Universidad Nacional de Ingeniería
Recinto Universitario Simón Bolívar
Facultad de Electrotecnia y Computación

MONOGRAFIA COMO FORMA DE CULMINAR ESTUDIOS PARA OPTAR AL TITULO DE INGENIERIA EN ELECTRONICA

Propuesta de Seguridad en la Red Inalámbrica WIFI del Recinto Universitario UNI-IES mediante Monitoreo y Portal Cautivo usando Nagios y m0n0wall.

Autor:

Br. Francisco Roberto Zeas Vivas **Carnet 2010-33108.**

Tutor:
MGP. Sixto Chavarría

Managua, Nicaragua 10 de agosto de 2022

DEDICATORIA.

Primero agradezco al gran soberano celestial, Dios, ante todo, por concederme la oportunidad de llegar hasta el final de mi carrera, por darme fuerza y voluntad, ante todo.

A mi familia, mi papá por siempre darme palabras de aliento e impulsarme a seguir adelante, a mi mamá por brindarme todo el apoyo que cualquier hijo querría, en los momentos difíciles, en los desvelos y en los momentos de duda, siempre estuvieron conmigo dándome su apoyo incondicional.

A mi tutor, el ingeniero Sixto Chavarría, por la paciencia, por su disposición y su apoyo en todo el trayecto de la tesis.

A mis amistades, compañeros universitarios que a pesar del tiempo ellos fueron parte fundamental para identificarme como ingeniero, Fátima Centeno, Cinthya Elizabeth, Cristian Escorcia, Steven Zambrana y toda mi generación de entonces que formó parte de mi carrera.

A todos los docentes que aportaron para que sea un profesional con todas las actitudes necesarias, al profesor Juan Toribio, Fernando Flores y Auner García, grandes ejemplos en su materia, profesionales que brindaron el invaluable pan del saber.

Como mención especial, al Ingeniero Carlos Ortega que participó como jurado, mas siempre fue abierto a cualquier consulta, nunca negó de su conocimiento y su tiempo para orientarme en la dirección correcta para con mi proyecto. Que nuestro Dios padre celestial lo guarde en su reino y que su ejemplo permanezca en nuestra alma máter.

RESUMEN.

El proyecto es un Sistema de Autenticación en una Red inalámbrica que verifica el nombre de usuario y contraseña de cada “host”, se les da un seguimiento y también es capaz de monitorizar los equipos de red críticos, alertando si están en funcionamiento o no.

Consta de dos partes, una para el monitoreo mediante Nagios y la otra se encargará del portal cautivo que abarca la autenticación, ambos como máquinas virtuales bajo el sólido VirtualBox, todo esto una sola computadora que hará el papel de servidor. Nagios estará montado en el sistema operativo Debian Buster 10, un sistema operativo flexible y confiable, toda la configuración de los usuarios se puede agregar desde la terminal de Linux en tiempo real, así mismo llevar el seguimiento del estado de los equipos Wi-Fi solo con conocer su dirección IP en caso que uno deje de funcionar, fortaleciendo la calidad del servicio.

Monowall se encargará en la parte de la autenticación de los usuarios mediante uno de sus servicios más útiles, el portal cautivo, forzando a cada persona que se quiera conectar a la red del recinto universitario que se autentique con un usuario y contraseña, esto para impedir que usuarios ajenos a la universidad accedan y hagan mal uso del recurso que es el internet.

LISTA DE ACRÓNIMOS.

AAA: Authentication, Authorization, Accounting / Autenticación, autorización, contabilización.
NAS: Network Access Server / Servidor de acceso a la red
LAN: Local Area Network / Red de área local.
VLAN: Virtual Local Area Network / Red virtual de área local.
WLAN: Wireless Local Area Network / Red de área local inalámbrica.
WAN: Wide Area Network / Red de área amplia.
IP: Internet Protocol.
Wi-Fi: Wireless Fidedelity / Fidelidad inalámbrica.
AP: Access Point / Punto de acceso.
VM: Virtual Machine / Máquina virtual.
LAMP: Linux-Apache-MySQL-PHP.
HTTP: Hypertext Transfer Protocol / Protocolo de transferencia de hipertexto.
WPA: Wi-Fi Protected Access / Wi-Fi de acceso protegido.
PSK: Pre-Shared Key / Clave pre compartida.
ISP: Internet Service Provider / Proveedor de servicios de internet.
SU: Superuser / Super usuario (administrador).
GUI: Graphics User Interface / Interfaz Gráfica de Usuario
SNMP: Simple Network Management Protocol
MIB: Management Information Base / Base de información gestionada

Índice de contenido

1 INTRODUCCIÓN.

Hoy en día, el incremento de los usuarios en las redes inalámbricas con dispositivos móviles, ha creado la necesidad de más controles y seguridad en los equipos de acceso. Un solo usuario puede tener dos o más dispositivos conectados concurrentemente, esto incrementa la cantidad de sesiones conectadas.

La seguridad y el control en las redes requieren más atención día con día, por lo tanto, es necesario reforzar el sistema de seguridad en el acceso. Esto obliga a la institución a ejecutar mejores controles de seguridad para que los recursos (sistemas de información, ancho de banda, aplicaciones, etc.) sean optimizados en su uso, en pro, de prevenir el uso de los recursos en ocio, así como también evitar los ataques cibernéticos a través de más y mejores controles, así como estrategias de seguridad.

En el recinto universitario UNI-IES, el uso del internet es para fines académicos, investigación, administrativos y gestión, los cuales son de vital importancia como en toda universidad. Así que planteé la posibilidad de regular a todo aquel que desee conectarse a la red inalámbrica de la universidad, a través de un sistema de autenticación de usuarios en la red Wi-fi, lo cual filtraría a las personas que no deben tener acceso, propicio para este tipo de redes abiertas con el propósito de brindar servicio solamente a usuarios de la institución.

Así mismo, para prevenir el uso indebido de los medios, se proyectó la idea de un sistema capaz de garantizar que dichos aspectos sean cubiertos, no solo en los usuarios sino también en los equipos inalámbricos del UNI-IES. Se hará uso del sistema de monitoreo Nagios y de un portal cautivo mediante m0n0wall. De esta manera se mejora el acceso y la seguridad de los usuarios de nuestra alma mater logrando así acercarnos más a lo que se conoce como calidad de servicio, dándole al usuario acceso ágil y seguro.

2 OBJETIVOS.

2.1 Objetivo general.

Proponer un Sistema de Monitoreo y Portal Cautivo en la Red Inalámbrica del Instituto de Estudios Superiores (IES) de la Universidad Nacional de Ingeniería, utilizando las herramientas Nagios y m0n0wall.

2.2 Objetivos específicos.

Controlar el acceso a los usuarios de la red inalámbrica mediante un portal cautivo amigable al usuario utilizando m0n0wall.

Configurar un servidor con máquinas virtuales capaz de realizar tareas de monitoreo y autenticación.

Monitorear el estado de conexión de los equipos inalámbricos fundamentales mediante Nagios.

3 JUSTIFICACION

Puesto que el Instituto de Estudios Superiores (IES) de la Universidad Nacional de Ingeniería consta de una red que necesita fortalecerse para cubrir la creciente expansión de los usuarios y la demanda latente de una red más segura y ordenada es concebible que se traten de mejorar aspectos como lo es el control en el acceso a la red y el monitoreo de los equipos críticos como lo son los puntos de acceso inalámbricos.

Mediante el sistema de autenticación (portal cautivo), se logrará el control ante la vulnerabilidad del acceso a la red inalámbrica dado que la persona que quiera conectarse deberá dar su correspondiente “usuario” y contraseña, dejando de un lado el problema de usuarios no deseados, además de autenticación este sistema puede hacer caducar la conexión de un usuario al cabo de un tiempo límite.

Por otra parte, la inclusión del sistema de monitoreo alertará de cualquier anomalía que se presente en los equipos importantes (configurados previamente en el servidor) de tal forma que se puedan ejecutar medidas y soluciones antes que la red se vea afectada por el mal funcionamiento del equipo en cuestión.

Sin olvidar un factor importante como lo es el económico con la implementación de este sistema se ahorra la compra de programas (software) y equipos electrónicos sumamente costosos, los cuales ya llevan integrada la aplicación además de que todos los programas a utilizar en este proyecto son libres lo que hace que sea amigable al bolsillo.

4 ANTECEDENTES

En la revisión de literatura de la base de datos de la Universidad Nacional de Ingeniería, no se encontraron trabajos previos o documentación que antecedan directamente el objetivo de este proyecto. En cambio, se encontró que se ha hecho uso de estas herramientas como son Nagios y Monowall en ciertas casas de estudio como la Universidad Nacional Autónoma de Nicaragua de León y la Universidad Nacional de Ingeniería.

En esta sección se recopila información de experiencia de los autores utilizando las herramientas estudiadas, cabe señalar que no se especifica una documentación oficial, sino una compilación de los datos compartidos de los proyectos realizados en las instituciones antes mencionadas.

4.1 UNAN – LEON

Universidad Nacional Autónoma de Nicaragua–León, estuvo en funcionamiento por más de 15 años un portal cautivo basado en la herramienta Monowall, en compañía de personal de la Dirección de tecnología de la comunicación se realizó una gira de campo a dicha universidad, técnicos del recinto nos dieron una descripción técnica del sistema.

En dicha universidad disponían de un solo servidor Monowall, cabe mencionar que también contaban con un servidor Radius (acrónimo en inglés de Remote Authentication Dial-In User Service) dedicado a la parte de base de datos de todos los usuarios de la red de manera organizada.

Y es por el hecho que la universidad es un conjunto de edificios a lo largo de la ciudad de León es que surgió la necesidad de autentificar a los usuarios que solamente son miembros de la universidad, ya que cualquier ciudadano con conocimiento de la contraseña ya sea filtrada o mediante programas (software) malintencionado (hacker), podría acceder a la red de la universidad.

4.2 UNI – RUSB

La UNI cuenta con un sistema Nagios que monitorea sus principales equipos, la vigilancia está desplegada en el mapa de Nagios por VLAN (red de área local virtual) de una forma simple, pero sin dejar de ser efectiva que mantiene al tanto si un equipo está inactivo (down) o activo (up).

5 MARCO TEÓRICO.

5.1 Nagios.

Nagios es un sistema de monitorización de redes de código abierto, ampliamente usado, que vigila los equipos (hardware) y servicios (software) que se le orienten, alertando cuando el funcionamiento de los mismos no sea el deseado. Aunque originalmente fue diseñado para ser ejecutado en GNU/Linux, también se ejecuta bien en variantes de Unix y actualmente existen versiones para Windows.

Entre sus principales características figuran la monitorización de servicios y –protocolos de red (SMTP, POP3, ICMP, HTTP, SNMP), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos), independencia de sistemas operativos, la opción de monitorización remota mediante túneles SSL cifrados o SSH y la posibilidad de configurar complementos (plugins) específicos para nuevos sistemas.

Las alertas generadas por este software pueden ser enviadas a los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Informando así sobre el estado del servicio que ha ocasionado el error, también se incluyen los informes de registros (logs), estado y los históricos webs. Este sistema posee una interfaz web básica, con muchas funcionalidades de Open Source, se encuentra programado en lenguaje C y Perl; funciona con las plataformas de Linux y Windows.

A continuación, algunas de las principales funciones.

- Monitorea servicios de red como (SMTP, POP3, HTTP, HTTPS, Network Time Protocol [NTP], ICMP, SNMP, File Transfer Protocol [FTP], DNS, etc.).
- Es capaz de supervisar los recursos de equipos hardware (carga del procesador, uso de los discos, procesos del sistema) en varios sistemas operativos.
- Soporta monitoreo de equipos remotos, a través de túneles SSL cifrados o SSH.

- Posee un diseño simple de plugins, permitiendo la posibilidad de crearlos, para aquellos usuarios que optan por desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus lenguajes de programación preferidos (Bash, C++, Perl, Ruby, Python, PHP, C#).
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Envía notificaciones a los contactos cuando ocurren problemas en servicios o hosts (siempre y cuando se configure), así como cuando son resueltos.
- Soporta rotación automática del archivo de registro, lo cual administra de una manera eficaz los archivos de registro ahorrando almacenamiento.
- Visualiza el estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas y archivos de registros.

Requisitos mínimos para su funcionamiento

- Procesador: P4 1.8 Ghz
- Memoria RAM: 1 GB
- Sistema Operativo: Linux
- Tarjeta de Red: 10/100/1000

5.2 Nagios plugins.

Los complementos (plugins) son extensiones independientes de Nagios Core (versión libre de Nagios) que permiten monitorear cualquier cosa con Nagios Core. Los complementos procesan los argumentos de la línea de comandos, realizan una verificación específica y luego devuelven los resultados a Nagios Core. Pueden ser binarios compilados (escritos en C, C ++, etc.) o scripts ejecutables (Shell, Perl, PHP, etc.).

Además de los complementos oficiales de Nagios, se pueden encontrar miles de otros complementos para monitorear todo tipo de hardware, servicios, métricas y aplicaciones en Nagios Exchange. (Nagios, s.f.)

5.3 Debian.

El Proyecto Debian es una asociación de personas que han hecho causa común para crear un sistema operativo (SO) libre. Un sistema operativo es un conjunto de programas y utilidades básicas que hacen que su computadora funcione. El centro de un sistema operativo es el núcleo (N. del T.: kernel). El núcleo es el programa más importante en la computadora, realiza todo el trabajo básico y le permite ejecutar otros programas.

Los sistemas Debian actualmente usan el núcleo de Linux o de FreeBSD. Linux es una pieza de software creada en un principio por Linus Torvalds y desarrollada por miles de programadores a lo largo del mundo. (Debian, 2021)

A continuación, ventajas del sistema operativo que validan la elección.

- Por defecto es estricto respecto a utilizar código abierto. Viene sin software propietario pre instalado y sus repositorios por defecto no contienen softwares privativos.
- Cualquier persona capaz de codificar puede contribuir, modificar, mejorar y distribuir el código a cualquier persona y para cualquier propósito.
- Es de propósito general y su curva de aprendizaje es relativamente fácil y rápida de adquirir.
- En el proceso de instalación, solo se indica lo que se necesita. El sistema queda listo para trabajar desde su primer arranque.
- Cuenta con el mayor proyecto comunitario de código abierto de la historia, el proyecto actualmente afirma que son más de 50.000 los paquetes que ofrecen los repositorios oficiales de Buster.
- Es la segunda distribución de Linux más antigua y actualmente mantenida.
- Debian es flexible, desde el momento inicial de su instalación y muy personalizable.
- En su rama estable, es la más innovadora y actual. Esta contiene el software más estable posible, revisado y probado por sus desarrolladores.

Requisitos mínimos Debian 10.

Estos son los requisitos mínimos para que funcione Debian según su página web. A como se puede observar, es bastante flexible y cualquier computadora personal promedio puede cumplir mucho más que el mínimo.

- Procesador: Pentium 4 a 1 Ghz
- RAM: 256 Mb o más.
- Disco Duro: 10 Gb.

5.4 m0n0wall.

m0n0wall es un proyecto dedicado a la creación de un paquete completo para servidor de seguridad, utilizando una computadora como sistema principal, proporcionando características importantes de cortafuegos (firewall) comerciales, el cual permite una facilidad de uso y reduciendo los costos de licenciamientos por ser Software Libre.

m0n0wall está basado en una versión básica de Free-Berkeley Distribution (FreeBSD), con servicios web, Hypertext Preprocessor (PHP) y maneja una Graphical User Interface (GUI), como también su configuración de arranque. La configuración principal es almacenada en archivos XML (Buechler, 2015).

