológicos que posee la FISEI son de uso y disposición exclusivamente para la investigación.

4.2.3. Factibilidad Técnica

La implementación del presente proyecto de investigación es factible técnicamente, ya que el investigador cuenta con el material e información necesaria tanto en software como en hardware, además es factible técnicamente debido a que estaba vinculado de forma directa con la parte de administración de redes de la FISEI, debido a que laboré en la Institución como Auxiliar de Laboratorio del 1 de enero al 31 de diciembre del 2016.

4.2.4. Factibilidad Económica

El presente proyecto de investigación es factible económicamente ya que el Software utilizado es libre y de distribución gratuita, en cuanto al hardware, la FISEI cuenta con los equipos necesarios para la implementación del proyecto. Los recursos adicionales que se requieran serán cubiertos por el investigador.

N°	**Detalle**	**Unidad**	**Cant.**	**V. U**	**V.T**
1	Computador	c/u	1	1300,00	1300,00
2	Hojas	c/u	100	3,50	350
3	Impresiones (b/n)	c/u	220	0,10	22
4	Impresiones Color	c/u	100	0,25	25
5	Transporte	veces	100	0,30	30
6	Internet	horas	400	0,80	320
7	Alimentación	c/u	100	2.50	250
				Total	2047
				Imprevistos	300,00
				TOTAL	2347

Tabla 5: Recursos Económicos

4.3. Ejecución de la Propuesta

ESTRUCTURA DE LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

4.3.1. Descripción

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI) de la Universidad Técnica de Ambato (UTA), se crea como Escuela de Informática y Computación, mediante resolución de H. Consejo Universitario No. 347-91-CU-P del 13 de octubre de 1991.

Los rápidos cambios y avances del mundo moderno, necesidades de automatización de las empresas públicas y privadas, que requerían profesionales en Informática a nivel de ingeniería, hizo necesario realizar cambios en los planes y programas de estudio, para que, mediante resolución de H. Consejo Universitario No. 386-92-CU-P del 4 de agosto de 1992 pase a ser la Facultad de Ingeniería en Sistemas.

Con el transcurso del tiempo y la necesidad creciente de crear nuevas oportunidades profesionales para los estudiantes de la zona central del país, mediante resolución de H. Consejo Universitario No. 804-CU-P del 20 de octubre de 1998, se crean las carreras de Ingeniería en Electrónica y Comunicaciones e Ingeniería Industrial en Procesos de Automatización, que junto con la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, pasan a formar la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Las autoridades que han dirigido la misma son: Ing. Washington Medina (1994-1997), Ing. Oswaldo Paredes (1997-2000), Ing. Víctor Guachimboza (2000-2006), Ing. Alexis Sánchez (2006-2009) , Ing. Oswaldo Paredes (2010-2013), y actualmente el Ing. Vicente Morales (2015-2017).

4.3.2. Organigrama

El organigrama de la Facultad de Ingeniería en Sistemas Electrónica e Industrial se puede ver en la siguiente figura.

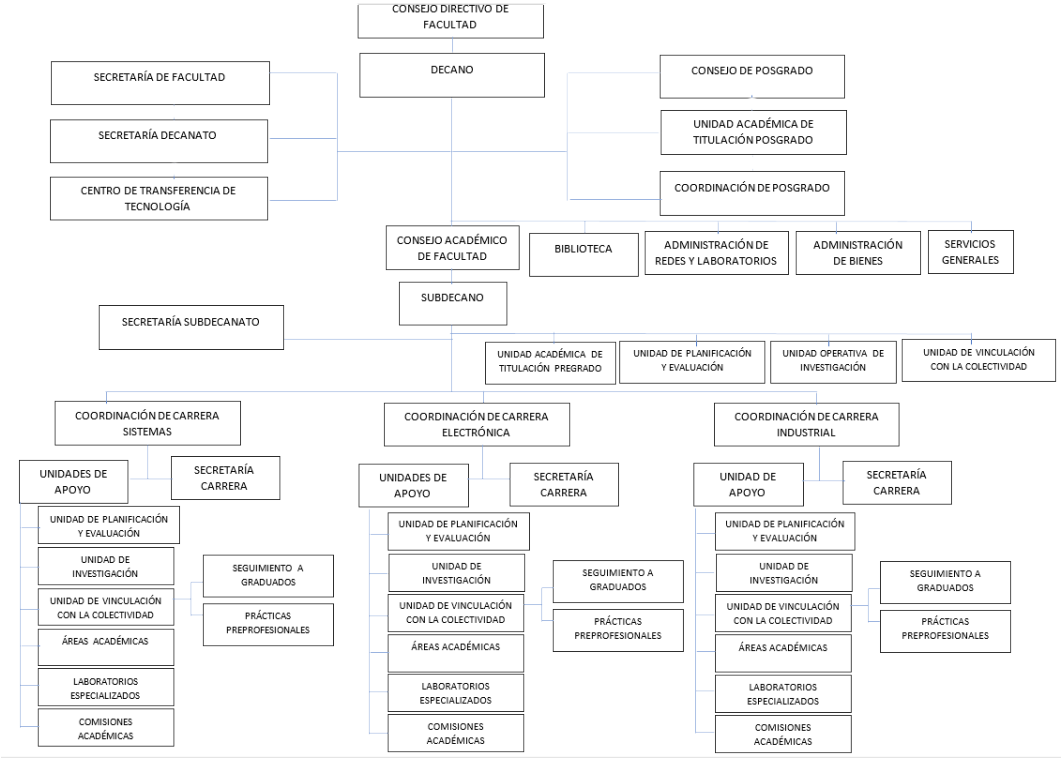


Figura 16: Organigrama Funcional de la Facultad de Ingeniería en Sistemas Electrónica e Industrial

4.3.3. Instalaciones

A continuación se presenta mediante imágenes la Facultad de Ingeniería en Sistemas Electrónica e Industrial en las cuales se realizo la aplicación del presente proyecto de investigación:

Figura 17: Fachada anterior de la FISEI

Infraestructura de la fachada posterior de la FISEI

Figura 18: Fachada posterior de la FISEI

4.3.4. Oficinas Administrativas

Las oficinas administrativas de la FISEI. se encuentran en la parte anterior de los edificios, cumpliendo con las funciones administrativas competentes a cada área.

Figura 19: Oficinas administrativas Subdecanato

Figura 20: Oficinas administrativas Decanato

4.3.5. Administración de Redes

A continuación se muestra el servidor de control de red de la FISEI:

Figura 21: Administración de redes

4.4. Análisis de la entrevista

Para el análisis se establece una entrevista no estructurada con un máximo de 3 preguntas realizadas por el autor Fernando Sánchez, establecidas al ex administrador de redes Ing. Eduardo Chaso y a la actual administradora de redes Ing. Christina Frutos del periodo 2016.

Este departamento es quien brindo información técnica en cuanto a la infraestructura física y lógica de la red, brindando los requerimientos necesarios para el monitoreo de los servicios y dispositivos de la red de datos durante la operación y mantenimiento de la misma.

- Preguntas no estructuradas:

  ¿Existe algún mecanismo de monitoreo de red de datos?

  En la facultad no existe un sistema de monitoreo de red de datos que diagnostique los problemas y recopile estadísticas que brinde información de los daños que pueden existir.

  ¿Existe algún mecanismo de seguridad informática?

  La facultad no cuenta con un sistema de seguridad informática que permita la protección de la información y servicios informáticos, ya que no son muy importantes para usuarios ajenos a la Facultad. Se maneja la seguridad informática por las configuraciones de los Servidores y Routers, en la cual la parte Académica y lo Administrativo esta separado por VLANs.

  ¿Es factible la implementación de un sistema de monitoreo y protección de datos en la red de la FISEI?

  Si es factible ya que es muy útil para prevenir algún tipo de acceso no autorizado a la red, ya que la parte administrativa tiene en sus computadores información valiosa, como facultad es necesario tener un sistema de protección informática que sea estable y seguro así no sea muy complejo.

Una vez terminada la entrevista se concluye que no existe un sistema de monitoreo y protección de datos integrado en sus redes y como seguridad tiene las configuraciones de los Servidores y Routers en la red de datos de la FISEI.
Esta información permitió tener la factibilidad de implementar un sistema de monitoreo y protección de datos como medio de investigación, estableciendo los siguientes requerimientos específicos:

- Analizar la infraestructura de la facultad.
- Qué servicios y dispositivos se necesitan monitorear.
- Analizar que dispositivos se pueden encontrar, sus configuraciones y funciones dentro de la red de dato.

en base a la entrevista se a evidenciado se ha evidenciado que se ha localizado tales problemas como se cae la red ancho de banda.

4.4.1. Equipos y Sistemas de Seguridad en la FISEI.

En la facultad cuenta con 3 Servidores los cuales son:
Servidor Proxy.

- Niveles de acceso: el acceso al Servidor o a la red de datos, es configurado por el Protocolo AAA; en inglés, Authentication, Authorization and Accounting, además por las políticas de seguridad establecidas en la institución.
- Reglas ACL: reglas de control de acceso las cuales determinan políticas centralizadas para la mejor efectividad en cuanto a la administración de la red en la FISEI.

  Servidor de Enrutamiento.
- Determina comunicaciones con alta seguridad en el acceso para usuarios característicos.
- Mejora el alcance de las redes, para determinar reglas de conexión entre varias subredes y accesos a las mismas.

4.4.2. Estructura de la red de la FISEI

A continuación se muestra la distribución de la red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

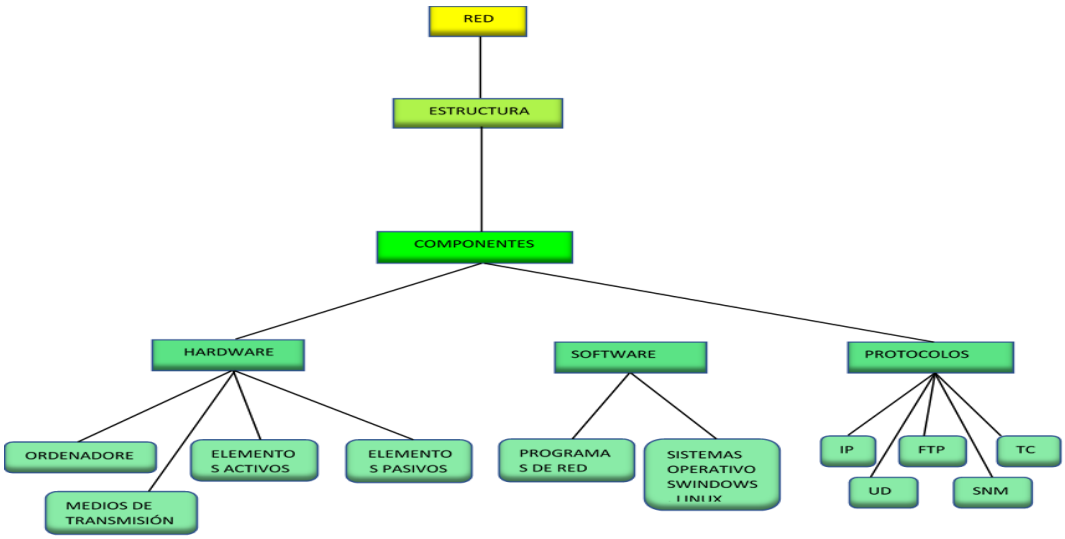
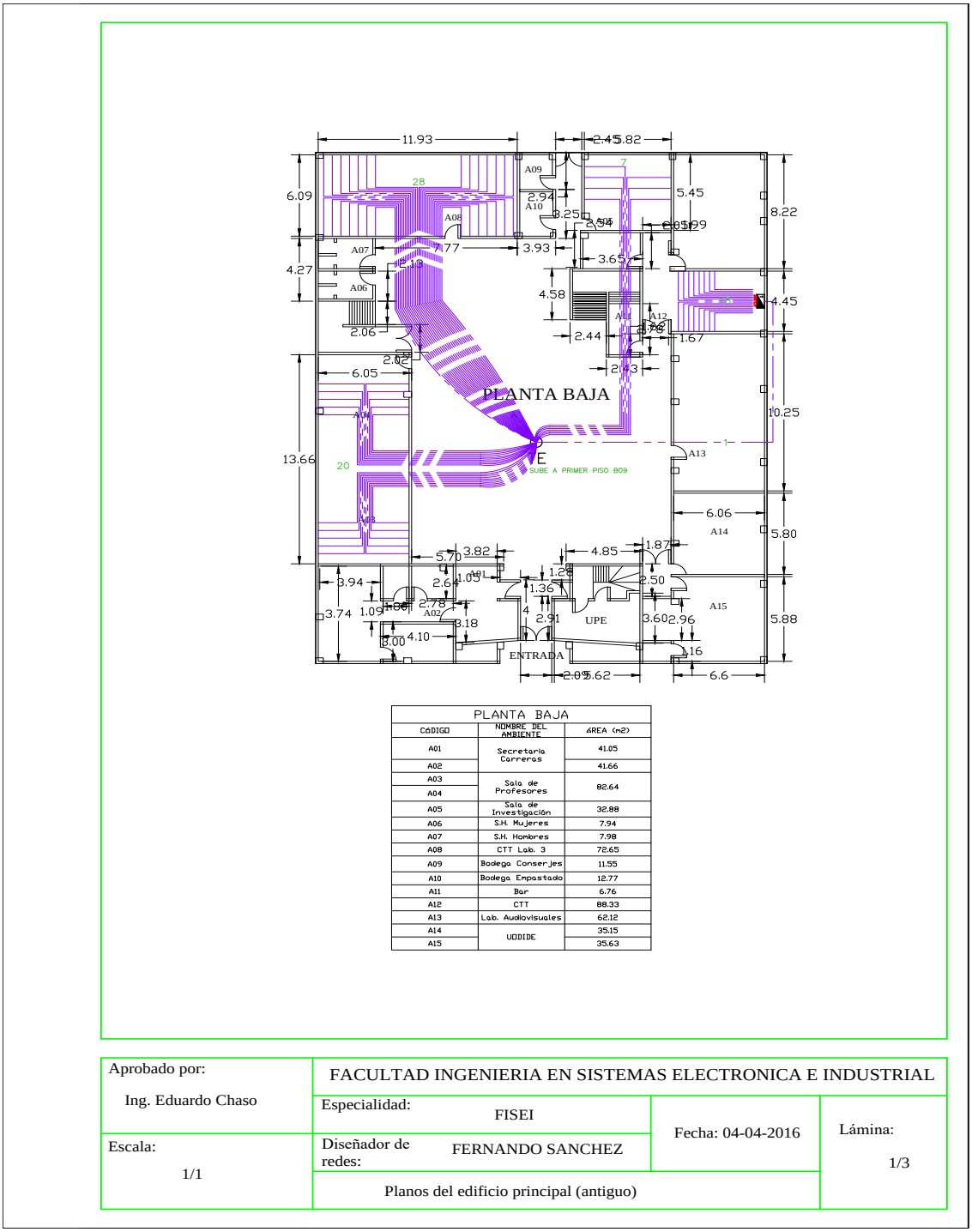


Figura 22: Estructura de la red de la FISEI

4.4.3. Planos del Diseño de Red de la FISEI

Se ha realizado la infraestructura del diseño de la red de datos de la FISEI a continuación los planos:

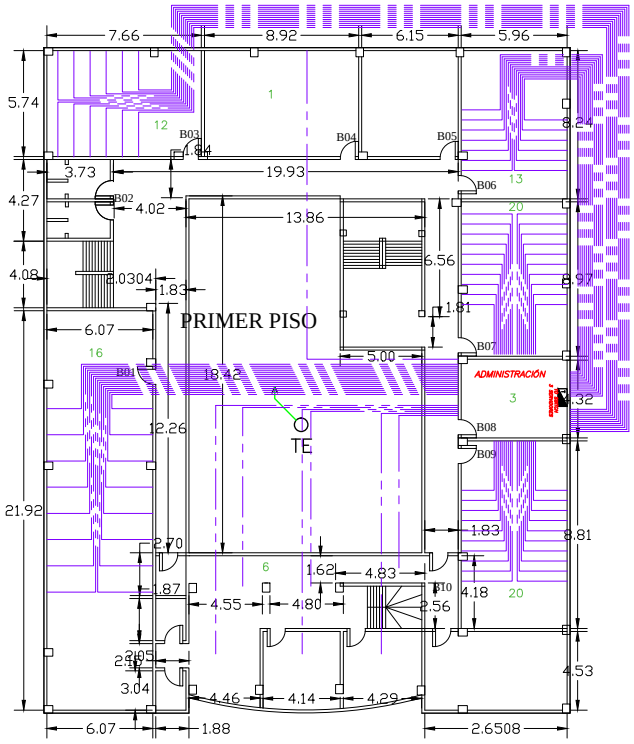


PLANTA BAJA

CÓDIGO	NOMBRE DEL AMBIENTE	ÁREA (m2)
A01	Secretaria Carreras	41.05
A02		41.66
A03	Sala de Profesores	82.64
A04		
A05	Sala de Investigación	32.88
A06	S.H. Mujeres	7.94
A07	S.H. Hombres	7.98
A08	CTT Lab. 3	72.65
A09	Bodega Conserjes	11.55
A10	Bodega Empastado	12.77
A11	Bar	6.76
A12	CTT	88.33
A13	Lab. Audiovisuales	62.12
A14	UDDIDE	35.15
A15		35.63

Aprobado por: Ing. Eduardo Chaso	FACULTAD INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL		
	Especialidad: FISEI	Fecha: 04-04-2016	Lámina: 1/3
Escala: 1/1	Diseñador de redes: FERNANDO SANCHEZ		
	Planos del edificio principal (antiguo)		

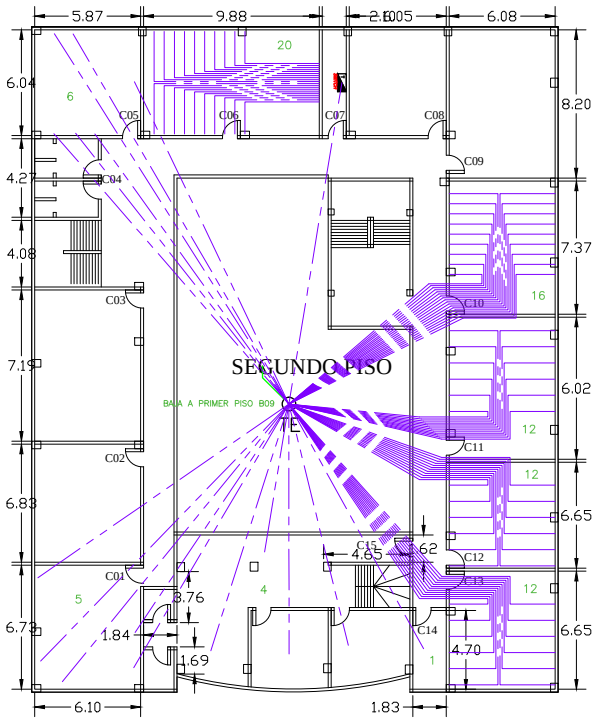
Figura 23: Planta baja Edificio principal (antiguo)



PRIMER PISO		
CÓDIGO	NOMBRE DEL AMBIENTE	ÁREA (m2)
B01	Biblioteca FISEI	369.63
B02	Servicios Higiénicos	15.82
B03	Lab. Redes	43.97
B04	Lab. Electrónica II	51.20
B05	Máquinas Eléctricas I	35.30
B06	Lab. Arquitectura	49.11
B07	Lab. 2	53.46
B08	Administración de Redes	26.88
B09	Lab. 1	52.69
B10	Subdecanato	152.11

Aprobado por: Ing. Eduardo Chaso	FACULTAD INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL		
	Especialidad: FISEI	Fecha: 04-04-2016	Lámina: 2/3
Escala: 1/1	Diseñador de redes: FERNANDO SANCHEZ		
	Planos del edificio principal (antiguo)		

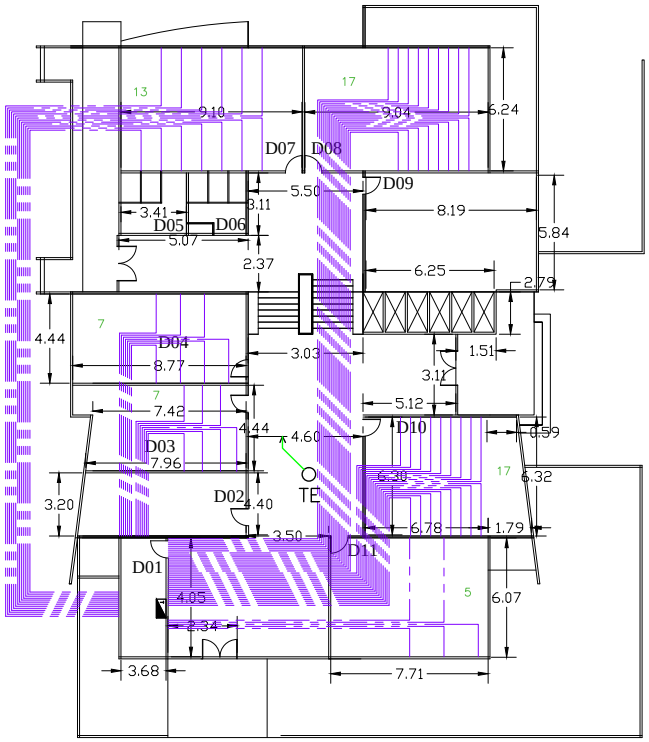
Figura 24: Primer piso Edificio principal (antiguo)



SEGUNDO PISO		
CÓDIGO	NOMBRE DEL AMBIENTE	ÁREA (m2)
C01	Cooperativa de Ahorro y Crédito UTA	41.05
C02	Aula	41.66
C03	Aula	43.66
C04	Servicios Higiénicos	15.82
C05	Dirección de Posgrados	35.45
C06	Lab. Maestrías	59.28
C07		12.6
C08	Sala de Grados	36.54
C09	Lab. Linux	48.87
C10	Lab. 6	43.93
C11	Lab. 5	36.60
C12	Lab. 4	40.43
C13	Lab. 3	40.76
C14	Oficina Sistemas	8.40
C15	Decanato	115.78

Aprobado por: Ing. Eduardo Chaso	FACULTAD INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL		
	Especialidad: FISEI	Fecha: 04-04-2016	Lámina: 3/3
Escala: 1/1	Diseñador de redes: FERNANDO SANCHEZ		
	Planos del edificio principal (antiguo)		

Figura 25: Segundo piso Edificio principal (antiguo)

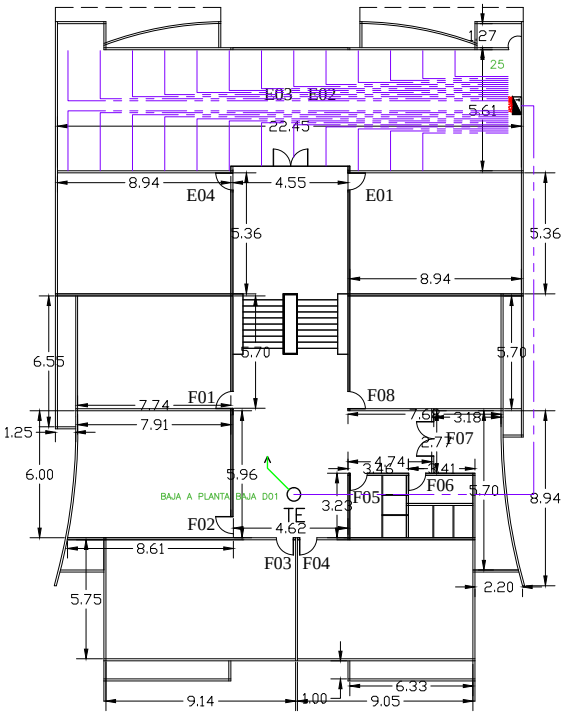


PLANTA BAJA

PLANTA BAJA		
CÓDIGO	NOMBRE DEL AMBIENTE	ÁREA (m2)
D01	Bodega	14.90
D02	Oficina Industrial	35.02
D03	Lab. CNC	32.94
D04	Lab. Neumática e Hidráulica	38.93
D05	S.H. Hombres	10.68
D06	S.H. Mujeres	8.33
D07	Lab. Robótica	56.78
D08	Lab. Industrial II	56.40
D09	Lab. Electrónica I	65.59
D10	Lab. Industrial I	54.16
D11	Lab. PLCS	46.79

Aprobado por: Ing. Eduardo Chaso	FACULTAD INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL		
	Especialidad: FISEI	Fecha: 04-04-2016	Lámina: 1/4
Escala: 1/1	Diseñador de redes: FERNANDO SANCHEZ		
	Planos del edificio secundario (nuevo)		

Figura 26: Planta baja Edificio secundario (nuevo)



PRIMER PISO

PRIMER PISO		
CÓDIGO	NOMBRE DEL AMBIENTE	ÁREA (m2)
E01	Lab. Máquinas II	47.61
E02	Sala de Profesores	125.94
E03		
E04	Sala de Reuniones de Docentes	47.61
F01	Aula	42.80
F02	Aula	47.46
F03	Aula	54.10
F04	Aula	52.03
F05	S.H. Mujeres	11.17
F06	S.H. Hombres	10.14
F07	Balcon	5.90
F08	Aula	43.77

Aprobado por: Ing. Eduardo Chaso	FACULTAD INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL		
	Especialidad: FISEI	Fecha: 04-04-2016	Lámina: 2/4
Escala: 1/1	Diseñador de redes: FERNANDO SANCHEZ		
	Planos del edificio secundario (nuevo)		

Figura 27: Primer piso Edificio secundario (nuevo)

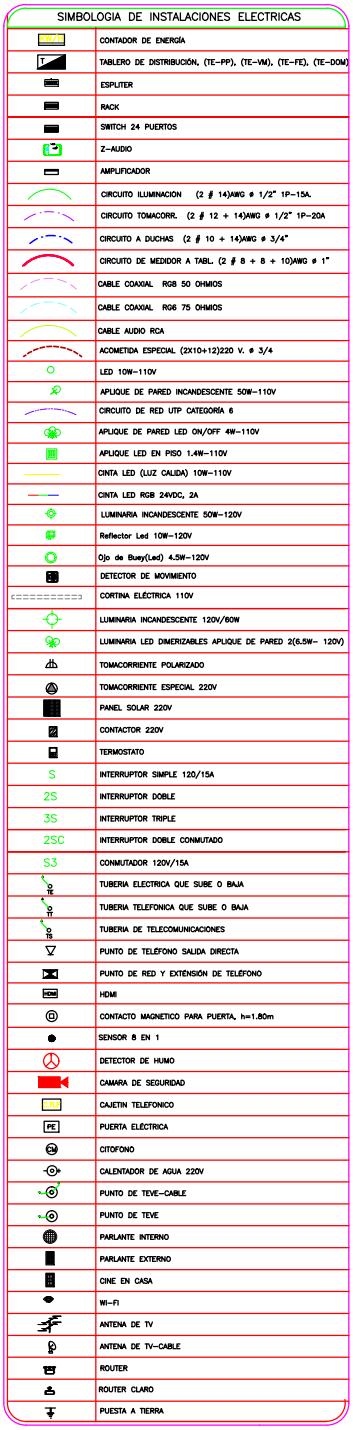


Figura 28: Simbología de las instalaciones eléctricas de los planos

4.4.4. Esquema de la red de datos de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

Un paso fundamental del presente proyecto de investigación es el estado actual de la red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, para conocer el modo de operación y encaminar de mejor manera la investigación, detectando así las fortalezas, debilidades y la selección de las herramientas adecuadas para mejorar los recursos de la red [23].

Mediante el análisis de ciclos de tráfico de red se determinaron los patrones de flujo de datos que muestran la utilización máxima, promedio y estándar de la red normal.

Para ello se utilizó el software MRTG, el cual se encarga de monitorear la Red. y SolarWinds que utilizan el protocolo SNMP para coleccionar la información del manejo de la red de la universidad, generada por el router, switches y otros elementos activos y emplean una arquitectura cliente/servidor para hacer visible la información disponible en formato HTML [23].

Además cabe mencionar que la red de Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato se encuentra configurada en VLANS, para organizar a los usuarios de la red en grupos de trabajo lógico que sean independientes de la topología física del armario de instalación. Esto, a su vez, puede reducir el costo de movimientos, agregación, y cambios mientras se aumenta la flexibilidad de la red. Cada VLAN debe soporta el algoritmo Spanning Tree (IEEE 802.1d) para evitar bucles en la red. De la información obtenida mediante el monitoreo de la red de datos interna de la FISEI, se determinó el ancho de banda que utiliza, por otro lado se tiene en cuenta que el proveedor de Internet es Telconet con una comunicación de Fibra óptica..

A continuación se detallan los valores del tráfico individual y total, tomados en los meses de Febrero y Marzo del 2007, las unidades de tráfico son en Kbps [23].

FACULTAD	FEBRERO	MARZO	TOTAL
SISTEMAS	345.6	276.9	311.3

Tabla 6: Tráfico promedio en la Red de la FISEI

Se realizó un esquema general de comunicaciones y conectividad de la red de datos de la FISEI.

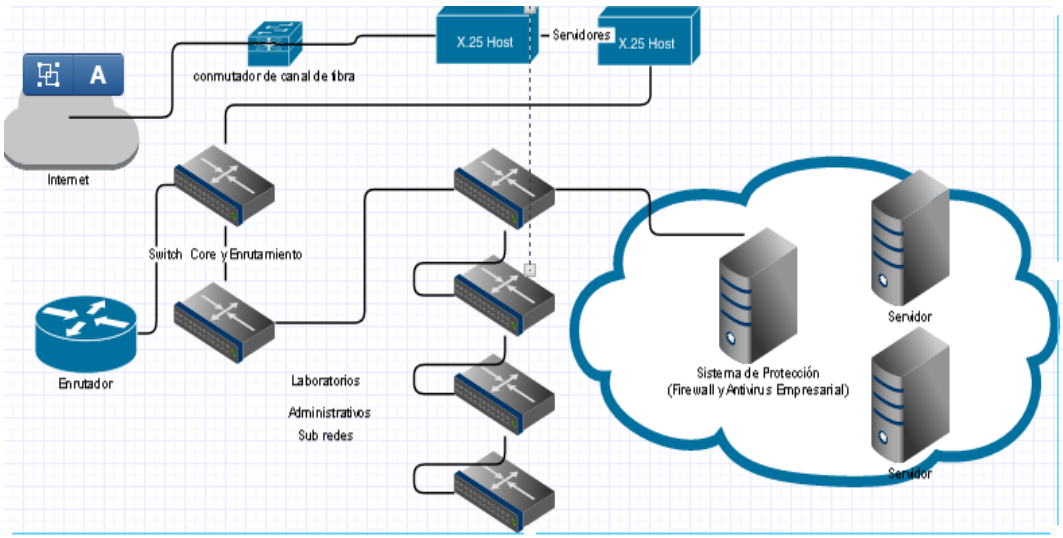


Figura 29: Esquema general de la red de la FISEI

4.4.5. Mapeo de la red de datos de la FISEI

La FISEI cuenta con un mapa de red de datos la cual fue realizada por el investigador como base fundamental para el desarrollo de la investigación.

Laboratorio 1

Cuadro del mapeo de red como se puede ver en el Anexo A.1

LABORATORIO 1					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	2	P2D14	172.21.101.11	PC01	101
2	26	P2D15	172.21.101.12	PC02	101
3	35	P2D33	172.21.101.13	PC03	101
4	11	P2D32	172.21.101.14	PC04	101
5	27	P2D17	172.21.101.15	PC05	101
6	3	P2D16	172.21.101.16	PC06	101
7	34	P2D31	172.21.101.17	PC07	101
8	10	P2D30	172.21.101.18	PC08	101
9	28	P2D19	172.21.101.19	PC09	101
10	4	P2D18	172.21.101.20	PC10	101
11	33	P2D29	172.21.101.21	PC11	101
12	9	P2D28	172.21.101.22	PC12	101
13	29	P2D21	172.21.101.23	PC13	101
14	5	P2D20	172.21.101.24	PC14	101
15	32	P2D27	172.21.101.25	PC15	101
16	8	P2D26	172.21.101.26	PC16	101
17	30	P2D23	172.21.101.27	PC17	101
18	6	P2D22	172.21.101.28	PC18	101
19	31	P2D25	172.21.101.29	PC19	101
20	7	P2D24	172.21.101.30	PC20	101
	25	P2D13			101

Tabla 7: Laboratorio 1

Laboratorio 2

Cuadro del mapeo de red como se puede ver en el Anexo A.2

Laboratorio 2

Laboratorio 3

Cuadro del mapeo de red como se puede ver en el Anexo A.3

LABORATORIO 3					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	7	P3D39	172.21.103.11	PC01	103
2	30	P3D38	172.21.103.12	PC02	103
3	25	P3D28	172.21.103.13	PC03	103
4	2	P3D29	172.21.103.14	PC04	103
5	29	P3D36	172.21.103.15	PC05	103
6	6	P3D37	172.21.103.16	PC06	103
7	26	P3D30	172.21.103.17	PC07	103
8	3	P3D31	172.21.103.18	PC08	103
9	28	P3D34	172.21.103.19	PC09	103
10	5	P3D35	172.21.103.20	PC10	103
11	27	P3D32	172.21.103.21	PC11	103
12	4	P3D33	172.21.103.22	PC12	103
	31	P3D40			103

Tabla 8: Laboratorio 3

Laboratorio 4

Cuadro del mapeo de red como se puede ver en el Anexo A.4

LABORATORIO 4					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	8	P3D15	172.21.104.11	PC01	104
2	32	P3D16	172.21.104.12	PC02	104
3	35	P3D22	172.21.104.23	PC03	104
4	37	P3D26	172.21.104.14	PC04	104
5	13	P3D25	172.21.104.15	PC05	104
6	12	P3D23	172.21.104.16	PC06	104
7	36	P3D24	172.21.104.17	PC07	104
8	9	P3D17	172.21.104.18	PC08	104
9	33	P3D18	172.21.104.19	PC09	104
10	10	P3D19	172.21.104.20	PC10	104
11	34	P3D20	172.21.104.21	PC11	104
12	11	P3D21	172.21.104.22	PC12	104
13	14	P3D27			104

Tabla 9: Laboratorio 4

Laboratorio 5

Cuadro del mapeo de red como se puede ver en el Anexo A.5

LABORATORIO 5					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	38	P3D2	172.21.105.11	PC01	105
2	15	P3D3	172.21.105.12	PC02	105
3	20	P3D13	172.21.105.13	PC03	105
4	44	P3D12	172.21.105.14	PC04	105
5	39	P3D4	172.21.105.15	PC05	105
6	16	P3D5	172.21.105.16	PC06	105
7	42	P3D10	172.21.105.17	PC07	105
8	19	P3D11	172.21.105.18	PC08	105
9	40	P3D6	172.21.105.19	PC09	105
10	17	P3D7	172.21.105.20	PC10	105
11	41	P3D8	172.21.105.21	PC11	105
12	18	P3D9	172.21.105.22	PC12	105
	43	P3D14			105

Tabla 10: Laboratorio 5

Laboratorio 6

Cuadro del mapeo de red como se puede ver en el Anexo A.6

LABORATORIO 6					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	30	P2D79	172.21.106.11	PC01	106
2	31	P2D78	172.21.106.12	PC02	106
3	32	P2D68	172.21.106.13	PC03	106
4	33	P2D69	172.21.106.14	PC04	106
5	34	P2D74	172.21.106.15	PC05	106
6	35	P2D77	172.21.106.16	PC06	106
7	36	P2D70	172.21.106.17	PC07	106
8	37	P2D71	172.21.106.18	PC08	106
9	38	P2D74	172.21.106.19	PC09	106
10	39	P2D75	172.21.106.20	PC10	106
11	40	P2D72	172.21.106.21	PC11	106
12	41	P2D73	172.21.106.22	PC12	106
13	42	P2D74	172.21.106.23	PC13	106
13	43	P2D76	172.21.106.24	PC14	106
14	44	P2D72	172.21.106.25	PC15	106
15	45	P2D73	172.21.106.26	PC16	106

Tabla 11: Laboratorio 6

Laboratorio Redes

Cuadro del mapeo de red como se puede ver en el Anexo A.7

LABORATORIO REDES					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	43	P2D79	172.21.107.11	PC01	107
2	19	P2D78	172.21.107.12	PC02	107
3	14	P2D68	172.21.107.13	PC03	107
4	38	P2D69	172.21.107.14	PC04	107
5	18	P2D76	172.21.107.15	PC05	107
6	42	P2D77	172.21.107.16	PC06	107
7	15	P2D70	172.21.107.17	PC07	107
8	39	P2D71	172.21.107.18	PC08	107
9	17	P2D74	172.21.107.19	PC09	107
10	41	P2D75	172.21.107.20	PC10	107
11	16	P2D72	172.21.107.21	PC11	107
12	40	P2D73	172.21.107.22	PC12	107

Tabla 12: Laboratorio Redes

Laboratorio de Maestrías

Cuadro del mapeo de red como se puede ver en el Anexo A.8

LABORATORIO MAESTRÍAS					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	2	P3D60	172.21.108.11	PC01-Maestrias	108
2	3	P3D61	172.21.108.12	PC02-Maestrias	108
3	20	P3D78	172.21.108.13	PC03-Maestrias	108
4	21	P3D79	172.21.108.14	PC04-Maestrias	108
5	4	P3D62	172.21.108.15	PC05-Maestrias	108
6	5	P3D63	172.21.108.16	PC06-Maestrias	108
7	18	P3D76	172.21.108.17	PC07-Maestrias	108
8	19	P3D77	172.21.108.18	PC08-Maestrias	108
9	6	P3D64	172.21.108.19	PC09-Maestrias	108
10	7	P3D65	172.21.108.20	PC10-Maestrias	108
11	16	P3D74	172.21.108.21	PC11-Maestrias	108
12	17	P3D75	172.21.108.22	PC12-Maestrias	108
13	8	P3D66	172.21.108.23	PC13-Maestrias	108
14	9	P3D67	172.21.108.24	PC14-Maestrias	108
15	14	P3D72	172.21.108.25	PC15-Maestrias	108
16	15	P3D73	172.21.108.26	PC16-Maestrias	108
17	10	P3D68	172.21.108.27	PC17-Maestrias	108
18	11	P3D69	172.21.108.28	PC18-Maestrias	108
19	12	P3D70	172.21.108.29	PC19-Maestrias	108
20	13	P3D71	172.21.108.30	PC20-Maestrias	108

Tabla 13: Laboratorio Maestrías

Laboratorio Arquitectura

Cuadro del mapeo de red como se puede ver en el Anexo A.9

LABORATORIO ARQUITECTURA		
N°	**ETIQUETA**	**VLAN**
1	P2D68	119
2	P2D69	119
3	P2D70	119
4	P2D71	119
5	P2D72	119
6	P2D73	119
7	P2D74	119
8	P2D75	119
9	P2D76	119
10	P2D77	119
11	P2D78	119
12	P2D79	119
13	P2D80	119

Tabla 14: Laboratorio Arquitectura

Laboratorio Audiovisuales

Cuadro del mapeo de red como se puede ver en el Anexo A.10

LABORATORIO AUDIOVISUALES		
N°	**ETIQUETA**	**PC**
1	P1D80	PCDocente

Tabla 15: Laboratorio Audiovisuales

Laboratorio Industrial I

Cuadro del mapeo de red como se puede ver en el Anexo A.11

LABORATORIO INDUSTRIAL 1					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	14	P1 Dato09	172.21.113.10	IND1-01	113
2	13	P1 Dato08	172.21.113.12	IND1-02	113
3	28	P1 Dato24	172.21.113.03	IND1-03	113
4	27	P1 Dato23	172.21.113.14	IND1-04	113
5	15	P1 Dato10	172.21.113.15	IND1-05	113
6	16	P1 Dato11	172.21.113.26	IND1-06	113
7	26	P1 Dato22	172.21.113.17	IND1-07	113
8	25	P1 Dato21	172.21.113.18	IND1-08	113
9	17	P1 Dato12	172.21.113.19	IND1-09	113
10	18	P1 Dato13	172.21.113.20	IND1-10	113
11	23	P1 Dato19	172.21.113.21	IND1-11	113
12	24	P1 Dato20	172.21.113.22	IND1-12	113
13	20	P1 Dato15	172.21.113.23	IND1-13	113
14	19	P1 Dato14	172.21.113.24	IND1-14	113
15	21	P1 Dato17	172.21.113.25	IND1-15	113
16	22	P1 Dato18	172.21.113.26	IND1-16	113

Tabla 16: Laboratorio Industrial 1

Laboratorio Industrial II

Cuadro del mapeo de red como se puede ver en el Anexo A.12

LABORATORIO INDUSTRIAL II					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	29	PoD19	172.21.114.11	IND2-01	114
2	30	PoD18	172.21.114.12	IND2-02	114
3	43	PoD33	172.21.114.13	IND2-03	114
4	44	PoD32	172.21.114.14	IND2-04	114
5	31	PoD21	172.21.114.15	IND2-05	114
6	32	PoD20	172.21.114.16	IND2-06	114
7	41	PoD30	172.21.114.17	IND2-07	114
8	42	PoD31	172.21.114.18	IND2-08	114
9	33	PoD22	172.21.114.19	IND2-09	114
10	34	PoD23	172.21.114.20	IND2-10	114
11	39	PoD29	172.21.114.21	IND2-11	114
12	40	PoD28	172.21.114.22	IND2-12	114
13	35	PoD25	172.21.114.23	IND2-13	114
14	36	PoD24	172.21.114.24	IND2-14	114
15	37	PoD26	172.21.114.25	IND2-15	114
16	38	PoD27	172.21.114.26	IND2-16	114
		PoD14			

Tabla 17: Laboratorio Industrial 2

Laboratorio Robótica

Cuadro del mapeo de red como se puede ver en el Anexo A.13

LABORATORIO DE ROBÓTICA					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	15	P0 Dato16	172.21.115.10	ROB01	115
2	14	P0 Dato15	172.21.115.12	ROB02	115
3	2	P0 Dato01	172.21.115.13	ROB03	115
4	7	P0 Dato07	172.21.115.14	ROB04	115
5	13	P0 Dato14	172.21.115.15	ROB05	115
6	12	P0 Dato13	172.21.115.16	ROB06	115
7	3	P0 Dato03	172.21.115.17	ROB07	115
8	4	P0 Dato04	172.21.115.18	ROB08	115
9	11	P0 Dato12	172.21.115.19	ROB09	115
10	10	P0 Dato11	172.21.115.20	ROB10	115
11	5	P0 Dato05	172.21.115.21	ROB11	115
12	6	P0 Dato06	172.21.115.22	ROB12	115
	8	P0 Dato09			115
	9	P0 Dato10			115

Tabla 18: Laboratorio Robótica

Laboratorio PLC

Cuadro del mapeo de red como se puede ver en el Anexo A.14

LABORATORIO PLC					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	7	P1 Dato02	DHCP	PLC S-01	112
2	11	P1 Dato06	DHCP	PLC S-02	112
3	12	P1 Dato07	DHCP	PLC S-03	112
4	10	P1 Dato05	DHCP	PLC S-04	112
5	9	P1 Dato04	DHCP	PLC S-05	112
6	8	P1 Dato03	DHCP	PLC S-08	112

Tabla 19: Laboratorio PLC

Laboratorio Electrónica 2

Cuadro del mapeo de red como se puede ver en el Anexo A.15

LABORATORIO DE ELECTRÓNICA 2		
N°	**ETIQUETA**	**PC**
1	P1D67	PCDocente

Tabla 20: Laboratorio Electrónica

Laboratorio CNC

Cuadro del mapeo de red como se puede ver en el Anexo A.16

LABORATORIO DE CNC		
N°	**ETIQUETA**	**PC**
1	P2D01	PC01
2	P2D02	PC02
3	P2D03	PC03
4	P2D04	PC04
5	P2D05	PC05
6	P2D06	PC06
7	P2D07	PC07

Tabla 21: Laboratorio CNC

Laboratorio de Hidráulica y Neumática

Cuadro del mapeo de red como se puede ver en el Anexo A.17

LABORATORIO DE CNC		
N°	**ETIQUETA**	**VLAN**
1	P2D08	116
2	P2D09	116
3	P2D10	116
4	P2D11	116
5	P2D12	116
6	P2D13	116
7	P2D14	116

Tabla 22: Laboratorio de Hidráulica y Neumática

Laboratorio CTT II

Cuadro del mapeo de red como se puede ver en el Anexo A.18

LABORATORIO CTT II					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	36	P1D03	DHCP	PC1-CTT2	111
2	13	P1D04	DHCP	PC2-CTT2	111
3	37	P1D05	DHCP	PC3-CTT2	111
4	14	P1D06	DHCP	PC4-CTT2	111
5	38	P1D07	DHCP	PC5-CTT2	111
6	15	P1D08	DHCP	PC6-CTT2	111
7	39	P1D09	DHCP	PC7-CTT2	111
8	16	P1D10	DHCP	PC8-CTT2	111
9	40	P1D11	DHCP	PC9-CTT2	111
10	17	P1D12	DHCP	PC10-CTT2	111
11	41	P1D13	DHCP	PC11-CTT2	111
12	18	P1D14	DHCP	PC12-CTT2	111
13	42	P1D15	DHCP	PC13-CTT2	111
14	19	P1D16	DHCP	PC14-CTT2	111
15	43	P1D17	DHCP	PC15-CTT2	111
16	20	P1D18	DHCP	PC16-CTT2	111
17	44	P1D19	DHCP	PC17-CTT2	111
18	21	P1D20	DHCP	PC18-CTT2	111
19	45	P1D21	DHCP	PC19-CTT2	111
20	22	P1D22	DHCP	PC20-CTT2	111

Tabla 23: Laboratorio CTT II

Laboratorio CTT III

Cuadro del mapeo de red como se puede ver en el Anexo A.19

LABORATORIO CTT II				
N°	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	P1D31	DHCP	PC1-CTT3	111
2	P1D30	DHCP	PC2-CTT3	111
3	P1D16	DHCP	PC3-CTT3	111
4	P1D17	DHCP	PC4-CTT3	111
5	P1D28	DHCP	PC5-CTT3	111
6	P1D29	DHCP	PC6-CTT3	111
7	P1D09	DHCP	PC7-CTT3	111
8	P1D10	DHCP	PC8-CTT3	111
9	P1D26	DHCP	PC9-CTT3	111
10	P1D27	DHCP	PC10-CTT3	111
11	P1D12	DHCP	PC11-CTT3	111
12	P1D13	DHCP	PC12-CTT3	111
13	P1D24	DHCP	PC13-CTT3	111
14	P1D25	DHCP	PC14-CTT3	111
15	P1D10	DHCP	PC15-CTT3	111
16	P1D11	DHCP	PC16-CTT3	111
17	P1D22	DHCP	PC17-CTT3	111
18	P1D23	DHCP	PC18-CTT3	111
19	P1D08	DHCP	PC19-CTT3	111
20	P1D09	DHCP	PC20-CTT3	111
21	P1D20	DHCP	PC21-CTT3	111
22	P1D21	DHCP	PC22-CTT3	111
23	P1D06	DHCP	PC23-CTT3	111
24	P1D07	DHCP	PC24-CTT3	111
25	P1D18	DHCP	PC25-CTT3	111
26	P1D19	DHCP	PC26-CTT3	111
27	P1D04	DHCP	PC27-CTT3	111
28	P1D05	DHCP	PC28-CTT3	111

Tabla 24: Laboratorio CTT III

Cooperativa UTA

Cuadro del mapeo de red como se puede ver en el Anexo A.20

COOPERATIVA UTA		
N°	**IP**	**PC**
1	DHCP	COO1
2	DHCP	COO2
3	DHCP	COO3
4	DHCP	COO4
5	DHCP	COO5

Tabla 25: Cooperativa UTA

Sala Docentes I

Cuadro del mapeo de red como se puede ver en el Anexo A.21

SALA DOCENTES I					
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**	**VLAN**
1	1	P0D01	DHCP	ING. OSWALDO PAREDES	118
2	3	P0D02	DHCP	ING. CLARA SANCHEZ	118
3	5	P0D03	DHCP	ING. JAIME REUIZ	118
4	7	P0D04	DHCP	ING. GABRIELA GALLARDO	118
5	9	P0D05	DHCP	ING. MONICA RUIZ	118
6	11	P0D06	DHCP	ING. DAVID MARTINEZ	118
7	13	P0D07	DHCP	DOCENTE	118
8	15	P0D08	DHCP	ING. HERNANDO BUENAÑO	118
9	17	P0D09	DHCP	ING. PATRICIO CORDOVA	118
10	2	P0D10	DHCP	DOCENTE	118
11	4	P0D11	DHCP	ING. FRANKLIN MAYORGA	118
12	6	P0D12	DHCP	DOCENTE	118
13	8	P0D13	DHCP	ING. OSCAR NAVARRETE	118
14	10	P0D14	DHCP	DOCENTE	118
15	12	P0D15	DHCP	ING. MARCO JURADO	118
16	14	P0D16	DHCP	ING. ANA LARREA	118
17	16	P0D17	DHCP	ING. WASHINGTON MEDINA	118

Tabla 26: Sala Docentes I

Sala Docentes II

Cuadro del mapeo de red como se puede ver en el Anexo A.22

SALA DOCENTES II				
N°	**PUERTO**	**ETIQUETA**	**IP**	**PC**
1	1	RED 3	DHCP	ING. ALEJANDRO BARBÁN
2	2	RED 2	DHCP	ING. PATRICIO GONZÁLEZ
3	3	RED 1	DHCP	ING. CARLOS NUÑEZ
4	4	RED 5	DHCP	ING. EDISSON JORDÁN
5	5	RED 4	DHCP	ING. CARMÉN BELTRAN
6	25	AP WIFI	DHCP	WIFI
7	7	RED 7	DHCP	ING. MARITZA CASTRO
8	9	RED 9	172.21.118.11	REGISTRO DOCENTE
9	24	RED 23	DHCP	ING. PAULINA AYALA
10	11	TELÉFONO	DHCP	ING. CARLOS SERRA
11	12	RED 26	DHCP	
12	13	RED 6	DHCP	ING. ALBA MIRANDA
13	14	RED 11	172.21.118.13	REGISTRO DOCENTE
14	23	RED 22	DHCP	ING. MANUEL OTORONGO
15	16	RED 15	DHCP	ING. GUSTAVO SALINAS
16	17	RED 14	DHCP	
17	18	RED 13	DHCP	ING. GEOVANNY BRITO
18	19	RED 19	DHCP	ING. SANTIAGO ALTAMIRANO
19	20	RED 27	DHCP	
20	21	RED 18	DHCP	ING. EDISON ALVAREZ
21	22	RED 16	DHCP	ING. VICTOR PEREZ
22	15	RED 12	DHCP	ING. MARCELO GARCIA
23	10	RED 10	DHCP	
24	6	RED 10	172.21.118.12	REGISTRO DOCENTE

Tabla 27: Sala Docentes II

Decanato

Cuadro del mapeo de red como se puede ver en el Anexo A.23

DECANATO			
N°	**PC**	**ETIQUETA**	**IP**
1	Decanato	P3D42	DHCP
2	Secretaria General	P3D45	DHCP
3	Secretaria Decano	P3D46	DHCP
4	Secretaria Contratos		DHCP

Tabla 28: Decanato

SUBDECANATO			
N°	**PC**	**ETIQUETA**	**IP**
1	Subdecano	P2D02	DHCP
2	Consejo Académico	P2D03	DHCP
3	Secretaria Subdecano	P2D07	DHCP
4	Secretaria Sistemas		DHCP
5	Secretaria Electrónica		DHCP
6	Coordinación Sistemas	P2D04	DHCP
7	Coordinación Electrónica	P2D06	DHCP

Tabla 29: Subdecanato

Subdecanato

Cuadro del mapeo de red como se puede ver en el Anexo A.24

Administración Redes I

Cuadro del mapeo de red como se puede ver en el Anexo A.25

Administración Redes I		
N°	**Dispositivo**	**Descripción**
1	SW Cisco SG300-52P	SW LAB1 – LAB2
2	SW Cisco SG300-52P	SW LAB3 – LAB4 -LAB5
3	SW Cisco SG300-52P	SW LAB6 – LAB REDES
4	SW Cisco SG300-52P	SW BIBLIOTECA - CTT
5	SW Cisco SG300-52P	SWITCH ENRUTAMIENTO
6	SW Cisco SG300-52P	SWITCH CORE
7	Servidor HP DL380p Gen8	ENRUTAMIENTO
8	SW Cisco SG300-52P	SWITCH WIIFI
9	SW Cisco SG300-52P	SWITCH CAMARAS
10	Servidor HP DL160G6	
11	Servidor HP DL360G5	
12	SW Catalys 2960G	
13	PC1, PC2, PC3	VLAN 120

Tabla 30: Administración Redes I

Administración Redes II

Cuadro del mapeo de red como se puede ver en el Anexo A.26

ADMINISTRACIÓN REDES II		
N°	**Dispositivo**	**Descripción**
1	SW Cisco SG300-52P	Labratorios Edificio 2
2	SW Cisco SG300-52P	Sala Docentes 2

Tabla 31: Administración Redes II

Biblioteca

Cuadro del mapeo de red como se puede ver en el Anexo A.27

BIBLIOTECA				
N°	**PUERTO**	**ETIQUETA**	**IP**	**VLAN**
20	10	P2D100	DHCP	110
16	39	P2D101	DHCP	110
17	11	P2D102	DHCP	110
7	2	P2D83	DHCP	110
6	25	P2D84	DHCP	110
11	26	P2D85	DHCP	110
9	3	P2D86	DHCP	110
8	29	P2D87	DHCP	110
10	4	P2D88	DHCP	110
18	7	P2D90	DHCP	110
3	29	P2D91	DHCP	110
2	6	P2D92	DHCP	110
19	30	P2D93	DHCP	110
13	7	P2D94	DHCP	110
12	31	P2D95	DHCP	110
5	8	P2D96	DHCP	110
4	32	P2D97	DHCP	110
1	5	P2D98	DHCP	110
14	9	P2D98	DHCP	110
15	33	P2D99	DHCP	110

Tabla 32: Biblioteca

Unidad de Investigación

Cuadro del mapeo de red como se puede ver en el Anexo A.28

UNIDAD DE INVESTIGACIÓN			
N°	**ETIQUETA**	**IP**	**PC**
1	D3P1	DHCP	
2	D8P1	DHCP	
3	D7P1	DHCP	PC4
4	D29P1	DHCP	
5	D6P1	DHCP	
6	D28P1	DHCP	
7	D13P1	DHCP	PC1
8	D35P1	DHCP	
9	D12P1	DHCP	
10	D34P1	DHCP	
11	D11P1	DHCP	PC2
12	D33P1	DHCP	
13	D10P1	DHCP	PC3
14	D32P1	DHCP	
15	D9P1	DHCP	
16	D31P1	DHCP	

Tabla 33: Unidad de Investigación

4.4.6. Equipos de red instalados

De acuerdo al esquema de comunicaciones de las figuras anteriores, se describirán los equipos de comunicaciones existentes en la red de la FISEI como se ve en la siguiente tabla:

N°	UBICACIÓN	EQUIPOS	CANTIDAD	MODELO	VLAN
1	Administración Redes Edificio1	Switch	1	Switch Catalys 2960G	
			9	Switch Cisco SG300-52P	101-102-103-104-105-106-107
		Servidor	5	Servidor HP DL380p Gen8	
				Servidor HP DL160G6	
				Servidor HP DL360G5	
				Servidor IBM	
				Servidor HP	
		Camaras	9	IP Camera Wireless/Wired Pan/Tilt	
		AP	8	AIR-CAP16021-A-K9	
		AP	1	AIR-CAP17021-A-K9	
2	Unidad Operativa de Investigación	Switch	1	Switch Cisco SG300-52P	
			2	Switch hp Procurve 2500-24	
		Servidor	4	Servidor hp Proliant DL380 Gen9	
				Servidor hp Proliant DL380e Gen8	
				Servidor hp Proliant DL380e Gen8 v2	
				Servidor hp Proliant DL160 G6	
		Router	1	Router cisco 2900 Series	
3	Laboratorio 1 2PISO E1	PC	20	QBEX	101
4	Laboratorio 2 2PISO E1	PC	20	QBEX	102
5	Laboratorio 3 3PISO E1	PC	12	ACER	103
6	Laboratorio 4 3PISO E1	PC	12	DELL	104
7	Laboratorio 5 3PISO E1	PC	12	ACER	105
8	Laboratorio 6 3PISO E1	PC	16	ACER	106
9	Laboratorio Redes 2PISO E1	PC	12	ACER	107
10	Laboratorio Maestrias 3PISO E1	PC	20	DELL	108
11	Biblioteca 2PISO E1	PC	17	QBEX	110
12	Subdecanato, Coordinacion Sistemas, Coordinacion Electrónica	PC	7	ACER, QBEX, DELL	DHCP
13	DECANATO 3PISO E1	PC	4	ACER, QBEX, DELL	DHCP
14	Coordinacion Industrial 1PISO E1	PC	2	ACER, QBEX	DHCP
15	Postgrados 3PISO E1	PC	5	ACER, QBEX, ESPIDING	DHCP
16	Docentes E1	PC	19	ACER, QBEX, DELL	DHCP
17	Unidad Operativa de Investigación 1PISO E1	PC	19	ACER, QBEX, DELL	DHCP
18	Unidad de Planificación y Evaluación (UPE) 1PISO E1	PC	2	ACER, CLON, ADIKTA	DHCP
19	CTT II	PC	18	QBEX	111
20	CTT III	PC	20	QBEX	111
21	Maestrias Edificio1 piso3	Switch	1	Switch Cisco SG300-52P	108
SUBTOTAL			279		
22	Administración Redes Edificio2	Switch	2	Switch Cisco SG300-52P	
		Camaras	8	IP Camera Wireless/Wired Pan/Tilt	
		AP	4	AIR-CAP16021-A-K9	
23	Docentes Edificio2	Switch	2	Switch Cisco SG300-52P	112-113-114-115-116
24	Laboratorio Industrial I 1PISO E2	PC	16	QBEX	113
25	Laboratorio Industrial II 1PISO E2	PC	16	ACER	114
26	Laboratorio Neumática 1PISO E2	PC	1	DELL	116
27	Laboratorio Robótica 1PISO E2	PC	12	ACER	115
28	Laboratorio PLC 1PISO E2	PC	9	ACER	112
SUBTOTAL			70		
TOTAL			349		

Tabla 34: Tabla de Equipos de red instalados

Se considerará monitorear 348 equipos bajo el siguiente detalle:

N°	EQUIPO	CANTIDAD
1	SWITCH	18
3	SERVIDORES	9
4	PC	290
5	AP	13
6	CÁMARAS	17
7	NODOS	348
TOTAL		348

Tabla 35: Equipos a ser monitorizados

4.4.7. Servicios de Red

Los servicios de red a ser monitoreados son:

- DHCP
- DNS
- SERVIDOR WEB
- APLICATIVOS INTERNOS

4.4.8. Direccionamiento IP

Se puede visualizar las direcciones ip que actualmente está configurado en la red de la FISEI.

UBICACIÓN	PC	VLAN	MÁSCARA	GATEWAY	PUNTO
LAB 1	20	101	255.255.255.0	172.21.101.1	P2D14 P2D15 P2D33 P2D32 P2D17 P2D16 P2D31 P2D30 P2D19 P2D18 P2D29 P2D28 P2D21 P2D20 P2D27 P2D26 P2D23 P2D22 P2D25 P2D24
LAB 2	20	102	255.255.255.0	172.21.102.1	P2D40 P2D39 P2D57 P2D58 P2D42 P2D41 P2D56 P2D55 P2D44 P2D43 P2D54 P2D53 P2D46 P2D45 P2D52 P2D51 P2D48 P2D47 P2D50 P2D49
LAB 3	12	103	255.255.255.0	172.21.103.1	P2D39 P2D38 P2D28 P2D29 P2D36 P2D37 P2D30 P2D31 P2D34 P2D35 P2D32 P2D33
LAB 4	12	104	255.255.255.0	172.21.104.1	P3D15 P3D16 P3D26 P3D25 P3D23 P3D24 P3D17 P3D18 P3D19 P3D20 P3D21 P3D22
LAB 5	12	105	255.255.255.0	172.21.105.1	P3D02 P3D03 P3D13 P3D12 P3D04 P3D05 P3D10 P3D11 P3D06 P3D07 P3D08 P3D09
LAB 6	16	106	255.255.255.0	172.21.106.1	P2D79 P2D78 P2D68 P2D69 P2D76 P2D77 P2D70 P2D71 P2D74 P2D75 P2D72 P2D73 P2D76 P2D77 P2D74 P2D75
LAB REDES	12	107	255.255.255.0	172.21.107.1	P2D79 P2D78 P2D68 P2D69 P2D76 P2D77 P2D70 P2D71 P2D74 P2D75 P2D72 P2D73
LAB MAESTRIAS	20	108	255.255.255.0	172.21.108.1	P2D14 P2D15 P2D33 P2D32 P2D17 P2D16 P2D31 P2D30 P2D19 P2D18 P2D29 P2D18 P2D21 P2D20 P2D27 P2D26 P2D23 P2D22 P2D25 P2D24
LAB INDUSTRIAL I	16	113	255.255.255.0	172.21.113.1	P1D09 P1D08 P1D23 P1D24 P1D10 P1D11 P1D22 P1D21 P1D12 P1D13 P1D19 P1D20 P1D14 P1D15 P1D16 P1D17
LAB INDUSTRIAL II	16	114	255.255.255.0	172.21.114.1	PoD19 PoD18 PoD33 PoD32 PoD21 PoD20 PoD30 PoD31 PoD22 PoD23 PoD29 PoD28 PoD25 PoD24 PoD26 PoD27
LAB ROBÓTICA	12	115	255.255.255.0	172.21.115.1	PoD15 PoD14 PoD1 PoD2 PoD13 PoD12 PoD3 PoD4 PoD10 PoD9 PoD6 PoD5
LAB PLC	9	112	255.255.255.0	172.21.112.1	P1D07 P1D06 P1D05 P1D04 P1D03 P1D02
LAB CTT II	18	111	255.255.255.0	172.21.111.1	P1D23 P1D22 P1D4 P1D3 P1D21 P1D20 P1D11 P1D19 P1D20 P1D13 P1D14 P1D9 P1D5 P1D6 P1D8 P1D7 P1D15 P1D16
LAB CTT III	20	111	255.255.255.0	172.21.111.1	P1D31 P1D30 P1D16 P1D17 P1D28 P1D29 P1D14 P1D15 P1D26 P1D27 P1D12 P1D13 P1D24 P1D25 P1D10 P1D11 P1D22 P1D23 P1D8 P1D9 P1D20 P1D21 P1D6 P1D7 P1D18 P1D19 P1D4 P1D5
BIBLIOTECA	17	110	255.255.255.0	172.21.110.1	P2D98 P2D92 P2D91 P2D97 P2D96 P2D84 P2D83 P2D87 P2D86 P2D88 P2D85 P2D95 P2D94 P2D98 P2D99 P2D101 P2D102 P2D90 P2D93 P2D100

Tabla 36: Tabla de direccionamiento IP

4.4.9. Resumen del análisis de la red de comunicaciones

N°		ANÁLISIS	OBSERVACIONES
		INFRAESTRUCTURA	
1	INSTALACIÓNES	FISEI, posee infraestructura propia	La Facultad de Ingeniería en Sistemas Electrónica e Industrial tiene su infraestructura propia, en la cual cuenta con acceso a las instalaciones para La implementación de soluciones.
		REDES	
2	Equipamiento	El 80% de los equipos de red es basado en tecnología CISCO	Al momento de existir algun problema en los equipos cisco de cualquier modelo, es fácil encontrar en el mercado los requerimiento de repuestos minimizando el tiempo de una paralización en la red
		Cuenta con repuesto de los equipos de red	
		ADMINISTRACIÓN Y SEGURIDAD	
3	Seguridad Física y Lógica	El acceso a las instalaciones del Data Center es restringido	Para El acceso a la administración de equipos e infraestructura de red se debe coordinar con el administrador de redes de la FISEI.
		El acceso a los equipos de la administración de redes se encuentra restingido	
		Cuentra con proxy	
4	Gestión de red	Cuenta con planes de mantenimiento	La gestión de La red de comunicaciones es realizado por el departamento de administración de redes.
		Organización de la implementación de nuevas medidas tecnológicas.	

Tabla 37: Tabla de análisis de red de comunicaciones

4.5. Determinación de las herramientas utilizadas para el monitoreo de la red.

Existe varias herramientas para solucionar el problema del monitoreo de redes de datos. Existen tanto comerciales como basadas en software libre. La selección de una herramienta depende de varias instancias, tanto económicos, de infraestructura y humanos.

1. Los recursos económicos disponibles

2. Equipos de infraestructura de la red

3. Conocimiento de los administradores en determinados sistemas operativos.

Las razones por las cuales se ha escogido las siguientes herramientas para el monitoreo de la red están basadas en cada una de las características, posibilidades y funcionalidad de cada una de ellas. Se ha creído de suma importancia establecer las siguientes herramientas de monitoreo.

4.5.1. MUNIN

Es una herramienta de monitorización de recursos en red mediante un proceso residente en el mismo que va almacenando históricamente lo que sucede y construye múltiples gráficas indicando un gran número de estadísticas lo cual nos permite observar todo lo que ocurre dentro del servidor. Esta diseñada para ser un plug and play. Munin ofrece monitoreo y servicios de alerta para los Switches, Routers, servidores, computadores, aplicaciones y servicios [24].

Características	**Estructura del Sistema Munin**
El sistema Munin cuenta con las siguientes características [25]:	Munin se divide en tres componentes principales [25]:
▪ Cuenta con una interfaz [web] que muestra la evolución histórica del uso de recursos. ▪ Monitorea el uso de recurso de cada máquina, recursos como disco, red, uso de CPU, RAM, Carga (load). ▪ Es capaz de monitorear indicadores de algunas aplicaciones como tamaño de cola de postfix, procesos de apache, consultas de mysql entre otras. ▪ Genera gráficas por día, semana, mes y año de cada uno de los indicadores. ▪ Muestra el mínimo, máximo, media y valor actual de los indicadores en cada período de tiempo. ▪ Es posible configurar umbrales de alerta para estado de advertencia y crítico.	▪ Servidor: Un demonio que corre en todas las máquinas monitoreadas, por default en el puerto 4949. Su función es configurar y llamar a los plugins. Cuando se habla de munin-node, se refiere al servidor. ▪ Plugins: Cada uno de los agentes de recolección de datos que son invocados por munin-node. Dan la información que monitorean, y son también capaces de describir su función y configuración. ▪ Cliente: Proceso que corre periódicamente (normalmente cada 5 minutos) desde un nodo central, interrogando a cada uno de los servidores munin-node, y generando las páginas Web.

Tabla 38: Características y Estructura del sistema Munin

Ventajas	Requerimientos
▪ Permite determinar con anticipación cuando un recurso estará sobre utilizado o será insuficiente. ▪ Permite monitorear errores o generar mejoras. Por ejemplo, detectar errores de red que pueden ser causados por la alta carga del servidor. ▪ Permite medir cuantitativamente el crecimiento del uso de los recursos, de esta manera es posible sustentar la compra de hardware o medir el crecimiento.	▪ Procesador: 2.33 GHz Single Core ▪ Memoria: 512 MB RAM ▪ Tarjeta gráfica: DirectX 9 compatible ▪ Disco duro: 2 GB espacio disponible ▪ DirectX 9 compatible ▪ Notas adicionales: Mouse, Keyboard

Tabla 39: Ventajas y Requerimientos del sistema Munin

4.5.2. MRTG

Es una herramienta para monitorizar la carga de tráfico en los enlaces de red. MRTG genera páginas HTML que contienen imágenes PNG que proporcionan una representación visual en vivo de este tráfico. MRTG no se limita a la supervisión del tráfico, sin embargo es posible monitorizar cualquier variable SNMP que elija. Ofrece el control de monitoreo de carga de sistemas, sesiones de login, la disponibilidad del módem e incluso permite acumular dos o más fuentes de datos en un mismo gráfico [26].

Características	Funcionalidades
MRTG utiliza SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (ruteadores o servidores), por tanto es requisito contar con al menos un sistema con SNMP funcionando y correctamente configurado. SNMP manda peticiones con dos objetos identificadores (OIDs) al equipo. Una base de control de información (MIB) controla las especificaciones de los OIDs. Después de recoger la información la manda sin procesar mediante el protocolo SNMP. MTRG graba la información en un diario del cliente. El software crea un documento HTML de los diarios, estos tienen una lista de gráficas detallando el tráfico del dispositivo. El software viene configurado para que se recopilen datos cada 5 minutos pero el tiempo puede ser modificado [17].	Las principales funcionalidades de MRTG son [17]: ▪ Monitoreo de Equipos con conexiones a redes IP ▪ Notificación de Alarmas y umbrales vía SMTP y SMS ▪ Monitoreo de Servicios de TI
La aplicación de MRTG consiste es una serie de scripts escritos en lenguaje PERL que usan el protocolo de red SNMP (Simple Network Management Protocol) para leer los contadores de trafico que están ubicados en los conmutadores (Switch) o los encaminadores (Routers) y mediante sencillos y rápidos programas escritos en lenguaje C y crea imágenes en formato PNG que representa el estado del tráfico de nuestra red. Estos gráficos los inserta en una página web que podemos consultar mediante cualquier navegador [17].	▪ Lectura de comunidades SNMP ▪ Acceso a la información de monitoreo vía Web ▪ Soporta servidores Web con Apache e Microsoft IIS ▪ Flexibilidad en la configuración del portal con desarrollo ASP y PSP ▪ Capacidad de almacenamiento de los log para históricos

Tabla 40: Características y Funcionalidades del sistemas MRTG

RRDtool MRTG

RRDTool, que proviene de Round Robin Databases, Bases de datos circulares, es un Sistema que permite almacenar y representar datos en intervalos temporales

(Ancho de banda, Temperatura, etc.). Guarda los datos en una base de datos que no crece en el tiempo y permite crear bonitas gráficas para representar los datos. RRDTOOL es una reimplementación de MRTG, un programa del mismo autor que permite tener gráficas del tráfico de datos a través de un dispositivo de red, una tarjeta de red, un Router, usando para ello el protocolo SNMP. RRDTOOL, lo que hace es aprovechar el mismo motor gráfico para implementar bases de datos Round Robin o bases de datos circulares, una vez llena toda la base de datos, los nuevos valores sobrescriben a los antiguos [27].
Con estos datos RRDtool es capaz de generar simples y complejos gráficos, altamente personalizables y visibles desde cualquier navegador web [28].

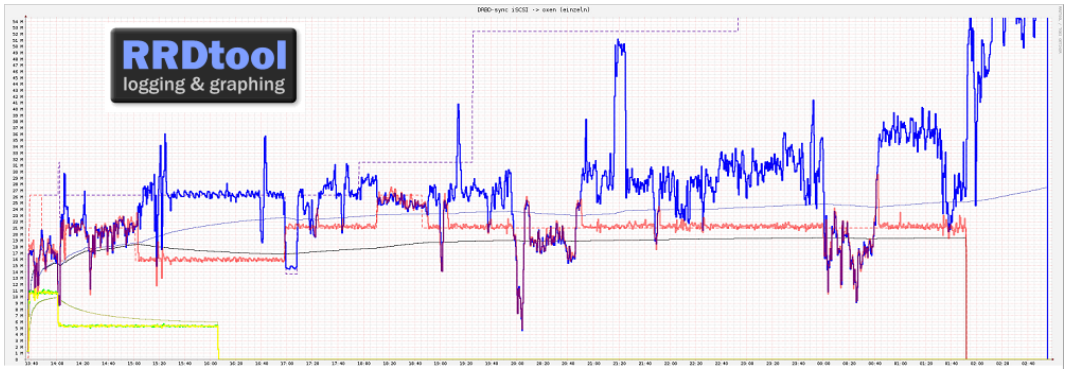


Figura 30: RRDtool

Requerimientos de Hardware en el MRTG

Se caracteriza por ser un aplicativo bastante liviano, los recursos que consume tanto en almacenamiento como en memoria de proceso son bastante bajos, podría decirse que prácticamente cualquier PC con requerimientos mínimos y una tarjeta de red está en condiciones de albergar a MRTG, en ese caso los requerimientos del hardware estarían supeditados a los necesarios para instalar la distribución de Linux [29].

REQUERIMIENTOS MÍNIMOS	RECOMENDADOS
PC Torre Estándar AT	Servidor Torre o Rack
Intel CELERON-AMD Sempron 2.0 GHz	Intel Core2Quad 2.0 GHz
256 MB RAM	1 A 2 GB RAM
1 GB de espacio libre en disco duro	10 GB de espacio libre en disco
NIC 10/100 BASE-T, dependiendo del entorno	NIC 100/1000 BASE-T

Tabla 41: Requerimientos de hardware para MRTG

Requerimientos de Software para MRTG

Por el lado del Software el sistema operativo debe estar basado en una variante de Linux Kernel 2.6.x, esto tomando en cuenta uno de los objetivos principales del proyecto, MRTG puede ser implementado sobre sistemas basados en Win32, para el presente proyecto se recomienda cualquiera de estas 4 distribuciones[29]:

- Fedora Core 7 al 11 ultimo release
- Ubuntu 7.10 Gutsy Gibbon al 9.04
- OpenSuse 10.03 al 11.1
- Centos 5 al centos 7.

4.5.3. CACTI

Es una herramienta de visualización basada en RRDtool, que emplea scripts en PHP y MySQL para almacenar información necesaria para crear gráficos del comportamiento de redes y sistemas en general. CACTI posee un sistema de autentificación que permite a los administradores crear y administrar perfiles con diferentes niveles de acceso para los usuarios [30].

Funciones	Esta aplicación cuenta con las siguientes funciones [31]:
Fuentes de datos:	Para hacer frente a la recolección de datos, se puede alimentar a Cacti con las rutas de acceso a cualquier script o comando externo, junto con todos los datos que el usuario necesitará para almacenar la base de datos MySQL. Por ejemplo, si un usuario quisiera traficar los tiempos de ping de un host, se podría crear una fuente de datos utilizando un script que hace ping a un host y devuelve su valor en mili segundos.
Gráficas:	Cacti le permite crear casi cualquier gráfico todos los tipos estándar de gráficos y funciones de consolidación, hay muchas formas de mostrar información. Junto con una "Vista de lista " estándar y un " modo de vista previa ", que se asemeja a la interfaz completa, hay una " vista de árbol ", que le permite poner los gráficos en un árbol jerárquico para los propósitos de la organización.
Gestión de usuarios:	Esto permitiría que alguien cree que algunos usuarios que pueden cambiar los parámetros del gráficas, mientras que otros sólo pueden ver las gráficas.
Plantillas:	Cacti es capaz de escalar a un gran número de fuentes de datos y gráficos mediante el uso de plantillas. Esto permite la creación de un único gráfico o plantilla de fuente de datos que define cualquier gráfico o fuente de datos asociada con él.