Proporciona una pequeña imagen que se puede colocar en tarjetas flash compactas, así como en CD-ROM y discos duros. La versión para PC se puede ejecutar con solo un CD vivo (Live CD) y un disquete para almacenar los datos de configuración, esto elimina la necesidad de un disco duro, lo que reduce los niveles de ruido y calor.

Funciones de Monowall.

m0n0wall proporciona una configuración basada en web y utiliza PHP exclusivamente para la GUI y la configuración de arranque. Además, adopta un único archivo XML para los parámetros de configuración (respaldo).

- Interfaz web; compatible con Secure Sockets Layer (SSL)
- Interfaz de consola en serie para la recuperación.
    - Establecer la dirección IP de la Local Area Network (LAN).
    - Restablecer contraseña.
    - Restaurar los valores predeterminados de fábrica.
    - Reinicio del sistema (reboot).
- Posee soporte para tarjetas inalámbricas.
- Filtrado de paquetes con estado.
    - Reglas de bloqueo / acceso
    - Inicio de sesión (logging).
- Network Address Translation / Port Address Translation (PAT) (incluido 1:1 o NAT estático).
- Soporta clientes por medio de Dinamic Host Client Protocol (DHCP), Point-to-Point Protocol over Ethernet (PPPoE) y Point to Point Tunneling Protocol (PPTP) en la interfaz WAN
- Soporta tecnología de túneles Virtual Private Network (VPN), Internet Protocol Security (IPsec), Internet Key Exchange (IKE).
- Point to Point Tunneling Protocol (PPTP) VPN.
- Compatible con rutas estáticas.
- Dispone de servidor DHCP.
- DNS forwarder de almacenamiento en caché.
- Posee agente *Simple Network Management Protocol* (SNMP).
- Proporciona conformado de tráfico (Traffic Shaper).
- Actualización de firmware a través del navegador web.

- Capaz de crear copias de seguridad y posee opción de restauración de la configuración.

Toda la configuración del sistema se almacena en un solo archivo de texto eXtensible Markup Language (XML) para mantener la transparencia. m0n0wall es probablemente el primer sistema UNIX que tiene su configuración de arranque realizada con PHP en lugar de los habituales scripts de Shell.

Requisitos mínimos del sistema.

Hay que destacar que m0n0wall dados sus mínimos requerimientos técnicos lo hace idóneo para trabajar desde una máquina virtual o un ordenador de bajos recursos. Cualquier sistema **x86** con estas características:

- **CPU:** 433 (LX700) o un AMD (LX800) a 500 MHz.
- **DRAM:** 128 o 256 MB DDR SDRAM (333 o 400 MHz)
- **Almacenamiento:** Todo el sistema operativo y aplicación pueden guardarse en una Compact Flash, mínimo recomendado 32MB.
- **Consumo:** La fuente de alimentación convencional de un ordenador y tendremos el Firewall funcionando.

5.5 Portal cautivo.

Un portal cautivo es un software o máquina de una red de computadoras que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si desean navegar por internet de forma normal. (Portal Cautivo, 2020)

En primer lugar, hay que aclarar que este sistema de control de acceso necesita un servidor (Monowall hará esta tarea) que realice el control de la conexión al exterior (internet). Con este método de autenticación, el cliente consigue conectarse a la red WIFI, se le asigna una IP, pero sin capacidad de comunicarse fuera del entorno que se haya previamente definido. Cuando el cliente/usuario intenta establecer

comunicación con una página web externa, automáticamente es redirigido a un portal web en el cual puede autenticarse.

Una vez hecho, ya sea con un simple usuario/clave o previo pago de una tarjeta de conexión (voucher) el usuario consigue conectividad a Internet durante el tiempo establecido. Para poder mantener la sesión viva, el cliente tiene que mantener una ventana flotante del navegador (pop-up) abierta que se encarga de comunicar automáticamente y cada cierto tiempo con el portal de acceso, garantizando que la conexión siga abierta. (Castro, 2005).

Este tipo de software se utiliza sobre todo en redes inalámbricas libres y abiertas al público en general, lo que las hace vulnerables, ese es el motivo por el que se implementan estas aplicaciones, para llevar un control sistemático de los usuarios.

Funciones del portal cautivo m0n0wall incluyen:

- Admite selección de interfaz a controlar (normalmente la interfaz LAN).
- Filtra direcciones IP o MAC seleccionadas por el administrador.
- Posee opciones de autenticación de usuario (ya sea acceso directo, modo local o RADIUS).
- Concede límites para el número máximo de conexiones simultáneas para el mismo usuario.
- Bloquea o autoriza inicios de sesión de usuarios concurrentes.
- Dispone de creación y gestión de perfiles de usuarios en su base de datos local.
- Proporciona restricciones de ancho de banda por usuario.
- Permite configurar un Tiempo de espera inactivo (idle timeout) y Tiempo de espera fijo (hard timeout) para las sesiones de los clientes.
- Reconoce cierre de sesión mediante ventana emergente.
- Permite re direccionamiento de Uniform Resource Locator (URL) al iniciar sesión.

- Filtrado de equipos mediante Media Access Control (MAC).
- Admite autenticación por Hypertext Transfer Protocol Secure (HTTPS).
- Permite personalizar el contenido de la página de inicio del portal, Página de “error de autenticación” y página de “desconectar” del portal.
- Soporte para administración de sistema de comprobantes (Vouchers).

5.6 Máquina virtual.

Las máquinas virtuales son ordenadores de software que proporcionan la misma funcionalidad que los ordenadores físicos. Como ocurre con los ordenadores físicos, ejecutan aplicaciones y un sistema operativo. Sin embargo, las máquinas virtuales son archivos informáticos que se ejecutan en un ordenador físico y se comportan como un ordenador físico. En otras palabras, las máquinas virtuales se comportan como sistemas informáticos independientes. (VMware, 2022)

La máquina virtual se conoce por “invitada” (Guest). El entorno informático que aloja dicha máquina es denominado” anfitrión” (Host). En un host pueden existir varias máquinas virtuales a la vez.

5.7 Software libre.

Software libre es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el *software libre* es una cuestión de libertad, no de precio.

Para entender bien el concepto, piense en “libre” como en *libre expresión*, no como en barra libre. En inglés, a veces en lugar de free software decimos “libre software”, empleando ese adjetivo francés o español, derivado de libertad, para mostrar que no queremos decir que el software es gratuito.

Se promueven estas libertades porque todos merecen tenerlas. Con estas libertades, los usuarios (tanto individualmente como en forma colectiva) controlan el programa y lo que este hace. Cuando los usuarios no controlan el programa, decimos que dicho programa no es libre, o que es “privativo”. Un programa que no es libre controla a los usuarios, y el programador controla el programa, con lo cual el programa resulta ser un instrumento de poder injusto (¿Qué es el software libre? - Proyecto GNU - Free Software Foundation, s.f.)

5.8 Punto caliente.

En el contexto de las comunicaciones inalámbricas, un *hotspot* o *punto caliente* es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador (router) conectado a un proveedor de servicios de Internet.

Es una zona de alta demanda de tráfico, y que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un punto de acceso o varios, y de este modo proporcionar servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP).

Tiene similitudes no más solo en funciones a una *estación* o (Workstation) con la diferencia que éste último es un ordenador que facilita a los usuarios el acceso a los servidores y los distintos periféricos de red.

5.9 Seguridad inalámbrica.

Esta funciona a base de encriptación de sus datos, en donde para poder saber el encriptado usado en la señal se debe conocer algún usuario y contraseña para así poder recibir correctamente los paquetes enviados desde la red. Es en este punto en donde se enfocan los ataques a las señales inalámbricas, en el lograr conocer de alguna manera el usuario y contraseña de la señal para poder recibir sus paquetes.

Para impedir que personas no deseables obtengan tal información es que existen diferentes sistemas de seguridad, tales como el WEP, el WPA, el WPA2 entre otros, los cuales se rigen bajo normas del IEEE (instituto de ingenieros eléctricos y electrónicos) encargada de estandarizar estos protocolos de seguridad, eso sí, todos basados en el sistema de usuario/contraseña.

5.10 Seguridad a nivel de protocolo.

La seguridad a nivel de protocolo es la encargada de que los datos transmitidos por una WLAN (Wireless Local Area Network) no puedan ser descifrados por alguien ajeno a la red. Para ello nuestra red ha de tener un algoritmo de codificación y gestión de claves. Haré énfasis en los protocolos wpa y wpa2 con sus características ya que son los más usados actualmente.

5.11 Agente SNMP.

El agente es un programa que está empaquetado dentro del elemento de red. La habilitación del agente le permite recopilar la base de datos de información de administración del dispositivo localmente y la pone a disposición del administrador SNMP, cuando se le solicita, usa el puerto UDP 161 y el 162, este último para enviar “trampas” SNMP. Estos agentes pueden ser estándar (por ejemplo, Net-SNMP) o específicos de un proveedor (por ejemplo, HP Insight Agent).
Funciones clave del agente SNMP:

- Recopila información de administración sobre su entorno local
- Almacena y recupera información de gestión según se define en la MIB (Management Information Base).
- Señala un evento al administrador.
- Actúa como proxy para algunos nodos de red administrables que no son SNMP.

5.12 WPA2 personal y WPA2 Enterprise.

WPA2 Personal proporciona una seguridad adecuada para el hogar y pequeñas redes inalámbricas de oficina. Prácticamente todos los enrutadores de fabricantes comerciales – incluyendo Linksys, Belkin, D-Link y Apple – permiten la configuración de WPA2 Personal en sus dispositivos. En la mayoría de los casos, WPA2 Personal ofrece una protección adecuada frente a los piratas informáticos y a otras amenazas en línea a las redes inalámbricas.

La mayor diferencia entre WPA2 Enterprise y WPA2 Personal es el grado de sofisticación de técnica necesaria para configurar WPA2 Enterprise. En concreto, se requiere de un servidor de autenticación RADIUS, algo que no se encuentra en lugares sin un administrador de red. Si bien WPA2 Enterprise proporciona un mayor grado de seguridad que WPA2 Personal, el tipo de fallos de seguridad contra los que protege el primero rara vez suceden en las redes de hogar y negocios pequeños.

5.13 Firewall embebido.

m0n0wall es principalmente un cortafuego, y el propósito de un cortafuego es proporcionar seguridad. Cuanta más funcionalidad se agregue, mayor será la posibilidad de que una vulnerabilidad en esa funcionalidad adicional comprometa la seguridad del firewall.

Los dispositivos integrados requieren un cortafuego especializado diseñado para funcionar en dispositivos de recursos limitados y especializados. Así mismo un cortafuego integrado debe ser portátil, escalable, fácil de administrar y adaptado para admitir casos de uso como lo son los puntos de acceso. (Sectigo, 2020)

5.14 Protocolo de autenticación Radius.

Aunque no haré uso de este protocolo en este trabajo, brindaré una breve reseña sobre Radius ya que siempre que se trate de autenticación este término saldrá expuesto.

RADIUS (acrónimo en inglés de ***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****ervice*) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Radius es uno de los protocolos más utilizados para implementar AAA. El protocolo RADIUS se usó inicialmente para administrar un gran número de usuarios dispersos que usan interfaces seriales y módems. Ahora, este protocolo se aplica ampliamente al sistema NAS (Network Access Server). El NAS transfiere la información de autenticación y contabilidad del usuario al servidor RADIUS.

El protocolo RADIUS define cómo el servidor NAS y RADIUS transfieren la información de autenticación y contabilidad del usuario, así como los resultados de autenticación y contabilidad. El servidor RADIUS recibe una solicitud de conexión de los usuarios, autentica a los usuarios y devuelve el resultado de la autenticación al NAS. Al utilizar UDP como el protocolo de transporte, RADIUS presenta un alto rendimiento en tiempo real. Debido al mecanismo de retransmisión y al mecanismo del servidor de reserva, RADIUS es de alta confiabilidad.

VI. DISEÑO METODOLÓGICO

Antes de continuar hay que hacer hincapié en que se limitó el alcance del proyecto debido a restricciones de la administración de dicha institución, porque en lugar de ser una propuesta se pretendía implementar el proyecto ya que es asequible por su naturaleza de software libre; sin dejar de lado, un portal cautivo resulta efectivo en este tipo de escenarios como lo son las redes abiertas al público y no tan pobladas como lo es la red inalámbrica del IES.

El enfoque de este proyecto es cualitativo, en este tipo de enfoque se utilizan técnicas para recolectar datos, como la observación no estructurada (también llamada simple o libre), entrevistas, revisión de documentación, y de ser posible evaluación de experiencias personales.

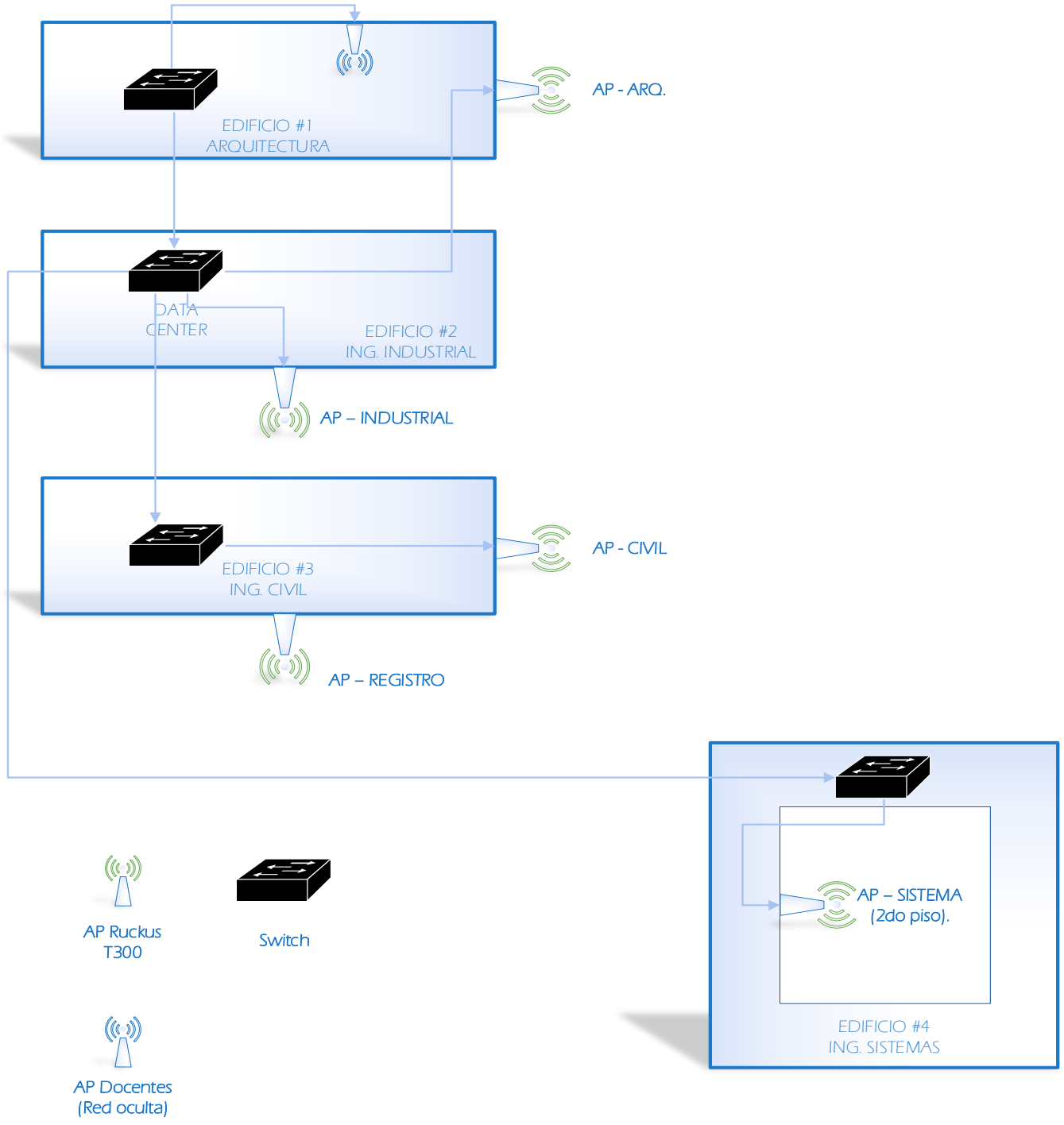
Se hará uso de información recolectada a través de entrevistas con personal del IES y UNI (ver Anexos, Entrevistas 1 y 2), además de referencias que se pueden encontrar vía web, así como observación del comportamiento de la red inalámbrica (ver Anexos, Figura 25, 26). El modelo de entrevista utilizado en este trabajo es semiestructurado. En la metodología cualitativa, la entrevista no se basará en cuestionarios cerrados y altamente estructurados, aunque se puedan utilizar, se inclina a preguntas con mayor libertad.