Tabla 42: Funciones del sistema Cacti

RRDTool

RRDTool	Es el acrónimo de Round Robin Database tool, se trata de una herramienta que trabaja con una BD que maneja Planificación Round-Robin. Esta técnica trabaja con una cantidad fija de datos y un puntero al elemento actual. El modo en que trabaja una base de datos utilizando Round Robin es el siguiente; se trata la BD como si fuera un círculo, sobrescribiendo los datos almacenados, una vez alcanzada la capacidad de la BD. La capacidad de la BD depende de la cantidad de información como historial que se quiera conservar [12].
Tipo de datos que pueden ser almacenados en una RRD	Se puede almacenar cualquier tipo de datos, siempre que se trate de una serie temporal de datos. Esto significa que se puede realizar medidas en algunos puntos de tiempo y proveer esta información a la RRDTool para que la almacene. Un concepto ligado a las RRDtool es el de SNMP, acrónimo de Simple Network Management Protocol. Este protocolo puede ser usado para realizar consultas a dispositivos acerca del valor de los contadores que ellos tienen (ej: una impresora). El valor obtenido de esos contadores es el que queremos guardar en la RRD [12].
Uso de RRDtool	Con esta herramienta a través de Cacti se puede representar gráficamente los datos almacenados en la RRD: uso de conexión a Internet, datos como temperatura, velocidad, voltaje, número de impresiones, etc. La RRD va a ser utilizada para almacenar y procesar datos recolectados vía SNMP. En definitiva, para hacer uso de una RRDtool, lo que se necesita es un sensor para medir los datos y poder alimentar al RRDtool con esos datos. Entonces, la RRDtool crea una base de datos, almacena los datos en ella, recupera estos datos y basándose en ellos, Cacti crea gráficos en formato PNG [12].
Tipo de datos que pueden ser almacenados en una RRD	Se puede almacenar cualquier tipo de datos, siempre que se trate de una serie temporal de datos. Esto significa que se tiene que poder realizar medidas en algunos puntos de tiempo y proveer esta información a la RRDTool para que la almacene. Un concepto ligado a las RRDtool es el de SNMP, acrónimo de Simple Network Management Protocol. Este protocolo puede ser usado para realizar consultas a dispositivos acerca del valor de los contadores que ellos tienen (ej: una impresora). El valor obtenido de esos contadores es el que queremos guardar en la RRD [12].
Uso de RRDtool	Con esta herramienta a través de Cacti se puede representar gráficamente los datos almacenados en la RRD: uso de conexión a internet, datos como temperatura, velocidad, voltaje, número de impresiones, etc. La RRD va a ser utilizada para almacenar y procesar datos recolectados vía SNMP. En definitiva, para hacer uso de una RRDtool, lo que se necesita es un sensor para medir los datos y poder alimentar al RRDtool con esos datos. Entonces, la RRDtool crea una base de datos, almacena los datos en ella, recupera estos datos y basándose en ellos, Cacti crea gráficos en formato PNG [12].

Tabla 43: RRDTool

Características de CACTI

Cacti cuenta con las siguientes características:

Fuente de datos	Para manejar la recopilación de datos, se le puede pasar a Cacti la ruta a cualquier script o comando junto con cualquier dato que el usuario necesitara ingresar; Cacti reunirá estos datos, introduciendo este trabajo en el cron (para el caso de un sistema operativo Linux) y cargará los datos en la BD MySQL y los archivos de Planificación Round-robin que deba actualizar [32].
Gráficos	Una vez que una o más fuentes de datos son definidas, una gráfica de RRDtool puede ser creada usando los datos obtenidos. Cacti permite crear prácticamente cualquier gráfica, utilizando todos los estándares de tipos de gráficas de RRDtool y funciones de consolidación. No sólo se puede crear gráficos basados en la RRDtool, sino que también hay varias formas de mostrarlas. Junto con una "lista de vistas" estándar y una "vista preliminar", también existe una "vista en árbol", la cual permite colocar gráficos un árbol jerárquico, para propósitos organizacionales [32].
Manejo de Usuarios	Dadas las muchas funciones que ofrece Cacti, la herramienta cuenta con la funcionalidad de manejo de usuarios embebida, para así hacer posible agregar un usuario y dar permisos a ciertas áreas de Cacti. Esto permite tener usuarios que puedan cambiar parámetros de un gráfico, mientras que otros sólo pueden ver los gráficos. Asimismo, cada usuario mantiene su propia configuración de vista de gráficos [32].
Plantillas	Cacti puede escalar a un gran número de fuentes de datos y gráficos a través de plantillas. Esto permite la creación de una única plantilla de gráficos o fuente de datos, la cual define cualquier gráfico o fuente de datos asociada con esta plantilla. Las plantillas de hosts permiten definir las capacidades de un host, así Cacti puede utilizar esta información a la hora de agregar un nuevo host [32].

Tabla 44: Características de CACTI

Requisitos de Software y Hardware

Para la instalación de Cacti se necesita de algunas aplicaciones que tienen que estar funcionando en el software y en hardware tiene que cumplir con los siguientes requerimientos:

Software	Hardware
RRDTool 1.0.49 o 1.2.x o superior MySQL 4.1.x o 5.x o superior PHP 4.3.6 o superior, 5.x más recomendable para funciones avanzadas Un Servidor Web ejemplo. Apache o IIS	▪ Memoria RAM: 2 Gbps (mínimo, sin embargo con valores inferiores CACTI funciona) ▪ Espacio en disco duro: 20 GB (mínimo) – 40 GB (recomendado) ▪ La Plataforma más estable para la instalación de CACTI, es CENTOS (Community ENTerprise Operating System) ya que es una distribución LINUX y es aprueba de errores, aunque CACTI soporta multiplataforma[32].

Tabla 45: Requisitos de Software y Hardware del sistemas Cacti

4.5.4. Topología del sistema de monitoreo

El sistema radica en un servidor que realiza las solicitudes mediante el SNMP que enviá información dirigido a los dispositivos de red.

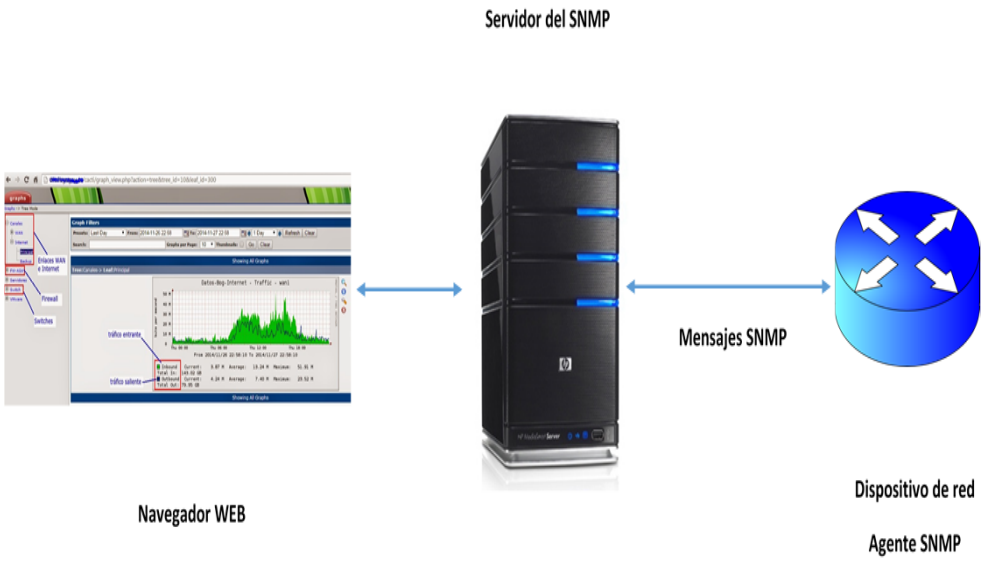


Figura 31: Topología SNMP

Puede ser que el dispositivo envié mensajes trap al servidor SNMP anunciando con alarmas lo que esta sucediendo en el monitoreo de red.

Figura 32: Mensajes trap

En este trabajo se hará énfasis en 3 herramientas de monitoreo:

4.5.5. Cisco SG300-52 52-Port Gigabit Managed Switch

Figura 33: Switch SG300-52 52-Port Gigabit Managed Switch

El Switch Cisco SG300-52 52-Port es un Switch Ethernet administrado de configuración fija, es el modelo de 52 puertos con conectividad Gigabit Ethernet (10/100/1000) y 2 puertos SFP, admite funciones de red y de administración de seguridad avanzadas para utilizar equipos de tecnologías de voz y datos, permite administrar un sistemas de seguridad y conectividad optima para toda clase de equipos de clase empresarial.

4.5.6. Cisco Catalyst 2960G-8TC-L

Figura 34: Switch Cisco Catalyst 2960G-8TC-L

El Switch Cisco Catalyst 2960G-8TC-L 10/100 + 1 SFP es un Switch Ethernet administrado de configuración fija, es el modelo de 8 puertos de conmutación RJ-45 Ethernet y 2 puertos con conectividad Gigabit Ethernet, que brindan un nivel óptimo de flexibilidad, posee un sistema de seguridad avanzada protegiendo la información de usuarios no autorizados y consiguiendo un funcionamiento ininterrumpido.

4.5.7. VLANS establecidas en los Switch cisco

Las VLANS establecidas en los Switch cisco es para cada laboratorio o sección administrativa de la facultad.

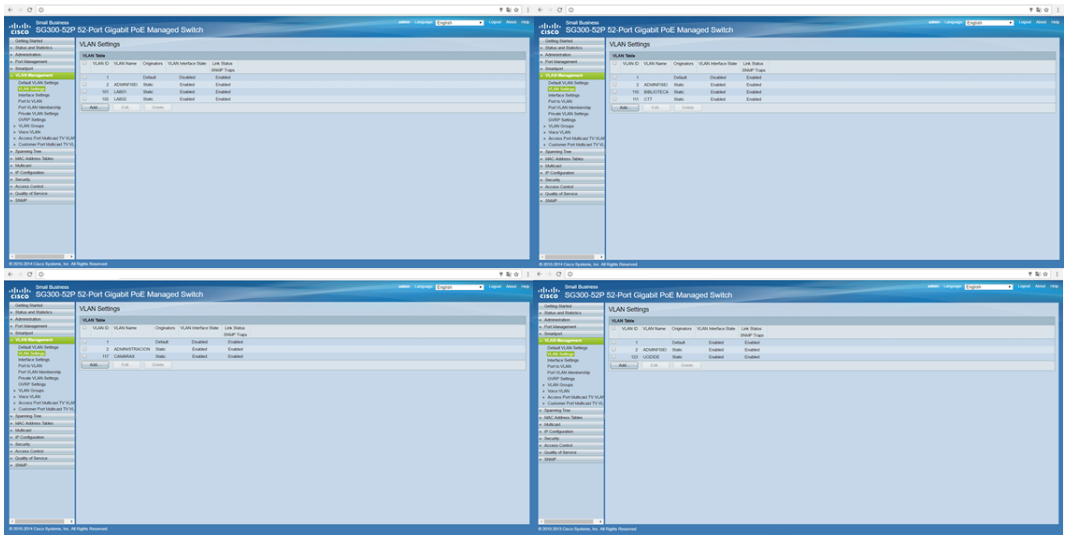


Figura 35: VLANS de los Switch cisco SG300-52 52-Port

4.5.8. Configuración del agente SNMP en los Switch Cisco

A continuación se observa la configuración del SNMP en el cual soporta versiones v1,2,3, por lo cual en estos equipos se configuró SNMP v1.
Primero para configurar la comunidad es necesario establecer el grupo colocando el nombre y el modelo de seguridad.

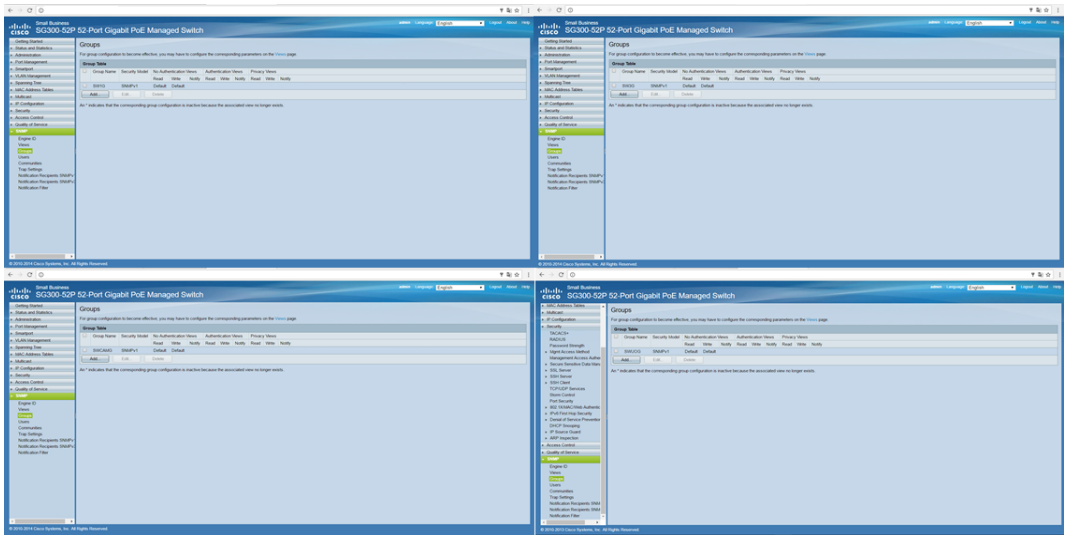


Figura 36: Configuración del Grupo en Switch

Luego de la configuración de grupos se establece la comunidad en SNMP/Communities, para este equipo se seleccionó IP Versión 4, en IP Addres se colocó la IP del servidor a monitorear, Community String - Comunidad se configuró la comunidad que también se usará en la configuración de adición del Host en sistemas de monitoreo de red.

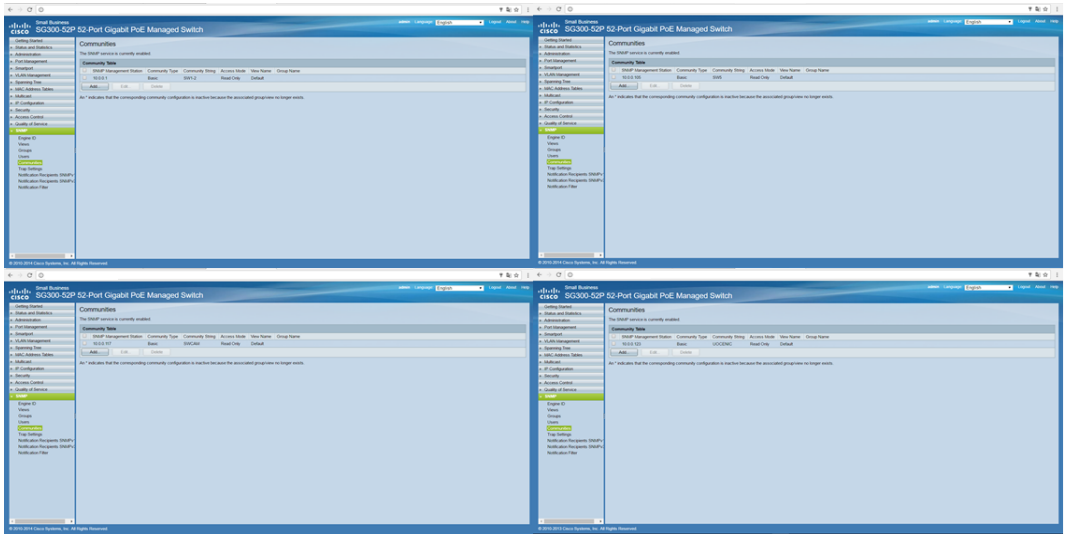


Figura 37: Configuración SNMP en los equipos Cisco SG300-52 52-Port

Se habilita el servicio SNMP en los equipos ya que por defectos están deshabilitados, se guarda los cambios y se reinicia el equipo.

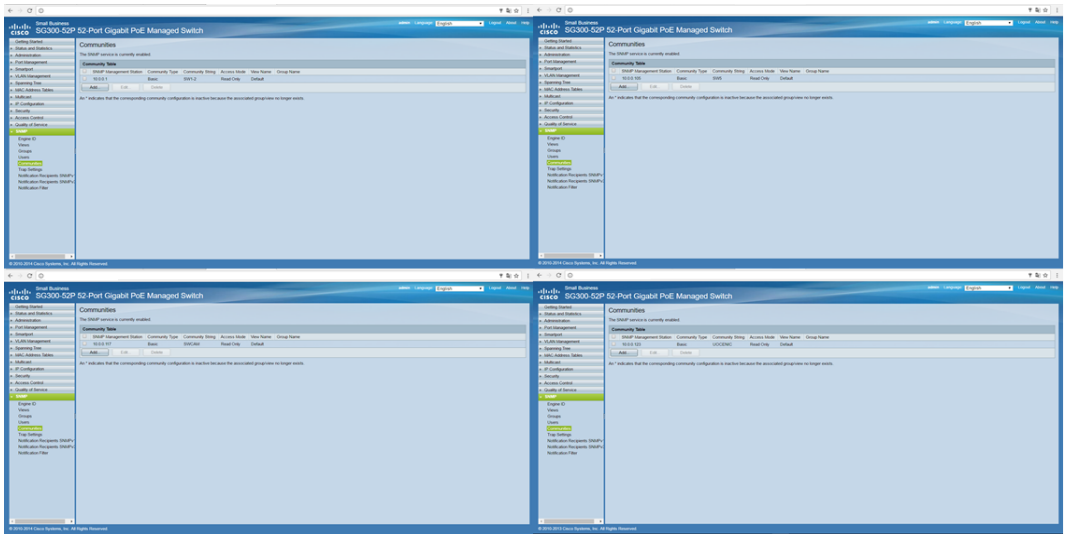


Figura 38: Habilitación del servicio SNMP en los equipos Cisco SG300-52 52-Port

4.5.9. Instalación de Network Monitoring Tool (MUNIN)

Figura 39: MUNIN

En la instalación de Munin se necesita de un repositorio EPEL como se ve a continuación.

- http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
- rpm -ivh EPEL-release-6-8.noarch.rpm

A continuación, se realizó una actualización del sistema para asegurarse que el repositorio EPEL se cargue efectivamente

- yum -y update

Munin necesita de un servidor web para mostrar las estadísticas registradas como Apache o Nginx.

- yum install httpd

Una vez instalado Apache se inicia y se activa los servicios durante el inicio del sistema.

- service httpd start
- chkconfig --level 35 httpd on

Luego de haber instalado apache, se instala munin y munin-node como se muestra a continuación

- yum -y instalar munin munin- nodo

En la instalación de munin se crean los siguientes directorios:

- /etc/munin/munin.conf: es un archivo maestro de configuración Munin.
- /etc/cron.d/munin: es un archivo cron Munin.

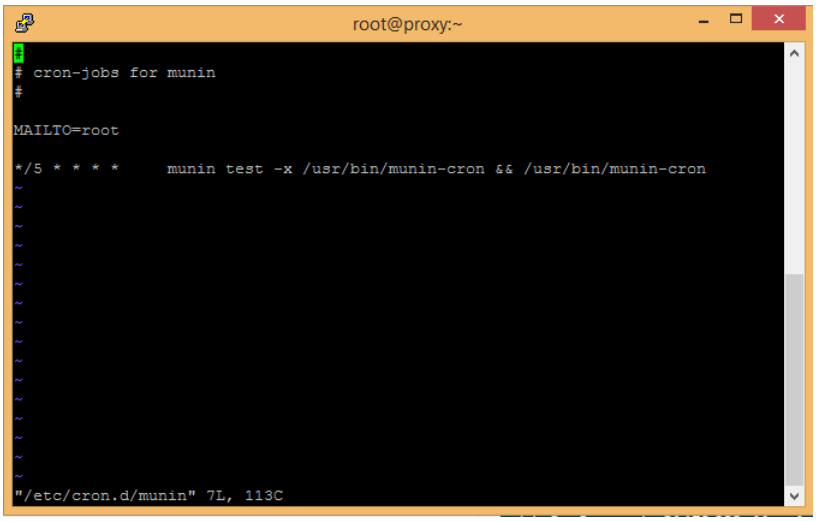


Figura 40: Archivo cron Munin

- /etc/httpd/conf.d/munin.conf: es un archivo de configuración Apache Munin.

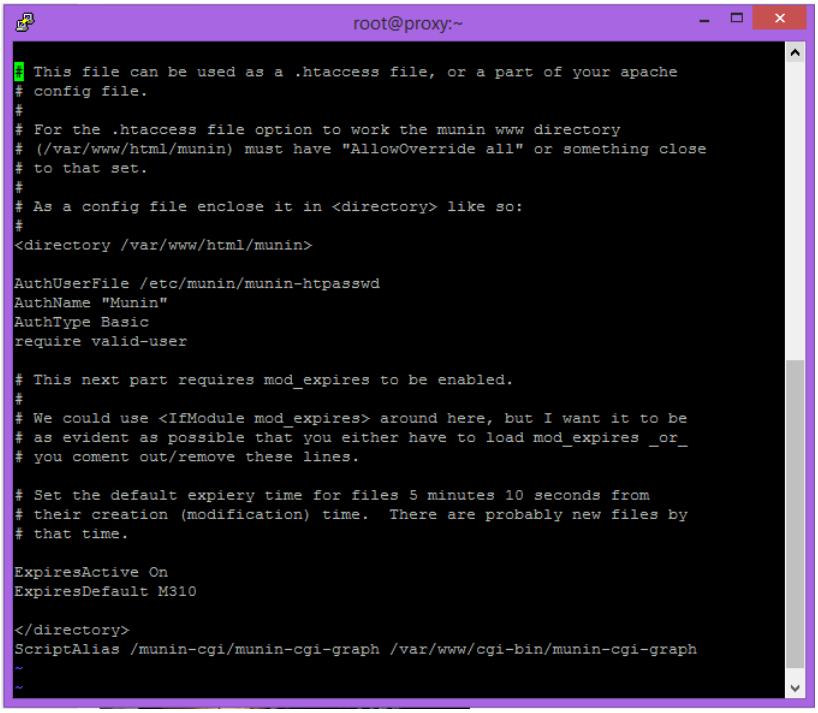


Figura 41: Archivo de configuración Apache MUNIN

- /var/log/munin: son los directorios de registro Munin.

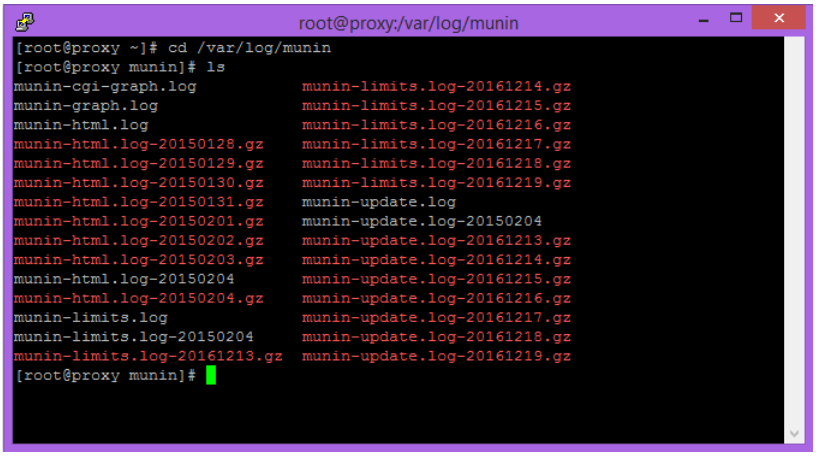


Figura 42: Registro de directorios

- /var/www/html/munin: es el directorio de registro web Munin.

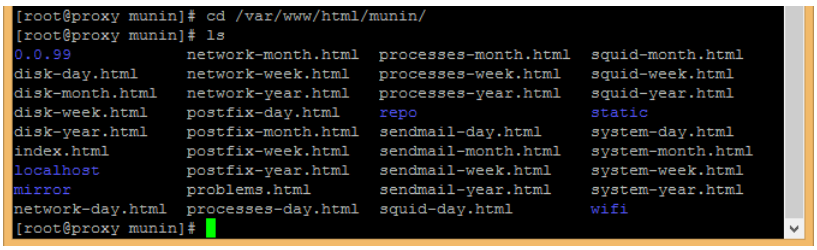


Figura 43: Registro de directorios web

- /etc/munin/munin-node.conf: es el archivo de configuración maestro Munin Nodo.

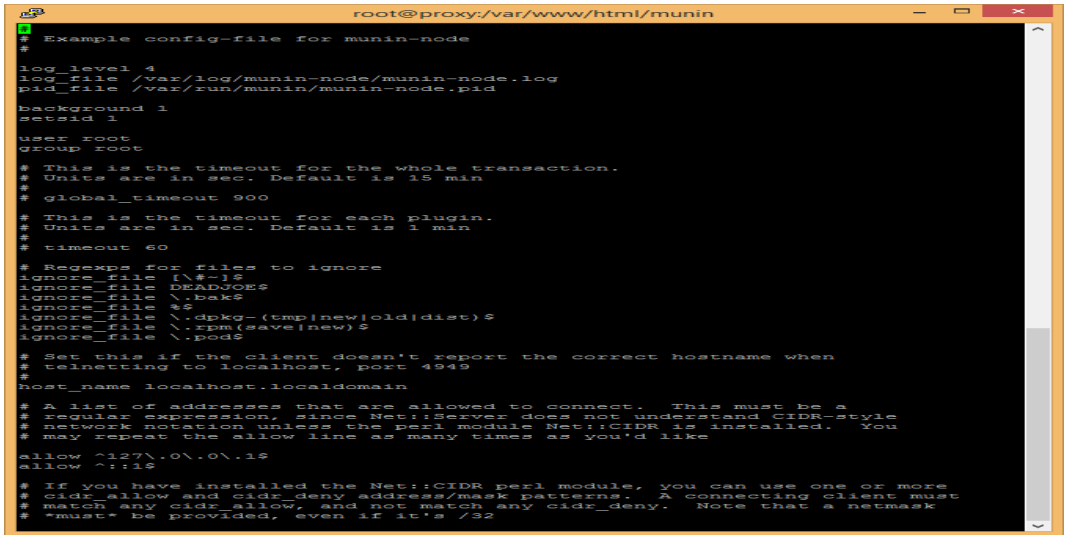


Figura 44: Archivo de configuración maestra Munin nodo

En este paso siguiente se abre el archivo de configuración /etc/munin/munin.conf y se realizar los siguientes cambios reemplazando [munin.tecmint.com] por [el nombre del servidor].

Figura 45: Archivo de configuración munin.conf

A continuación se procede a proteger con usuarios y contraseñas estáticas Munin utilizando el módulo básico de autenticación Apache.

- htpasswd /etc/munin/munin-htpasswd admin

```
[root@tecmint ~]# htpasswd /etc/munin/munin-htpasswd admin
New password:
Re-type new password:
Adding password for user admin
[root@tecmint ~]# _
```

Figura 46: Contraseña de Munin

Se reinicia Munin permitiendo que se inicie automáticamente.

- service munin-node start
- chkconfig --level 35 munin-node on

Para ver la salida de gráficos se procede abrir el navegador introduciendo las credenciales de acceso, caso contrario se cambia de usuario y contraseña y se reinicia Apache.

- /etc/httpd/conf.d/munin.conf

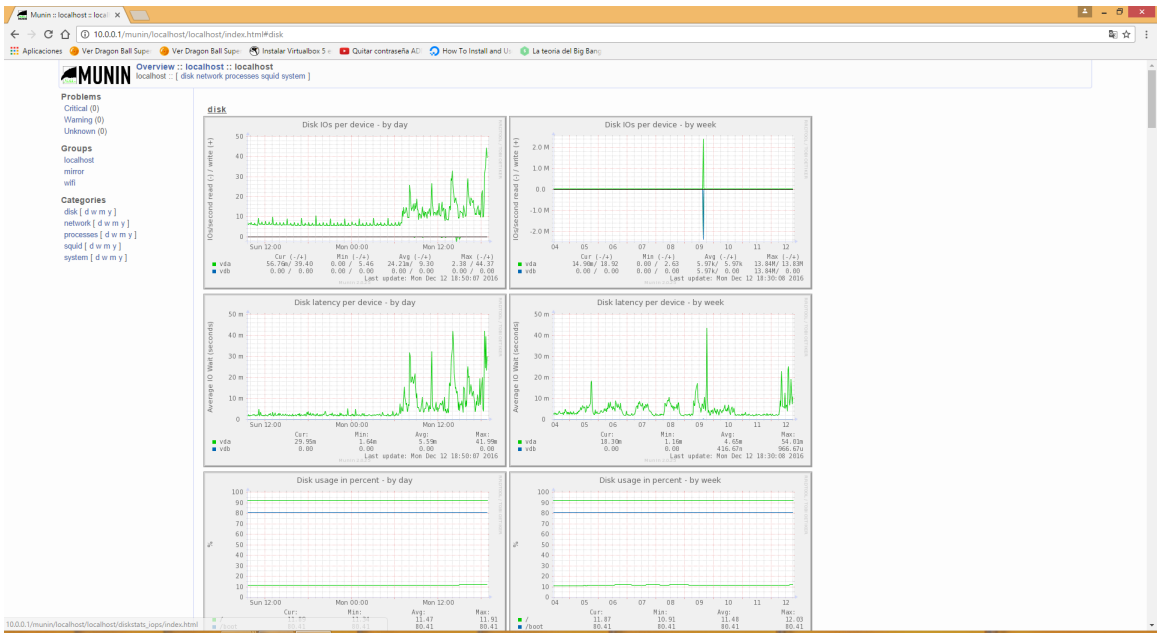


Figura 47: Gráficas de munin

4.5.10. Instalación de Multi Router Traffic Grapher (MRTG) en centos 6.5

Figura 48: MRTG

Requisitos para la instalación de MRTG:

- Instalación y configuración de httpd
- Instalación y configuración de SNMP
- Instalación y configuración de MRTG

4.5.11. Instalación de SNMP, MRTG

Mrtg utiliza SNMP (Simple Network Management Protocol o Protocolo Simple de administración de red) que recolecta la información del tráfico de un determinado dispositivo, por lo tanto es necesario supervisar su configuración correctamente. Para la instalación se utilizó los siguiente comandos.

- yum -y install net-snmp net-snmp-utils mrtg

El SNMP se ha evidenciado que requiere la agregación de las siguientes lineas para su configuración en el siguiente archivo.

- vi /etc/snmp/snmpd.conf

Se agrega el nombre del grupo, el modelo y el nombre de la seguridad

Figura 49: Archivo snmp.conf Grupo, Modelo y Nombre

Luego en la linea 75, 76 se descomenta y se cambia el nombre, la sección en la cual va la ip del equipo a monitorear y la comunidad.

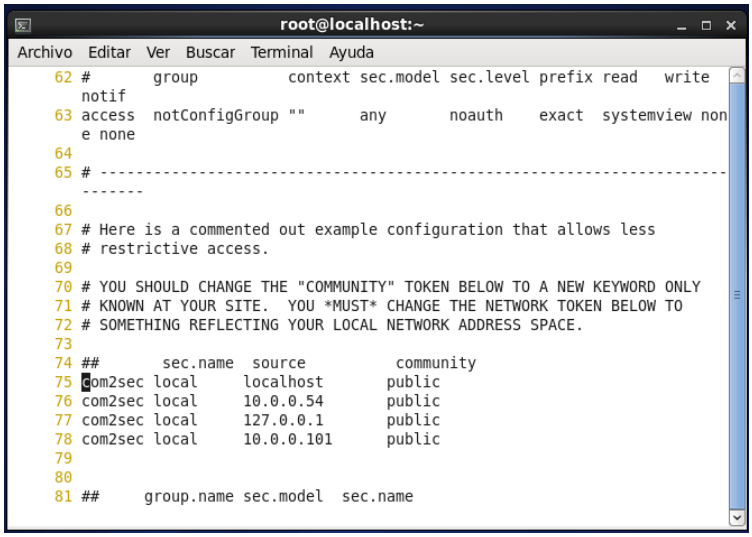


Figura 50: Archivo snmp.conf configuración de la comunidad

A continuación se descomenta las lineas 83, 84, 85, 95 y en la linea 104 se agrega “all”, “none”, “none”, de igual forma en la linea 105 se descomenta y se agrega “all”, “all”, “all” como se ve en la imagen a continuación.

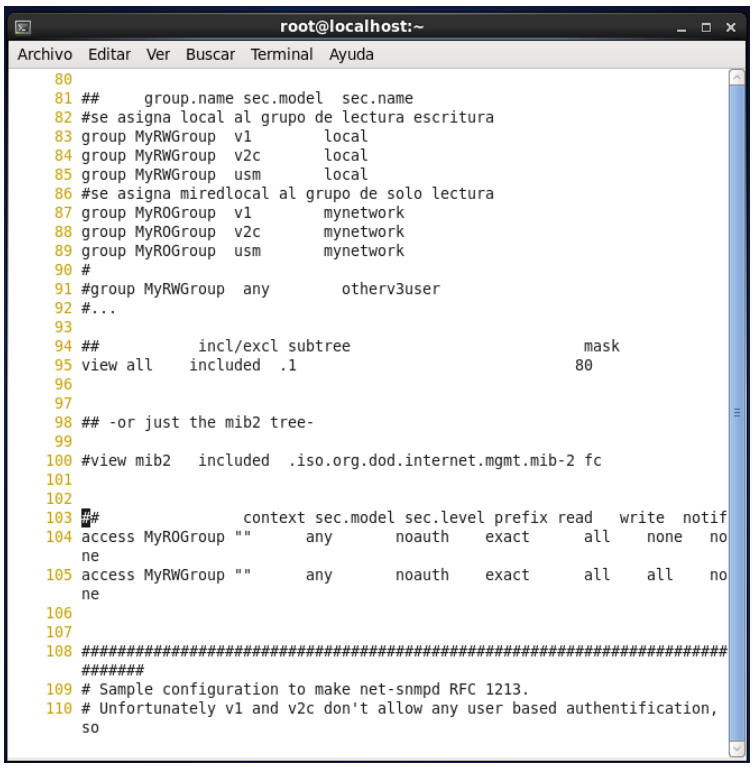


Figura 51: Archivo snmp.conf lectura y escritura de prefijos

A hora se inicia el snmpd con el siguiente comando

- /etc/rc.d/init.d/snmpd start
- chkconfig snmpd on.

A continuación se muestrar el estado en el cual se reemplazar el nombre de "Serverworld" por su comunidad.

- snmpwalk -v 1 -c public localhost IP-MIB::ipAdIntIfIndex

Seguidamente el mrtg necesita de un archivo de configuración, que se realiza con el comando: cfgmaker en el cual lleva de parámetros la clave de la comunidad (pública o privada) y la ip del equipo a monitorear:

- cfgmaker --ifref=descr --ifdesc=descr public@10.0.0.101 > /etc/mrtg/mrtg.cfg

Configuración de MRTG

- vi /etc/mrtg/mrtg.cfg

Se modifico las lineas 8 agregando WorkDir: /var/www/mrtg, descomentamos la linea 16 Options[_]: growright, bits, en la linea 73 se asegúra de que las líneas no se hayan comentado.

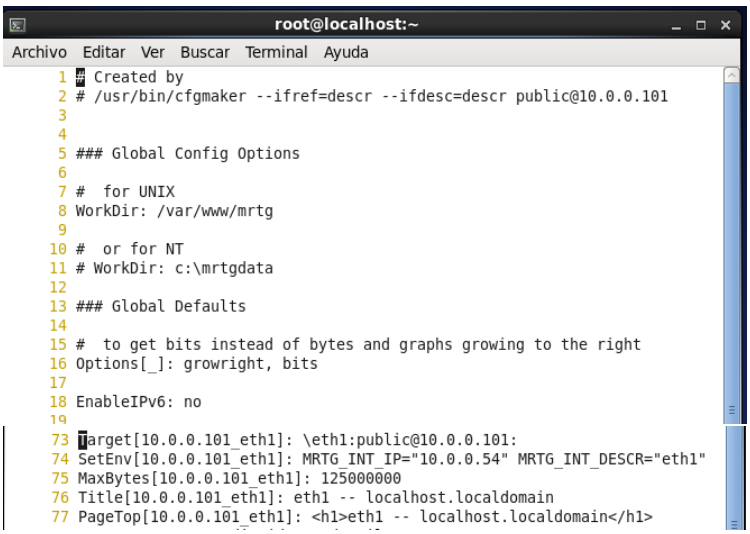


Figura 52: Archivo mrtg.cfg

Consecutivamente se genera el archivo index y luego se realiza automáticamente la actualización por cron

- indexmaker --columns=1 /etc/mrtg/mrtg.cfg > /var/www/mrtg/index.html
- cat /etc/cron.d/mrtg

Se configuro el archivo httpd para porder acceder al MRTG

- vi /etc/httpd/conf.d/mrtg.conf

En la linea 11 se agrega los siguientes permisos para acceder.

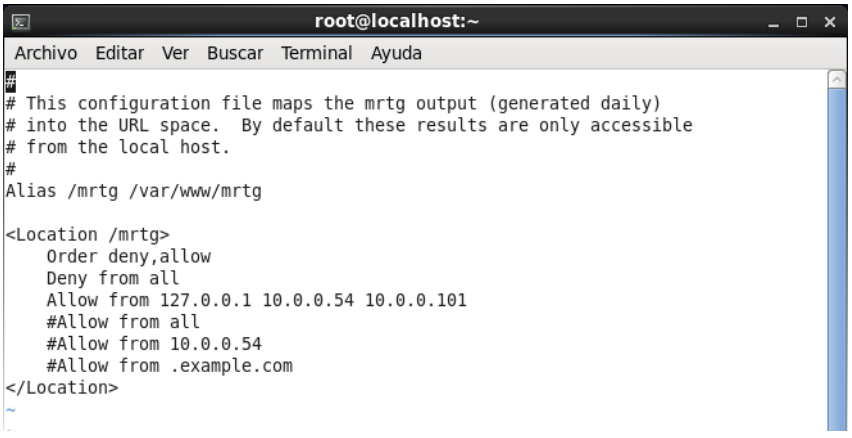


Figura 53: Configuración del Archivo mrtg.conf “permisos”

Terminando la instalación se accede a la siguiente dirección en el navegador.

- “http://10.0.x.x/mrtg”.