La red inalámbrica del recinto universitario de estudios superiores (IES) actualmente es una red abierta (libre acceso), según el Ingeniero Wilfredo García, el cual compartió mediante una entrevista (ver Anexos, Entrevista #2) entre otros datos “existen 5 Access Point funcionando para la actual red estudiantil.” (W. García, comunicación personal, 5 de julio de 2021).

Mediante la información de red brindada por parte de informática del IES, se realizó un esquema de red (ver Figura 1). Para validar la ubicación física de dichos puntos de acceso, se hizo uso de una “app” (aplicación) llamada “**Wifi Analizer”** (ver Anexos, Figura 27,28,29,30,31) y observaciones a modo personal.

Figura 1.

Diagrama físico de la red inalámbrica IES[1].



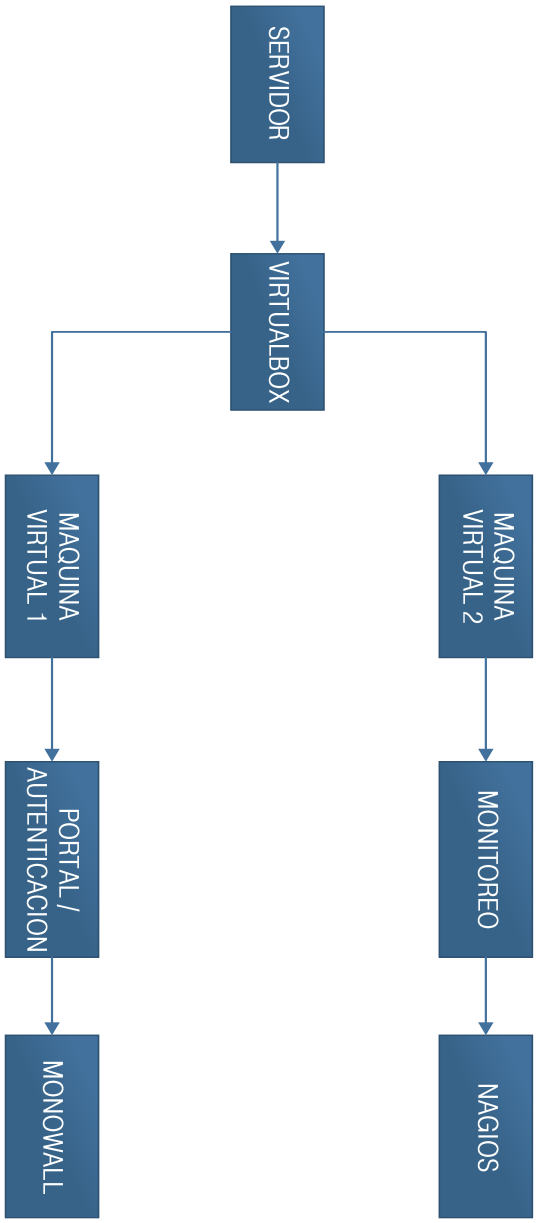
[1] Informática del IES no proporcionó en ningún momento ninguna dirección IP, puertos o cableado, solamente confirmaron la **ubicación** de cada punto de acceso.

CAPITULO 1 - VIRTUALIZACIÓN.

El proyecto básicamente consta de dos partes, a cómo pueden apreciar en la Figura 2, una máquina virtual para el monitoreo mediante Nagios y la otra se encargará del portal cautivo (autenticación), ambos como máquinas virtuales en **una sola computadora** que hará el papel de servidor.

Figura 2

Diagrama de bloque de la estructura del proyecto.



Las máquinas virtuales tomarán un papel importante, así que se tomaron en consideración virtualizadores como Virtualbox, HyperV y VMware como alternativas, aunque este último en menor grado como se indicará más adelante; comparando así sus características y bondades con el fin de encontrar el más cómodo y eficaz para este proyecto.

Se entrevistó a I. Jiménez, un ingeniero de soporte técnico del NIC.NI[2] de la UNI, ya familiarizado con el uso de virtualizadores (ver Anexo, entrevista #1). El ingeniero I. Jiménez, señaló que a la hora de seleccionar un virtualizador "hay que tener en cuenta tus requerimientos, o sea la necesidad de tu proyecto... VirtualBox, el que quieres usar, está bien en general, a mí personalmente no me ha dado problemas". (I. Jiménez, comunicación personal, 16 de junio de 2021).

También se discutió sobre VMware. "¿VMware?, si es bueno, solo que tenés que considerar que es en parte un software *con licencia*, o sea pagado. Claro puedes trabajar con ese, pero según lo que me has mencionado de tu proyecto puedes trabajar con los otros virtualizadores perfectamente". (I. Jiménez, comunicación personal, 16 de junio de 2021).

Para tener una perspectiva de los diferentes virtualizadores que se consideran, abajo la Tabla 1 que compara diversas características.

[2] Network Information Center Nicaragua

Tabla 1.

Comparación virtualizadores.

	VMware	VirtualBox	Hyper-V
Facilidad de uso	Medio	Fácil	Complicado
Rendimiento	Bueno	Medio	Bueno
Instantáneas	Si	Si	No
Compartir archivos	Si	Si	Si, pero complicado.
Integración con Windows	Si	Si	No
Cifrado	Si	Si (a través de Guest Additions)	Si
Sistemas compatibles	Windows, Linux, macOS	Windows, Linux, macOS	Windows y Linux (este con limitaciones)
Precio	Gratis / De pago	Gratis	Gratis
Otros	Excelente seguridad	OpenSource	Solo en Windows 10 Pro Soporte WSL y WSL2 W

Nota. Reproducido de *¿Qué programa es mejor?*, por R. Velasco, 2022, Softzone (https://www.softzone.es/programas/utilidades/diferencias-vmware-virtualbox-hyper-v/). Todos los derechos reservados 2022 por Velasco. Reproducido con permiso del autor.

Podemos observar que se consideran aspectos como la dificultad de uso, el rendimiento, precio y la capacidad de tomar “instantáneas”. Esta última, una característica muy importante en máquinas virtuales ya que permite poder capturar y guardar temporalmente el estado de una máquina, cerrar el virtualizador o apagar el ordenador y al volver a correr dicha máquina virtual, permanece en el mismo estado en que se guardó, y es de notar que no todos los virtualizadores se destacan en esto.

Después de analizar las distintas bondades y las necesidades del proyecto se hará uso de **VirtualBox**, se decidió por este software debido a su naturaleza gratuita, facilidad y flexibilidad de uso.

Además, que cubre las necesidades del proyecto, es con el cual me encuentro más familiarizado. Sin dejar de lado un aspecto muy importante, y es que este es un software libre, por lo tanto, no amerita licencia alguna.

1.1 Configuración de Virtual Box para la máquina virtual de Monowall.

No es necesario instalarle un sistema operativo a esta máquina virtual, puesto que al instalar m0n0wall se borra cualquier sistema operativo previamente instalado sea una máquina virtual o no.

Previamente se descarga del sitio oficial <http://m0n0.ch/wall/> el instalador de m0n0wall, se eligió la imagen "**generic-pc-1.8.1.iso**". Agregamos en VirtualBox un lector de cd y seleccionamos la imagen descargada *sin correr la máquina virtual.*
Son necesarios **2** adaptadores de red, uno siendo el que trae la tarjeta madre por defecto y el otro un adaptador inalámbrico módulo PCIe (ver Figura 3) por lo tanto, requerimos de una apropiada configuración de red de tal forma que tengamos una interfaz LAN y el otro como interfaz WAN.

Figura 3.

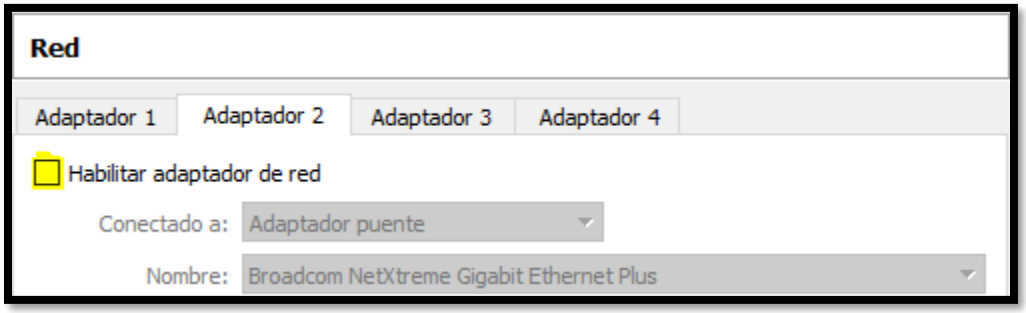
Realtek RTL8192CE Wireless LAN.

Nota. Reproducido de *CSL - 300Mbps WiFi PCI Express (PCIe) card / adapter*, por Csl Computer, 2022, Desertcart. (https://www.desertcart.ni/products/48569011-csl-300mbps-pci-express-pcie-wlan-card-with-mimo-technology-2x-omni-directional-rsma-antenna-realtek-rtl8192ce-chip-set-2-4-ghz-frequency-range-wep-with-64-128-bit-wpa2-psk-wpa-psk). CC-BY-NC-ND.

Antes de instalar Monowall, hay que activar el segundo adaptador dado que usualmente traen habilitado por defecto un sólo adaptador en modo NAT, lo cambiamos a "**adaptador puente**" (ver Figura 4), así mismo el segundo adaptador de igual modo.

Figura 4.

Configuración de red por defecto VirtualBox.



Para tener un mejor entendimiento de cómo será asignada cada interfaz para su correcto funcionamiento, véase Tabla 2.

Tabla 2.

Asignación de interfaces, Monowall VM.

Configuración de red Máquina virtual Monowall			
Adaptador 1 **WAN**		**Adaptador 2** **LAN**	
Interfaz física	Realtek RTL8192CE Wireless LAN 802.11n PCI-E NIC	**Interfaz física**	Broadcom Netxtreme Gigabit Ethernet plus. (Tarjeta madre)
Tipo de adaptador (VM)	Realtek PCIe GbE Family Control	**Tipo de adaptador (VM)**	Realtek PCIe GbE Family Control
Modo:	Puente	**Modo:**	Puente
Dirección MAC	xx:xx:xx:xx:xx:x1	**Dirección MAC**	xx:xx:xx:xx:xx:x2

Se deja como WAN la interfaz inalámbrica ya que ese es el medio por el que se recibe acceso a internet. Por lo tanto, la tarjeta NIC integrada en la computadora es la que hará de LAN, en otras palabras, la red que se desea tener control de acceso.

CAPITULO 2 - SERVIDOR DE M0N0WALL.

2.1 ¿Porque Monowall?

En primera instancia, se tomaron en cuenta otros softwares de características similares (ya sea como sistemas embebidos o firewalls) **todos** a disposición de ***software libre*** y que sean virtualizables. No obstante, hay que señalar que esta propuesta ha estado en planeación desde hace buen tiempo, por lo tanto, los mismos son actualizados o llegan a fase de "end of life" (fin de vida, ya no se da soporte ni parches). Véase Tabla 3.

Tabla 3.

Menú de instalación Monowall

Sistema	Monowall	OpenWrt	Zeroshell
End of Life	Vigente	Vigente	✗
Compatibilidad Con Puntos de Acceso Inalámbricos	✓	✓[3]	✓
Recomendable para redes pequeñas	✓	✓	✗
Virtualizable	✓	✗	✓
Dificultad de configuración (Del 1 a 10)	8	10	8
Costo de licencia	Ninguno	Ninguno	Ninguno

El primero en ser descartado fue Zeroshell, que a modo personal fue recomendado por un profesional en el campo de las redes (el cual prefirió anonimato por la naturaleza de su trabajo), pues dicho software llegó a "fin de vida" en septiembre de 2021 se dejó de brindar soporte y de actualizar, aunque cumplía con los requerimientos fundamentales se dejó de lado por lo ya mencionado.

[3] Depende del Fabricante

En el caso de Open-Wrt se hicieron numerosas pruebas en coordinación con el Ing. Moisés Aburto, antiguo Ingeniero del DiTi (Dirección de Tecnologías de la Información). El principal inconveniente era que el sistema en se trabajaba directamente a nivel de firmware en cada uno de los equipos inalámbricos, de que eran compatibles era dependiente del fabricante y solo si era soportado por OpenWrt.

Otro punto en contra era su dificultad a la hora de configurar y personalizar un punto de acceso, ya que se tenía que hacer **uno por uno**, requiere borrar cualquier Firmware previo del equipo y montar OpenWrt, en otras palabras había un riesgo de por medio sin contar que toda configuración del equipo se perdía. OpenWrt es sólido y conciso hasta donde el administrador pueda profundizar.

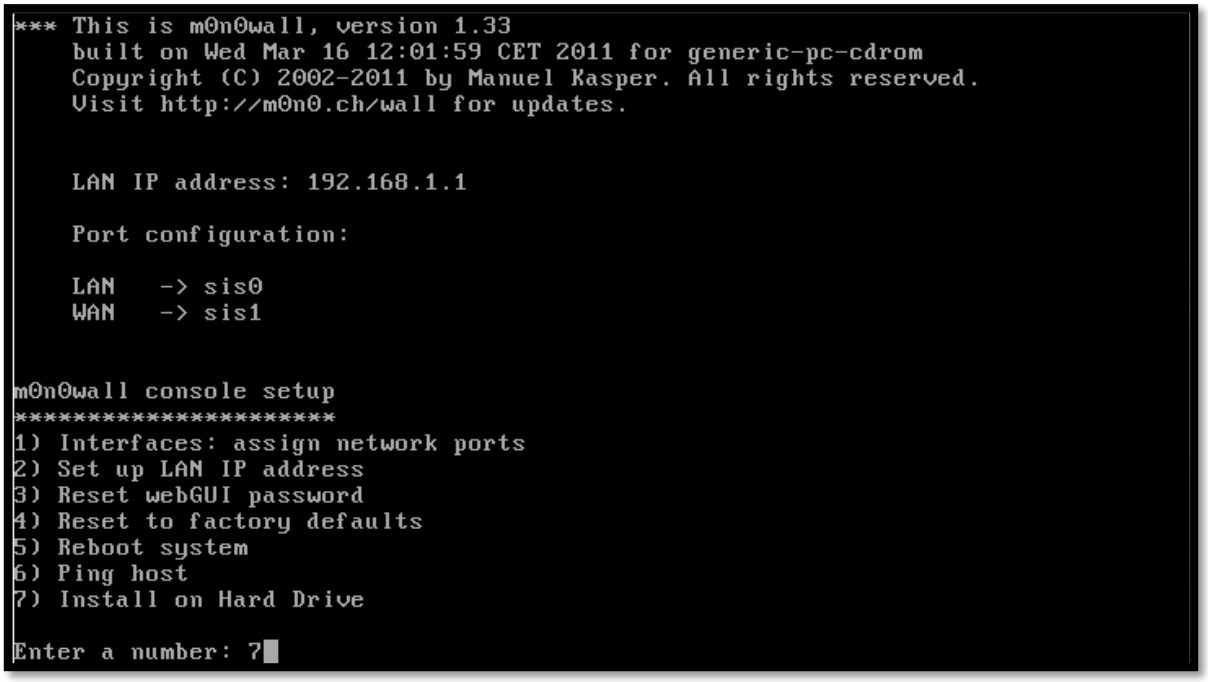
Sin embargo, ya que el enfoque en este trabajo es una propuesta y cualquier modificación a los equipos de acceso presentes está prohibido por informática del IES al final se optó por Monowall, es apto para redes no muy grandes, puede ser virtualizado sin problemas y es software libre, y aunque hoy en día existen versiones más modernas básicamente añaden mejor entorno gráfico y características que no se persiguen en esta propuesta.

2.2 Configuración de Monowall.

Después de haber puesto la imagen de instalación de m0n0wall en nuestra máquina virtual, la iniciamos, esperamos unos minutos y podremos ver que se desplegará una especie de menú (ver Figura 5). Presionamos un número código **7** (siempre es este número independiente de la versión descargada) y empieza la instalación.

Figura 5.

Menú de instalación Monowall



Luego, al haber instalado el sistema, asignamos una dirección IP destinada para nuestra LAN (es recomendable consultar al administrador de red por un IP que esté a disposición), por ejemplo: 192.168.2.1, nos preguntará si queremos habilitar el servicio DHCP en la LAN, le decimos que **no**.

No habilitamos DHCP por el simple hecho de que en la red que se estudia ya existe un servidor para dicha tarea, por consiguiente, tenemos que asignar la dirección IP de la LAN de nuestro sistema Monowall como la puerta de enlace por defecto asignada por el actual servidor DHCP.

El siguiente paso es asignar interfaces con respecto a cada tarjeta de red virtual que tengamos, al asignar y se generará una especie de dirección HTTP (http://192.168.2.1/) a la cual podemos acceder desde cualquier navegador web que dispongamos en nuestro ordenador cliente.

Al dirigirnos al vínculo se nos abrirá una ventana emergente pidiéndonos “usuario” y “contraseña”; al usuario por defecto le ponemos “admin” y a la contraseña “mono”, estos no son valores arbitrarios, el programa los trae por defecto para entrar a la web-GUI. Así mismo es recomendable cambiarlos al acceder a la interfaz web.

2.3 Servicios: Portal Cautivo.

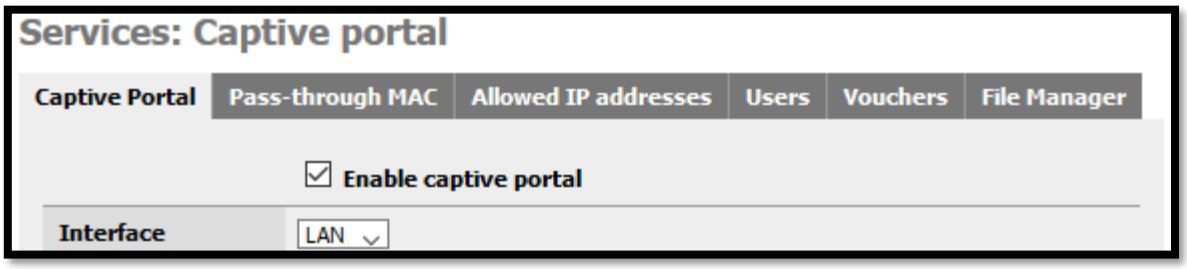
Según W. García el modelo de conexión de la actual red para los usuarios es por competencia, “…*cada estudiante se conecta por competencia, el que se conectó primero es el que va (a consumir) y así sucesivamente.”* (W. García, comunicación personal, 5 de julio de 2021).

Esto trae el inconveniente de que resulta complicado medir y controlar a cada estudiante que se conecta a la red inalámbrica, partiendo de esto el portal es una buena opción para asegurar el tiempo de conexión por usuario, el ancho de banda y entre otros.

Después de realizar las configuraciones básicas procedemos a la función de nuestro interés *“Services: Captive portal”* y marcamos la casilla de confirmación de *“Enable captive portal”*. (Ver Figura 6). Nos cercioramos que en el cuadro de diálogo que pone *“Interface”,* esté la opción “LAN” activada.

Figura 6.

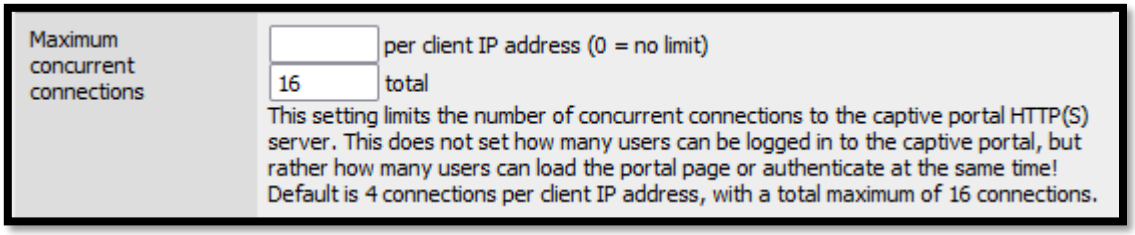
Servicio del portal cautivo.



Además, habilitamos el *"máximo al total de usuarios"* que se puedan usar simultáneamente el portal, le asignamos 16 (véase Figura 7), el cual es el recomendado[4] por el desarrollador.

Figura 7.

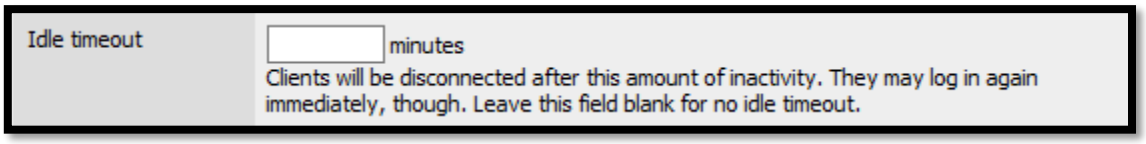
Conexiones concurrentes al portal.



Definimos el tiempo en que cada usuario será desconectado en caso de estar inactivo (de no hacer función alguna, aunque esté conectado) esto se puede dejar en blanco (ver Figura 8).

Figura 8.

Tiempo de inactividad.



Una opción de gran importancia es "desconexión brusca" que aparece en inglés (*hard timeout)*; esto hace que los usuarios sean desconectados al cabo de un

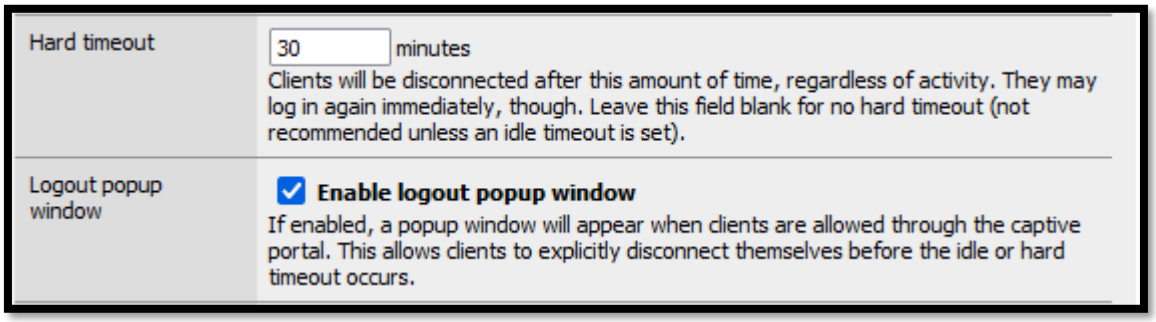
[4] Esto no es indicativo de que solo pueden estar 16 usuarios máximo en la red, sino, indica el número de usuarios *simultáneos* que pueden cargar la página del portal al mismo tiempo.

tiempo, por ejemplo 30 min, ellos podrán volver a conectarse si lo desean, pero tendrán que autenticarse de nuevo[5].

Si se habilita la opción *Enable logout popup window* (habilitar ventana emergente de desconexión) en nuestro sistema el usuario puede desconectarse antes (ver Figura 9).

Figura 9.

Desconexión brusca y ventana emergente.

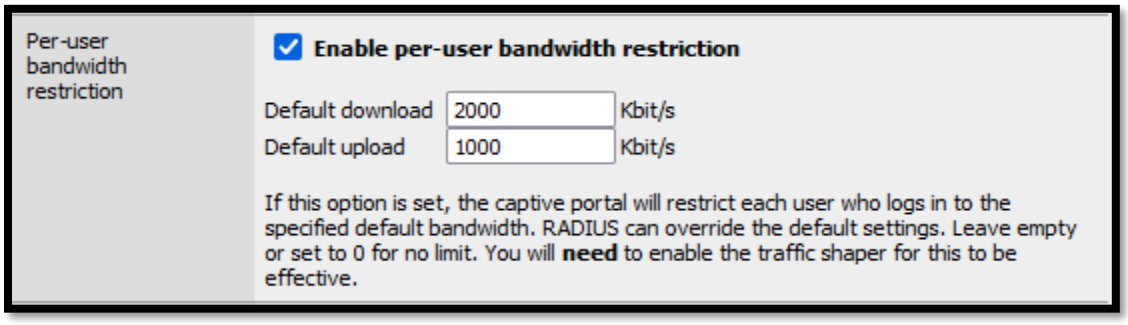


A continuación, esta es solo una de las formas de definir el límite de ancho de banda mediante monowall, por cada usuario, contrario a la configuración actual de la red inalámbrica del recinto UNI-IES (cada usuario se conecta por competencia, ver Anexos, Entrevista #2), de este modo cada usuario tendría un límite de uso de ancho de banda, en la Figura 10 se muestra un ejemplo, a lo que equivalen 2 megabit por segundo de descarga y 1 megabit de subida (ver Anexos, Figura 32 y Tabla 4).

[5] Algunos navegadores web bloquean las ventanas emergentes por defecto, así que requiere permisos de parte del usuario.

Figura 10.

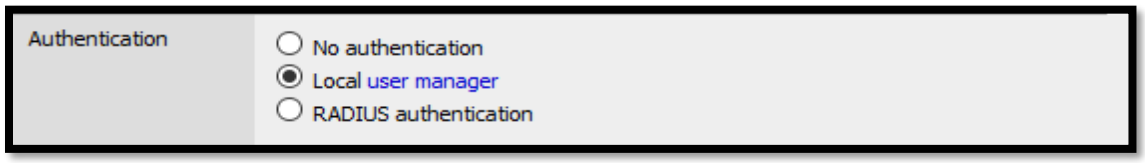
Restricción de Ancho de Banda



Muy importante en la parte de *Authentication* elegir la opción *"local user manager"* (administrador de usuarios local) porque no disponemos de servidor Radius y con gran satisfacción se procede a "*save"*. (véase Figura 11).

Figura 11.

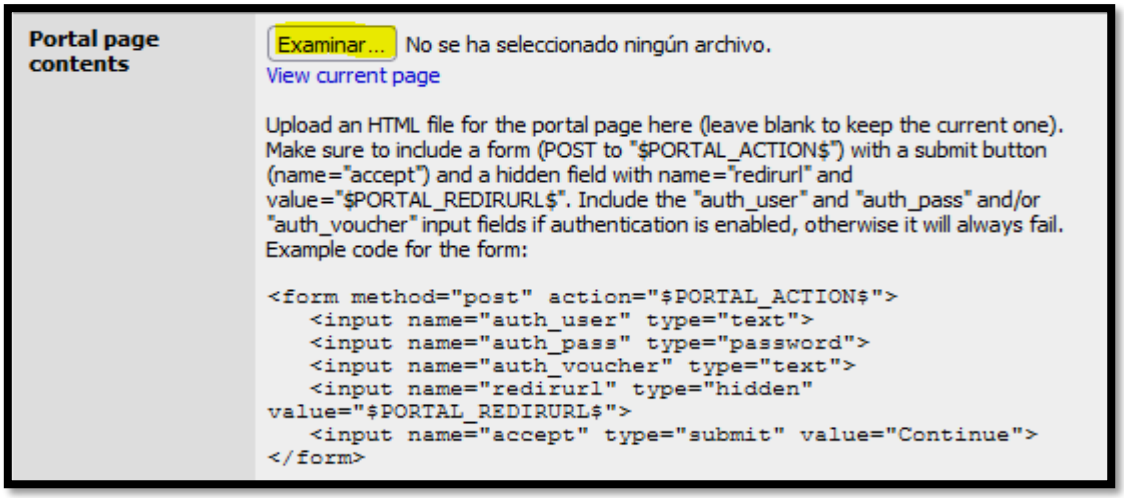
Administrador de usuarios local.



Luego de hacer eso nos podemos desplazar a través de las pestañas de la interfaz gráfica web de m0n0wall para restringir ciertas direcciones IP o bien cargar las páginas.html que verán nuestros usuarios a la hora de conectarse (ver Figura 12). Monowall solo reconoce código .html, para observar la página web del portal (ver Anexos Figura 34) y su correspondiente código.

Figura 12.

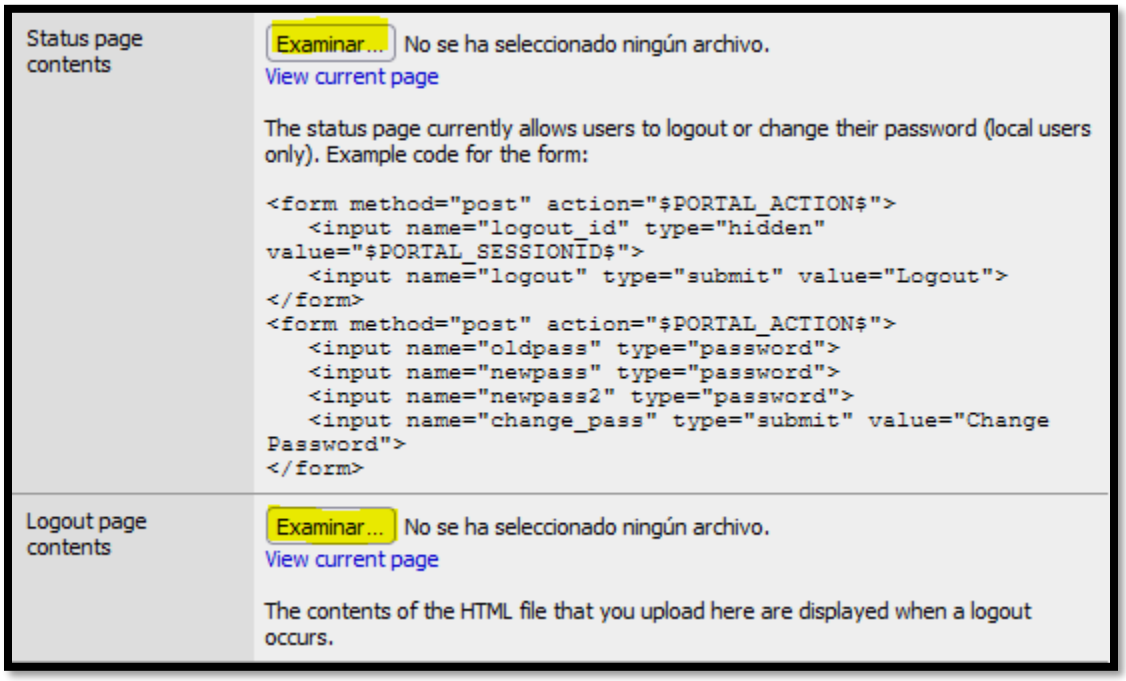
La página web de login se carga en esta sección.