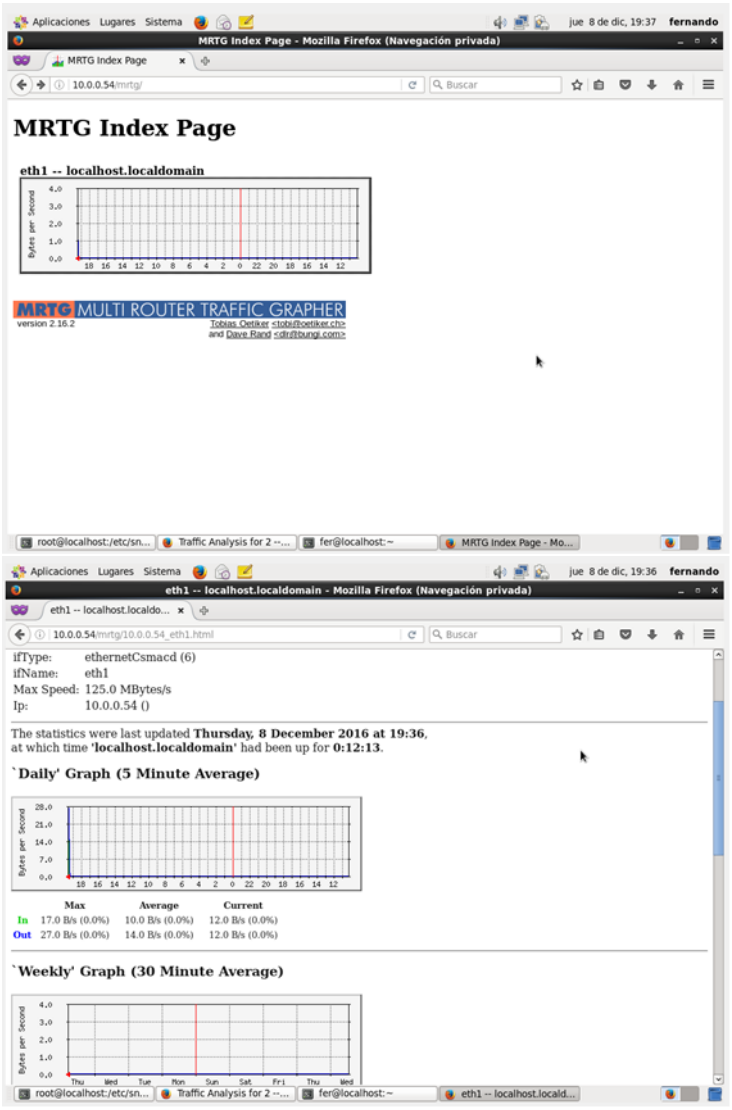


Figura 54: Gráficas MRTG

4.5.12. Instalación de CACTI versión 0.8.8 en centos 6.5

Figura 55: CACTI

Se instaló las siguientes dependencias:

- # yum install httpd httpd-devel
- # yum install mysql mysql-server

Luego se instaló MariaDB que es una bifurcación desarrollada por la comunidad del proyecto de base de datos MySQL.

- # yum install mariadb-server -y

Se realizó la instalación de PHP

- yum install php-mysql php-pear php-common php-gd php-devel php php-mbsstring php-cli

Acontinuación de realizó la instalación de php-snmp y net-snmp

- # yum install php-snmp
- # yum install net-snmp-utils net-snmp-libs

Instalación de RRDTool para representar gráficamente los datos almacenados en la RRD

- # yum install rrdtool

Una vez instalado todos los requerimientos se inician los servicios de cada uno como se muestra a continuación.

- # service httpd start
- # service mysqld start
- # service snmpd start

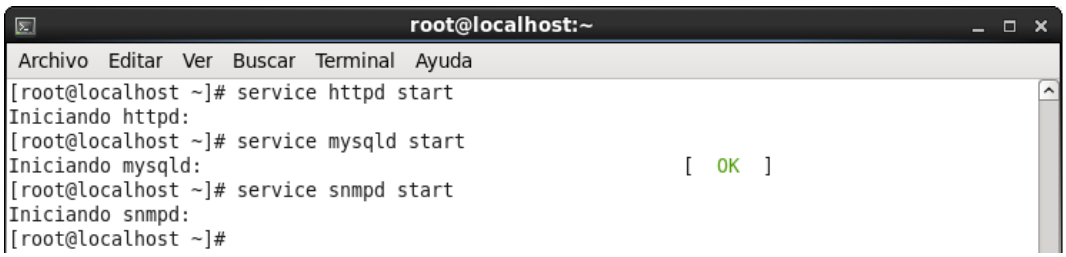


Figura 56: Inicialización de Servicios

Se configuró Apache, MySQL and SNMP para iniciar el arranque.

- # /sbin/chkconfig –levels 345 httpd on
- # /sbin/chkconfig –levels 345 mysqld on
- # /sbin/chkconfig –levels 345 snmp on

Para la instalación de cacti es necesario instalar y habilitar el repositorio EPEL.

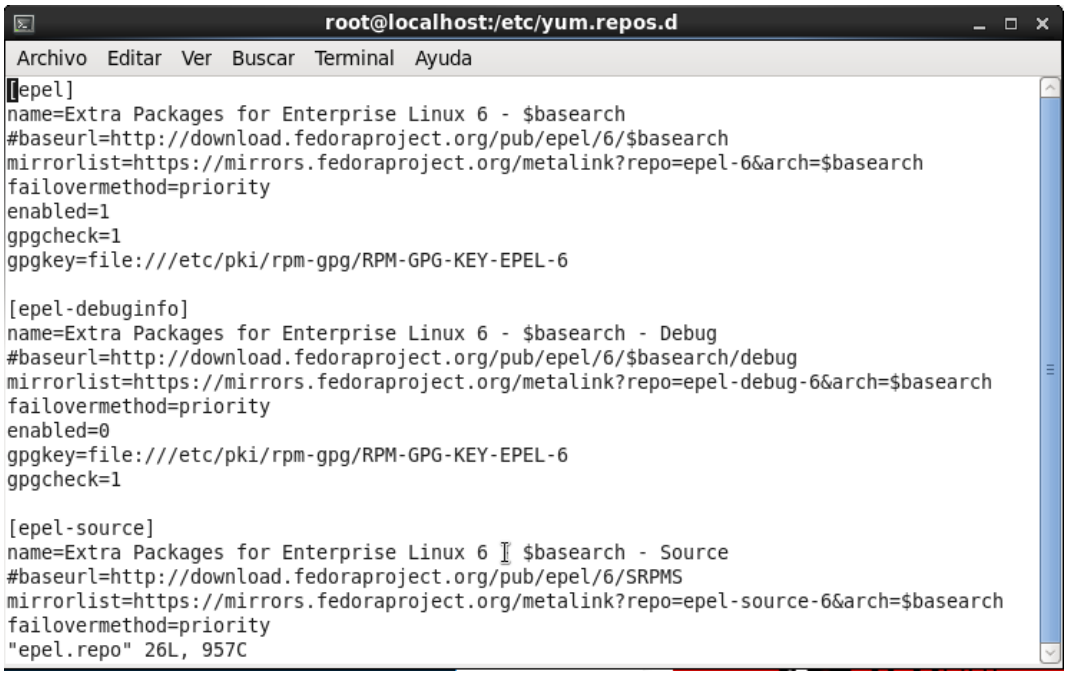


Figura 57: Repositorios EPEL

Una vez habilitado el repositorio se instaló la aplicación Cacti.

- # yum install cacti

Para la instalación de Cacti se configuró el servidor MySQL, para lo cual se estableció una contraseña y luego se crearía la base de datos Cacti con el usuario Cactus.

- # mysqladmin -u root password [Contraseña]

A continuación se instala tablas de Cacti a MySQL en la cual se busca la dirección con el siguiente comando

- rpm -ql cacti | grep cacti.sql

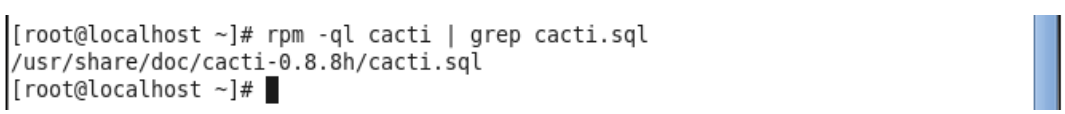


Figura 58: Comando para buscar la ruta de la base de datos

Encontrado la ubicación del archivo Cacti.sql se instala las tablas y se coloca la contraseña del usuario Cacti.

- mysql -u cacti -p cacti < /usr/share/doc/cacti-0.8.8b/cacti.sql

A continuación se habre el archivo /etc/cacti/db.php con cualquier editor y se realiza los siguientes cambios.

- # vi /etc/cacti/db.php

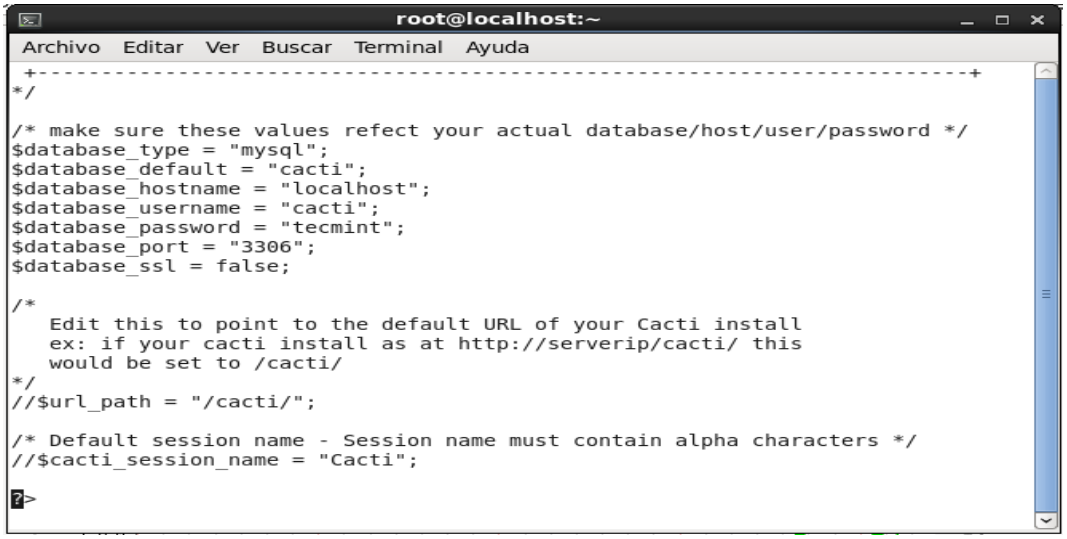


Figura 59: Configuración Mysql para Cacti

Configuración de Firewall for Cacti

- # iptable -A INPUT -p udp -m state –state NEW –dport 80 -j ACCEPT
- # iptable -A INPUT -p tcp -m state –state NEW –dport 80 -j ACCEPT
- # service iptables save

Configuración de apache server para la instalación de Cacti
En el archivo /etc/httpd/conf.d/cacti.conf se necesita habilitar los accesos a Cacti para la red local o para la ip configurada.

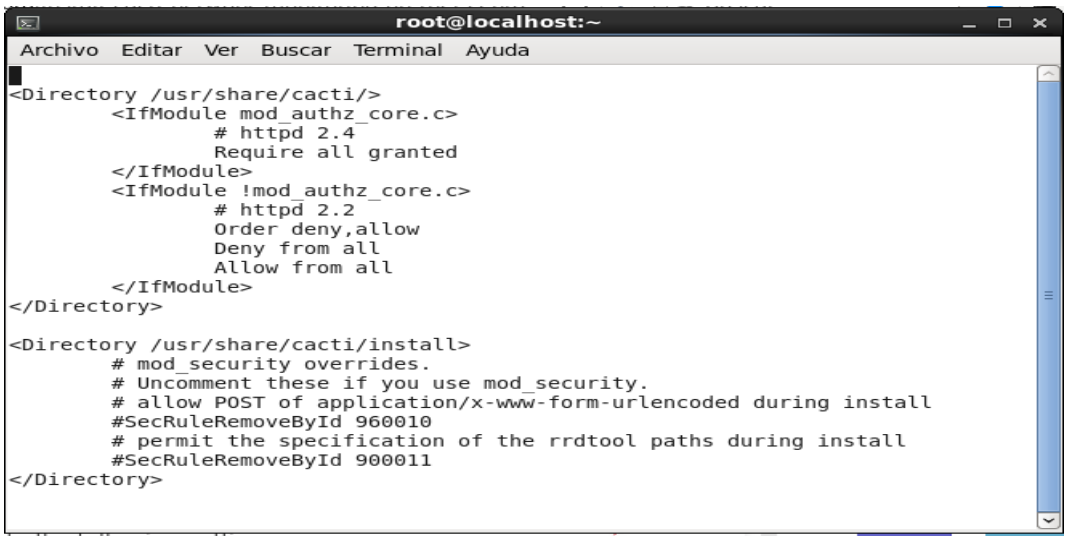


Figura 60: Accesos para habilitar Cacti

Finalmente se reinició el servicio Apache

- service httpd restart

En el archivo /etc/cron.d/cacti se descomenta las siguientes líneas
El scrip poller.php se ejecuta cada 5 minutos y recoge datos de host conocidos que es utilizado por la aplicación Cacti para mostrar gráficos.

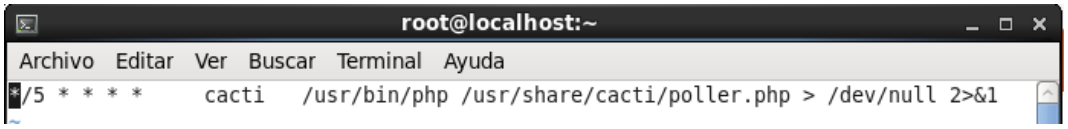


Figura 61: Archivo cron.d

Por último, con el siguiente url: http://172.21.123.235(ip del servidor)/cacti/ se configura la instalación como se ve acontinuación.

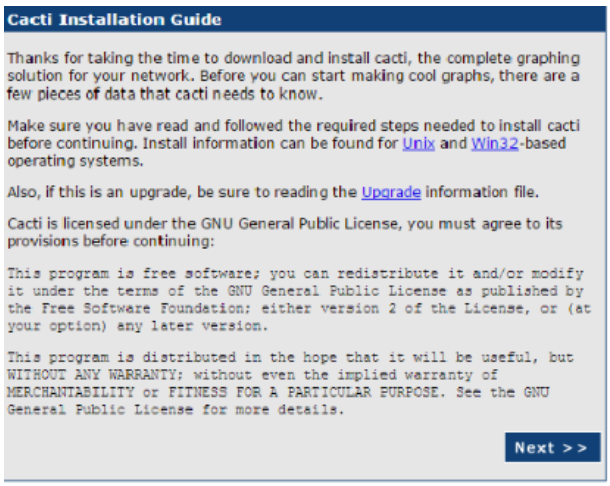


Figura 62: Inicio de configuración de CACTI

Aquí se elige el tipo de instalación “Nueva Instalación”

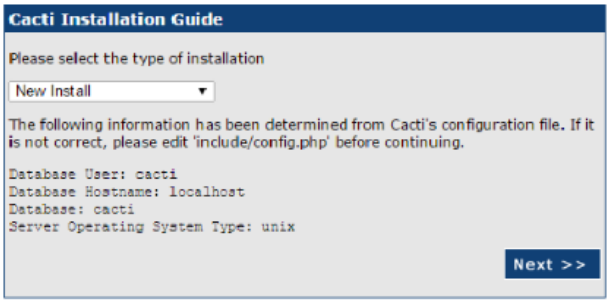


Figura 63: Tipo de instalación

Se asegura de que los valores siguientes son correctos antes de continuar y finalizar.

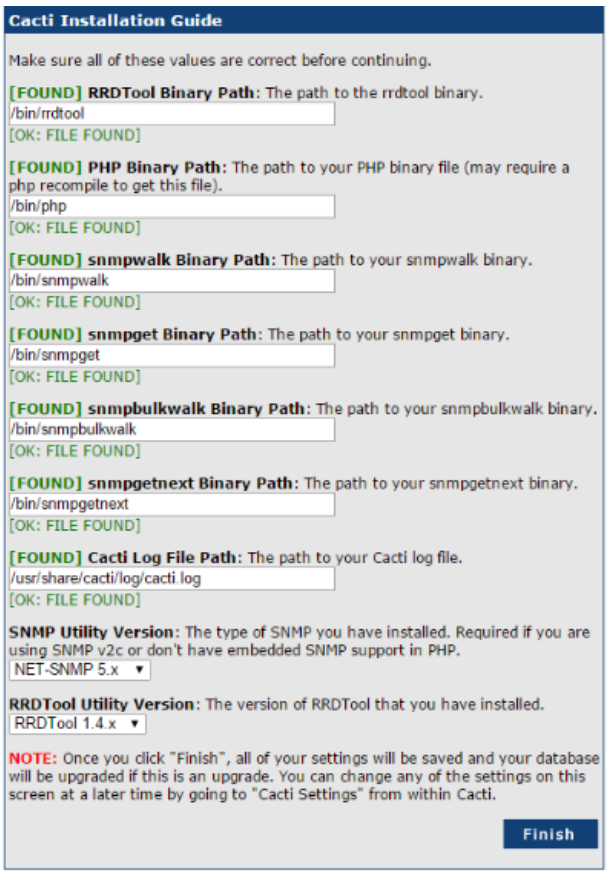


Figura 64: Guia de instalación de CACTI

Pantalla de conexión, de introducción de usuario y contraseña.

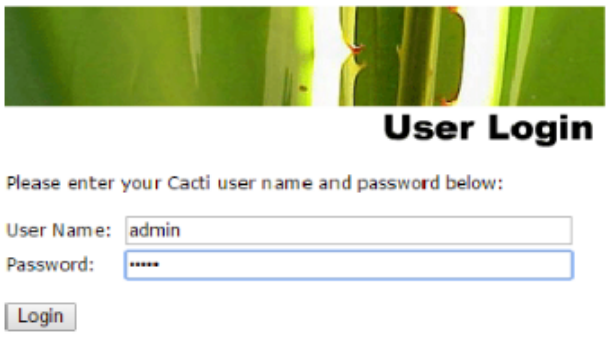


Figura 65: Loguin de Usuarios

Por consiguiente la visualización de la consola de Cacti.

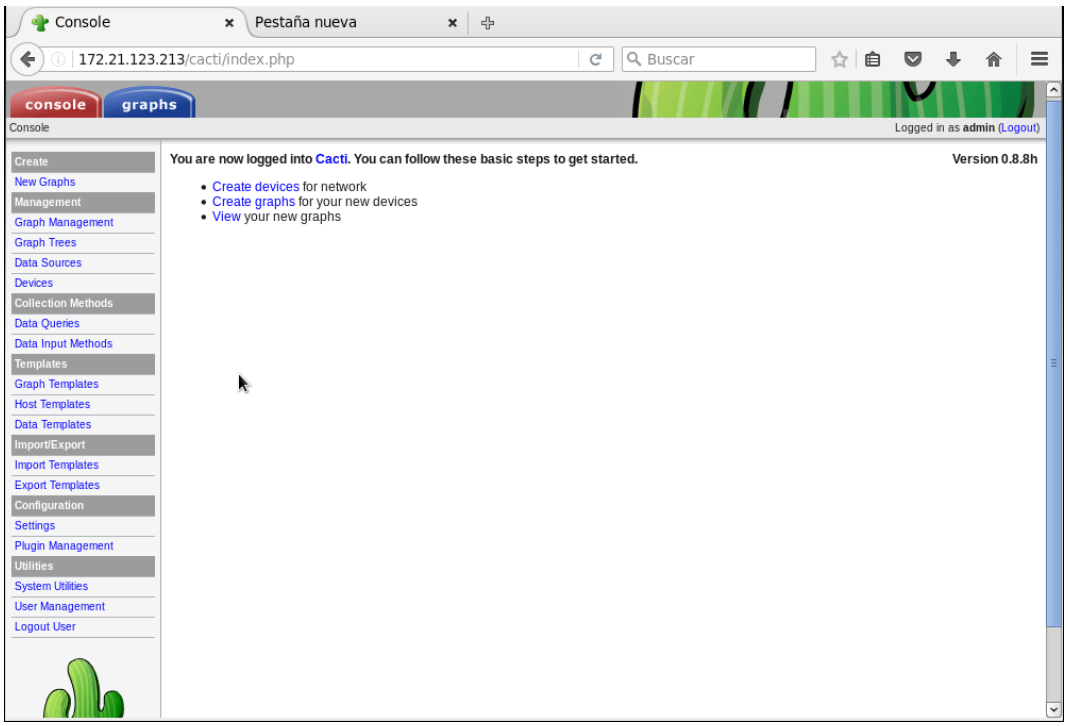


Figura 66: Pantalla de consola y graficas de CACTI

Para la configuración y la union de los switch y el servidor cacti se realiza de la siguiente manera:

- Se agrega un nuevo dispositivo.

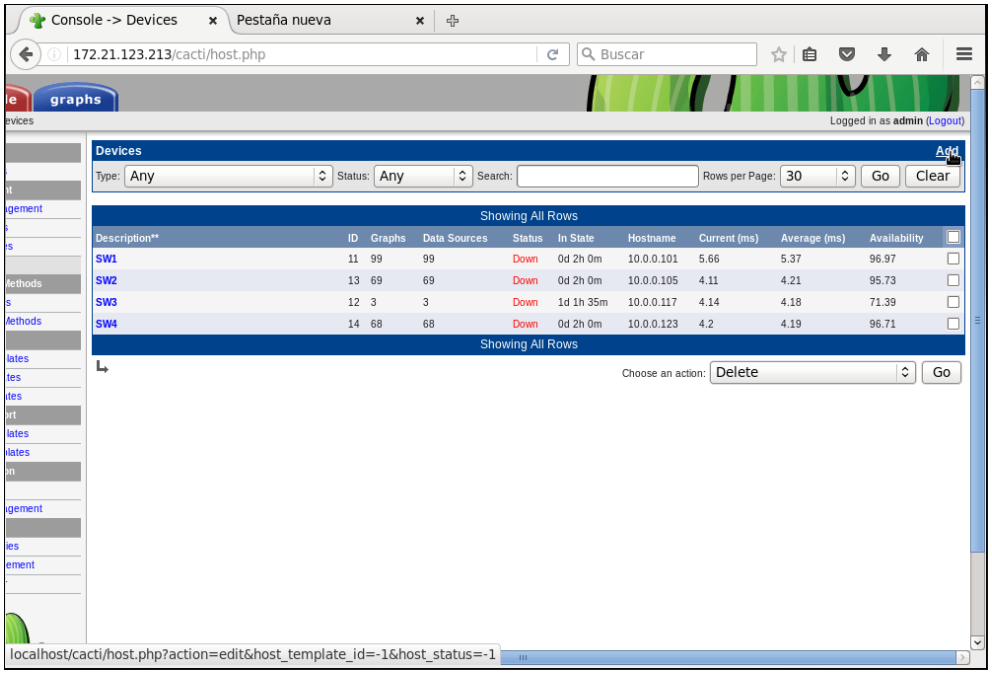


Figura 67: Agregación de nuevos Dispositivos

- A continuación se agrega los datos de los switch para el monitoreo de red de la FISEI
- En Opciones generales del host se coloca la “Description” y el “Hostname”
- En Opciones de accesibilidad de disponibilidad se elige “SNMP Uptime” que es el tiempo de actividad del host.
- En Opciones de SNMP se selecciona “Version 2” que es la version configurada del SNMP en los switch y en Cacti, a continuación de la comunidad “ComunidadLab”.

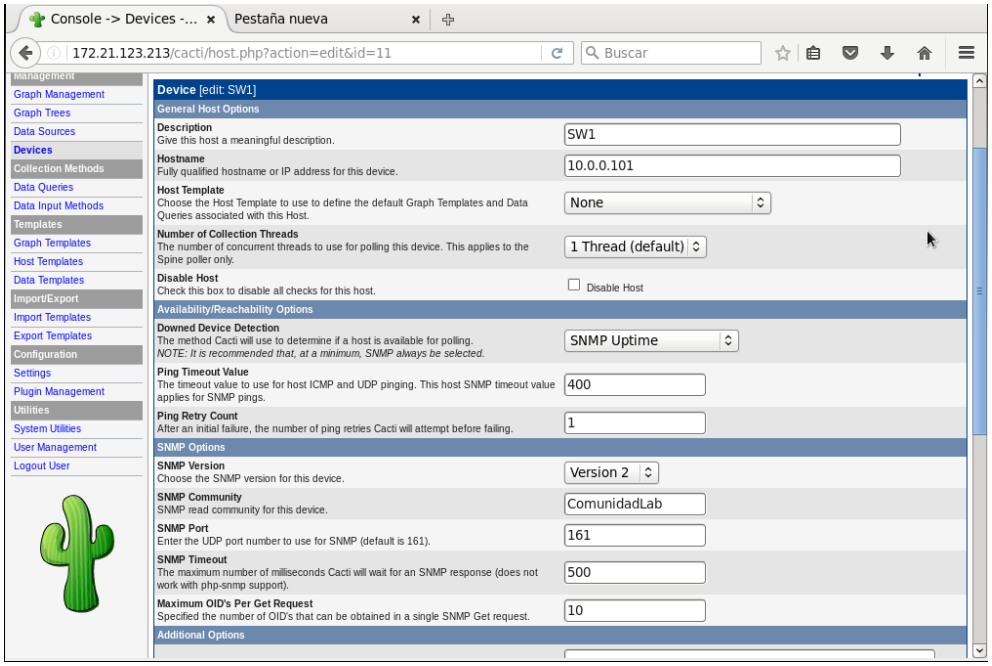


Figura 68: Configuración de los Dispositivos

- Se agrego una plantilla para los equipos cisco que sirvió para los análisis de gráficas “Cisco-CPU Usage”.
- En las consultas de datos asociados se ecogío “SNMP-Get Mounted Partitions”, “SNMP-Get Processor Information”, “SNMP-Interface Statistics” y guardar.

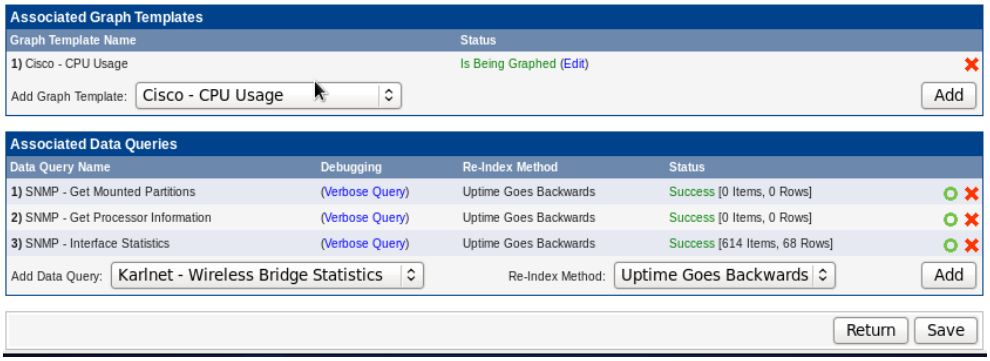


Figura 69: Plantillas de gráficos asociadas y Consultas de datos asociadas

Posteriormente se selecciona en "Create Graphs for this Host" que es para la configuración de la consulta de datos del anális de monitoreo de la red.

- En Data Query se selecionó todos las estadísticas de la interfaz para ser analizadas y seguidamente crear.

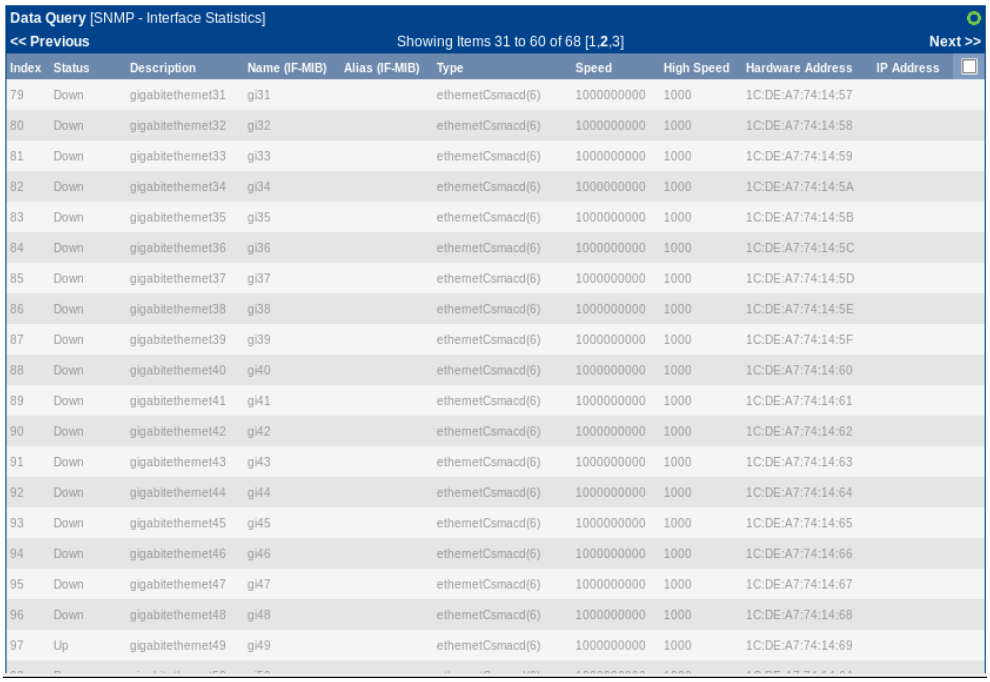


Figura 70: Data Query

- Por consiguiente en "Graph Trees" se agrega el arbol que va a visualizar los dispositivos de la red.

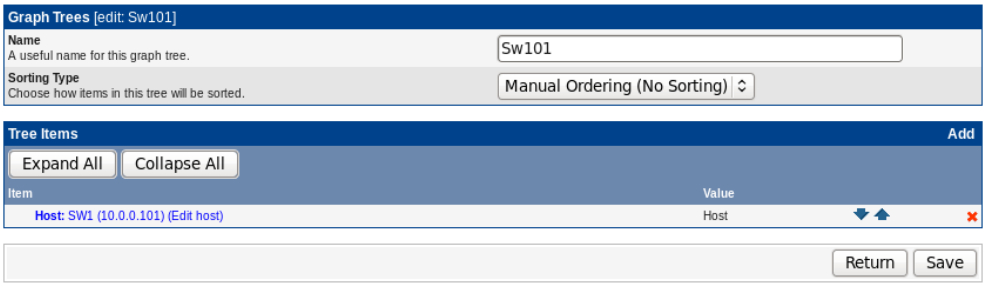


Figura 71: Graph Trees

- Por último se puede visualizar los gráficos con sus respectivos arboles.

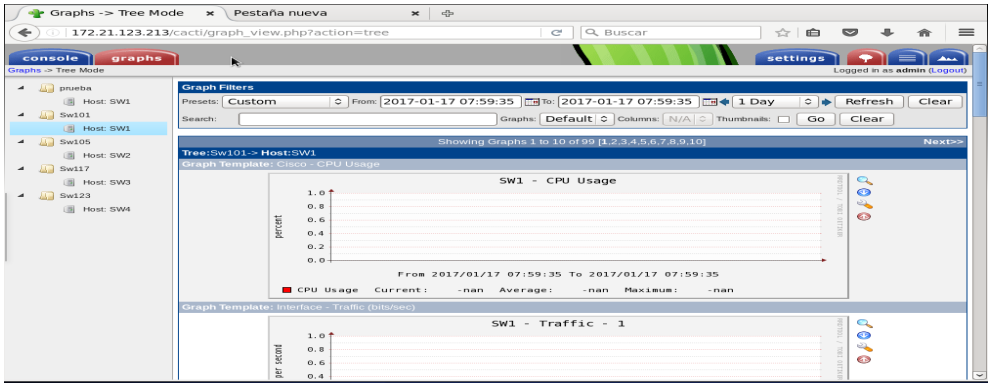


Figura 72: Filtros de gráficos

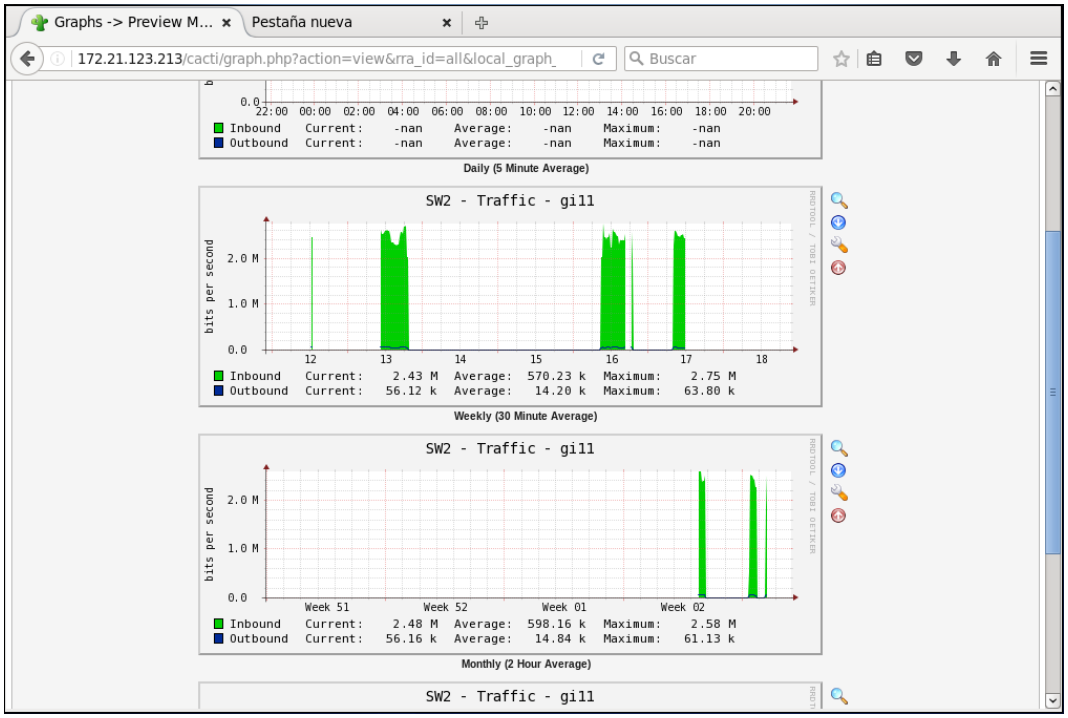


Figura 73: Estadísticas de tráficos de red

Evaluación	Parámetros
1	Muy Malo
2	Malo
3	Bueno
4	Muy Bueno
5	Excelente

Tabla 48: Evaluación de las tablas de requerimientos de los sistemas de monitoreo de red

4.5.13. Análisis comparativo de las herramientas utilizadas para el monitoreo de la red.

En base al análisis realizado a cada uno de los sistemas implementados se ha determinado que se debe cumplir con una tabla específica de características mínimas para implementar el control de monitoreo de red de la FISEI.

Nombre	Informes SLA	Estadisticas	Predicción de Estadísticas	Grupos lógicos	Autodescubrimiento Automático	SNMP	Logs	Plugins	Alarmas y Alertas	Aplicación web	Históricos	Agentes
MUNIN	SI	SI	Desconocido	SI	SI	SI	SI	SI	SI	SI	SI	SI
MRTG	SI	SI	NO	SI	SI	SI	SI	NO	NO	SI	NO	
CACTI	SI	SI	NO	SI	SI (plugins)	SI	SI	SI	NO	SI	SI	SI

Tabla 46: Tabla de especificaciones de requerimientos para sistemas de control de red

Nombre	Gráficas	Monitorización distribuida	Plataforma	Estadísticas	Almacenamiento	Mapas	Licencias	Control de Usuarios	Fecha del ultimo Lanzamiento
MUNIN	SI	SI	Perl	SI	RRDtool	Desconocido	GPL	NO	2016-12
MRTG	SI	NO	C, Perl	SI	RRDtool	NO	GPL	NO	2013-08
CACTI	SI	SI	PHP	SI	RRDtool y My SQL	Con plugins	GPL	SI	2017-01

Tabla 47: Tabla de especificaciones de requerimientos para sistemas de control de red

4.5.14. Evaluación de los parámetros de las herramientas de monitoreo de red de datos.

A fin de calificar e identificar que sistema de monitoreo es el más aptos se evaluó de la siguiente manera:

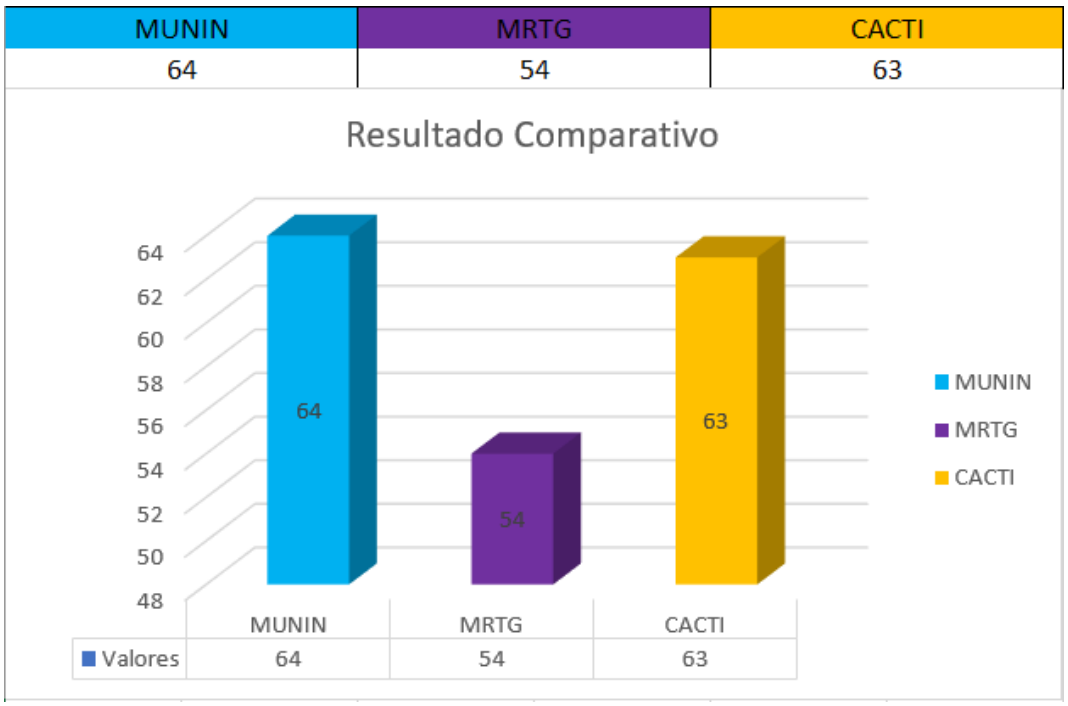


Figura 74: Resultado cuadro comparativo

4.5.15. Evaluación comparativa de las herramientas utilizadas para el monitoreo de la red.

Nombre	Informes SLA	Estadisticas	Predicción de Estadísticas	Grupos lógicos	Autodescubrimiento Automático	SNMP	Logs	Plugins	Alarmas y Alertas	Aplicación web	Históricos	Agentes
MUNIN	1	5	1	3	5	5	4	4	5	4	4	2
MRTG	1	4	1	3	4	5	4	2	1	4	1	2
CACTI	1	5	1	3	5	5	4	4	1	4	4	2

Tabla 49: Tabla de evaluación comparativa

Nombre	Gráficas	Monitorización distribuida	Plataforma	Estadísticas	Almacenamiento	Mapas	Licencias	Control de Usuarios	TOTAL
MUNIN	4	2	2	4	4	1	3	1	64
MRTG	4	2	3	4	4	1	3	1	54
CACTI	4	2	1	4	5	2	3	3	63

Tabla 50: Tabla de evaluación comparativa

4.5.16. Análisis de resultados comparativos

Se realizó la gráfica en columnas de los resultados obtenidos de cada herramienta de monitoreo de red.

Con los parámetros alcanzados en las tablas anteriores en el que se ha dado un grado de ponderación del 1 al 5, siendo el parámetro 1 en de menor factibilidad

y el 5 el de mayor factibilidad se concluye que de acuerdo al análisis de la gráfica de las herramientas Munin, Mrtg y Cacti de monitoreo de red basadas en SNMP se tuvieron los siguientes resultados comparativos: MUNIN con la ponderación de 64 en comparación con MRTG y CACTI es la herramienta mas confiable con una facilidad de controlar el rendimiento de las redes y dar una buena gestión a la red de datos solucionando los requerimientos de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, así también se puede observar que la herramienta MRTG muestra características muy básicas sin cumplir con todos los parámetros establecidos en las tablas anteriores.
Una vez que se ha estudiado y analizado los resultados emitidos de cada una de las herramientas Munin, Mrtg y Cacti cabe mencionar que debido a los datos obtenidos se considera que la herramienta mas óptima para ser aplicada en el presente proyecto de investigación es MUNIN.

4.6. Monitoreo de la red de datos para detectar fallos y congestionamiento.

Una vez realizado el monitoreo de la red de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, los resultados obtenidos son los detallados a continuación:

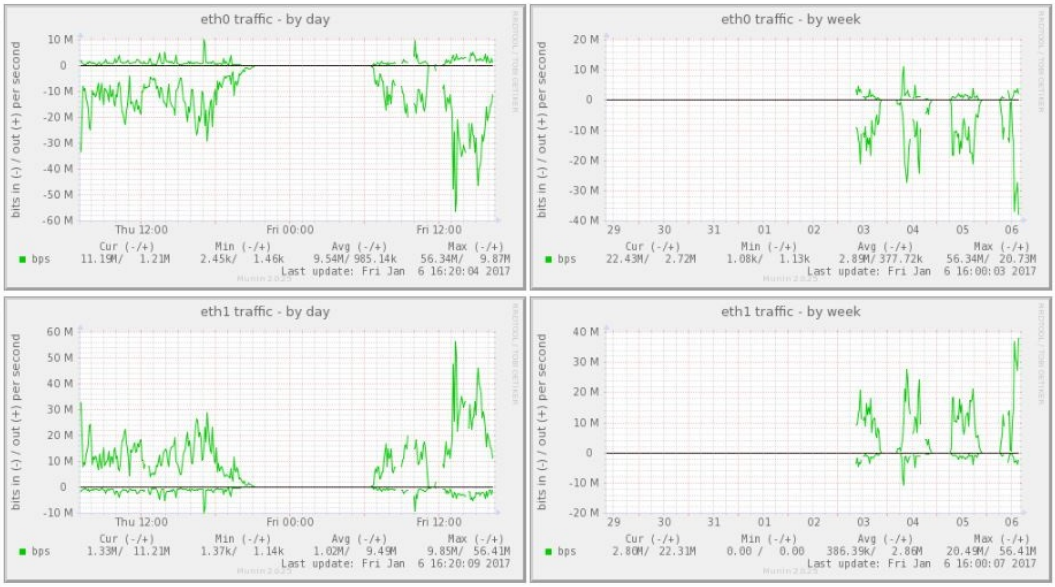


Figura 75: Fallos y congestionamiento de la red de datos de la FISEI.

- De acuerdo al análisis de tráfico de red de la Figura 4.54, los picos más altos se producen a las 12:00 AM, superan los niveles de 56M por

segundo y los niveles más bajos llegan a 1.33M por segundo ocasionando congestionamiento en la red causados por problemas físicos o lógicos. Los problemas físicos son ocasionados por el cambio del medio de transmisión o un ajuste a los conectores de los elementos de la red, por otro lado, los problemas lógicos son causados internamente en los dispositivos de red, por el mal dimensionamiento de los buffers en los equipos, lo cual produce que no se guarden los paquetes durante los periodos de congestión, por lo tanto las velocidades de Internet llegan a cientos de Gigabits por segundo e incluso a más, los router llegan a una insuficiencia de memoria para albergar tantos paquetes de datos, principalmente en el dominio de la fibra óptica, donde se logran las mayores velocidades de transmisión.

4.7. Análisis de los resultados del monitoreo para identificar actividad no autorizada y anomalías que provoquen degradación en la red

La interpretación de las estadísticas se ha dado en forma de árbol que ha permitido clasificarlo por problemas, grupos y categorías.
La herramienta de monitoreo MUNIN ha determinado mediante categorías su clasificación, es decir; Localhost, Mirror y Wifi en el cual se analizan sus estadísticas de acuerdo a la funcionalidad de la red.
Localhost mediante sus categorías: Disco, Red, Procesos, Proxy y Sistemas se han evaluado en un periodo de prueba con y sin ataques a la red, los que han permitido conocer la realidad de la herramienta de monitoreo.

VIRUS	FECHA	ALERTAS	PROBLEMAS	CATEGORÍAS	EVALUACIÓN DEL SISTEMA					
					L	M	M	J	V	S
		Amarillo	Critical	Disk						
		Anaranjado	Warning	Network				X	X	
		Rojo	Unknown	Processes						
	jueves, 5 de enero de 2017			squid				X	X	
DDoS Hping3	viernes, 6 de enero de 2017			system						

Tabla 51: Tabla de análisis con MUNIN

Mediante el cuadro precedente se ha logrado instaurar los resultados obtenidos a través del Sistema de Monitoreo MUNIN el cual ha recabado importante información que se señala ha continuación:
La evaluación del Sistema MUNIN en las fechas 06/01/2017 y 06/01/2017 arrojó los siguientes datos: en cuanto al virus DDoS Hping3 se realizó un escaneo a través del puerto 80 mediante el ingreso del código “hping3 -S ip_victima -p 80” dando como resultado un flag “SA” que corresponde a que la comunicación ha

sido aceptada, o caso contrario el valor de “RA” que se refiere a que la conexión no se ha realizado o que se encuentra cerrado el puerto.
De tal forma se realizó el ataque con el código “hping3 -S ip_victima –flood –rand-source -d 10000 -p 80” produciendo un gran número de paquetes en forma continua al servidor de destino, emitiendo un mensaje de advertencia en el ancho de banda y en el servidor proxy, colapsando los servicios de red en el servidor y limitando la conexión a Internet.

Parámetro	**Función**
-S	Seteo del flag SYN (es un bit de control dentro del segmento TCP)
-flood	Envío de paquetes en tiempo real y masivo.
-rand-source	Simulamos diferentes orígenes aleatoriamente al enviar los paquetes.
-d	Tamaño de los paquete que se desea enviar.
-p	Puerto de destino

Tabla 52: Descripción del código Hping3

Cabe destacar la relevancia en detallar que significa el virus DDoS Hping3, es una herramienta que se utiliza desde la consola o terminal en Linux, cuyo fin es el análisis y ensamblado de paquetes TCP/IP. Similar al comando Ping, generando paquetes ip a discreción, esto quiere decir que permite crear y analizar paquetes TCP/IP. No solo es capaz de enviar paquetes ICMP, sino que también es capaz de enviar paquetes TCP, UDP y RAW-IP[33].
A continuación se detalla los datos estadísticos reales mediante interpretación realizada por el investigador, datos que fueron analizados en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

GRÁFICA IDEAL DISK

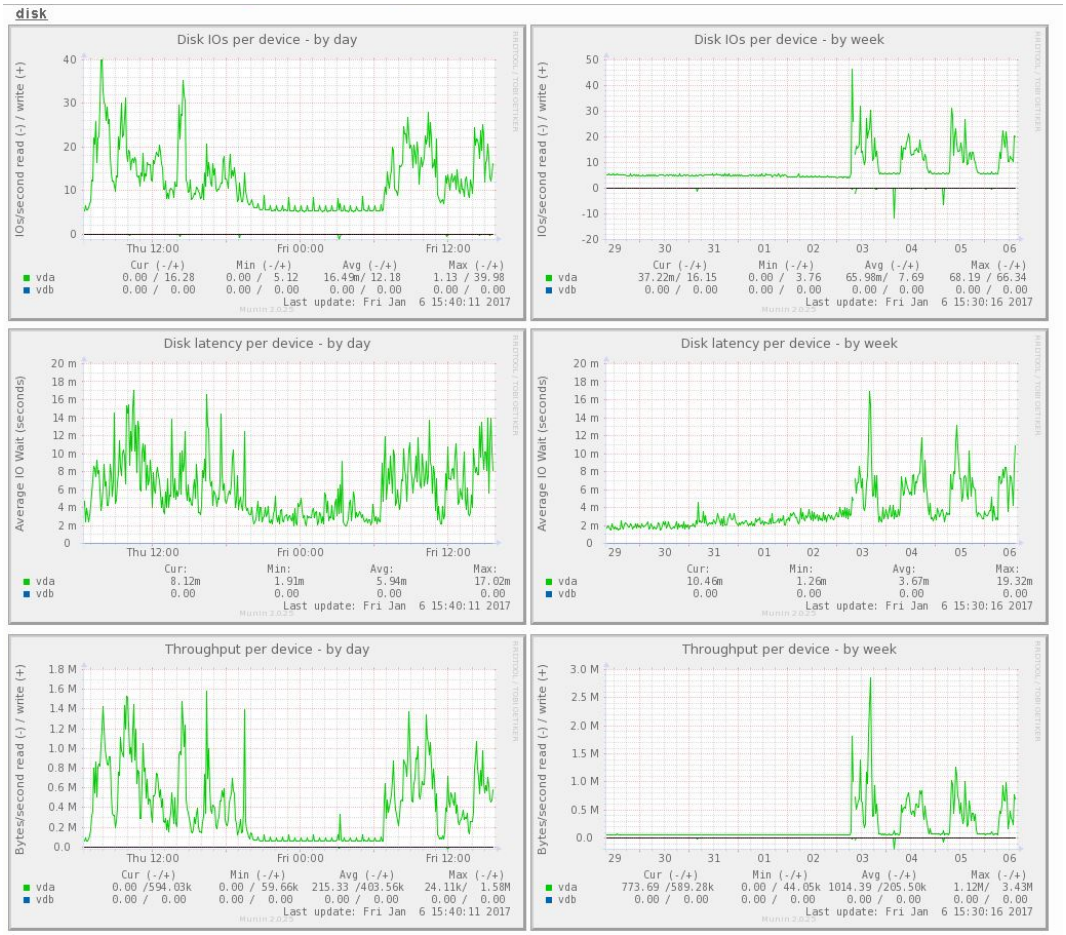


Figura 76: Gráfica Ideal Disk

Resultados Gráfica Ideal Disk

RESULTADO	
DISK IOs por dispositivo	• Máximo= 68.19(-) 66.34(+)
Lectura (-) y escritura (+)	• Mínimo= 0.00(-) 3.76(+)
	• Promedio=65.98m (-) 7.69(+)
	• Concurrencia= 37.22m (-) y 16.15(+)
Latencia del disco por dispositivo	• Máximo=19.32m
	• Mínimo=1.26m
	• Promedio=3.67m
	• Concurrencia=10.46m
Porcentaje de rendimiento del disco	• Máximo=1.12M (-) 3.43M (+)
Lectura (-) y escritura (+)	• Mínimo=0.00(-) 44.05k (+)
	• Promedio=1014.39(-) 205.50(+)
	• Concurrencia=773.69(-) 589.28k (+)

Tabla 53: Resultados Gráfica Ideal Disk

Descripción de la Tabla 53.

Descripción
DISK IOs por dispositivo En las gráficas estadísticas del grupo localhost en la categoría disk da como resultado un máximo en lectura y escritura de 68.19(-) 66.34(+) analizados en un periodo de tiempo de una semana llegando a un promedio de 65.98m (-) 7.69(+) por lo cual es un valor estable en el que no está sobrecargado el disco. **Latencia del disco por dispositivo** Estas gráficas nos indica cual es la suma de retardos temporales en el consumo de disco en el cual en un periodo de una semana se ha tenido como pico más alto el de 19.32m, teniendo una latencia diaria de 17.02m como máxima llegando a tener un promedio de 3.67m y una concurrencia de 10.46m. **Porcentaje de rendimiento del disco** En el rendimiento del disco en lectura y escritura en el periodo de una semana es de 1.12M (-) 3.43M (+) como máximo y como mínimo 0.00(-) 44.05k (+), comparando diariamente se obtiene un máximo de 24.11k (-) 1.58M (+), llegando a un promedio de rendimiento de 1014.39(-) 205.50 (+), indicando que la utilización del disco no sobrepasa los valores mencionados ya que si superaran este sería alertado por el sistema MUNIN. **VDA:** Es el primer controlador de disco para virtualización detectado. Es el disco raíz de su sistema. **VDB:** Es el volumen que acaba de adjuntar.

Tabla 54: Descripción y explicación de la gráfica ideal Disk

Gráfica Network Ideal y con virus

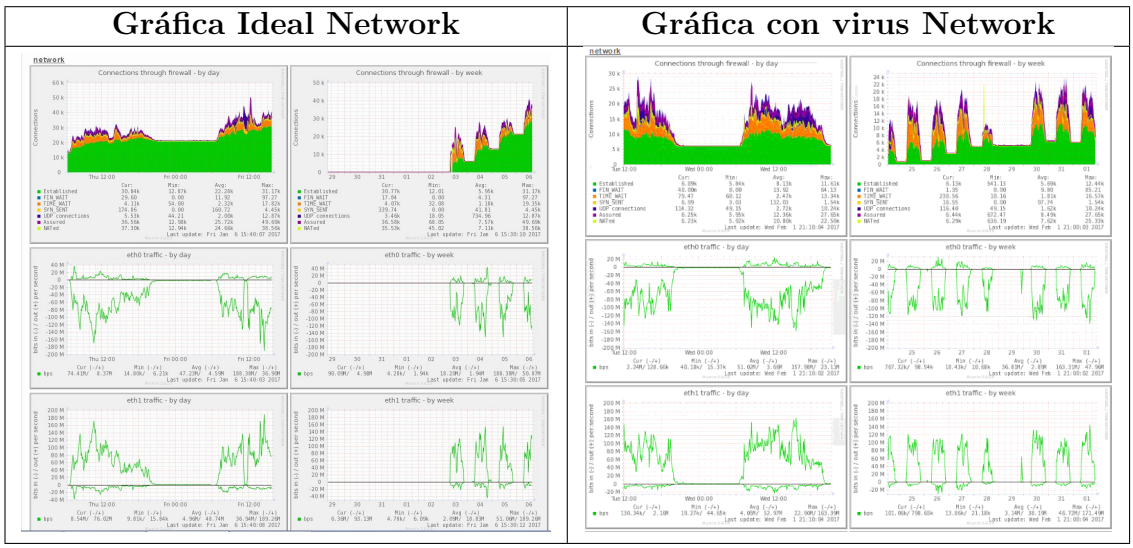


Figura 77: Gráfica Network Ideal y con virus

Resultados de la Gráfica Network Ideal y con virus

RESULTADO SIN VIRUS	
NETWORK	• Máximo= 12.44k
ESTABLISHED	• Mínimo= 541.13k
(CONEXIÓN ESTABLECIDA)	• Promedio= 5.69k
	• Concurrencia= 6.13k
FIN_WAIT	• Máximo= 85.21
(FINALIZACIÓN DE CONEXIÓN)	• Mínimo= 00.00
	• Promedio= 9.80
	• Concurrencia= 1.35
TIME_WAIT	• Máximo= 16.57k
(TIEMPO DE ESPERA)	• Mínimo= 10.16
	• Promedio= 1.81k
	• Concurrencia= 230.56k
SYN_SENT	• Máximo= 4.45k
(INICIALIZACIÓN DE CONEXIÓN)	• Mínimo= 0.00
	• Promedio= 41.81
	• Concurrencia= 339.74
UDP CONNECIONS	• Máximo= 12.87k
(CONEXIÓN UDP)	• Mínimo= 18.05
	• Promedio= 734.96
	• Concurrencia= 116.40
ASSURED (SEGURO)	• Máximo= 49.69k
	• Mínimo= 68.05
	• Promedio= 7.57k
	• Concurrencia= 36.58k
TRAFICO ETH0	• Máximo= 188.38M (-) 50.87M (+)
BITS IN (-) BITS OUT (+)	• Mínimo= 4.28k (-) 1.94k (+)
	• Promedio= 18.20M (-) 1.94M (+)
	• Concurrencia= 90.09M (-) 4.98M (+)
TRAFICO ETH1	• Máximo= 51.06M (-) 189.26M (+)
BITS IN (-) BITS OUT (+)	• Mínimo= 4.78k (-) 6.09k (+)
	• Promedio= 2.09M (-) 18.83M (+)
	• Concurrencia= 6.36M (-) 93.13M (+)

Tabla 55: Resultados de la Gráfica Network Ideal

RESULTADO CON VIRUS	
NETWORK	• Máximo= 31.17k
ESTABLISHED	• Mínimo= 12.01k
(CONEXIÓN ESTABLECIDA)	• Promedio= 5.95k
	• Concurrencia= 30.77k
FIN_WAIT	• Máximo= 97.27
(FINALIZACIÓN DE CONEXIÓN)	• Mínimo= 00.00
	• Promedio= 4.31
	• Concurrencia= 17.84
TIME_WAIT	• Máximo= 19.35k
(TIEMPO DE ESPERA)	• Mínimo= 32.08
	• Promedio= 1.18k
	• Concurrencia= 4.07k
SYN_SENT	• Máximo= 1.54k
(INICIALIZACIÓN DE CONEXIÓN)	• Mínimo= 0.00
	• Promedio= 97.74
	• Concurrencia= 16.55
UDP CONNECIONS	• Máximo= 10.24k
(CONEXIÓN UDP)	• Mínimo= 49.15
	• Promedio= 1.62k
	• Concurrencia= 3.46k
ASSURED (SEGURO)	• Máximo= 27.65k
	• Mínimo= 672.47
	• Promedio= 8.49k
	• Concurrencia= 6.44k
TRAFICO ETH0	• Máximo= 163.31M (-) 47.96M (+)
BITS IN (-) BITS OUT (+)	• Mínimo= 18.43k (-) 10.68k (+)
	• Promedio= 36.81M (-) 2.89M (+)
	• Concurrencia= 767.32k (-) 98.54k (+)
TRAFICO ETH1	• Máximo= 46.72M (-) 171.49M (+)
BITS IN (-) BITS OUT (+)	• Mínimo= 13.86k (-) 21.18k (+)
	• Promedio= 3.14M (-) 38.19M (+)
	• Concurrencia= 101.06k (-) 798.65k (+)

Tabla 56: Resultados de la Gráfica Network con virus

Descripción de las Tablas 55 y 56

Descripción
Firewall de rendimiento de conexiones En los cuales existe varios parámetros de evaluación en el cual el día jueves 5 de enero del 2017 se realizó una prueba ingresando un ataque DDoS con la herramienta Hping3 teniendo los resultados siguientes: El pico máximo con el virus ingresado es de 31.17k comparando con el pico máximo ideal en la red es de 12.44k observando que se ha tenido un incremento de 18.73k con una concurrencia de 30.77k. **Inicialización, tiempo de espera y finalización de la conexión.** Estos parámetros indican cuando el servidor tiene una conexión activa con un cliente y desean cerrar o iniciar un vínculo, los cuales existe varios parámetros de evaluación en base a la finalización de conexión. Con el virus ingresado existe un pico máximo de 97.27 y mínimo 0.00 en comparación con un análisis normal teniendo un máximo de 85.21 y mínimo de 0.00, en el promedio se ha tenido un incremento de 5.49 y en su concurrencia con un incremento de 16.49. Al momento de la inicialización de la conexión en un instante ideal tiene un máximo de 4.45k en comparación al análisis con virus llegando a un máximo de 1.54k sobrepasando con un promedio de 55.93 y una concurrencia de 323.19 en exceso. **La conexión UDP** En la conexión UDP el pico más alto es de 734.96 de promedio en comparación al promedio ideal de 1.62k y una concurrencia de 116.40 en paralelo al de 3.46k, por otro lado, en la traducción de direcciones de red la concurrencia es de 35.53k como pico máximo en comparación de la concurrencia ideal de 3.29k **ASSURED SEGURO** En la parte de seguridad se ha reducido a un mínimo de 604.42 con una concurrencia de 30.14. **TRAFICO ETH0 BITS IN (-) BITS OUT (+) POR SEGUNDO** El tráfico de la tarjeta en entrada y salida es de 163.31M (-) 47.96M (+) siendo este el estado ideal en cambio en sus picos más altos llega a los siguientes valores 188.38M (-) 50.87M (+) y su valor mínimo sin virus es de 18.43k (-) 10.68k (+), con virus 4.28k (-) 1.94k (+) con una concurrencia de 737249.96k **TRAFICO ETH1 BITS IN (-) BITS OUT (+) POR SEGUNDO** El tráfico de la tarjeta en la entrada y salida de bits es de 51.06M (-) 189.23M (+) siendo este el estado ideal en cambio en sus picos más altos llega a los siguientes valores 46.72M (-) 171.49M (+) y su valor mínimo sin virus es de 13.86k (-) 21.18k (+), con virus 4.78k (-) 6.09k (+) con una concurrencia de 6411.58k

Tabla 57: Descripción y explicación Gráfica Network Ideal y con virus

Gráfica ideal de Procesos

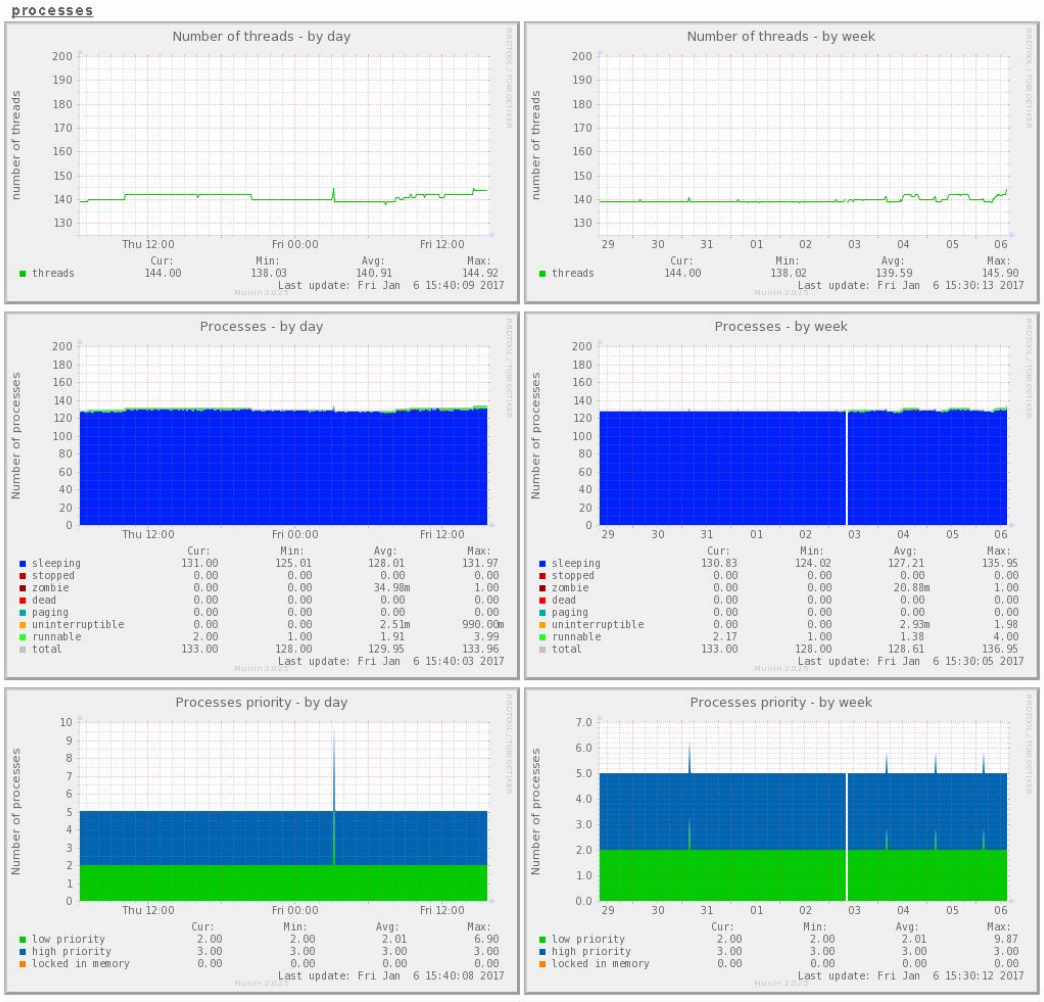


Tabla 58: Gráfica ideal de Procesos

Resultados de la gráfica ideal de Procesos

RESULTADO	
Número de amenazas	• Máximo= 145.90
	• Mínimo= 138.02
	• Promedio= 139.59
	• Concurrencia= 144.00
Número de Procesos	• Máximo= 135.95
SLEEPING (Durmiendo)	• Mínimo= 124.02
	• Promedio= 127.21
	• Concurrencia= 130.83
ZOMBIE	• Máximo= 1.00
	• Mínimo= 0.00
	• Promedio= 20.88m
	• Concurrencia= 0.00
UNINTERRUPTIBLE	• Máximo= 1.98
	• Mínimo= 0.00
	• Promedio= 2.93m
	• Concurrencia= 0.00
RUNNABLE	• Máximo= 4.00
	• Mínimo= 1.00
	• Promedio= 1.38
	• Concurrencia= 2.17
TOTAL	• Máximo= 136.95
	• Mínimo= 128.00
	• Promedio= 128.61
	• Concurrencia= 133.00
Prioridad de Procesos	• Máximo= 9.87
LOW PRIORITY	• Mínimo= 2.00
	• Promedio= 2.01
	• Concurrencia= 2.00
HIGH PRIORITY	• Máximo= 3.00
	• Mínimo= 3.00
	• Promedio= 3.00
	• Concurrencia= 3.00

Tabla 59: Resultados de la gráfica ideal de Procesos

Descripción de la Tabla 59

Descripción
Número de amenazas El máximo en las estadísticas es de 145.90 con un mínimo de 138.02, promediando a un valor de 139.59 y una concurrencia de 144.00 debido a los procesos que se ejecutan como Windows o Linux. **Número de Procesos** **SLEEPING (Durmiendo)** Tiene un pico máximo de 135.95 que es el valor ideal para el número de procesos que se esté utilizando con un mínimo de 138.02 y promediando 139.59, tiene una concurrencia de 144.00. **ZOMBIE** Genera un pico máximo de 1.00 con un promedio de 20.88m por lo cual es un proceso que ha consumado su ejecución, pero incluso tiene una entrada en la tabla de procesos, permitiendo leer el curso de su salida. **UNINTERRUPTIBLE** Este tipo de proceso no se puede interrumpir por lo cual llega a tener un máximo de 1.98 con un promedio de 2.93m, generalmente este proceso se halla esperando una acción de entrada o salida con algún dispositivo. **RUNNABLE** Es un test de falla en el cual en un proceso ideal tiene como máximo 4.00 y un mínimo de 1.00 llegando a un promedio de 2.93m con una concurrencia de 2.17 **TOTAL** El total del análisis ideal de la gráfica de procesos llega a un máximo de 136.95 con un mínimo de 128.00 dando un promedio de 128.61 y una concurrencia de 133.00. **Prioridad de Procesos** Este tipo de procesos se explica por una cola de precedencias con los de baja y alta prioridad, los de baja pueden ser expropiados cuando llegue otro proceso a la cola de alta prioridad, pero los procesos de prioridad alta no pueden ser expropiados por los de baja. **LOW PRIORITY** Estos procesos llegan a un máximo de 9.87 con un mínimo de 2.00 promediando se tiene un valor de 2.01 y una concurrencia de 2.00 **HIGH PRIORITY** En los de alta prioridad tiene como pico más alto de 3.00 con un mínimo de 3.00 llegando a un promedio de 3.00 con una concurrencia de 3.00.

Tabla 60: Descripción de la gráfica ideal de Procesos

Gráfica Ideal y con Virus del Squit

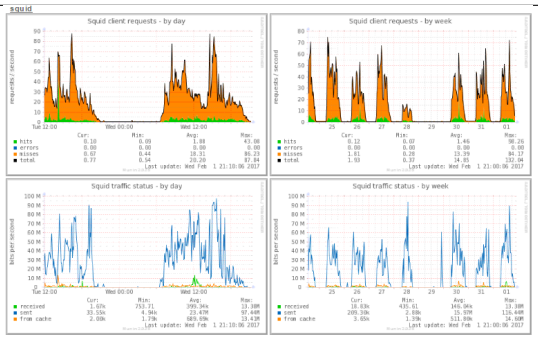
Gráfica Ideal Squit	Gráfica con virus Squit
	

Tabla 61: Gráfica Ideal y con Virus del Squit

Resultados de la gráfica Ideal y con Virus del Squit

RESULTADO IDEAL DE LA GRÁFICA SQUIT	
Solicitudes del cliente	• Máximo= 98.26
HITS	• Mínimo= 0.07
	• Promedio= 1.46
	• Concurrencia= 0.12
ERRORS	• Máximo= 0.00
	• Mínimo= 0.00
	• Promedio= 0.80
	• Concurrencia= 0.12
MISSES	• Máximo= 84.17
	• Mínimo= 0.28
	• Promedio= 13.39
	• Concurrencia= 1.81
TOTAL	• Máximo= 132.04
	• Mínimo= 0.37
	• Promedio= 14.85
	• Concurrencia= 1.93
Estado de tráfico squit	• Máximo= 13.38M
RECEIVED	• Mínimo= 435.61
	• Promedio= 146.04k
	• Concurrencia= 18.83k
SENT	• Máximo= 116.44M
	• Mínimo= 2.88k
	• Promedio= 15.97M
	• Concurrencia= 209.30k
FROM CACHE	• Máximo= 14.60M
	• Mínimo= 1.39k
	• Promedio= 511.80k
	• Concurrencia= 3.65k

Tabla 62: Resultados de la gráfica Ideal del Squit

RESULTADOS DE LA GRÁFICA CON VIRUS DEL SQUIT	
Solicitudes del cliente	• Máximo= 9.70
HITS	• Mínimo= 0.00
	• Promedio= 0.55
	• Concurrencia= 2.93
ERRORS	• Máximo= 0.07
	• Mínimo= 0.00
	• Promedio= 0.55
	• Concurrencia= 2.93
MISSES	• Máximo= 155.90
	• Mínimo= 0.30
	• Promedio= 9.04
	• Concurrencia= 26.90
TOTAL	• Máximo= 157.81
	• Mínimo= 0.30
	• Promedio= 9.59
	• Concurrencia= 29.83
Estado de tráfico squit	• Máximo= 1.52M
RECEIVED (Recibido)	• Mínimo= 377.66
	• Promedio= 52.79k
	• Concurrencia= 385.33k
SENT (Enviado)	• Máximo= 108.23M
	• Mínimo= 1.84k
	• Promedio= 8.30M
	• Concurrencia= 18.46M
FROM CACHE	• Máximo= 6.21
	• Mínimo= 0.00
	• Promedio= 198.41k
	• Concurrencia= 636.94k

Tabla 63: Resultados de la gráfica con virus del Squit

Descripción de las Tablas 62 y 63

Descripción
Solicitudes de clientes **HITS** El virus DDoS Hping3 se envió el día jueves 5 de enero del 2017 obteniendo los siguientes datos. De acuerdo a cada solicitud de errores golpes o perdidas se ha comparado el total ideal con un máximo de 132.04 y un mínimo de 0.37, el total con virus alcanza un pico máximo de 157.81 y un mínimo de 0.30 con un exceso en la concurrencia de 27.9. **Estado de tráfico squit** **RECEIVED** En el tráfico del squit se puede ver que tiene un pico alto de una concurrencia de 385.33k en comparación con la concurrencia ideal recibida 18.83k en el cual de observa que la afluencia enviada por el virus Hping3 es de un exceso de 366.5k **SENT** En el tráfico que se envía no hay mucha concurrencia ni hay mucha variación en los picos altos y bajos en comparación con el estado ideal, por otro lado, existe picos altos en estado ideal debido a las horas pico teniendo como máximo 116.44M y mínimo 2.88k promediando 15.97M. **FROM CACHE** En su concurrencia existe un exceso de 633.29k llegando a un promedio de 198.41k con virus y sin virus llega 511.80k.

Figura 78: Descripción de la gráfica Ideal y con Virus del Squit

Gráfica ideal del System

Figura 79: Gráfica ideal system

Resultados de la gráfica ideal del System

RESULTADO IDEAL DEL SYSTEM			
Uso del CPU	• Máximo= 37.00	**VIRTIO4-config**	• Máximo= 89.78m
SYSTEM	• Mínimo= 0.94		• Mínimo= 0.00
	• Promedio= 5.69		• Promedio= 293.78u
	• Concurrencia= 18.11		• Concurrencia= 0.00
USER	• Máximo= 94.69	**VIRTIO4-INPUT.0**	• Máximo= 6.02k
	• Mínimo= 1.82		• Mínimo= 0.00
	• Promedio= 17.66		• Promedio= 671.31
	• Concurrencia= 79.44		• Concurrencia= 3.14k
IDLE	• Máximo= 394.98	**VIRTIO4-OUTPUT.0**	• Máximo= 4.44k
	• Mínimo= 223.20		• Mínimo= 0.00
	• Promedio= 365.82		• Promedio= 19.02
	• Concurrencia= 249.69		• Concurrencia= 194.13m
IOWAIT	• Máximo= 2.25	**SND_HDA_INTEL**	• Máximo= 186.60m
	• Mínimo= 0.02		• Mínimo= 0.00
	• Promedio= 0.19		• Promedio= 714.28u
	• Concurrencia= 0.49		• Concurrencia= 0.00
IRQ	• Máximo= 0.12	**LOCAL TIMER**	• Máximo= 2.74k
	• Mínimo= 0.00	**INTERRUPTS**	• Mínimo= 106.28
	• Promedio= 0.01		• Promedio= 509.81
	• Concurrencia= 0.05		• Concurrencia= 2.15k
SOFTIRQ	• Máximo= 68.27	**RESCHEDULING**	• Máximo= 1.09k
	• Mínimo= 0.01	**INTERRUPTS**	• Mínimo= 6.56
	• Promedio= 3.47		• Promedio= 53.12
	• Concurrencia= 30.83		• Concurrencia= 201.84
STEAL	• Máximo= 7.06	**FUNCTION CALL**	• Máximo= 90.20m
	• Mínimo= 0.06	**INTERRUPTS**	• Mínimo= 0.00
	• Promedio= 0.72		• Promedio= 187.97u
	• Concurrencia= 5.01		• Concurrencia= 3.33m
Interrupción individual	• Máximo= 39.62	**TLB SHOOTDOWNS**	• Máximo= 7.88
VIRTIO2-REQUESTS	• Mínimo= 1.57		• Mínimo= 818.38
	• Promedio= 3.61		• Promedio= 1.25
	• Concurrencia= 5.76		• Concurrencia= 966.70m
VIRTIO0-INPUT.0	• Máximo= 5.66k	**MACHINE CHECK**	• Máximo= 13.79m
	• Mínimo= 0.00	**POLLS**	• Mínimo= 13.25m
	• Promedio= 586.75		• Promedio= 13.33m
	• Concurrencia= 3.01k		• Concurrencia= 13.33m
VIRTIO0-OUTPUT.0	• Máximo= 3.35k		
	• Mínimo= 0.00		
	• Promedio= 12.91		
	• Concurrencia= 70.57		

Tabla 64: Resultados de la gráfica ideal del System

Descripción de la Tabla 64

Descripción
Uso del CPU **SYSTEM** Es el tiempo de CPU empleado por el núcleo de las actividades del sistema indicando su uso con un máximo de 37.00 y un mínimo de 0.94 promediando a 5.69 con una concurrencia de 18.11 **USUARIO** Es el tiempo de CPU gastado por programas llegando a un pico estándar de 94.69 y un mínimo de 1.82 con un promedio de 17.66 y una concurrencia de 79.44 **IDLE** En el tiempo de inactividad de la CPU llega a un promedio de 365.82 con una cantidad de concurrencia de 249.69. **IOWAIT** El tiempo de CPU que pasó esperando para que las operaciones finalicen cuando no hay nada más que hacer es de 2.25 teniendo una concurrencia de 0.49 y picos de 2.25 y mínimo de 0.02. **IRQ** tiempo de CPU se emplea en gestionar las interrupciones llega a una concurrencia de 0.05 **SOFTIRQ** tiempo de CPU gastado con un promedio de 3.47 y una concurrencia de 30.83 que trata las alarmas "por lotes" **STEAL** El tiempo que una CPU virtual empleada en tareas ejecutables, con un promedio de 0.72 y una concurrencia de 5.01 con un funcionamiento bajo. **Interrupción individual** En la interrupción individual en el que trabajan las tarjetas de red virtualizadas, ha llegado a un promedio de 251.1 y una concurrencia de 121.99. **Local timer interrupts** Llega a un pico máximo de 2.74k con un mínimo de 106.28 promediando a 509.81 y llegando a una concurrencia de 2.15k.

Tabla 65: Descripción de la gráfica Ideal System

4.8. Instauración de mecanismos de control y protección de datos para mejorar el rendimiento de la red.

Para la finalización del presente proyecto de investigación se ha tomado como iniciativa establecer mecanismos de control y protección de datos para mejorar el rendimiento; ejecutado la determinación de las herramientas para monitorear la red, así como el monitoreo con el objetivo de detectar fallos y congestionamiento,

una vez obtenido los mismos, realizar el respectivo análisis de los resultados y así establecer un mecanismo de control y protección para lo cual se ha concluido con la necesidad de instalar y configurar el sistema IDS/IPS Suricata.