También es posible agregar opcionalmente una página de estados y de desconectado (Ver Figura 13).

Figura 13.

Página de estado y desconexión (opcional).

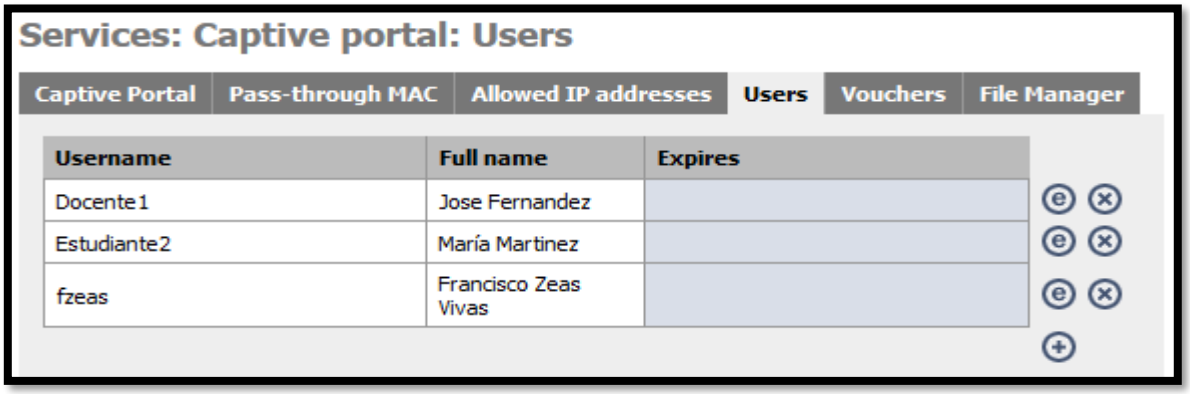


2.4 Usuarios.

Al ir a la pestaña *Users* podemos darnos cuenta que no existen usuarios, tenemos que agregarlos manualmente, ahí podemos asignarle la contraseña a cada usuario para que ellos puedan autenticarse[6] a través del portal cautivo, los cuadros de diálogo donde se registran a los usuarios tienen la siguiente nomenclatura (véase Figura14).

Figura 14.

Lista de usuarios.




```
User_name           fzeas
Full_name           Francisco Zeas Vivas
Password            uni123
Password (confirm)  uni123
(optional)          ****
```

Terminando de llenar los datos de la persona le damos SAVE y listo, así podremos agregar más usuarios sucesivamente, a continuación, algunos ejemplos.

```
User_name           Docente1
Full_name           José Fernandez
Password            Jfer321
Password (confirm)  Jfer321
(optional)          ****
```

[6] El DNS Forwarder debe estar habilitado para que funcionen las búsquedas de DNS por parte de clientes no autenticados.

```
User_name           Estudiante2
Full_name           María Martinez
Password            m2021
Password (confirm)  m2021
(optional)          ****
```

CAPITULO 3 – SERVIDOR NAGIOS

Nagios es un software de monitorización de equipos y servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren en la infraestructura antes de que los usuarios de la misma los perciban.

Aunque en esta propuesta se persigue el monitoreo de puntos de acceso inalámbrico, cabe destacar que Nagios es un sistema complejo y completo en cuanto a sus características que además hace uso en algunos casos de diversos sistemas como por ejemplo sistemas gestores de bases de datos, servidores web, etc. Está implementado en lenguaje PHP y fue diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta correctamente en variantes de Unix. Liberado bajo licencia GPL de la Free Software Foundation, en otras palabras, forma parte del amplio contenido de software libre que nos ofrece la red.

Se hará uso del sistema operativo Linux Debian 10 Buster, debido a su naturaleza de software libre lo hace una opción viable, es de fácil de instalación, estable y sencillamente confiable sin dejar de ser un sistema robusto y seguro, idóneo para este tipo de proyectos, todo esto como **máquina virtual** en VirtualBox.
Sin embargo, es necesaria la instalación previa de un servidor L.A.M.P., lo cual son un conjunto de aplicaciones que garantizarán el correcto funcionamiento de Nagios, además instalaré el complemento llamado Guest Additions (adiciones de invitado) de VirtualBox el cual es muy recomendable tenerlo en cualquier máquina virtual que haga de servidor.

3.1 Guest Additions.

De ahora en adelante todo se planteará en un entorno con el sistema operativo **Linux Debian 10 Buster**. Este complemento brinda funciones como mejoras visuales (posibilita modo pantalla completa), permite usar carpetas compartidas, integración del ratón (libertad de usar el cursor entre la máquina huésped y la

invitada), la utilidad de compartir el portapapeles y entre otros. Antes de instalar dicho complemento es recomendable hacer lo siguiente:

```
#apt-get update
```

Una vez actualizados los repositorios tenemos que actualizar el sistema operativo virtualizado ejecutando el siguiente comando en la terminal:

```
#apt-get upgrade
```

Al haber actualizado el sistema operativo virtual, tenemos que instalar el paquete build-essential[7].

```
#apt-get install build-essential
```

Ahora tendremos que asegurar que tengamos instaladas las cabeceras del núcleo. La función de las cabeceras del núcleo es la de compilar módulos para el kernel. Por lo tanto, en el caso que no tener las cabeceras instaladas tendríamos problemas a la hora de instalar las Guest Additions.

```
#apt-get install linux-headers-$(uname -r) dkm
```

Después de este procedimiento hay que reiniciar nuestra máquina virtual. Una vez reiniciada la máquina virtual hay que instalar el paquete module-assistant. Este paquete se encarga de compilar e instalar los módulos necesarios para usar un hardware no soportado por el kernel. Por lo tanto, necesitamos disponer de este paquete para instalar las Guest Additions.

```
#apt-get install module-assistant
```

Finalmente, tan solo falta asegurar que tengamos la versión de las cabeceras del núcleo necesarias y el paquete build-essential. Para ejecutamos el siguiente comando en la terminal:

```
#m-a prepare
```

[7] Este es un metapaquete que contiene la totalidad de software necesario para la generación de paquetes .deb y para la programación en diversos lenguajes como por ejemplo C/C++. Es imprescindible tener instalado este metapaquete para poder instalar Guest Additions.

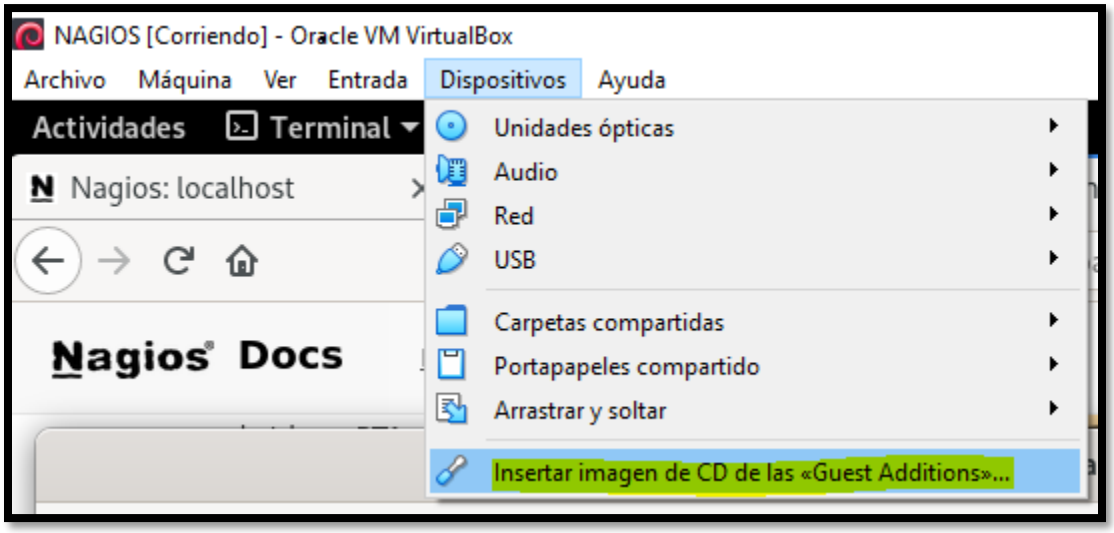
En teoría este paso no es necesario ya que en pasos anteriores hemos instalado las cabeceras del núcleo y el paquete build-essential. No obstante, no perdemos nada en hacer la comprobación.

3.1.2 Instalación.

El primer paso es introducir/montar el CD virtual de las Guest Additions en el sistema operativo virtualizado. Para realizar esto, tal y como se puede ver en la captura de pantalla, tenemos que ir al menú *dispositivos* de VirtualBox y clicar sobre la opción "Insertar Imagen CD de las Guest Additions" (véase Figura 15).

Figura 15.

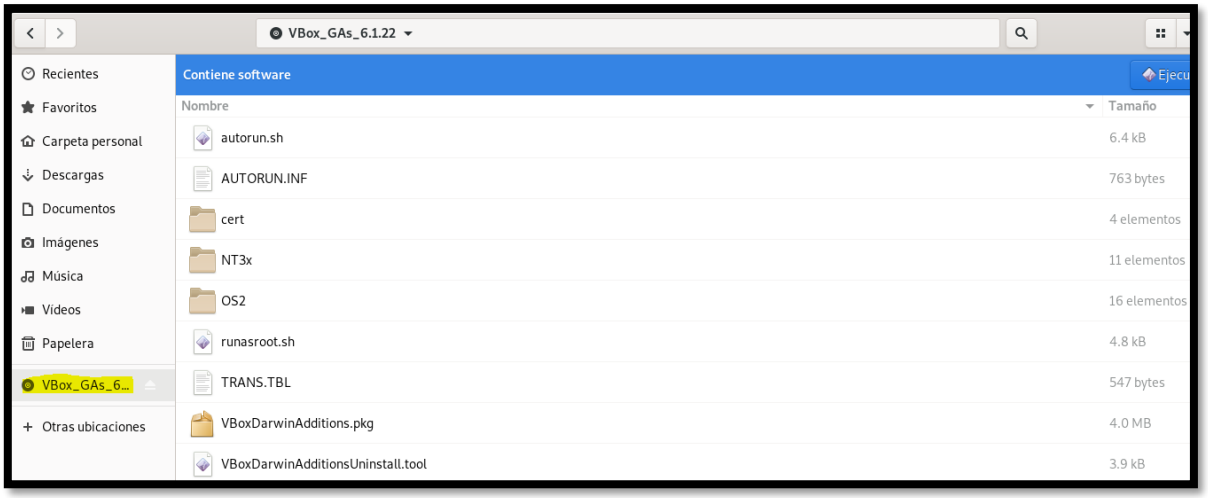
Imagen de Guest addtions.



Si el gestor de archivos no abre de forma automática, tendremos que abrirlo nosotros de forma manual. Podemos apreciar en la Figura 19, la unidad montada de Virtual Box Guest Additions en resaltado.

Figura 16.

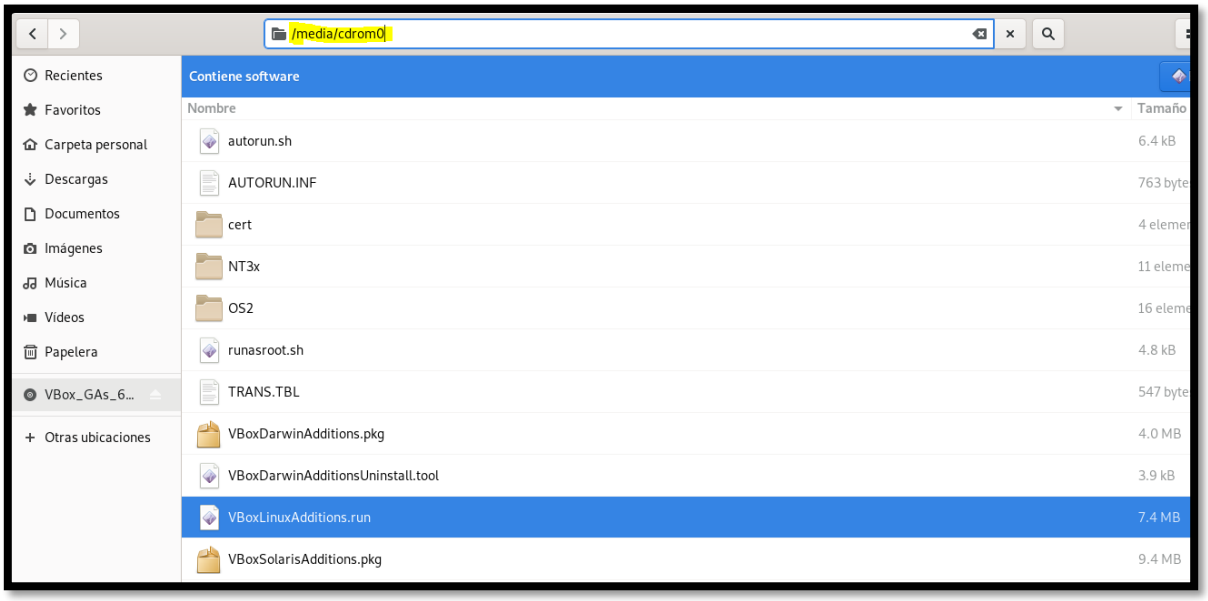
Ubicación de instalador.



Al estar en la barra de búsqueda presiono CTRL + L para determinar la ubicación, esto es necesario para la instalación (véase Figura 17).

Figura 17.

Comando y dirección exacta de montaje



Una vez disponemos de la dirección de montaje de Guest additions copiada en el portapapeles, ahora procedo en la terminal.

```
#cd /media/cdrom0
```

Finalmente, tan solo nos falta introducir el comando para poder instalar las Guest Additions. Por lo tanto, tan solo tenemos que ejecutar el siguiente comando en la terminal:

```
#sudo sh ./VBoxLinuxAdditions.run
```

Después de ejecutar este comando empezará la instalación de las Guest Addtions. Durante el proceso de instalación es importante observar que no se produzca ningún error. Ahora tan solo resta reiniciar la máquina virtual.

3.3 Servidor LAMP.

Es necesario instalar un servidor L.A.M.P. (particularmente en Linux) que hará que nuestra herramienta de monitoreo (Nagios) cumpla con todas sus funciones. LAMP viene de las siglas Linux (el sistema operativo), Apache (el servidor web), MySQL / MariaDB (un gestor de base de datos) y PHP / Perl / Python (alguno de estos lenguajes de programación). Todo lo mencionado es paquetería descargable como software libre, una de las bondades de mi proyecto.

3.3.1 Linux.

- Sistema operativo Linux (Debian[8]).

Debian GNU/Linux es un sistema operativo libre, desarrollado por miles de voluntarios alrededor del mundo, que colaboran a través de Internet, por ende, es un software libre del cual haré uso para este proyecto. Es posible descargar dicho software desde la página web oficial.

[8] El procedimiento y cada uno de los pasos para la instalación de Linux Debian Buster 10 no se abordará en este documento.