- Para lo cual se realizado un análisis previo de comparación con otras soluciones IDS/IPS [34].
    - Soluciones Propietarias: Se compara algunas características de Suricata con otras soluciones IPS propietarias en general. La ventaja de Suricata al ser una solución de código abierto, es la flexibilidad de agregar nuevas funcionalidades al motor, según vayan siendo requeridas por las comunidades [35].

Características	**Soluciones Comerciales IDS/IPS**	**Suricata**
Multi-Threading	x	SI
Soporte para IPV6	Cisco, IBM, Stonesoft	SI
IP Reputation	Cisco	SI
Detección Automática de Protocolos	NO	SI
Aceleración con GPU	NO	SI
Variables Globales/Flowbit	NO	SI
GeoIP	NO	SI
Análisis Avanzado de HTTP	NO	SI
HTTP Access Logging	NO	SI
SMB Access Logging	NO	SI
Anomaly Detection	SI	NO
Alta Disponibilidad	SI	NO
GUI de Administración	SI	NO
GRATIS	NO	SI

Tabla 66: Comparación de Suricata con IPS/IDS´s propietarias

- Soluciones Open Source
    - Bro y Snort:

En cuanto a las soluciones de código abierto existen los que únicamente funcionan como Detección de intrusos, siendo Bro uno de los más conocidos.
En cuanto a Detección y Prevención de intrusos, el más conocido es SNORT, un IDS/IPS desarrollado por Sourcefire; tiene más de 10 años de antigüedad

y actualmente se encuentra cerca de la versión 2.9. Cuando la primera versión de Suricata disponible fue lanzada, muchos se preguntaron si el proyecto Snort moriría, pues últimamente no ha habido mucha innovación ente los IPS. Sin embargo la entrada de suricata significó una "competencia" para Snort, a la que la comunidad de sourcefire respondió con un mayor empeño en su proyecto.
Actualmente Suricata posee características únicas que no se encuentran en Snort (Tampoco en otros IPS) y de hecho, muchas veces se menciona a suricata como una actualización o mejora basada en Snort, hecho que no es del todo cierto [36].

Características	**Bro**	**Snort**	**Suricata**
Multi -Threading	NO	X	SI
Soporte para IPV6	SI	SI	SI
IP Reputation	ALGO	NO	SI
Detección Automática de Protocolos	SI	NO	SI
Aceleración con GPU	NO	NO	SI
Variables Globales/Flowbits	SI	NO	SI
GeoIP	SI	NO	SI
Análisis Avanzado de HTTP	SI	NO	SI
HTTP Access Logging	SI	NO	SI
SMB Access Logging	SI	NO	SI

Tabla 67: Comparación de Suricata con IPS/IDS´s de código abierto

Una vez realizado el análisis comparativo de los sistemas de IDS/IPS se concluye que: El programa Suricata es la mejor opción para la protección de datos de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

4.8.1. Instalación y configuración de SURICATA

Figura 80: Suricata

Instalación y Configuración base Oinkmaster

Permite realizar un upgrade automático de las reglas (IDS Policy Manager). Permite gestionar las reglas en forma de políticas por cada sensor.
Este software no se encuentra dentro de los repositorios por lo cual se requiere descargar lo siguiente paquetes.
Se crea un directorio en /etc

- mkdir /etc/oinkmaster

Se ingresa al directorio creado

- cd /etc/oinkmaster

Seguidamente se descarga el software Oinkmaster

- wget http://prdownloads.sourceforge.net/oinkmaster/oinkmaster-2.0.tar.gz

Se descomprime el archivo descargado dentro del directorio

- tar xvzf oinkmaster/oinkmaster-2.0.tar.gz

A continuación, se mueve el contenido al directorio base

- mv oinkmaster-2.0/*

En el archivo oinkmaster.conf se agrega al inicio del archivo la siguiente línea

- url = https://rules.emergingthreatspro.com/open/suricata/emerging.rules.tar.gz

Al final del archivo se coloca las siguiente líneas
modifysid emerging-web_specific_apps.rules "alert" | "drop"
modifysid emerging-web_server.rules "alert" | "drop"
modifysid emerging-web_client.rules "alert" | "drop"
modifysid emerging-sql.rules "alert" | "drop"
modifysid emerging-scan.rules "alert" | "drop"
modifysid emerging-shellcode.rules "alert" | "drop"
modifysid emerging-worm.rules "alert" | "drop"
modifysid emerging-malware.rules "alert" | "drop"
modifysid emerging-icmp.rules "alert" | "drop"
modifysid emerging-exploit.rules "alert" | "drop"
Esto se realiza para el drop de varias cosas que se detecte y no solo se realice el alert, de otra forma seguiría en modo IDS.

Instalación y Configuración suricata IPS

Se instala los siguientes repositorios

- yum -y install http://codemonkey.net/files/rpm/suricata/el7/suricata-release-el-7-1.el7.noarch.rpm
- yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

A continuación, se prosigue con la configuración de suricata, en la instalación anterior las configuraciones se encuentran en el directorio /etc/suricata y dentro del mismo se configura el archivo suricata.yaml.
La siguiente sección es por defecto:
a line based information for dropped packets in IPS mode
- drop:
enabled: no
filename: drop.log
append: yes
#filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
Cambios que se debe realizar:

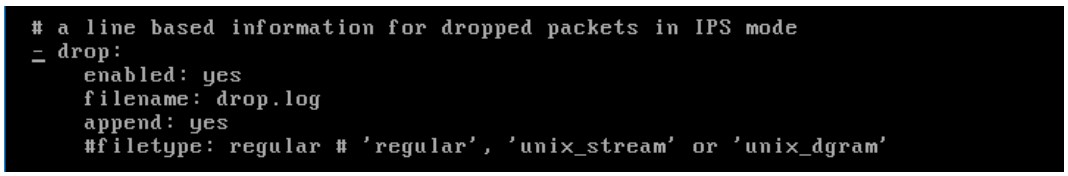


Figura 81: Archivo suricata.yaml sección drop

En la sección por defecto nfq:
mode: accept
#repeat-mark: 1
#repeat-mask: 1
route-queue: 2
batchcount: 20
fail-open: yes
Se configura de la siguiente manera:

Figura 82: Archivo suricata.yaml sección nfq

El valor “mode: repeat” es para re-inyectar los paquetes a la tabla de netfilter. Los valores “repeat-mark: 1” y “repeat-mark: 1” son para eliminar los paquetes que ya han sido analizados con anterioridad de no ser habilitados estos valores en conjunto con las reglas iptables los paquetes entran en un ciclio infinito saturando los dispositivos.

Configuración del inicio del servicio

Para que Suricata empiece en modo de IPS es necesario hacer hook a la pila de netfilter y por ello se cambia las siguientes líneas en el archivo "/etc/sysconfig/suricata"

- OPTIONS="-q 0 "

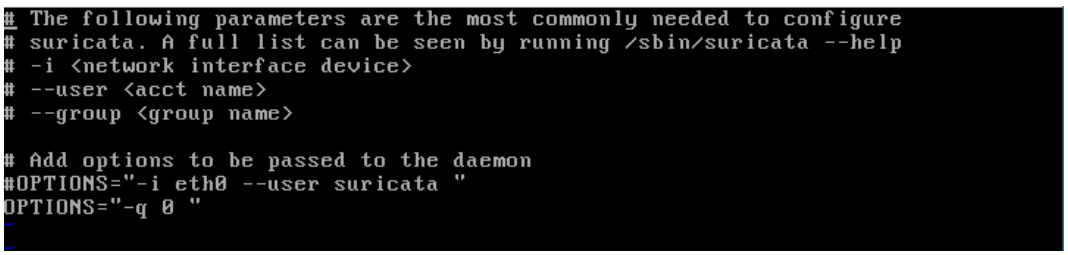


Figura 83: Archivo suricata

Nota: No es necesario detallar la interfaz de red ya que se ubica dentro de la pila de netfilter.
De esta forma Suricata cada vez que se inicie se pondrá en modo IPS.

Desconfiguración de firewall por defecto

Para establecer las reglas de iptables se deshabilita el servicio colocado por defecto, aplicando las siguientes líneas:

- systemctl disable firewalld.service
- systemctl stop firewalld.service

Habilitar el firewall basado en iptables

Se instala el firewall clásico como se ve a continuación:

- yum -y install iptables-services.x86_64

Configuración del firewall

En el archivo "/etc/sysconfig/iptables" se configura lo siguiente:

Figura 84: Archivo iptables

Estas son las reglas por defecto y es en la cual se define la política a denegar, así como también para que el tráfico forward sea operado por Suricata.

Scripts

Se crea un directorio dentro del "/root" llamado "scripts" el cual contiene 2 archivos llamados "startsuricata.sh" y "updaterules.sh" en los cuales se detalla lo siguiente:

#!/bin/bash
Activado de FORWARD de paquetes
echo 1 > /proc/sys/net/ipv4/ip_forward
#Reglas de PREROUTING
segmento de ssh
iptables -t nat -F PREROUTING
iptables -t nat -I PREROUTING -s 200.x.x.x -d 192.168.10.2 -p tcp --dport 22 -j DNAT --to-destination 192.168.2.10
#segmento de servicio
iptables -t nat -I PREROUTING -d 192.168.10.2 -p tcp -m multiport --dports 80,443 -j DNAT --to-destination 192.168.2.10
#Reglas de postrouting o masquerading
iptables -t nat -F POSTROUTING
iptables -t nat -I POSTROUTING -o ens192 -j MASQUERADE

En la sección inicial se activa el forward de paquetes al ras del kernel, caso contrario el IPS y el firewall no funcionará.
PREROUTING es el direccionamiento del trafico conforme al mapeo de puertos.
La sección final se refiere al enmascarado de salida del tráfico, describe el tráfico que se genera por el IPS y no se revele información de las máquinas internas.
En el script de inicio del sistema "/etc/rc.local", se debe mencionar el startsuricata.sh

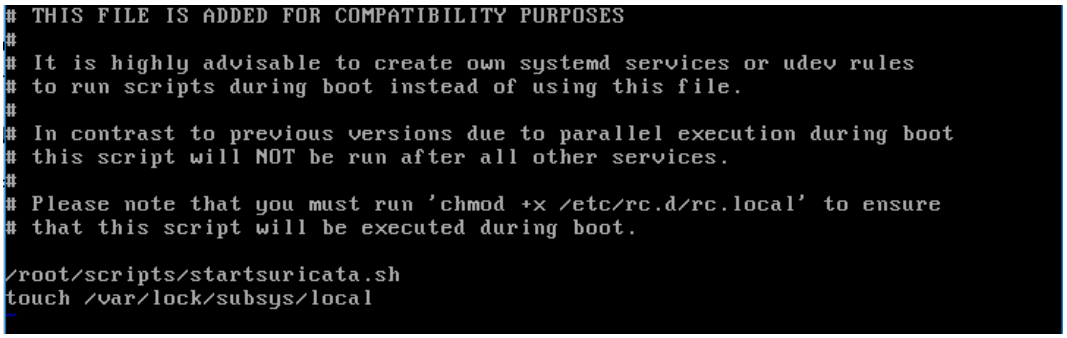


Figura 85: Archivo rc.local

Actualización de las reglas de suricata con Oinkmaster

En el script "updaterules.sh" ubicado en "/root/script" se actualiza todas las reglas del IPS, el contenido es el siguiente:

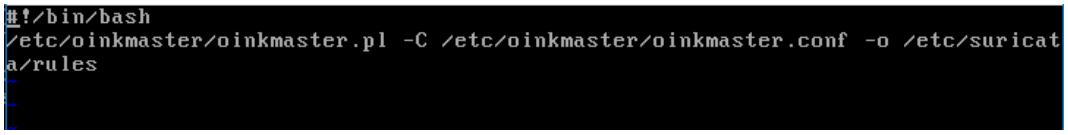


Figura 86: Archivo updaterules.sh

A continuación, se agrega un contrab en el sistema para que se automatice de otra forma no servirá el script.

- 0 */6 * * * /root/scripts/updaterules.sh

Cada 6 horas será actualizado el sistema aplicando las tareas del sistema y a continuación se realiza un restart del Suricata para que las reglas se refresquen.

Algoritmo de descubrimiento de irregularidades en el tráfico TCP

El algoritmo organiza los paquetes por tuplas SYN, las cuales consiste en un agrupamiento de atributos básicos con una dirección IP con la cual será monitoreada.
(IP Source address, SYNS, SYNACKS, FINSSENT, FINSBACK, RESETS, ICMP ERRORS, PKTSSENT, PKTSBACK, port signature data)
SYNS son contadores de paquetes SYN enviados desde el IP fuente.
SYNACKS es un subset de aquellos SYN enviados con la bandera ACK.
Los FINS son una bandera que notifica que no hay más datos que mandar desde la fuente.
RESETS son contados cuando son enviados de regreso a la IP fuente.
ICMP Errors se refiere a ciertos errores de ICMP que son inalcanzables.
PKTSSENT cuenta los paquetes que han sido enviados por la IP fuente.
PKTSBACK son los paquetes que retornan a la fuente IP.

Irregularidades en los paquetes UDP

El front-end toma paquetes UDP en forma de tuplas durante el periodo de recolección de datos, aproximadamente ocurre cada 30 segundos. Las tuplas UDP producidas por el periodo de recolección de datos son llamados UDP Port Report. La tupla tiene la siguiente forma:

(IPSRC, WEIGHT, SENT, RECV, ICMPERRORS, L3D, L4D, SIZEINFO, SA/RA, APPFLAGS, PORTSIG).
La clave lógica en esta tupla es la dirección IP IPSRC (IP Source).
SENT y RECEIVED son contadores de los paquetes UDP enviados desde/hasta el host en cuestión.
ICMPERRORS es un contador de tipos distintos de errores ICMP que pueden haber, normalmente la mayoría de los errores se dan porque el destino es inalcanzable.
L3D es el contador de la capa 3 de direcciones IP destino durante el periodo recolectado.
L4D es el contador de los puertos UDP destino.
SIZEINFO es un histograma de tamaño de paquetes enviados a nivel capa 7.
SA/RA es un promedio de la carga útil del tamaño de los paquetes UDP en capa 7 enviados por el host (SA) y recibidos por el host (RA).
APPFLAGS es un campo programable basado en expresiones regulares y es usado para inspeccionar el contenido en capa 7.

4.8.2. Herramientas utilizadas para Pruebas

Hping3

Es una herramienta multi-usos para generar paquetes TCP/IP. Provee flexibilidad en el manejo y customización de paquetes y es ampliamente usado en pruebas de desempeño de red, servidores y dispositivos de red [33].

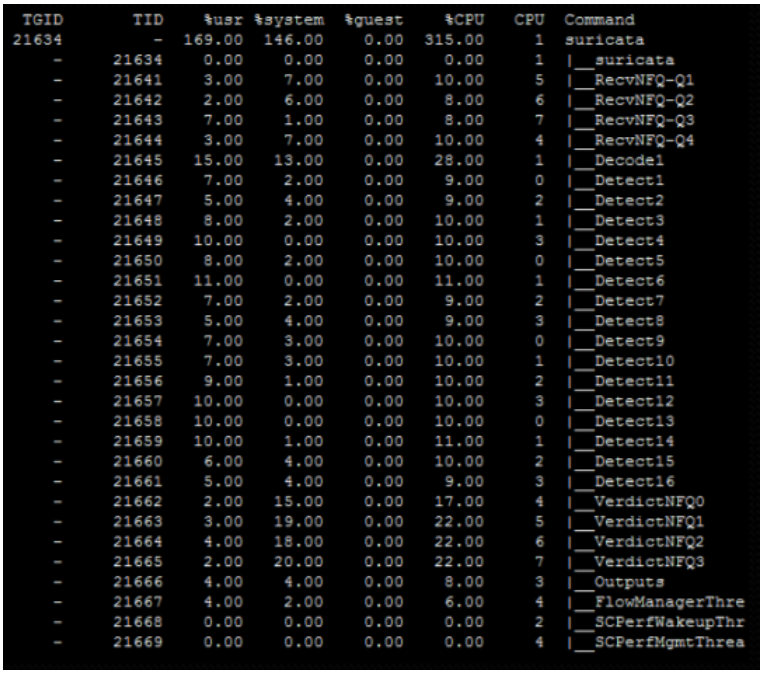
Httperf

Herramienta desarrollada para realizar pruebas de desempeño en los servidores HTTP. Es más usado en pruebas de stress para medir las capacidades de los servidores web [37].

Siege

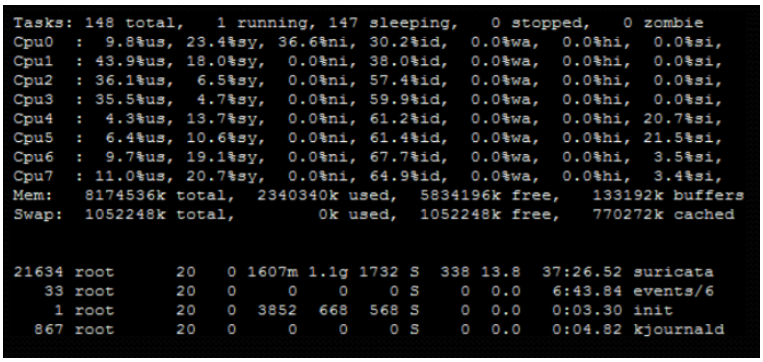
Simula tráfico real hacia servidores web generando peticiones constantes desde varios navegadores web virtuales. Permite cargar una lista de peticiones web para luego repetirlas simulando tráfico de Internet [22].

4.8.3. Resultados de pruebas de rendimiento de Suricata



TGID	TID	%usr	%system	%guest	%CPU	CPU	Command
21634	-	169.00	146.00	0.00	315.00	1	suricata
-	21634	0.00	0.00	0.00	0.00	1	|__suricata
-	21641	3.00	7.00	0.00	10.00	5	|__RecvNFQ-Q1
-	21642	2.00	6.00	0.00	8.00	6	|__RecvNFQ-Q2
-	21643	7.00	1.00	0.00	8.00	7	|__RecvNFQ-Q3
-	21644	3.00	7.00	0.00	10.00	4	|__RecvNFQ-Q4
-	21645	15.00	13.00	0.00	28.00	1	|__Decode1
-	21646	7.00	2.00	0.00	9.00	0	|__Detect1
-	21647	5.00	4.00	0.00	9.00	2	|__Detect2
-	21648	8.00	2.00	0.00	10.00	1	|__Detect3
-	21649	10.00	0.00	0.00	10.00	3	|__Detect4
-	21650	8.00	2.00	0.00	10.00	0	|__Detect5
-	21651	11.00	0.00	0.00	11.00	1	|__Detect6
-	21652	7.00	2.00	0.00	9.00	2	|__Detect7
-	21653	5.00	4.00	0.00	9.00	3	|__Detect8
-	21654	7.00	3.00	0.00	10.00	0	|__Detect9
-	21655	7.00	3.00	0.00	10.00	1	|__Detect10
-	21656	9.00	1.00	0.00	10.00	2	|__Detect11
-	21657	10.00	0.00	0.00	10.00	3	|__Detect12
-	21658	10.00	0.00	0.00	10.00	0	|__Detect13
-	21659	10.00	1.00	0.00	11.00	1	|__Detect14
-	21660	6.00	4.00	0.00	10.00	2	|__Detect15
-	21661	5.00	4.00	0.00	9.00	3	|__Detect16
-	21662	2.00	15.00	0.00	17.00	4	|__VerdictNFQ0
-	21663	3.00	19.00	0.00	22.00	5	|__VerdictNFQ1
-	21664	4.00	18.00	0.00	22.00	6	|__VerdictNFQ2
-	21665	2.00	20.00	0.00	22.00	7	|__VerdictNFQ3
-	21666	4.00	4.00	0.00	8.00	3	|__Outputs
-	21667	4.00	2.00	0.00	6.00	4	|__FlowManagerThre
-	21668	0.00	0.00	0.00	0.00	2	|__SCPerfWakeupThr
-	21669	0.00	0.00	0.00	0.00	4	|__SCPerfMgmtThrea

Figura 87: Tratamiento de Suricata por Hilos con 4 colas



```
Tasks: 148 total,   1 running, 147 sleeping,   0 stopped,   0 zombie
Cpu0  :  9.8%us, 23.4%sy, 36.6%ni, 30.2%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu1  : 43.9%us, 18.0%sy,  0.0%ni, 38.0%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu2  : 36.1%us,  6.5%sy,  0.0%ni, 57.4%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu3  : 35.5%us,  4.7%sy,  0.0%ni, 59.9%id,  0.0%wa,  0.0%hi,  0.0%si,
Cpu4  :  4.3%us, 13.7%sy,  0.0%ni, 61.2%id,  0.0%wa,  0.0%hi, 20.7%si,
Cpu5  :  6.4%us, 10.6%sy,  0.0%ni, 61.4%id,  0.0%wa,  0.0%hi, 21.5%si,
Cpu6  :  9.7%us, 19.1%sy,  0.0%ni, 67.7%id,  0.0%wa,  0.0%hi,  3.5%si,
Cpu7  : 11.0%us, 20.7%sy,  0.0%ni, 64.9%id,  0.0%wa,  0.0%hi,  3.4%si,
Mem:   8174536k total,  2340340k used,  5834196k free,   133192k buffers
Swap:  1052248k total,        0k used,  1052248k free,   770272k cached


21634 root      20   0 1607m 1.1g 1732 S  338 13.8  37:26.52 suricata
   33 root      20   0     0    0    0 S    0  0.0   6:43.84 events/6
    1 root      20   0  3852  668  568 S    0  0.0   0:03.30 init
  867 root      20   0     0    0    0 S    0  0.0   0:04.82 kjournald
```

Figura 88: Tratamiento de Suricata por procesador con 4 colas

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1. Conclusiones

- En relación a enunciar las bases teóricas y las características de implementación referente al monitoreo y protección de datos de red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, existen varias fuentes de consulta en las cuales se determinó los componentes teóricos de la tecnología hardware y software necesarios para su ejecución.

  Una vez comprendida la necesidad de monitoreo de la red de datos de la FISEI se establece que el sistema MUNIN presta todas las características para este fin, contemplando los conceptos básicos para un correcto control de monitoreo de red.

- El monitoreo de la red de datos ha sido eficaz en cuanto a la detección de fallos y congestionamiento, debido a la utilización de sistemas de monitoreo implementados en la red de la FISEI en el sector de administración de redes.

  Se efectuó el análisis de las herramientas de monitoreo más idóneas para la observación de la red de datos de la FISEI, por lo cual el sistema Munin fue el más idóneo cumpliendo con todas las proyecciones necesarias para la detección de fallos y congestionamiento en el ancho de banda.

- En referencia al análisis de los resultados del monitoreo, las anomalías que provocan degradación en la red son aquellas que producen embotellamientos en el ancho de banda además de la inexistencia de Internet.

  Cuenta con un seguimiento del comportamiento de los dispositivos de la red de la FISEI alertando pérdida de paquetes de transmisión, ataques a la red y deterioros de la misma, con un pico máximo de 31.17k y un incremento de 18.73k de concurrencia en la red, teniendo un tiempo de espera con una conexión activa hacia un cliente de 92.82k de efectividad en beneficio de la institución.

- En relación a lo estudiado a lo largo de la presente proyecto de investigación,

se determinó establecer mecanismos de control y protección de datos para mejorar el rendimiento de la red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.

Respecto al desarrollo del Sistema de Prevención de Intrusos e Identificación de intrusos (IPS/IDS) se implementó Suricata, herramienta necesaria para protección de cualquier arquitectura computacional ya que posee características únicas que no se encuentran en otros sistemas de acuerdo a la comparación realizada en la Tabla 67 en la que se demuestra su superioridad en cuanto a sus peculiaridades técnicas.

- Respecto a realizar las pruebas para comprobar el funcionamiento del sistema, se ingresó el virus Hping3, Httperf y Siege que se fue probando su correcto funcionamiento teniendo como resultado que entre más colas de hilos aumenta el procesamiento del servidor.

5.2. Recomendaciones

- Utilizar la implementación de la aplicación MUNIN para el monitoreo de la red de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, porque en base al cuadro comparativo cumple con todos los parámetros exigibles para su aplicación una ves realizada la investigación correspondiente.

- Identificar claramente las necesidades del administrador de redes respecto al control que requiere en la red de la FISEI para determinar e implementar reglas de seguridad en los sistemas de monitoreo y protección de datos, mediante un plan de contingencia como la implementación de un manual de redes, para conocer de forma oportuna cada una de las aristas de manejo, control entre otras sobra la seguridad de la red.

- Se sugiere al personal de la Administración de redes de la FISEI realizar actualizaciones de los dispositivos a medida que la red va creciendo y configurando los grupos y comunidades de SNMP, con la finalidad de precautelar y ordenar los datos de la red.

- Se recomienda la precaución al momento de ejecutar las actualizaciones en su versión del sistema MUNIN y sus componentes, ya que existe varias librerías que varía en el uso, y al realizar mal este proceso conlleva a una caída del servidor.

- En vista de la inexistencia de una red de datos estructurada en la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato es factible dividir en varias subredes fraccionados por medio de router o switch administrables para un mayor control y presión de la distribución de la red facilitando así el monitoreo con la incorporación de nuevas tecnologías.

Bibliografia

[1] CISCO, "Cisco visual networking index: Forecast and methodology, 20142019," *CISCO*, Abril 2016. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html

[2] T. d. l. I. y. C. (TIC'S)2013, "Inec," 2013.

[3] F. E. E. Vega, "Sistema de anÁlisis y control de red de datos & voip para el gobierno provincial de tungurahua," 2015.

[4] S. J. G. Ulloa, *SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO UNIÓN POPULAR LTDA*, Universidad Técnica de Ambato Std., Febrero 2015.

[5] M. Payero, *Administración de dispositivos Informáticos Vía Wireless orientado a Open Source.*, Universidad de Palermo, Facultad de Ingeniería Argentina Std.

[6] L. Alegsa, *DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA*, ALEGSA, Ed., 2016. [Online]. Available: http://www.alegsa.com.ar/Dic/servidor.php

[7] H. Mike, "Punto de acceso inalámbrico (wap)," 2005. [Online]. Available: http://www.pearsonitcertification.com/articles/article.aspx?p=398091&seqNum=12

[8] C. SYSTEMS, "Lo que usted necesita saber sobre routers y switches." 1992-2012. [Online]. Available: http://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

[9] M. G. y Barrio Guzmán, "IntroducciÓn a la configuraciÓn de routers cisco," UNIVERSIDAD ORT URUGUAY, Tech. Rep., 2007. [Online]. Available: http://www.ort.edu.uy/fi/pdf/configuracionroutersciscomatturro.pdf

[10] S. William, *Network Security Essentials Applications and Standards*, M. Hirsch, Ed. Horton Marcia J., 2011.

[11] Seguinfo, “Herramientas para el monitoreo del estado de red,” 2007. [Online]. Available: https://seguinfo.wordpress.com/2007/09/12/herramientas-para-el-monitoreo-del-estado-de-red/

[12] C. C. E. N. ARELLANO AUCANCELA JUANA KARINA, “AnÁlisis de herramientas opensource de administraciÓn y monitoreo basado en snmp, aplicado a la red de datos del ilustre municipio de ambato,” ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZON, Tech. Rep., 2011.

[13] A. L. C. FIGUEROA, *ESTUDIO DE LA IMPLEMENTACION DE REDUNDANCIA PARA UN SISTEMA DE MONITOREO EN EMPRESAS DE TELECOMUNICACIONES*, UNIVERSIDAD CENTRAL DEL ECUADOR, FACULTAD DE INGENIERÍA, CIENCIAS FÍSICAS Y MATEMÁTICA Std., 2016.

[14] M. G. J. Romero, “El monitoreo de los recursos de red,” vol. 11, no. 2, 2013. [Online]. Available: http://www.pedagogiaprofesional.rimed.cu/Numeros/Vol%2011%20No%202/gera.pdf

[15] J. I. B. Villagómez, “Servidor de control de dispositivos y servicios mediante el protocolo snmp para la red de datos en celec .e.p. unidad de negocio hidroagoyan.” Julio 2015.

[16] *SNMP PROTOCOL*, Std. [Online]. Available: http://www.ebah.com.br/content/ABAAAfctoAG/snmp?part=1

[17] E. G. T. LOAYZA, “Desarrollo de una guÍa prÁctica para la mediciÓn del trÁfico de red ip y monitoreo de dispositivos en tiempo real mediante herramientas mrtg y prtg,” 2010.

[18] G. A. A. Jorge E. RODRÍGUEZ, Diana C. MACHADO, Bogotá Colombia Patent, 2012. [Online]. Available: http://www.iiis.org/CDs2012/CD2012SCI/CISCI_2012/PapersPdf/CA087KI.pdf

[19] R. Julio, “Seguridad informática.” [Online]. Available: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml

[20] M. Katz, *Redes y Seguridad*, A. G. Editor, Ed., 2013. [Online]. Available: http://site.elibro.com

[21] A. Alex, “Ips e ids sus diferencias y funcionamiento,” 2013. [Online]. Available: https://prezi.com/ewpc5tkijdot/ips-e-ids-sus-diferencias-y-funcionamiento/

[22] *Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial*, 2012. [Online]. Available: https://www.dspace.espol.edu.ec/bitstream/123456789/20914/1/Paper-Suricata%20(1).pdf

[23] C. D. I. C. E. N. I, “InvestigaciÓn y desarrollo revista de la universidadtÉcnica de ambato,” 2010. [Online]. Available: https://issuu.com/publicarrevista/docs/_revista2___ceni_sistemas/14

[24] W. JONATHAN, “Cómo monitorear los recursos de un servidor utilizando munin,” 2014. [Online]. Available: http://codehero.co/como-monitorear-los-recursos-de-un-servidor-utilizando-munin/

[25] EcuRed, “Sistema de monitoreo munin,” 2013. [Online]. Available: https://www.ecured.cu/Sistema_de_monitoreo_Munin

[26] T. Oetiker, “Mrtg,” 2012. [Online]. Available: http://oss.oetiker.ch/mrtg/doc/mrtg.en.html

[27] Ecured, “Rrdtool,” 2017. [Online]. Available: https://www.ecured.cu/RRDtool

[28] P. Francesc, “Monitorización de red con snmp y mrtg,” Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, Tech. Rep., 2011.

[29] T. C. J. ALBERTO, “ImplementaciÓn de un sistema de mediciÓn y monitoreo de trÁfico ip basado en software libre, con el fin de realizar una planeaciÓn adecuada de las capacidades de la red wan de la empresa alianzanet s.a.” p. 82 y 83, 2009.

[30] M. L. Ricardo González, Giancarlos Cataldo, “Prismi: Prototipo de una red inalámbrica de sensores para monitorización industrial,” Universidad Simón Bolívar, Caracas, Venezuela, Tech. Rep., 2009. [Online]. Available: https://www.researchgate.net/profile/Ricardo_Gonzalez20/publication/228735919_PRISMI_Prototipo_de_una_Red_Inalambrica_de_Sensores_para_Monitorizacion_Industrial/links/00b7d524b3f0e6ccb7000000.pdf

[31] *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO BASADO EN SNMP PARA LA RED NACIONAL ACAEMICA DE TECNILOGÍA AVANZADA*, UNIVERSIDAD SANTO TOMAS FACULTAD DE INGENIERIA DE TELECOMUNICACIONES BOGOTÁ D.C. Std., 2014. [Online]. Available: http://porticus.usantotomas.edu.co:8080/bitstream/11634/766/1/diseno%20e%20implementacion%20de%20un%20sistema%20de%20monitoreo%20basado%20en%20snmp%20para%20la%20red%20naciona%20academica%20de%20tecnologia%20avanzada.pdf

[32] L. R. S. María, "Estudio e implementaciÓn de una consola de monitoreo prototipo para evaluar el desempeÑo de las redes ip instaladas en los clientes de la empresa cineto telecomunicaciones s.a." Master's thesis, PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, 2016.

[33] R. Velasco, "Hping3: Manual de utilización de esta herramienta para manipular paquetes tcp/ip," 2015. [Online]. Available: https://www.redeszone.net/gnu-linux/hping3-manual-de-utilizacion-de-esta-herramienta-para-manipular-paquetes-tcp-ip/

[34] O. F. Astudillo Juan, Jimenez Alberto, "Adaptación del ids/ips suricata para que se pueda convertir en una solución empresarial." 2012. [Online]. Available: https://www.dspace.espol.edu.ec/bitstream/123456789/19502/1/Diapositivas_tesina.pdf

[35] R. R MCREE, "Suricata in toolsmith: Meet the meerkat," 2010. [Online]. Available: http://holisticinfosec.blogspot.com/2010/08/suricata-in-toolsmith-meet-meerkat.html

[36] P. SCARFONE, K. MEL, *GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GAITHERSBURG Std., 2007.

[37] G. Gheorghiu, "Http performance testing with httperf, autobench and openload," 2005. [Online]. Available: http://agiletesting.blogspot.com/2005/04/http-performance-testing-with-httperf.html

Anexos y Apéndices

Anexo A

Anexo A

A.1. Mapa de red de la Faculatad de Ingeniería en Sistemas Electrónica e Industrial Laboratorio 1

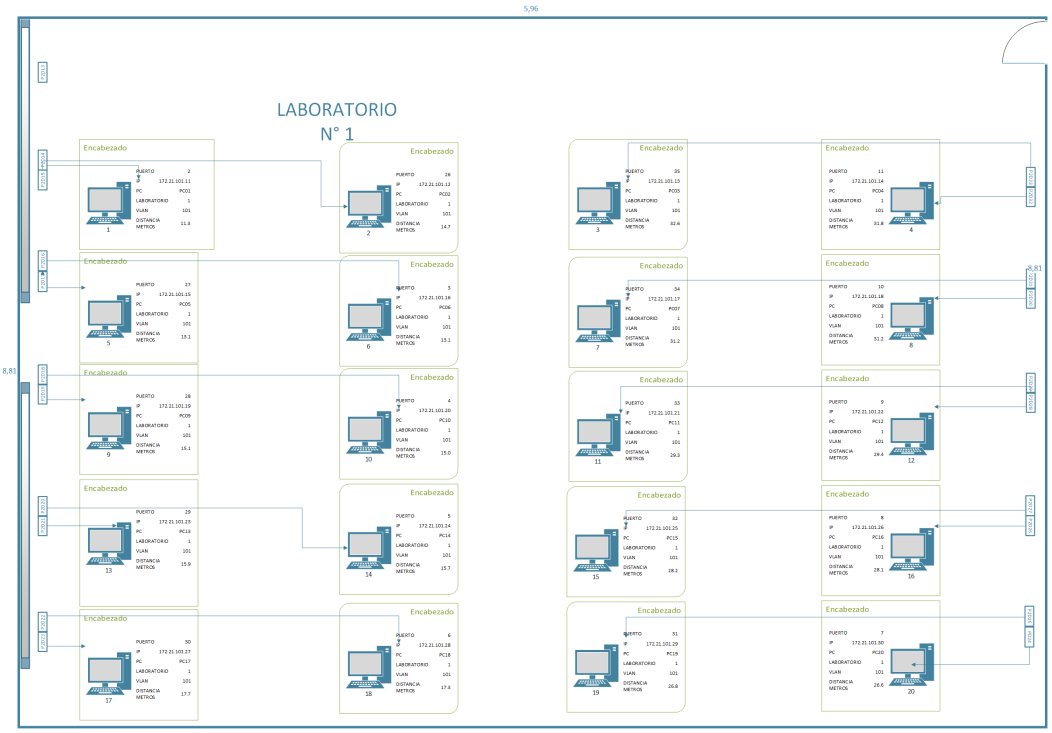


Figure 89: Laboratorio 1

A.2. Laboratorio 2

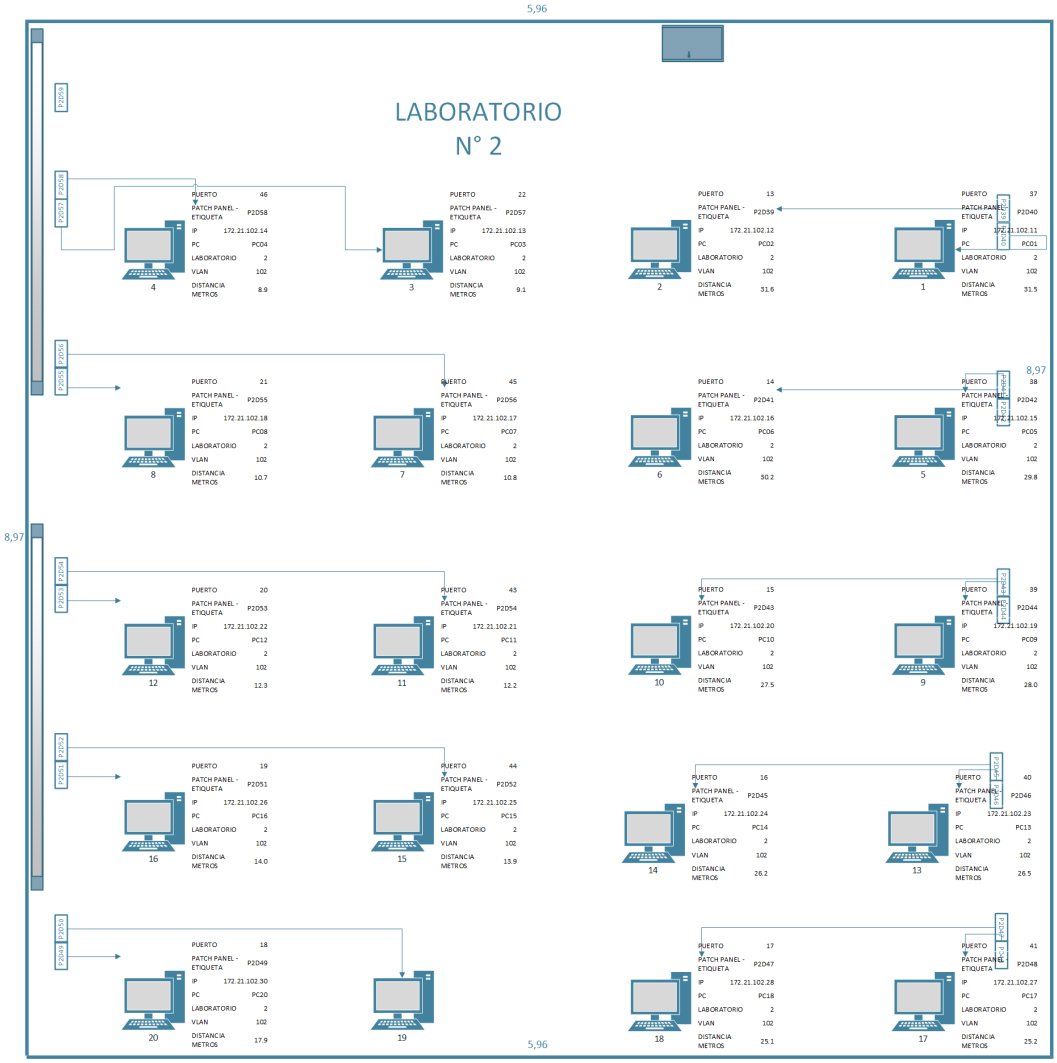


Figure 90: Laboratorio 2

A.3. Laboratorio 3

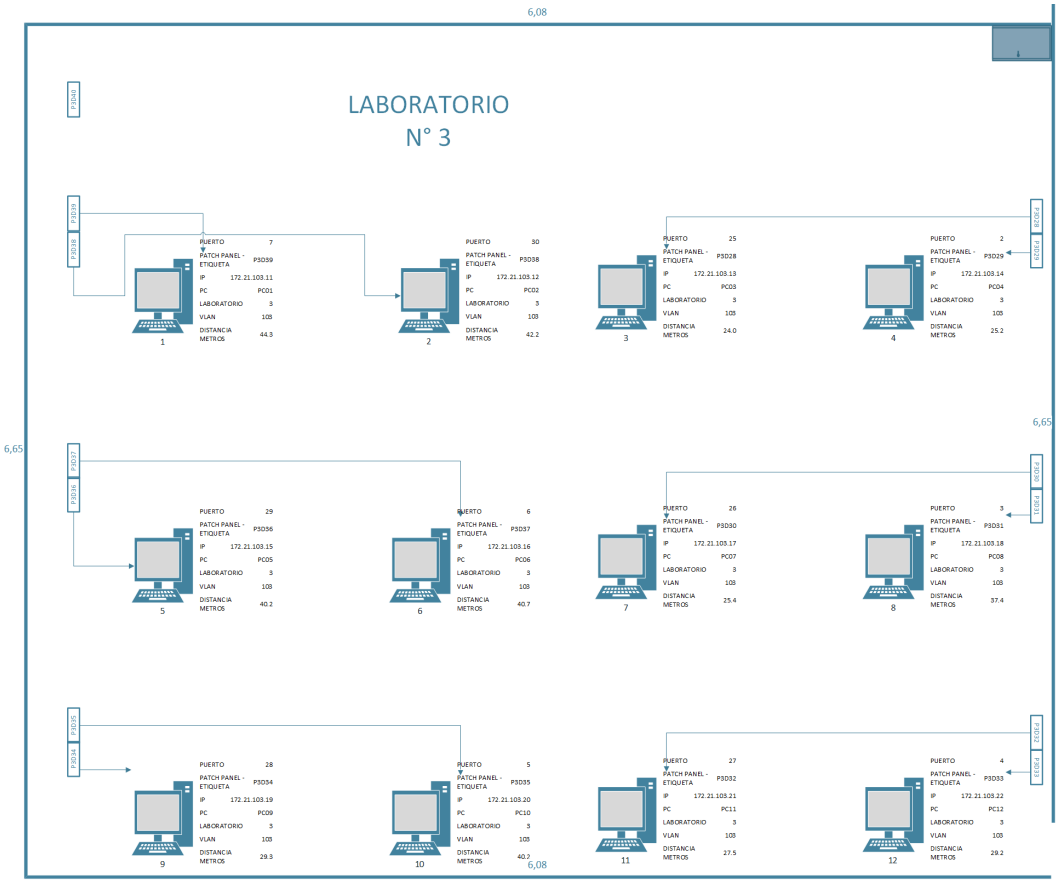


Figure 91: Laboratorio 3

A.4. Laboratorio 4

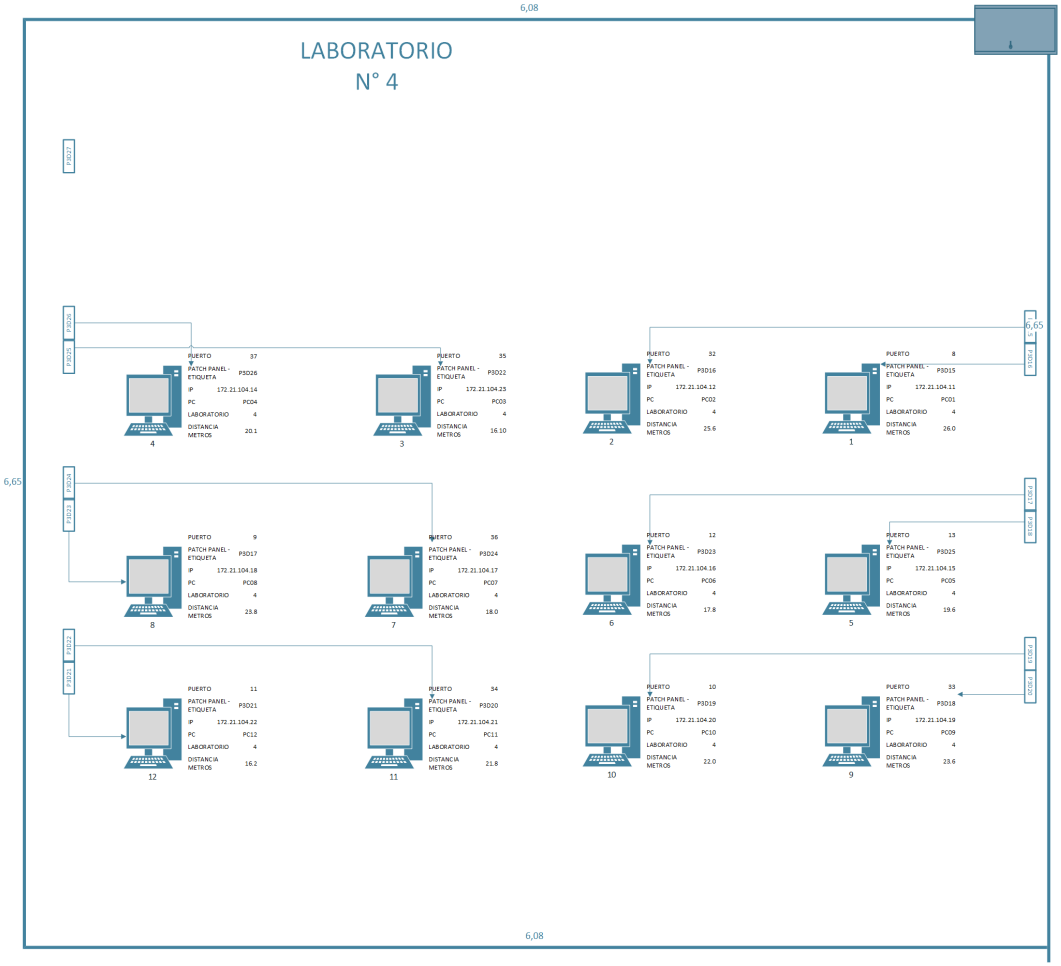


Figure 92: Laboratorio 4

A.5. Laboratorio 5

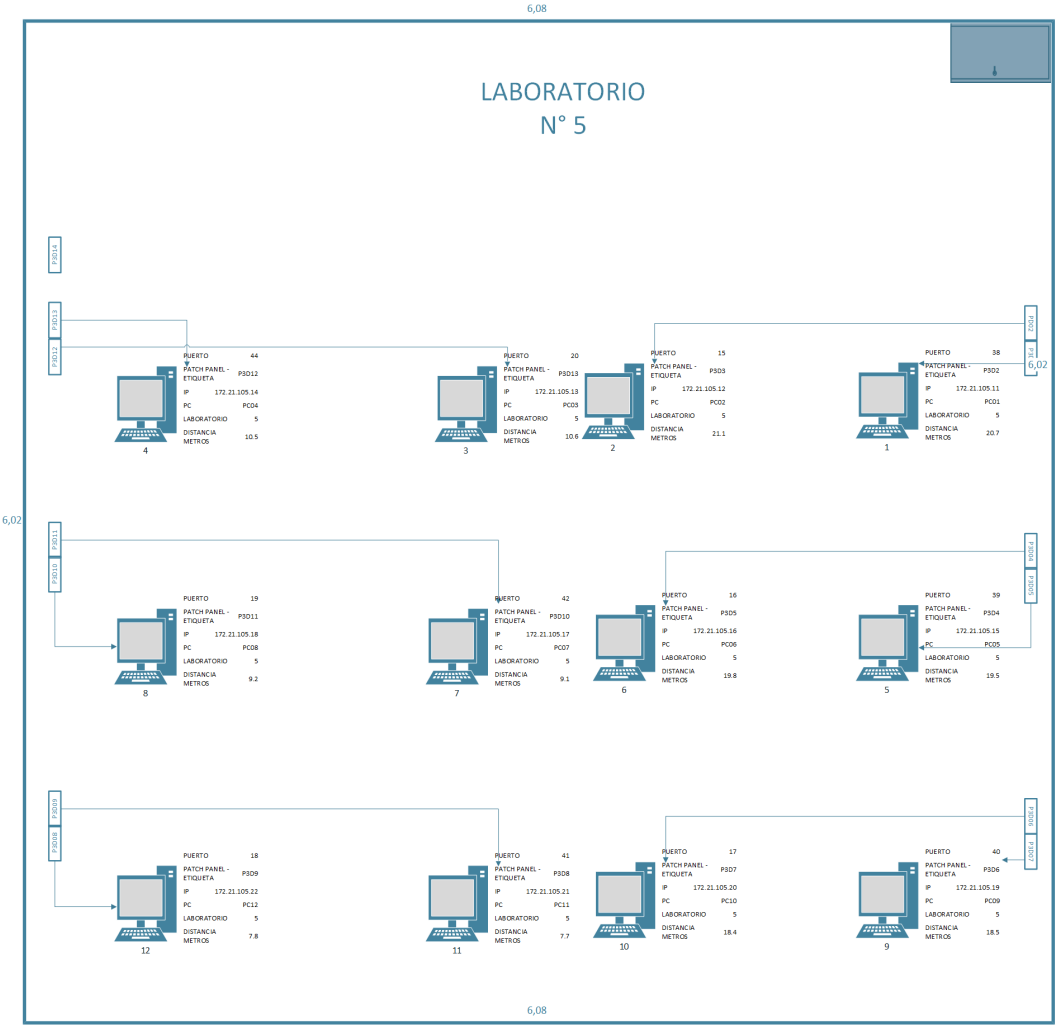


Figure 93: Laboratorio 5

A.6. Laboratorio 6

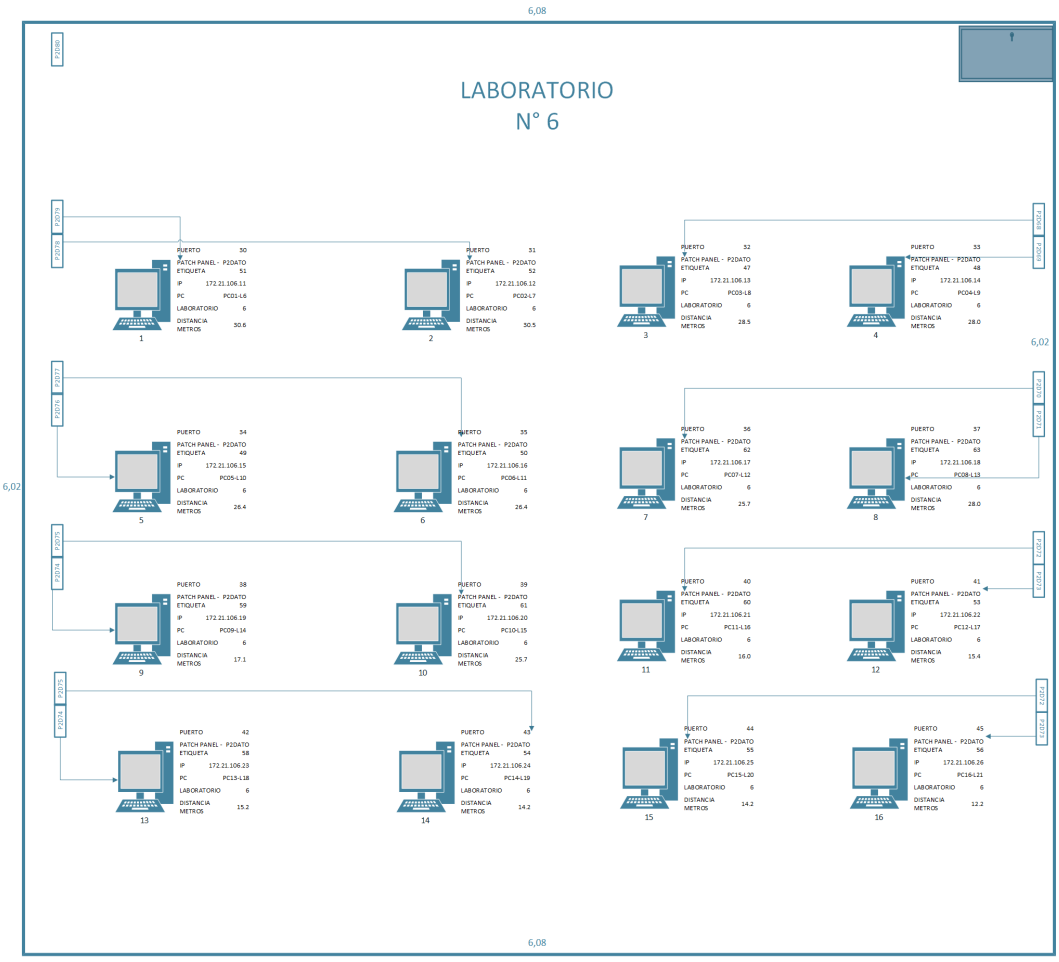


Figure 94: Laboratorio 6

A.7. Laboratorio Redes

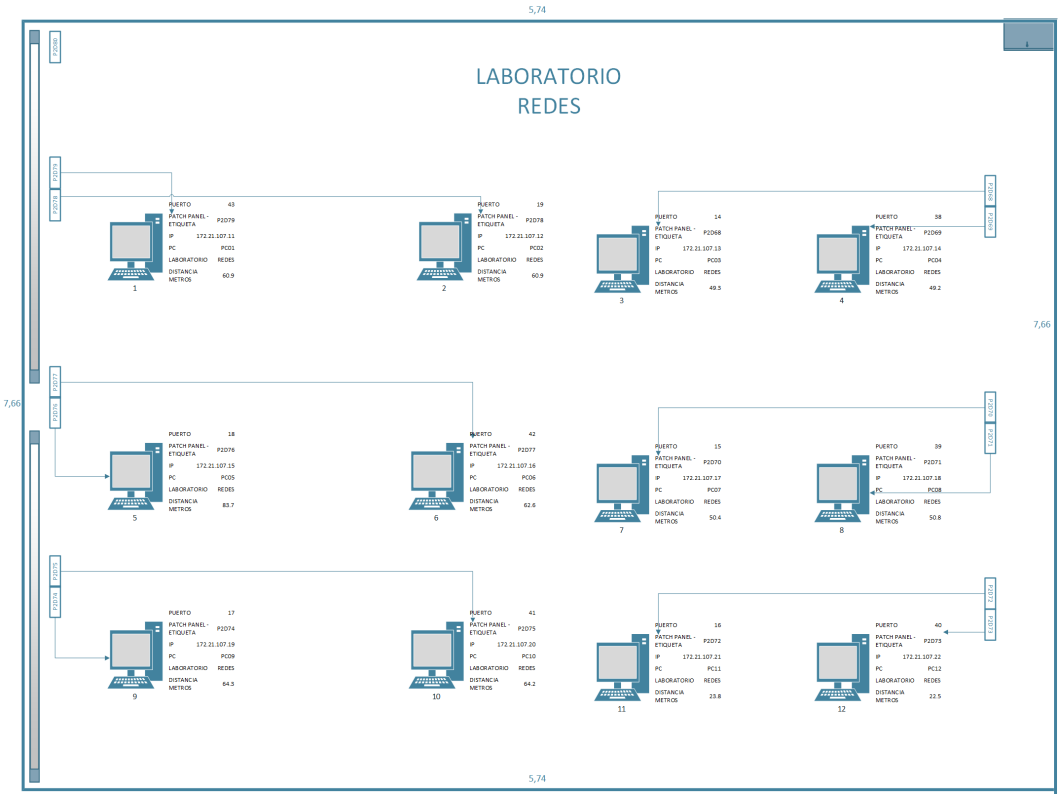


Figure 95: Laboratorio Redes

A.8. Laboratorio Maestrias

Figure 96: Laboratorio Maestrias

A.9. Laboratorio Arquitectura

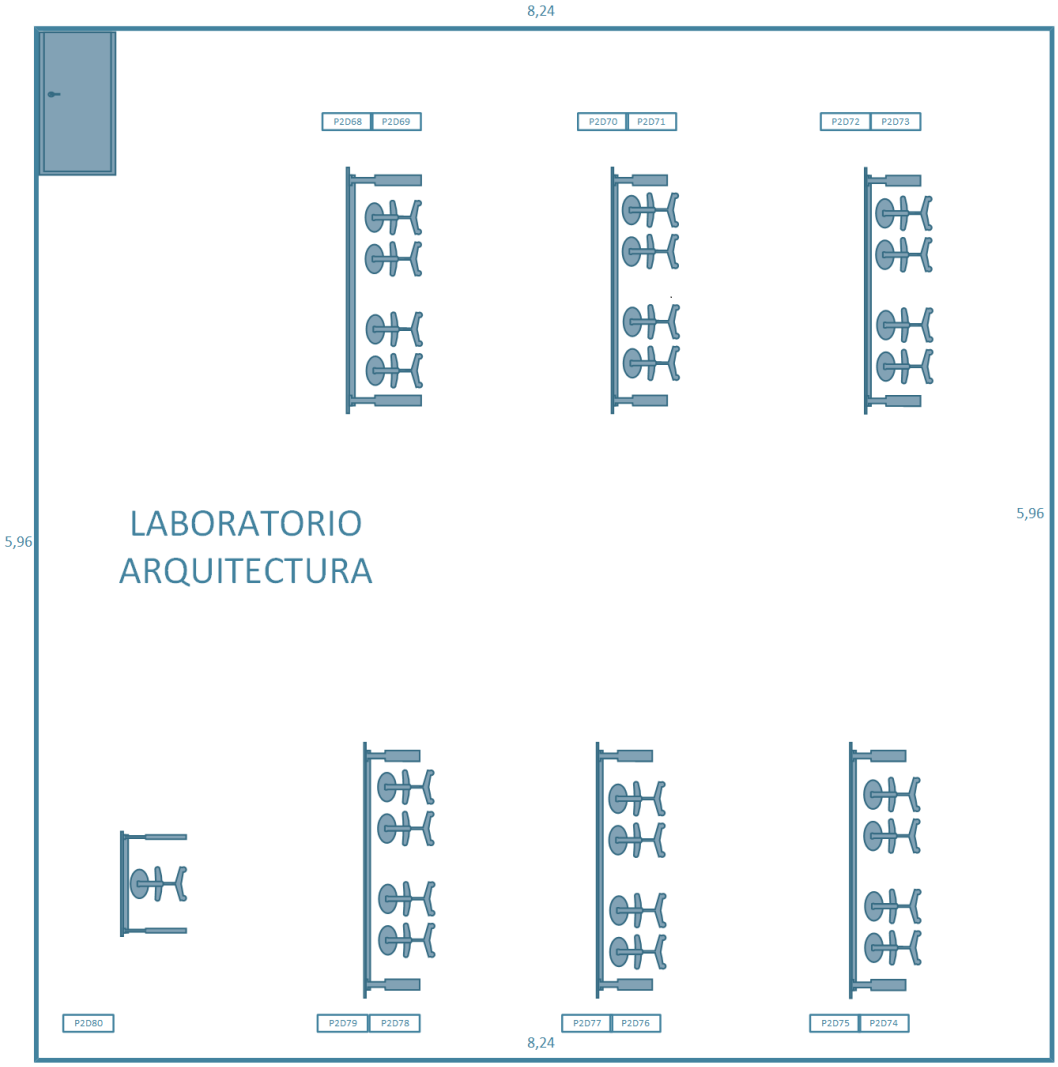


Figure 97: Laboratorio Arquitectura

A.10. Laboratorio Audiovisuales

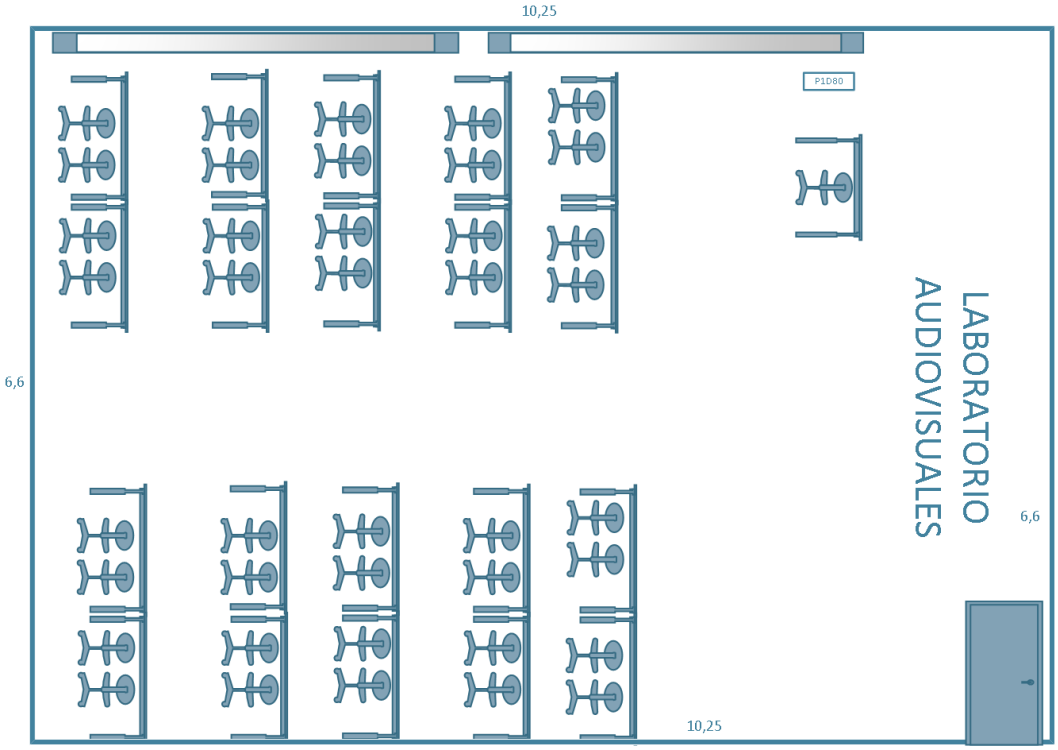


Figure 98: Laboratorio Audiovisuales

A.11. Laboratorio Industrial I

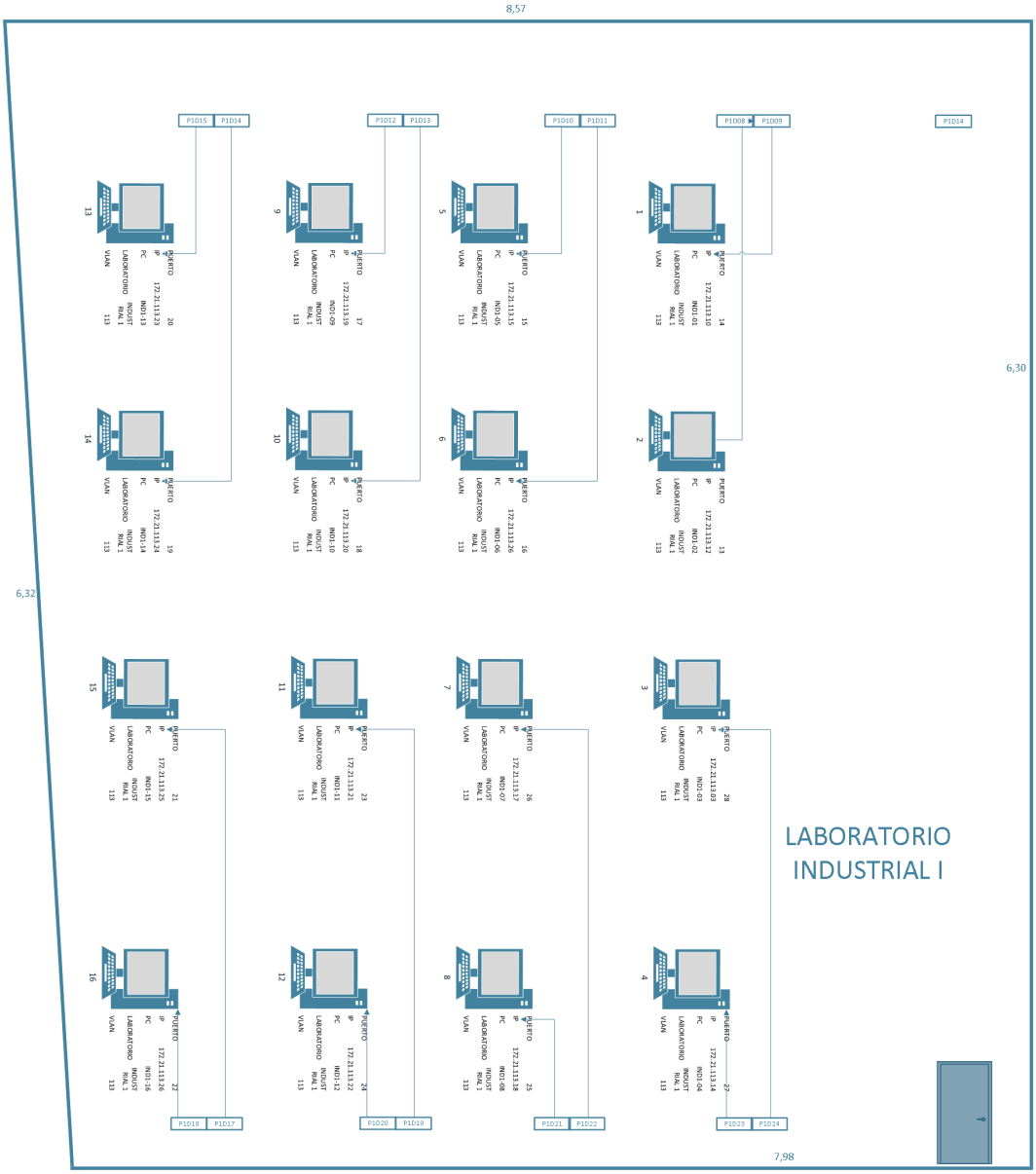


Figure 99: Laboratorio Industrial I

A.12. Laboratorio Industrial II

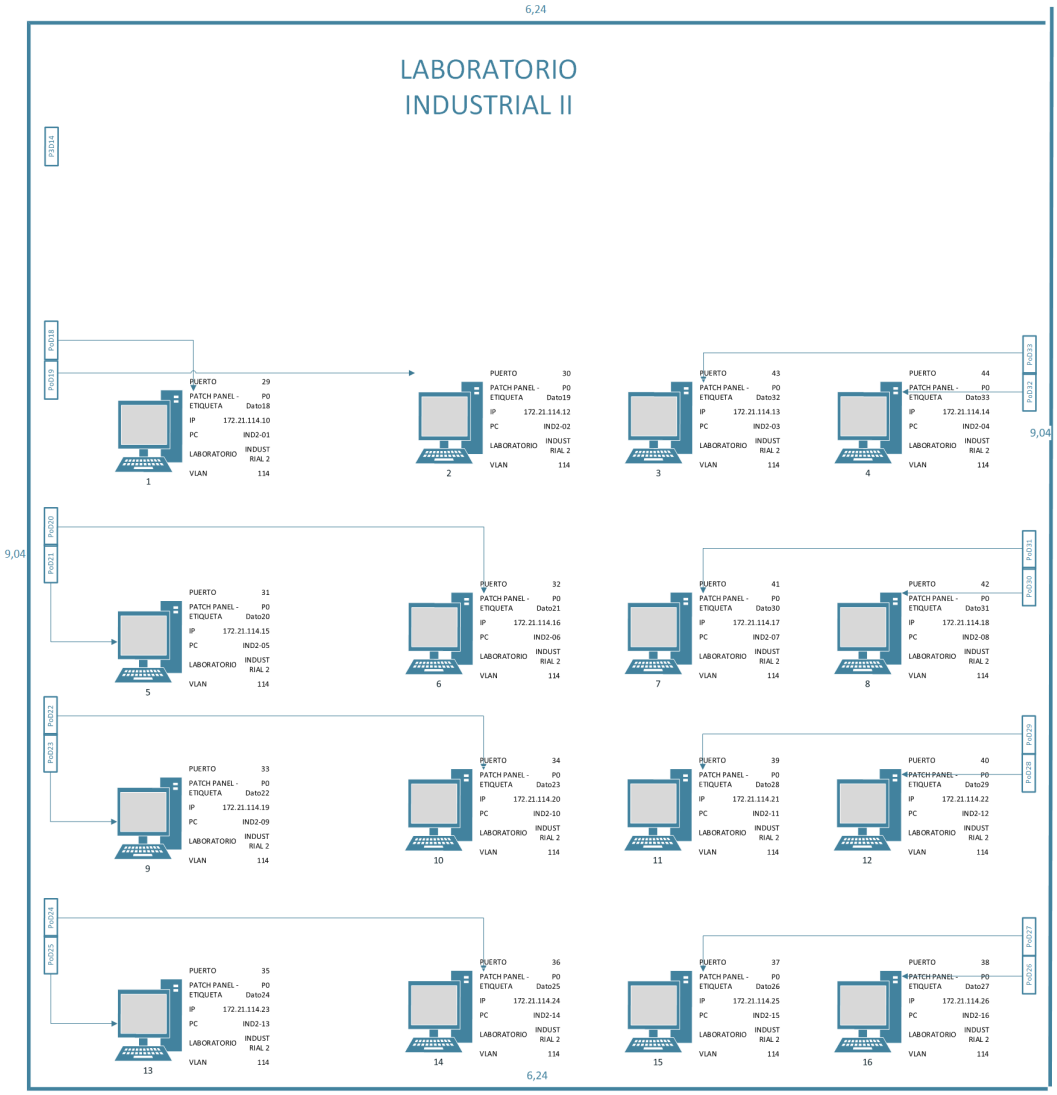


Figure 100: Laboratorio Industrial II

A.13. Laboratorio Robótica

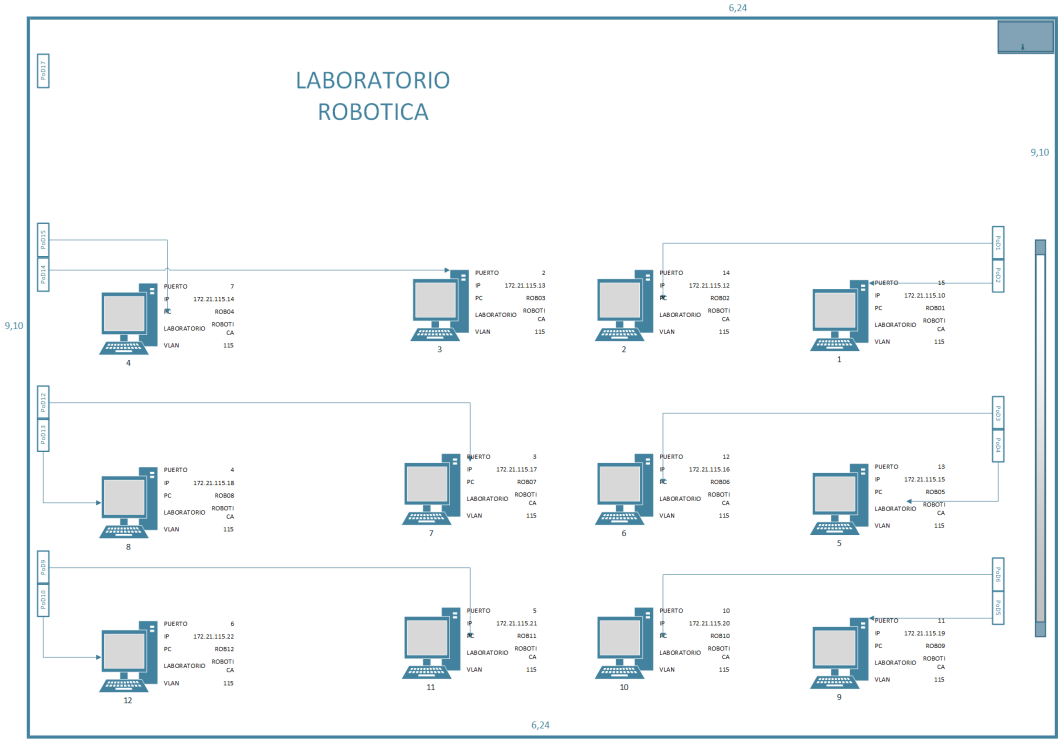


Figure 101: Laboratorio Robótica

A.14. Laboratorio PLC