A partir de aquí mostraré líneas de comando que se ejecutan en la Terminal de Linux en modo superusuario (modo máximo de privilegio).

```
#nano /etc/apt/sources.list
```

Repositorio utilizado, contenido del archivo “sources.list”.

```
#
# deb cdrom:[Debian GNU/Linux 10.4.0 _Buster_ - Official amd64
NETINST 20200509-10:25]/ buster main

#deb cdrom:[Debian GNU/Linux 10.4.0 _Buster_ - Official amd64
NETINST 20200509-10:25]/ buster main


deb http://deb.debian.org/debian/ buster main contrib non-free
deb-src http://deb.debian.org/debian/ buster main contrib non-
free

deb http://security.debian.org/debian-security buster/updates
main contrib non-free
deb-src            http://security.debian.org/debian-security
buster/updates main contrib non-free

# buster-updates, previously known as 'volatile'
deb http://deb.debian.org/debian/ buster-updates main contrib
non-free
deb-src  http://deb.debian.org/debian/  buster-updates  main
contrib non-free
```

Luego de agregar los repositorios procedemos a actualizar el sistema

```
#aptitude update
#aptitude upgrade
```

3.3.2 Apache server.

El servidor HTTP Apache es un servidor web libre y de código abierto, el más popular en cuanto a uso, sirviendo de facto como plataforma de referencia para el diseño y evaluación de otros servidores web.

```
#aptitude install apache2
```

3.3.3 MySQL.

MySQL es un Sistema de Gestión de Bases de Datos (SGBD) relacional, que por lo tanto utiliza SQL, multihilo y multiusuario del que se estiman más de un millón de instalaciones.

```
# aptitude search mysql-common
# aptitude install mysql-common
```

3.3.4 PHP.

PHP (acrónimo recursivo de "PHP: Hypertext Preprocessor") es un lenguaje de programación diseñado para producir sitios web dinámicos. PHP es utilizado en aplicaciones del lado del servidor, aunque puede ser usado también desde una interfaz de línea de comandos o como aplicación de escritorio.

Cabe destacar que todo lo mencionado es software libre, por ende, no se necesita pagar licencia alguna.

```
# aptitude search php7.3
# aptitude install php7.3
```

Nota: Al descargar la paquetería correspondiente a php 7.3 instala varios módulos virtuales de mysql.

3.4 Configuración de Nagios.

Al haber instalado satisfactoriamente el servidor L.A.M.P. podemos proceder a la descarga de la versión Nagios Core más reciente (nagios 4.4.6) desde el sitio web oficial o podemos ejecutar el siguiente comando para descargarlo directamente desde consola.

```
#cd root
#wget
https://github.com/NagiosEnterprises/nagioscore/releases/down
load/nagios-$VER/nagios-4.4.6.tar.gz
```

Sin embargo, antes de proceder a instalar Nagios es necesario descargar los siguientes paquetes ya que son prerrequisitos de dicho software.

```
#apt-get install vim wget curl build-essential unzip openssl
libssl-dev libapache2-mod-php php-gd libgd-dev
```

Después de haber realizado todo lo anterior, finalmente descomprimimos nagios:

```
#tar xvzf nagios-4.4.6.tar.gz
```

Ahora procedemos a entrar a la carpeta y a configurar:

```
#cd nagios-4.4.6
#./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

Al final debería aparecer algo como esto (Figura 18):

Figura 18.

Resumen de instalación de Nagios.

```
*** Configuration summary for nagios 4.4.6 2020-04-28 ***:
 General Options:

     Nagios executable:  nagios     Nagios user/group:
nagios,nagios    Command user/group:  nagios,nagios
Event Broker:  yes     Install ${prefix}:  /usr/local/nagios
Install ${includedir}:  /usr/local/nagios/include/nagios
Lock file:  /run/nagios.lock
 Check result directory:  /usr/local/nagios/var/spool
/checkresults
            Init directory:  /lib/systemd/system
   Apache conf.d directory:  /etc/apache2/sites-enabled
              Mail program:  /bin/mail
                   Host OS:  linux-gnu
           IOBroker Method:  epoll
 Web Interface Options:

              HTML URL:  http://localhost/nagios/
CGI URL:  http://localhost/nagios/cgi-bin/
 Traceroute (used by WAP):  /usr/bin/traceroute
```

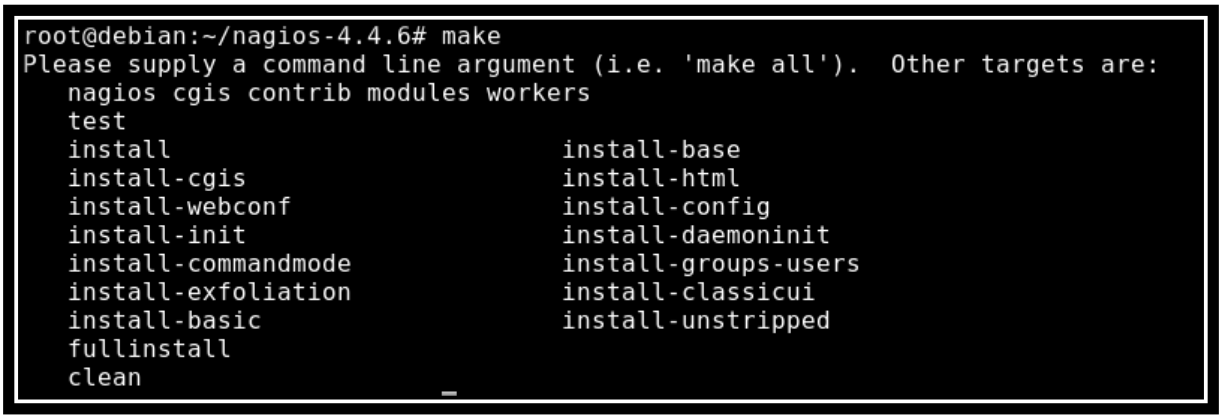
Ahora a instalar y compilar los paquetes del programa principal:

```
#make all
```

Para cerciorarme de algunos paquetes procedí a instalarlos manualmente por medio del comando make (véase la Figura 19):

Figura 19.

Módulos disponibles de Nagios.




```
#sudo make install-webconf
#sudo make install-init
#sudo make install-config
#sudo make install-daemoninit
#sudo make install-commandmode
#sudo make install-groups-users
```

Antes que todo crearemos un nuevo grupo “nagcmd” para permitir que comandos externos sean vinculados a través de la interfaz web, añadimos el usuario Nagios y www-data (que es el usuario de apache).

```
#usermod -a -G nagcmd nagios
#usermod -a -G nagcmd www-data
```

3.5 Interfaz web de nagios.

Primero que nada, hay que habilitar apache y sus módulos CGI, con este comando

```
sudo a2enmod rewrite cgi
```

Crearemos una cuenta ***nagiosadmin*** por la cual nos conectaremos a la interfaz web de nagios. Tengamos en cuenta la contraseña que asignemos a esta cuenta al

ejecutar el comando puesto que será necesaria para entrar a la interfaz web, como ejemplo usaré de contraseña “nagpass123”.

```
#htpasswd      -c      /usr/local/nagios/etc/htpasswd.users
nagiosadmin
```

Lo mejor es asegurarnos que este fichero tenga los permisos necesarios, el “777” para el comando chmod otorga todos los permisos.

```
#chown www-data:www-data /usr/local/nagios/etc/htpasswd.users
#chmod 777 /usr/local/nagios/etc/htpasswd.users
```

3.6 Nagios plugins

Nagios Core depende esencialmente de este complemento para que pueda realizar el monitoreo de servicios y recursos de red. Los complementos procesan los argumentos de la línea de comandos, realizan una verificación específica dependiendo del elemento que se esté monitoreando y luego devuelven los resultados a Nagios Core, en otras palabras, sin este el monitoreo a los equipos no podría darse.

```
#cd ~
#wget                https://github.com/nagios-plugins/nagios-
plugins/releases/download/release-2.3.3/nagios-plugins-
2.3.3.tar.gz
#tar xvf nagios-plugins-2.3.3.tar.gz
```

Entramos a la carpeta a instalar y compilar.

```
cd nagios-plugins-2.3.3
./configure
make
make install
```

Iniciamos los servicios de Nagios y Apache:

```
#systemctl start nagios
#systemctl restart apache2
```

3.7 Acceso por red a nagios.

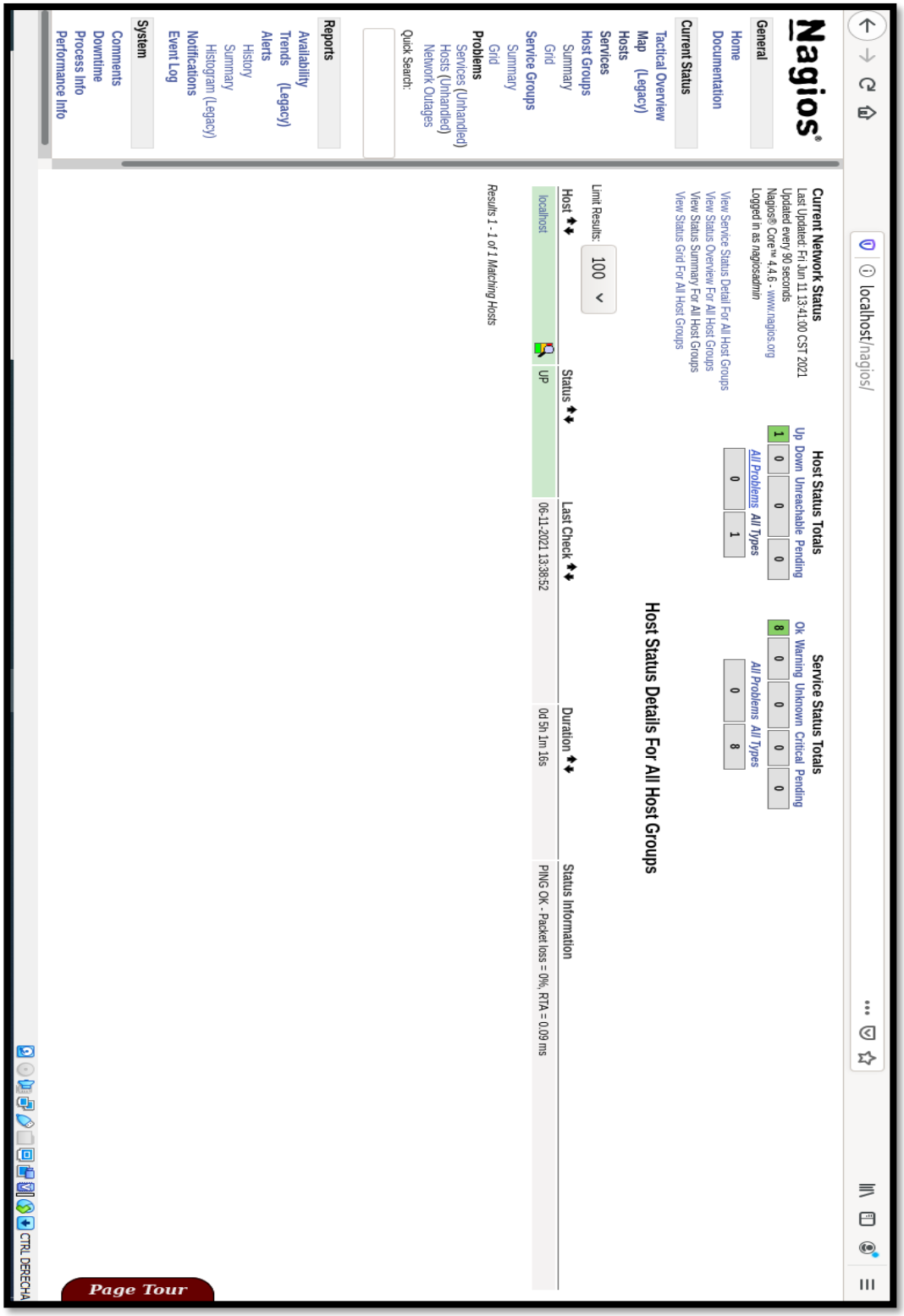
En el navegador de preferencia introducir lo siguiente: “http://localhost/nagios/”, (esto solo si se trabaja desee el mismo servidor, ver Figura 20) solicitará usuario y

contraseña para acceder ingresando como “nagiosadmin” y la contraseña que haya asignado al crear el usuario web.

Si damos clic en la sección de “Hosts” en el panel izquierdo de la interfaz, nos daremos cuenta que no hay ningún equipo añadido a excepción de “localhost” que aparece por defecto el cual es nuestro ordenador.

Figura 20.

Interfaz web de Nagios (recién instalado).



3.8 Acceso por telnet (SSH)

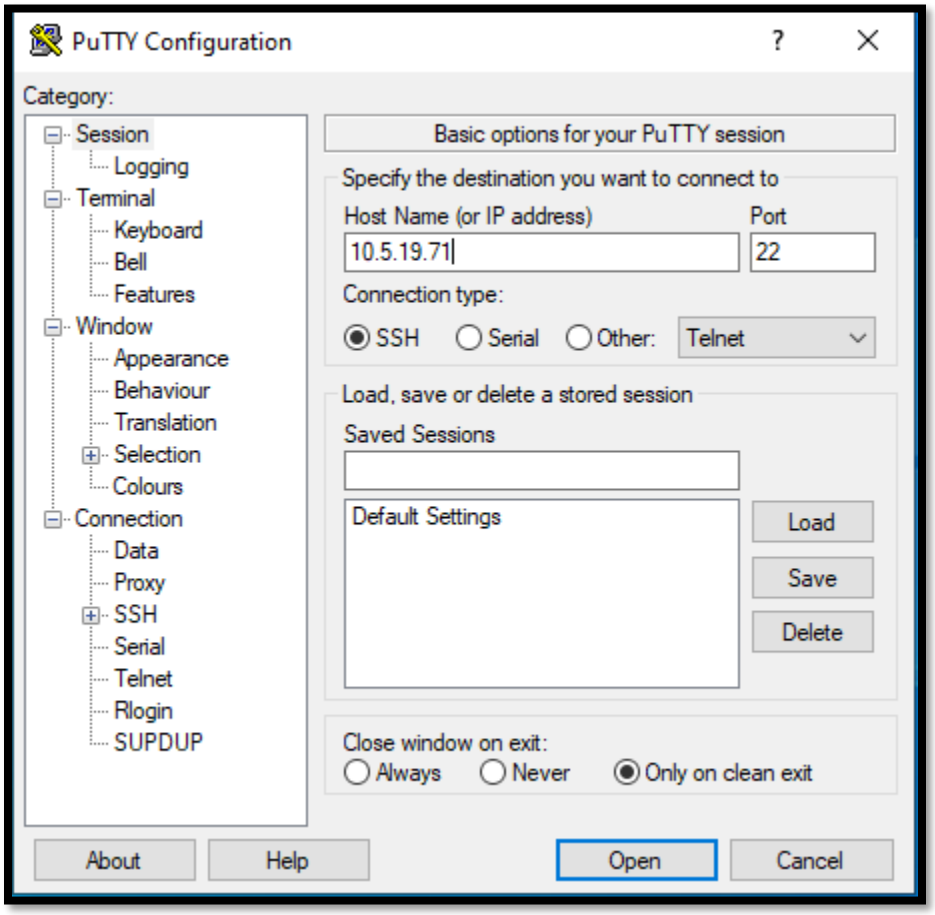
Instalar openssh en el servidor Debian abre la posibilidad de la conexión remota, esto ayuda al administrador de red a no moverse hasta el sitio en caso de alguna configuración importante.