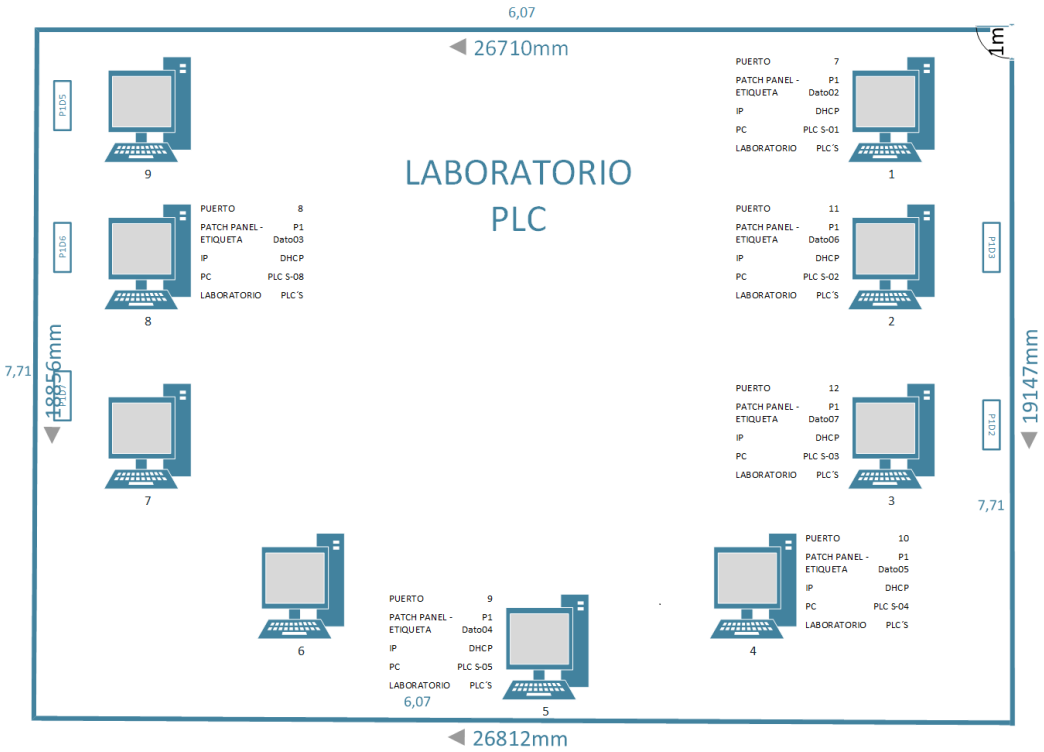


Figure 102: Laboratorio PLC

A.15. Laboratorio Electrónica 2

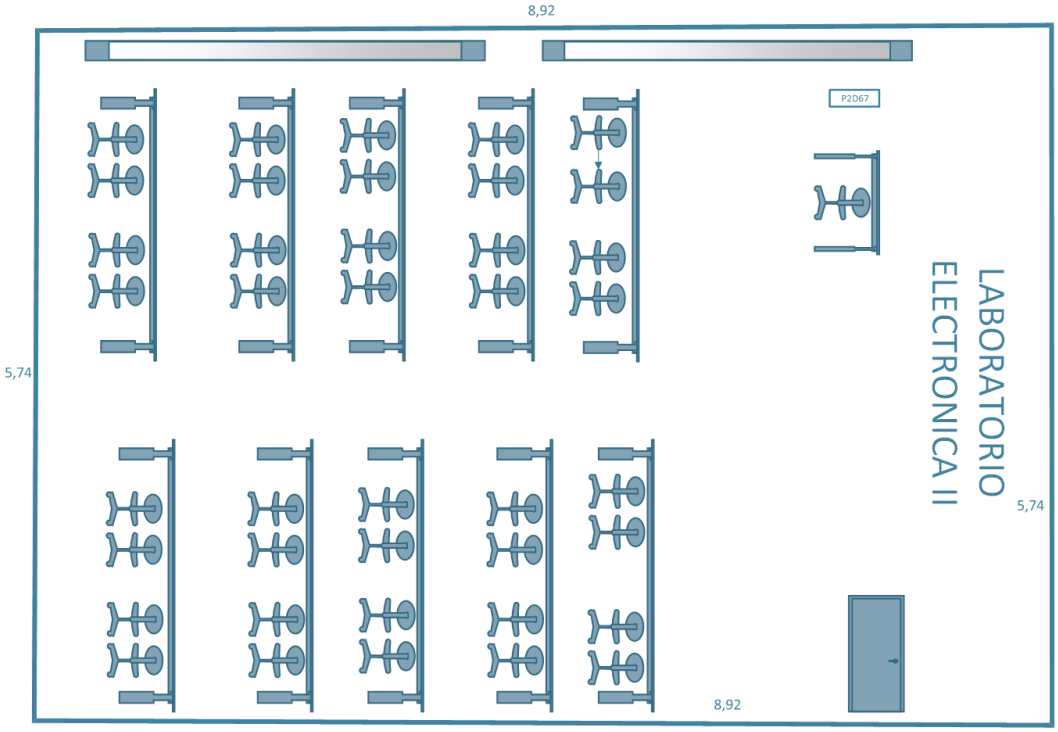


Figure 103: Laboratorio Electrónica 2

A.16. Laboratorio CNC

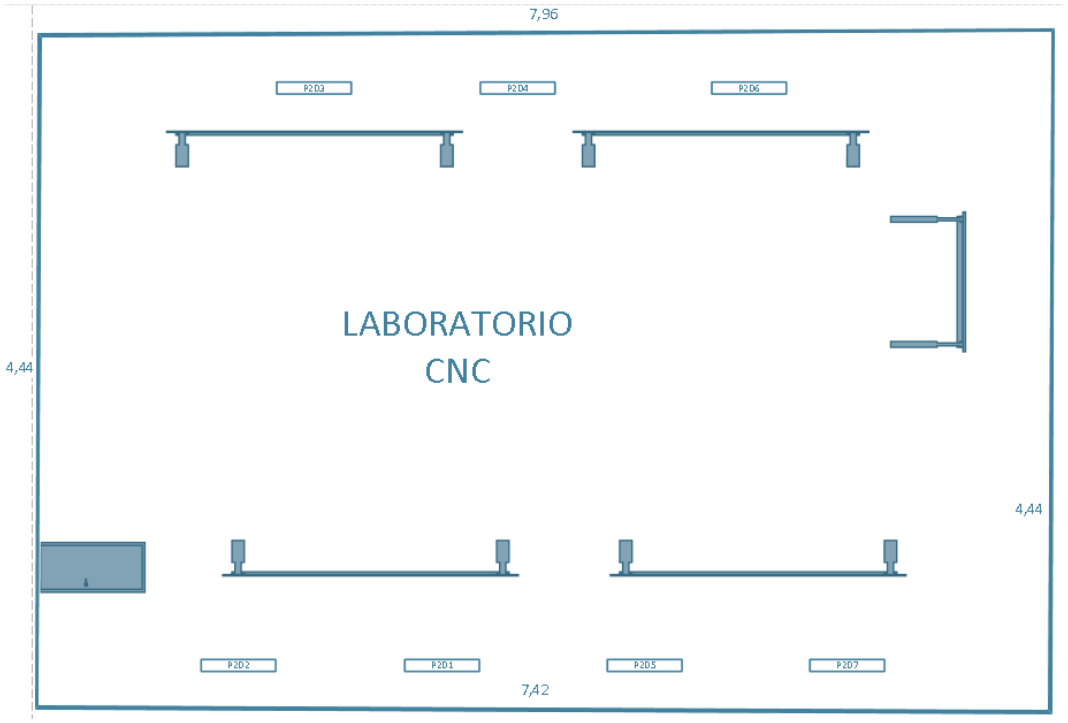


Figure 104: Laboratorio CNC

A.17. Laboratorio de Hidráulica y Neumática

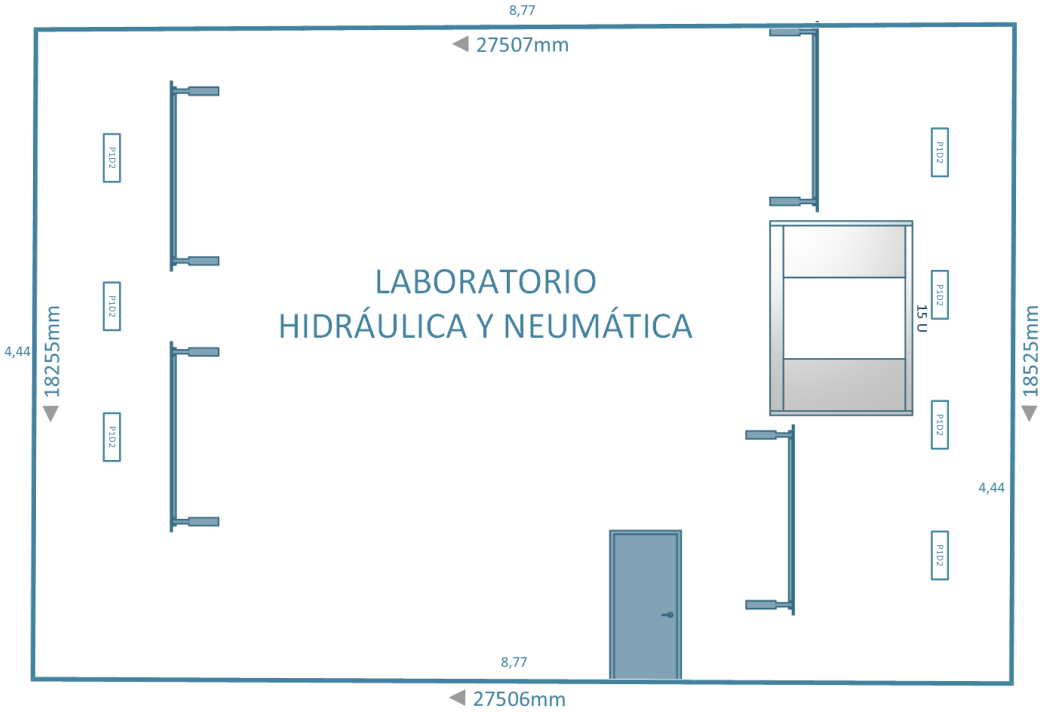


Figura 105: Laboratorio de Hidráulica y Neumática

A.18. Laboratorio CTT II

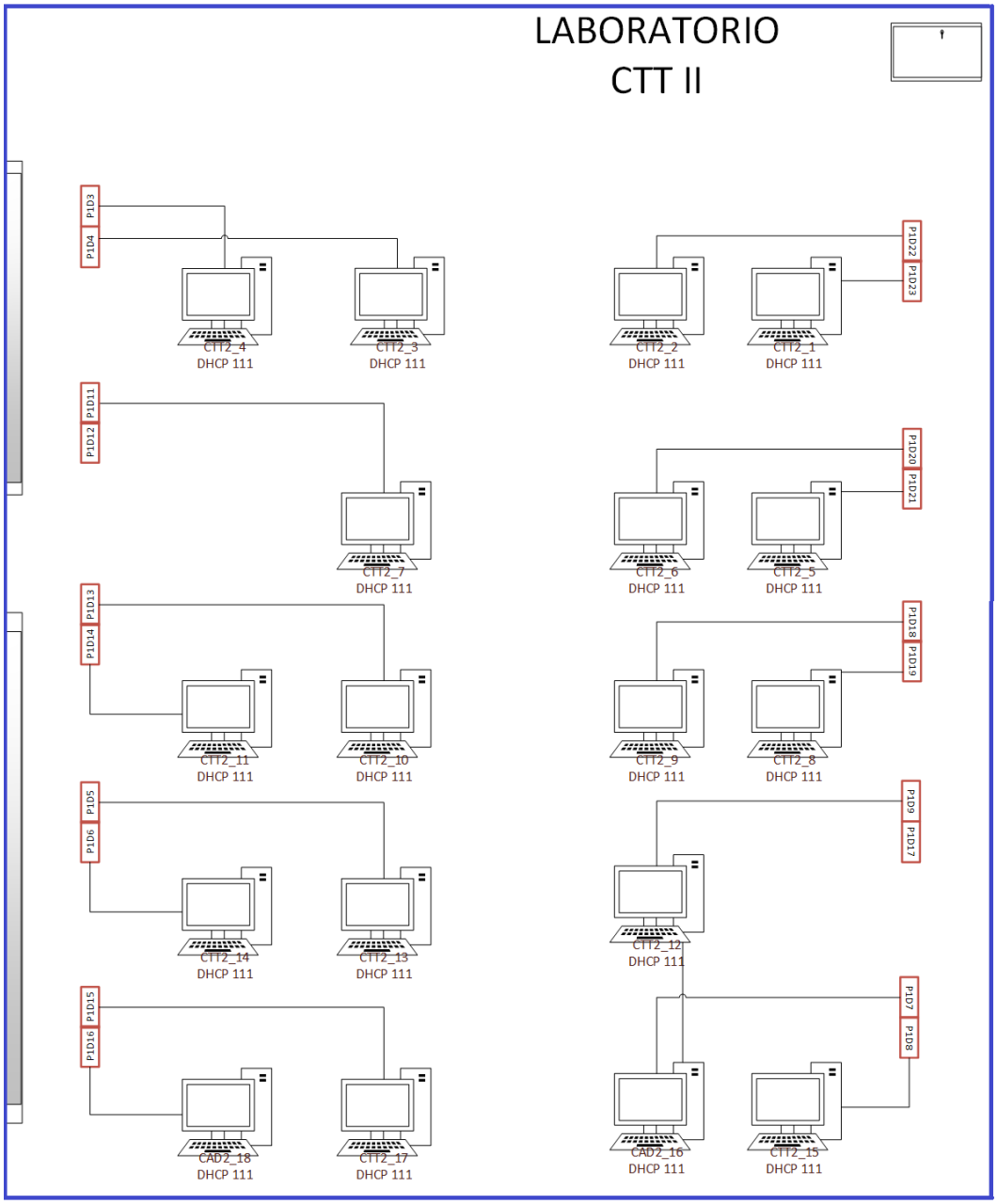


Figure 106: Laboratorio CTT II

A.19. Laboratorio CTT III

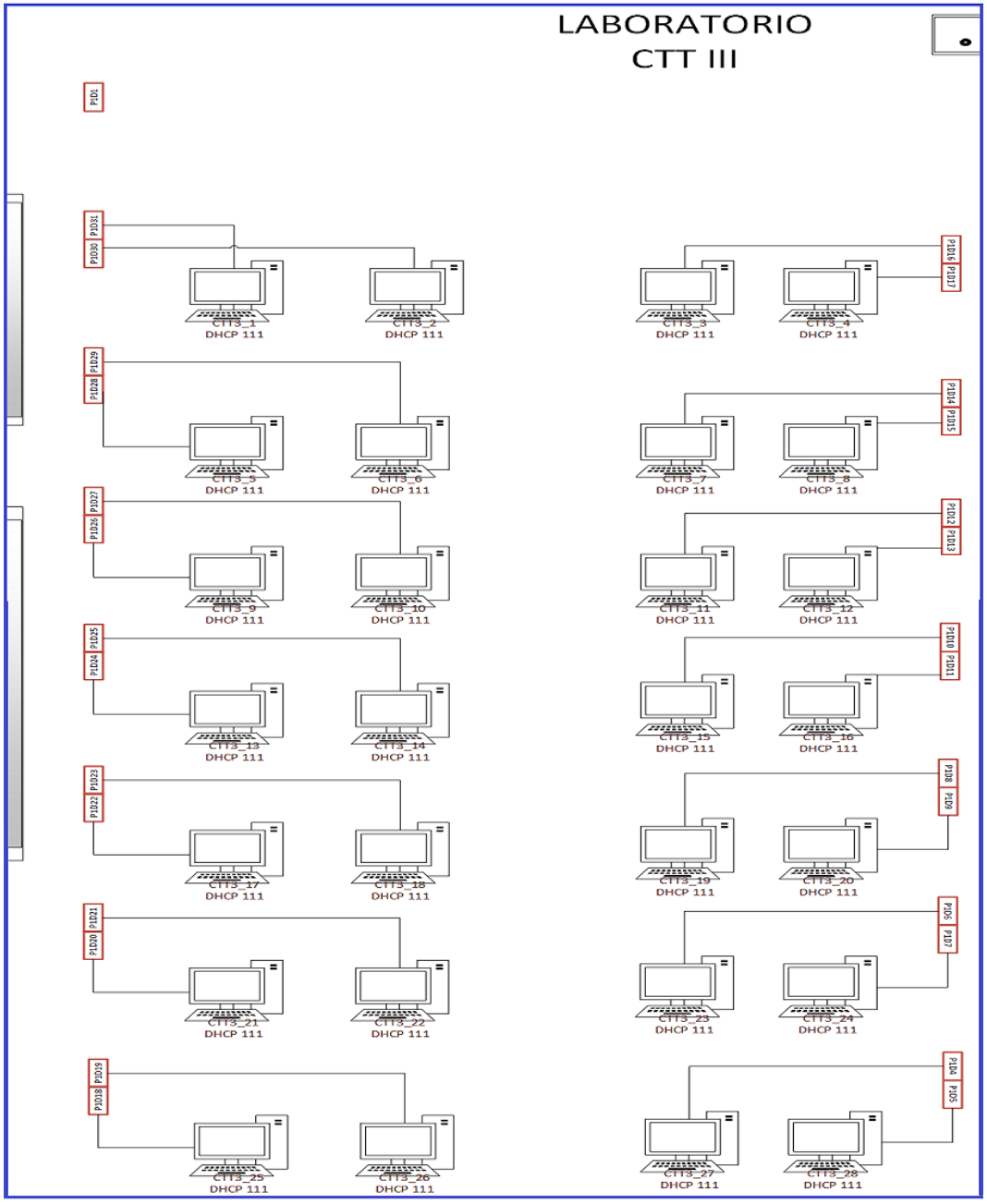


Figure 107: Laboratorio CTT III

A.20. Cooperativa UTA

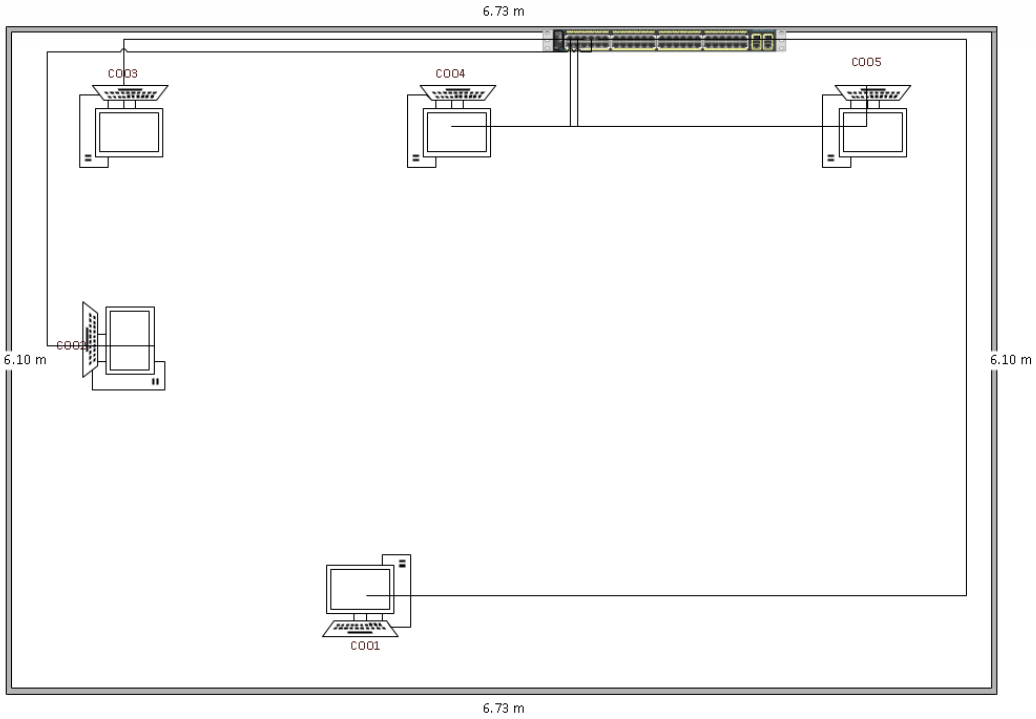


Figure 108: Cooperativa UTA

A.21. Sala Docentes I

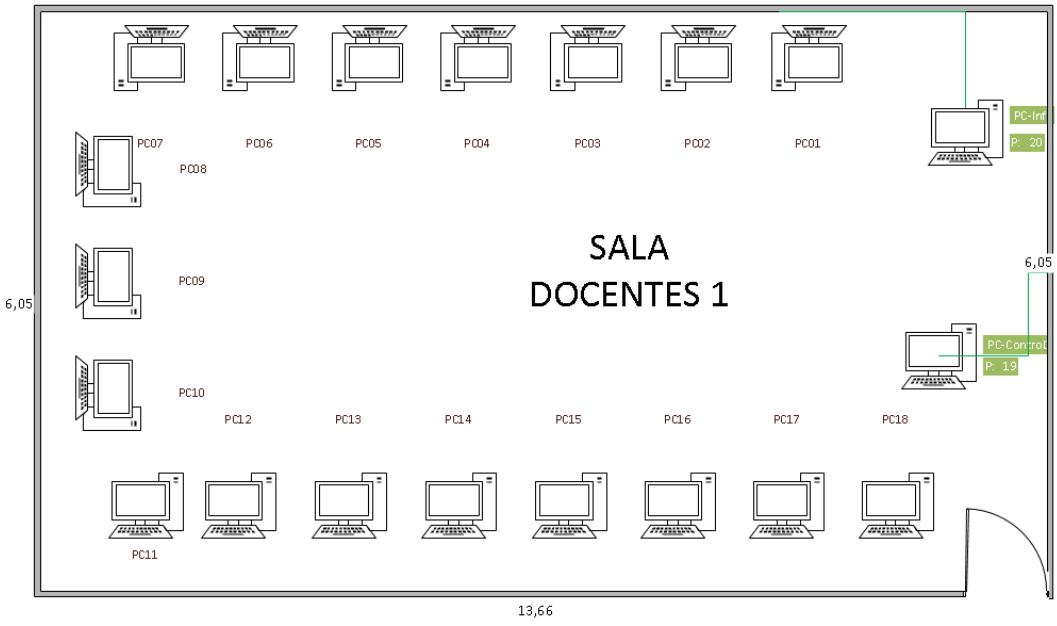


Figure 109: Sala Docentes I

A.22. Sala Docentes II

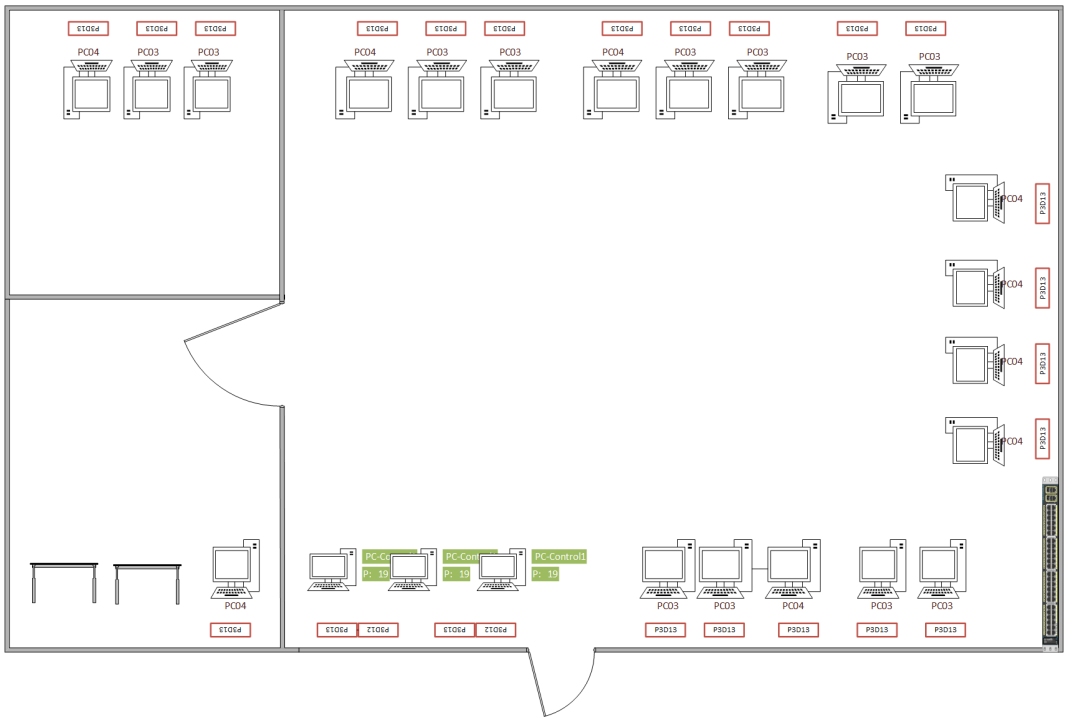


Figure 110: Sala Docentes II

A.23. Decanato

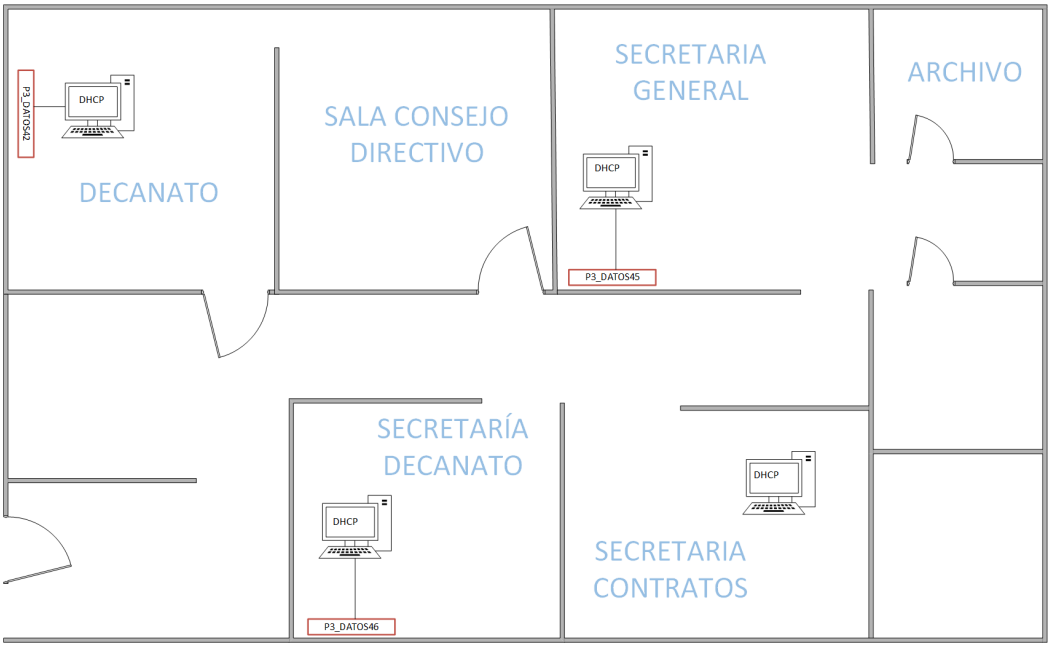


Figure 111: Decanato

A.24. Subdecanato

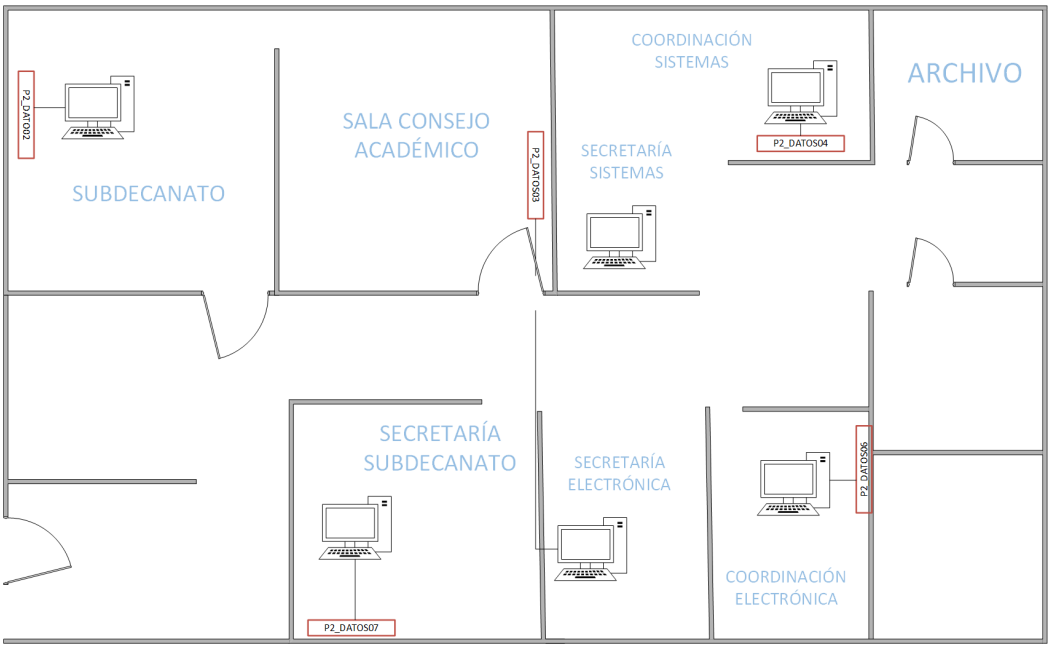


Figure 112: Subdecanato

A.25. Administración de Redes I

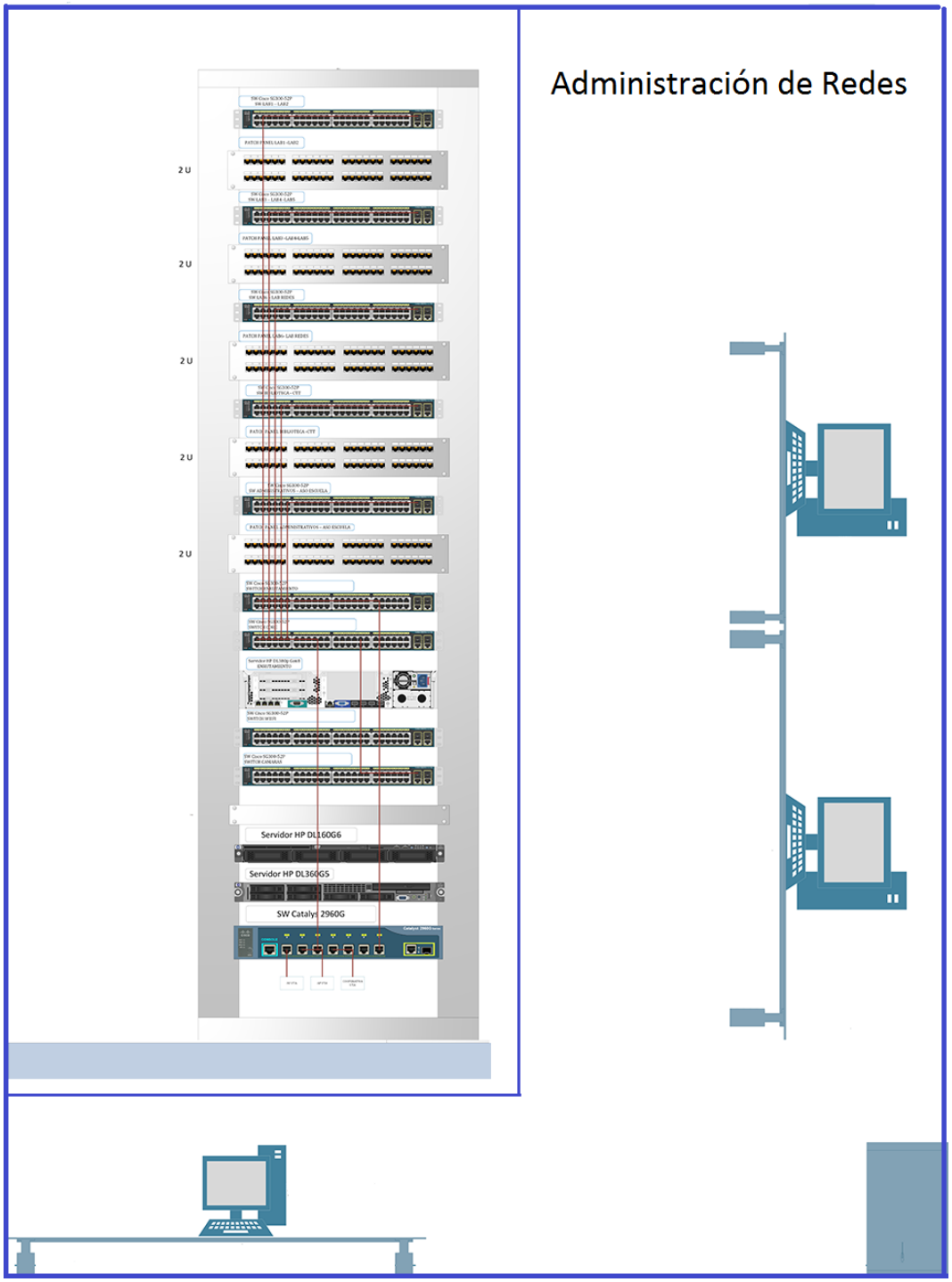


Figure 113: Administración de Redes I

A.26. Administración de Redes II

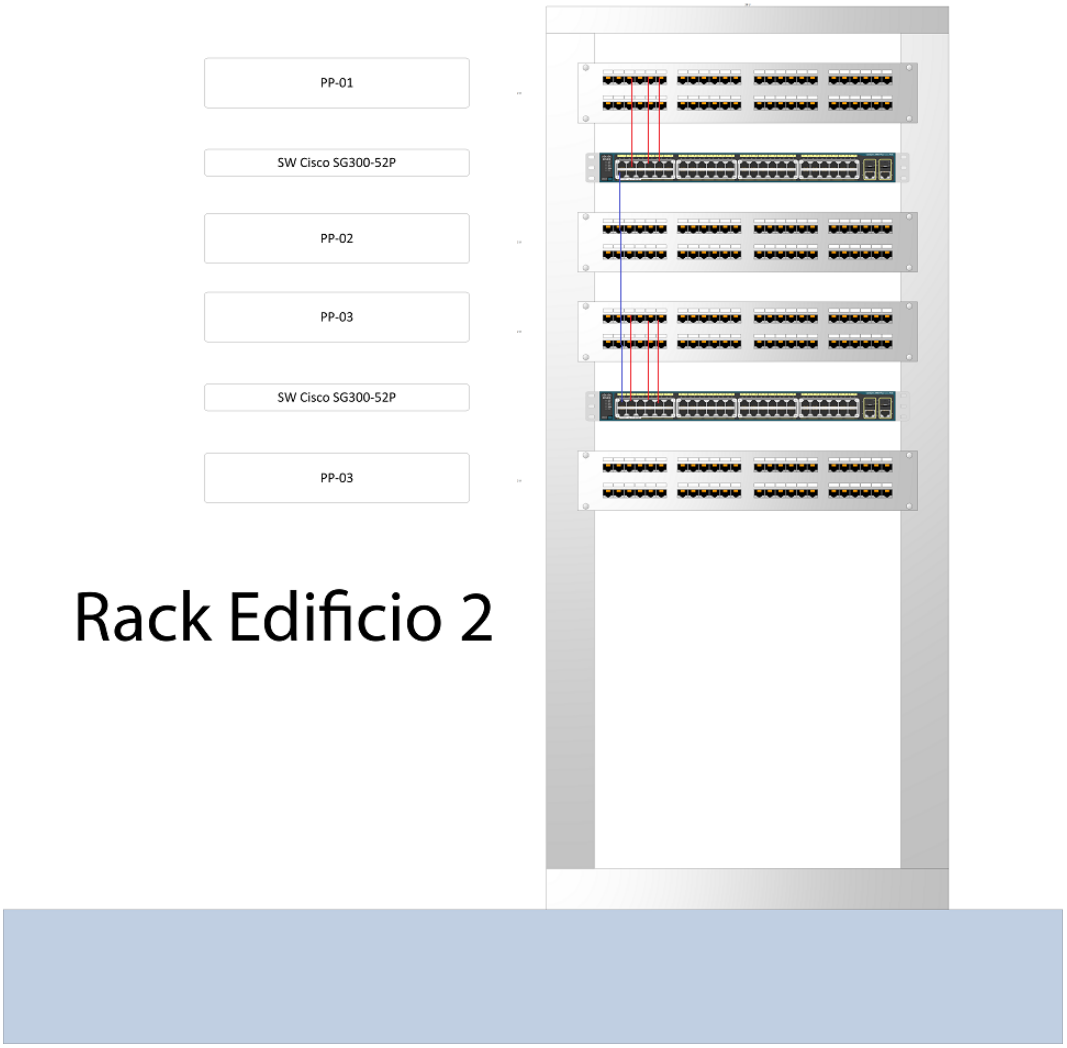


Figure 114: Administración de Redes II

A.27. Biblioteca

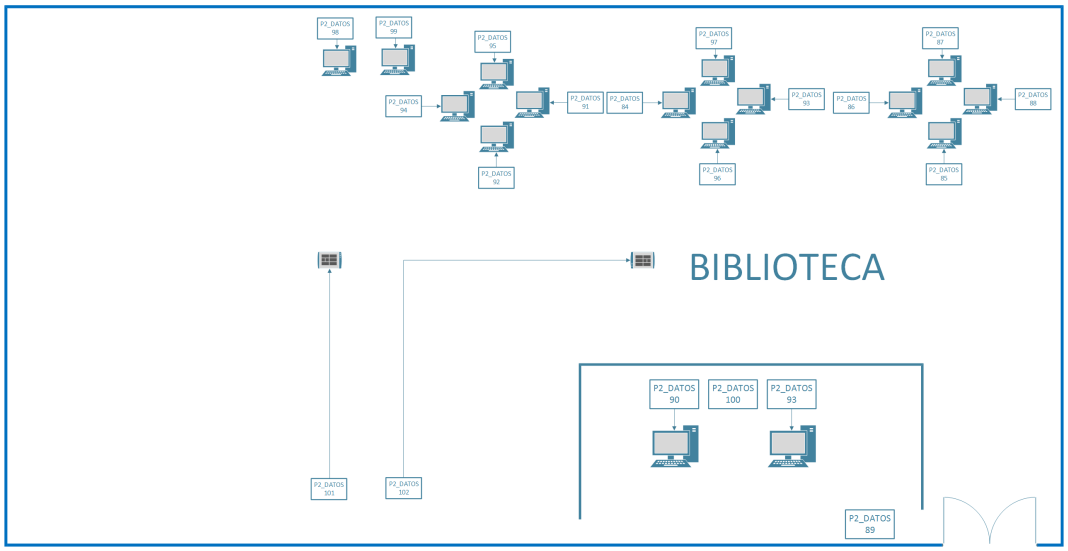


Figure 115: Biblioteca

A.28. Unidad de Investigación

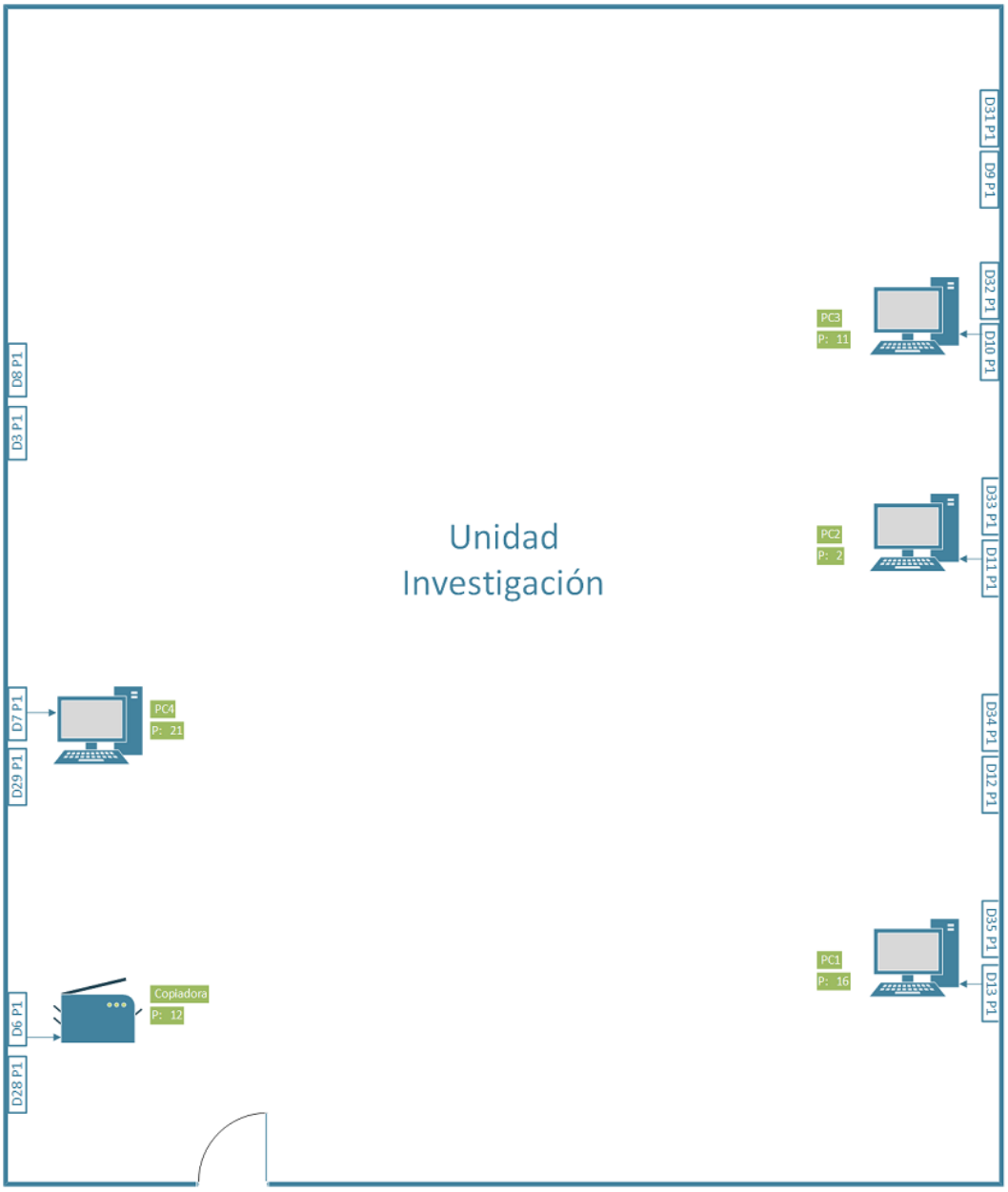


Figure 116: Unidad de Investigación

Appendix B

Anexo B

B.1. Gráficas estadística ideal Disk