```
#aptitude install openssh-server
#aptitude install openssh-client
```

Después de que el sistema operativo realice toda la paquetería, es posible conectar con el servidor vía telnet desde cualquier máquina de la red LAN, siempre y cuando tenga el usuario y contraseña requeridos, mediante el software **Putty** haré una sesión remota (ver Figura 21).

Figura 21.

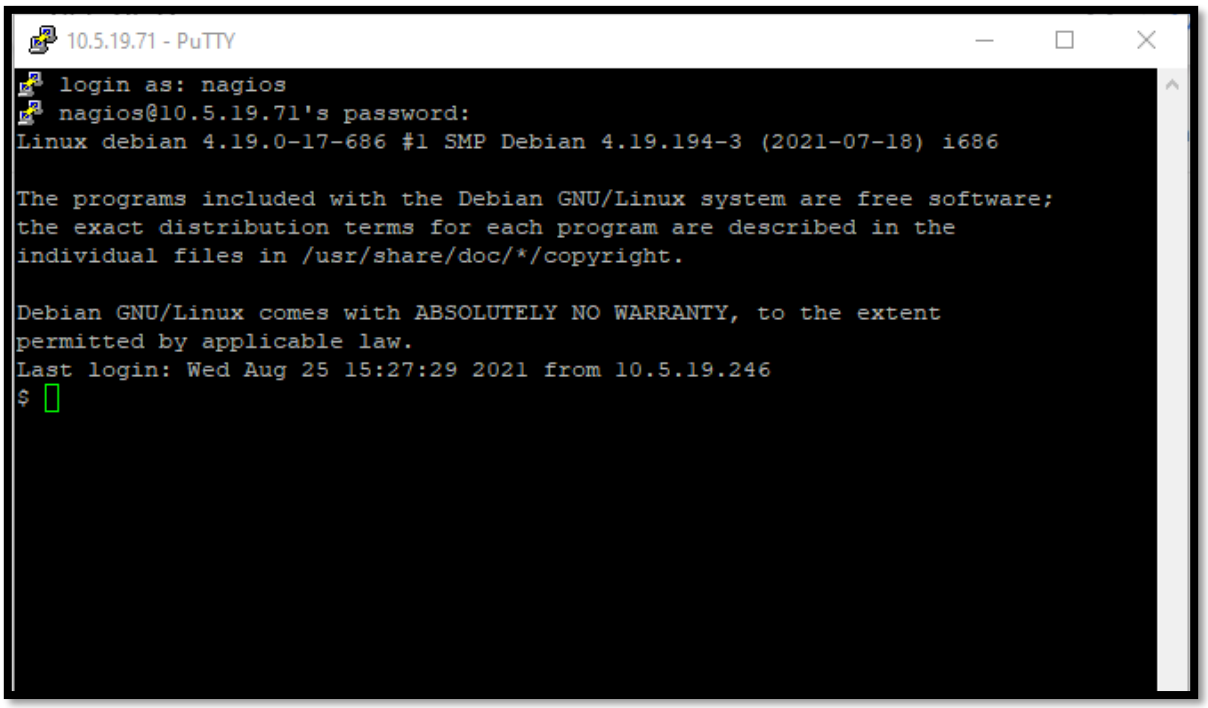
La dirección IP del servidor Nagios (puerto22)



Solicita usuario y contraseña, estos pueden ser del usuario root (si eres el admin) o un usuario de prueba como en este caso (ejemplo en Figura 22).

Figura 22.

Acceso a consola mediante Putty usando una conexión SSH.



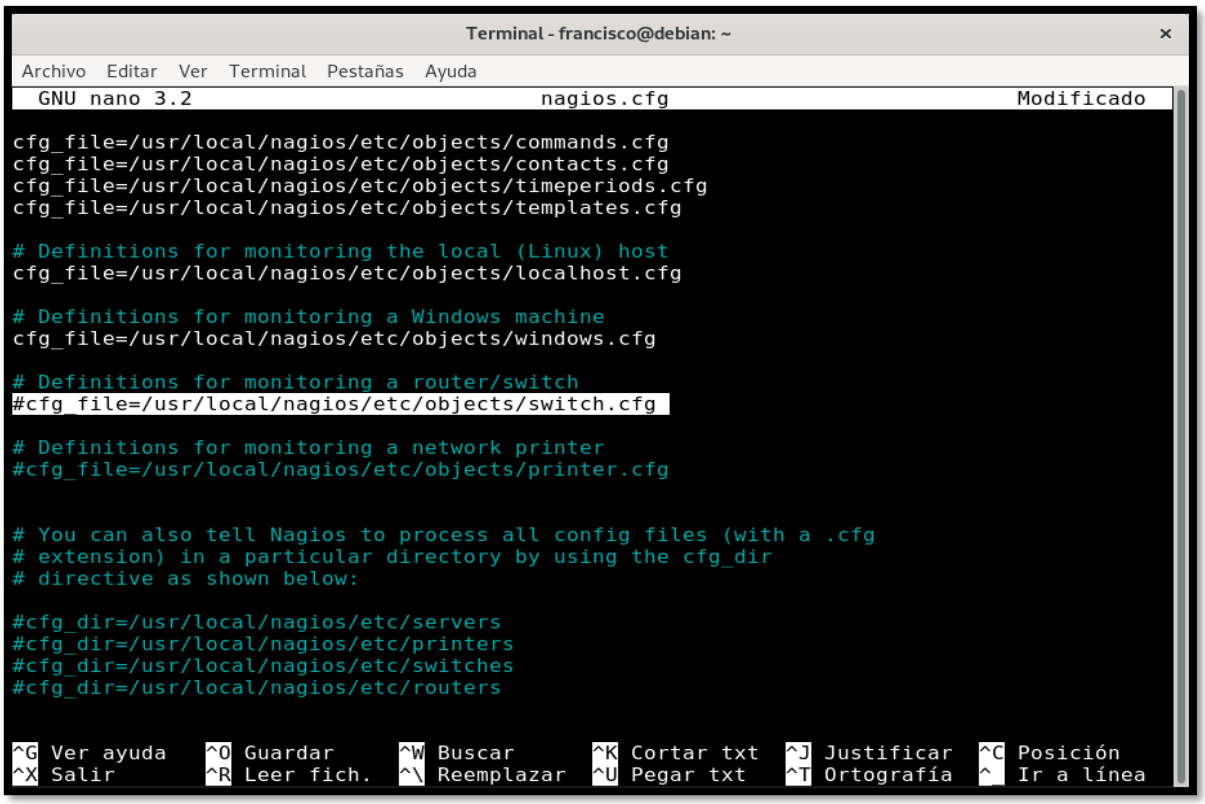
3.9 Agregando equipos a Nagios.

Para ello primero debemos de editar el siguiente fichero (ver Figura 26):

```
#nano usr/local/nagios/etc/nagios.cfg
```

Figura 23.

Nagios.cfg



Removemos el símbolo “#” al principio de la línea que está sombreada en la imagen ya que esta aparece comentada por defecto. Habiendo hecho esto, me dirijo al siguiente fichero:

```
#cd /usr/local/nagios/etc/objects
```

En este fichero se alojan todos los tipos de usuarios/equipos que pueden ser monitoreados por Nagios, los que aparecen ahí son “templates” predeterminados de Nagios, pueden ser usados sin ningún inconveniente, elegí el que se adapta más a los puntos de acceso Wi-Fi, así que lo agregaré en “switch.cfg”.

```
#nano switch.cfg
```

Este es el modelo o template para agregar equipos a monitorear, esto en la sección “Host definitions”

```
define host {
use                 generic-switch     ; Plantilla heredada por defecto
host_name           router-main        ; El nombre del equipo a monitorear
alias               routerclaro        ; Un nombre asociado al equipo
address             192.168.1.1        ; Dirección IP del equipo
hostgroups           switches          ; el grupo de host asociado a este equipo
}
```

CONCLUSIÓN.

El portal cautivo mediante Monowall es efectivo en este tipo de escenarios como lo son las redes abiertas al público, mediante este sistema se lograría alcanzar el control de acceso de cada uno de los usuarios a la red inalámbrica del IES. Sin dejar de lado un aspecto importante, Monowall reconoce cualquier equipo ya sea AP, switch o router que sea capaz de brindar acceso a internet con el simple hecho que esté como servidor antes que la LAN que se desea controlar, en resumen, puede usarse con los mismos equipos actualmente utilizados.

La idea de crear un solo servidor de Nagios y m0n0wall como máquinas virtuales para controlar la red inalámbrica es completamente posible, no implica gastos de licencias de software o costosos equipos de conocidas marcas o fabricantes ya que todo lo utilizado en esta propuesta es software libre, el único repito, el único requerimiento es una máquina con las características adecuadas.

El sistema Nagios es una excelente herramienta para monitorear los equipos de cualquier red inalámbrica y puede ser implementado en el recinto UNI-IES para vigilar el estado de los equipos de este recinto, así sus equipos Access Point pueden monitoreados desde una solicitud ICMP hasta donde el protocolo SNMP permita, lo que ofrece Nagios es la bondad de poder visualizar el estado desde la interfaz web del servidor, incluso enviar notificaciones por correo al administrador de red, en caso de alertas.

RECOMENDACIONES.

Siendo en principio una propuesta resulta difícil obviar el apartado gráfico de Nagios, una de tantas bondades que ofrece dicho software para estar al tanto del tráfico de los equipos a los que se desea monitorear desde una sola interfaz, aunque requeriría de cuidadosos ensayos y configuraciones adicionales en el servidor Nagios sería un aconsejable agregado a la red inalámbrica actual.

A futuro cuando la red siga creciendo lo mejor sería considerar un servidor Radius, el cual Monowall soporta y puede trabajar de la mano para así liberarle la carga en la parte de la autenticación, con este servidor sería posible administrar una gran cantidad de usuarios como base de datos, posee un apartado de reportes, soporta incluso VLAN dinámicas lo cual abre la posibilidad de organizar aún más la red actual, con la única desventaja que se tendría que considerar la adquisición de switches compatibles con Vlan dinámica en caso que lo soporten.

ANEXOS

Entrevista #1

Entrevista Isaac Jiménez 16/6/21

Ingeniero de Soporte técnico

1 ¿Existen inconvenientes al correr Nagios en una VM (Virtual Machine)?

Va dependiendo de la máquina virtual, pero realmente no hay inconvenientes, es completamente viable correrlo en una. Eso sí, tenés que considerar que hay varios virtualizadores.

2 ¿Cuál virtualizador me recomienda? ¿Alguna preferencia?

Podes usar cualquiera, el que sepas usar mejor, eso sí tienes que tener en cuenta tus requerimientos, o sea la necesidad de tu proyecto. Está proxmox (un virtualizador) que se estuvo usando a nivel institucional, es bastante bueno lo único que es más complejo al momento de manejarlo.

Tienes también este, Virtualbox, el que quieres usar, está bien en general, a mí personalmente no me ha dado problemas.

3 ¿Qué tal VMware? ¿Es bueno?

Bueno, si es bueno, solo que tenés que considerar que es en parte un software con licencia, o sea pagado. Claro puedes trabajar con el pero según lo que me has mencionado de tu proyecto puedes trabajar con los otros virtualizadores perfectamente.

4 ¿En qué parte de la red debe estar ubicado el servidor Nagios para que cumpla sus funciones pertinentes?

Después del router, por lo menos si quieres ver una sola LAN, y en el caso de monitorear varias, tiene que ser después del router que está en la "orilla" ya sabes el límite de la red.

5 ¿Se refiere al router borde (router fronterizo), el que gestiona a los otros?
Si y no, tenés que recordar que todas las redes están construidas diferente, claro, si siguen las normas y un orden para que sea funcional, por lo menos en el escenario que me planteas de una sola LAN, el servidor Nagios estaría ubicado después del router que les conecta a la red.

6 ¿Cómo cambiar el directorio donde se configuran los hosts, switches, Windows, etc? ¿Es recomendable hacer esta personalización?
Es posible, de momento no recuerdo, pero no es algo que te afecte el rendimiento, que mejore las gráficas, o el tiempo de respuesta, tiene que ver más con la parte de configurar a tu gusto. Es opcional a mi pensar.

7 ¿Qué se necesita para tener conexión remota a Nagios por medio de SSH?
Para eso necesitas open-ssh, es una aplicación para hacer las conexiones cifradas, como deberías de saber es free (gratuito) y la podés descargar en el Linux, la configuras para que escuche las peticiones del server, si tienes alguna duda le podemos preguntar a Walter, él fue el que configuró el de acá.

8 ¿Qué servicios / parámetros recomienda monitorear en equipos?
Pues lo esencial, vas a tener que usar el protocolo SNMP versión 2 en tus equipos del IES, crear una comunidad para poder monitorear su comportamiento mediante ICMP.
Nagios más que todo es para que se pueda estar al tanto de las alarmas, que es lo más importante, visualizar las gráficas y obviamente que todos los equipos estén UP.

Entrevista #2

Ing. Wilfredo García 5/7/21

Responsable de laboratorios IES.

1 ¿Con cuántos equipos inalámbricos dispone la red del recinto IES?

La otra vez te brindé el modelo que es el Ruckus T300, existen 5 Access Point funcionando para la actual red estudiantil. Uno por la dirección que no es para los estudiantes, hay en arquitectura, otro está por los bares, el último es en el segundo piso de sistemas… Ahí uno de los muchachos te puede decir donde están ubicados.

2 ¿Posee alguna forma de visualizar el tráfico de los usuarios conectados a la red wifi?

Si se puede, pues se entra a cada dispositivo AP para ver tráfico, ellos traen una ventana donde se puede ver el tráfico de los usuarios.

3 Si alguno de los equipos falla ¿Cómo se entera de esta incidencia?

Es posible validar que los equipos estén up, en nuestra consola personalizada aquí que el responsable de redes tiene en su máquina.

4 ¿Cuáles son las horas pico de tráfico según sus conocimientos o estadísticas?

A las horas de clase de la mañana que es cuando están todos los chavalos, de 7:00 AM a … (pausa) 3:00 PM más o menos. Llegan a topar los 100Mb en la mañana cuando tienen hasta un máximo de 300 MB del ancho de banda.

5 ¿Cómo cuánto baja el uso de ancho de banda después de las horas pico? ¿Un 20% o 30%?

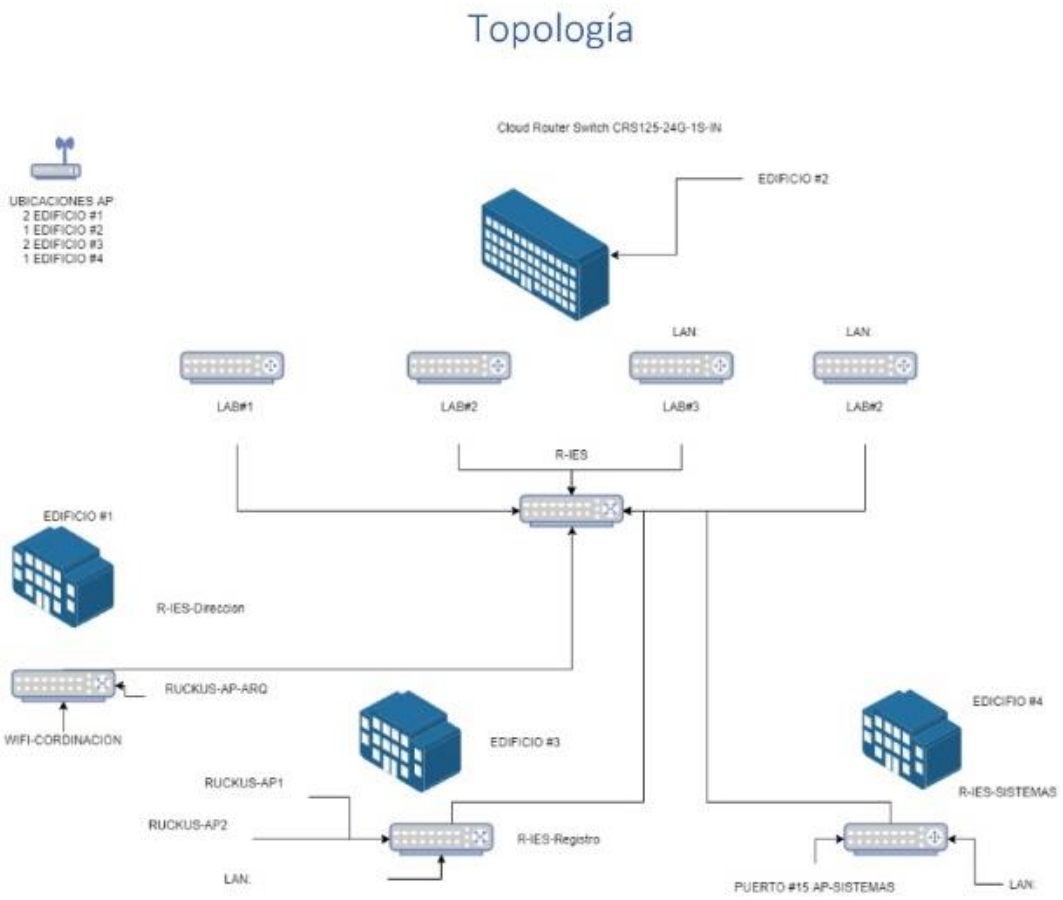
De 4:10 PM en adelante es cuando se baja el consumo, quizás un 30% del ancho de banda total.

6 ¿Posee algún medio para regular a los usuarios de la red actual?
Tenemos implementadas reglas en el switch, ahí mismo están declaradas las vlan por lo tanto todos están limitados a las políticas de ahí.
Todo lo que es juegos, páginas pornográficas, ocio y todo eso está filtrado desde el nic.ni.

7 ¿Qué tal los usuarios de la red inalámbrica? ¿Cómo les limita el ancho de banda?
Pues es por cada aparato (AP), cada Ruckus tiene configurado cierto ancho de banda y cada estudiante se conecta por competencia, el que se conectó primero es el que va (a consumir) y así sucesivamente.

Figura 24.

Topología original RED IES



Nota: Diagrama (alterado) de la red del recinto IES. Este fue modificado por informática por razones de confidencialidad de la ubicación de sus equipos importantes, este fue un punto de partida para determinar cuantos puntos de acceso inalámbricos poseen.

Figura 25.

Consumo estándar de un AP, medio día.

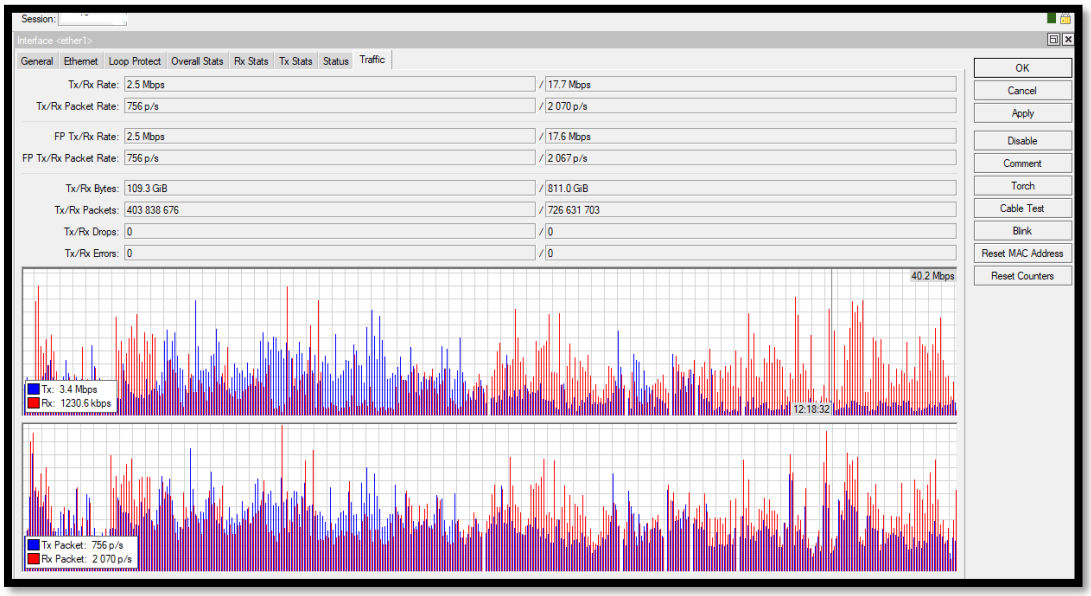


Figura 26.

Consumo estándar del AP (zona de Registro), tarde (4:00 PM).

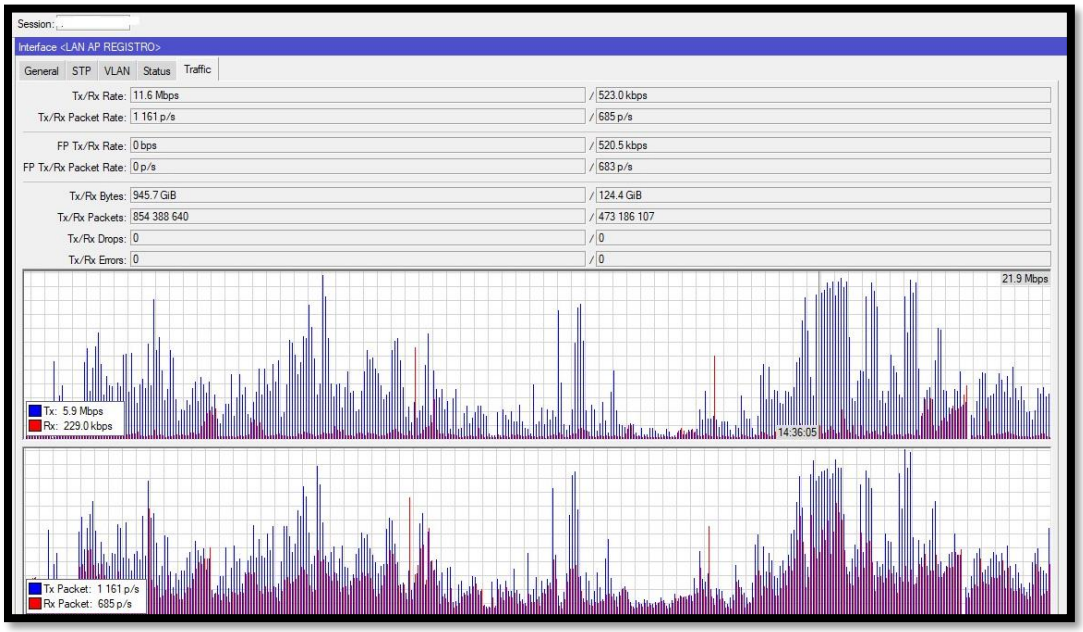
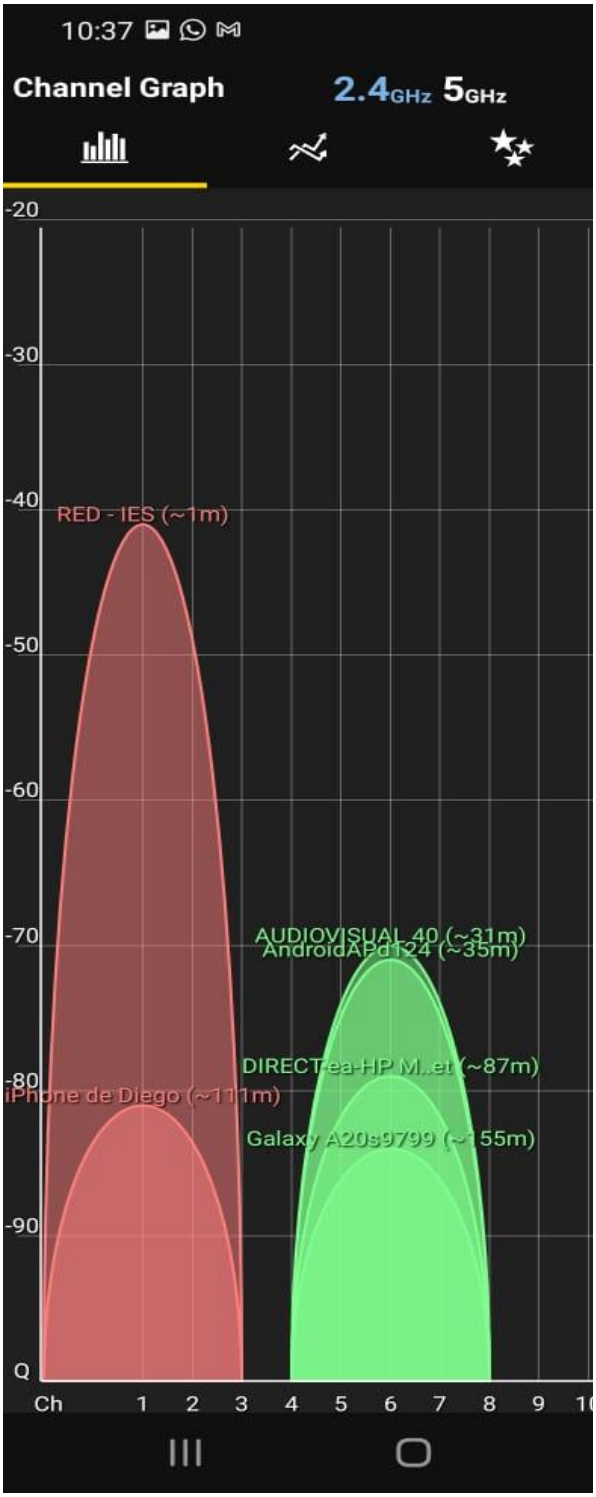


Figura 27.

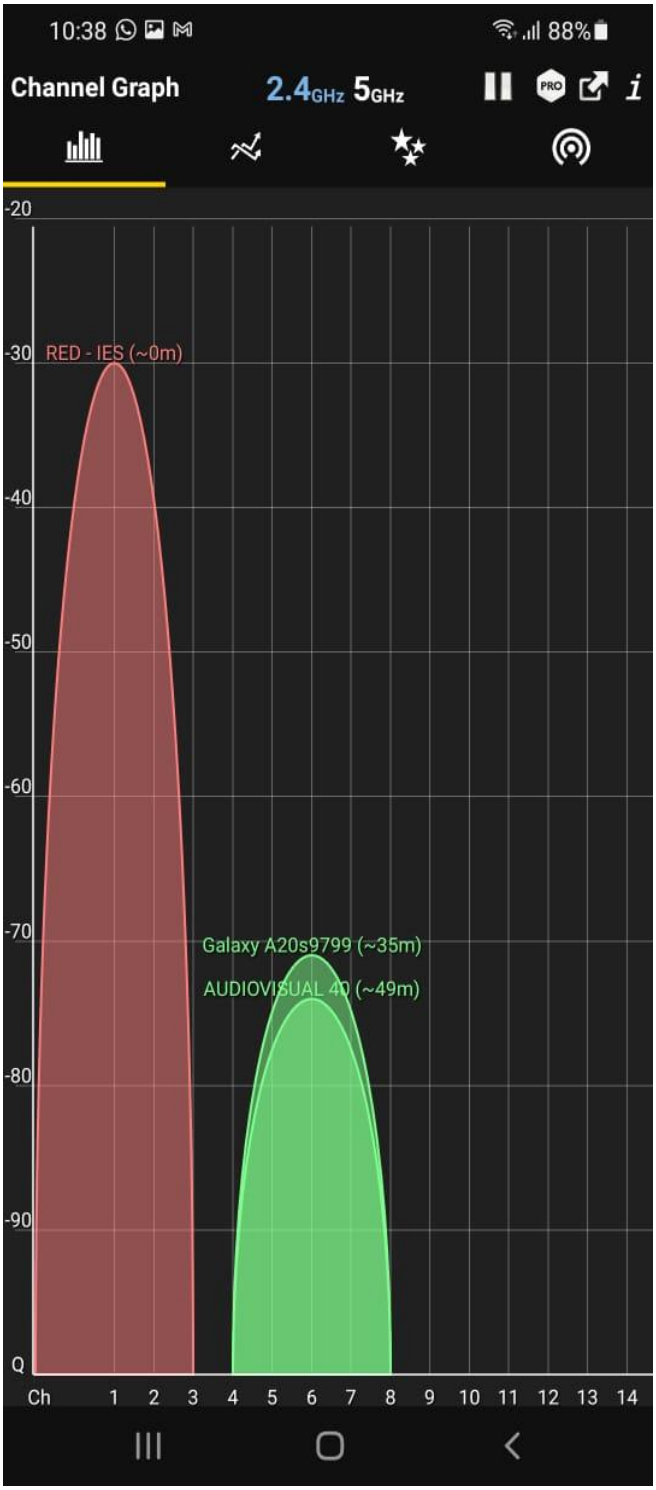
AP “RED-IES” (5GHz) a 1metro.



Nota: Desde APP wifi analyzer.

Figura 28

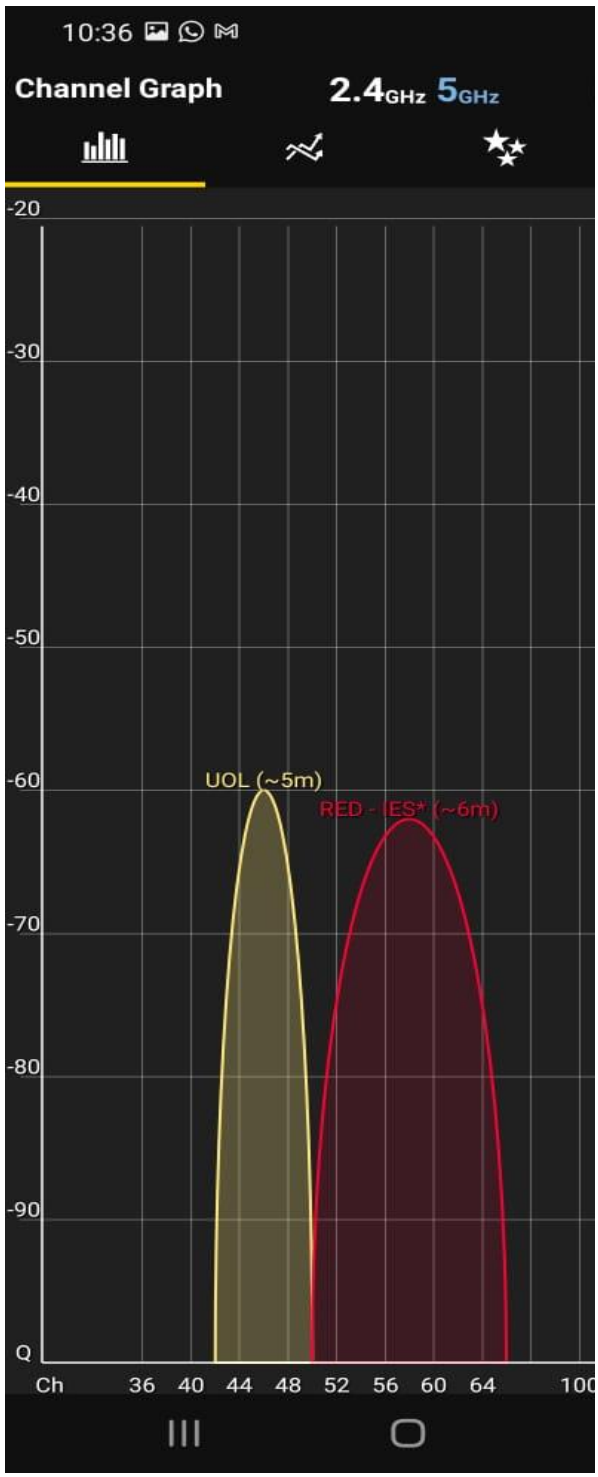
AP “RED-IES” (5GHz) localizado.



Nota: Desde APP wifi analyzer.

Figura 29.

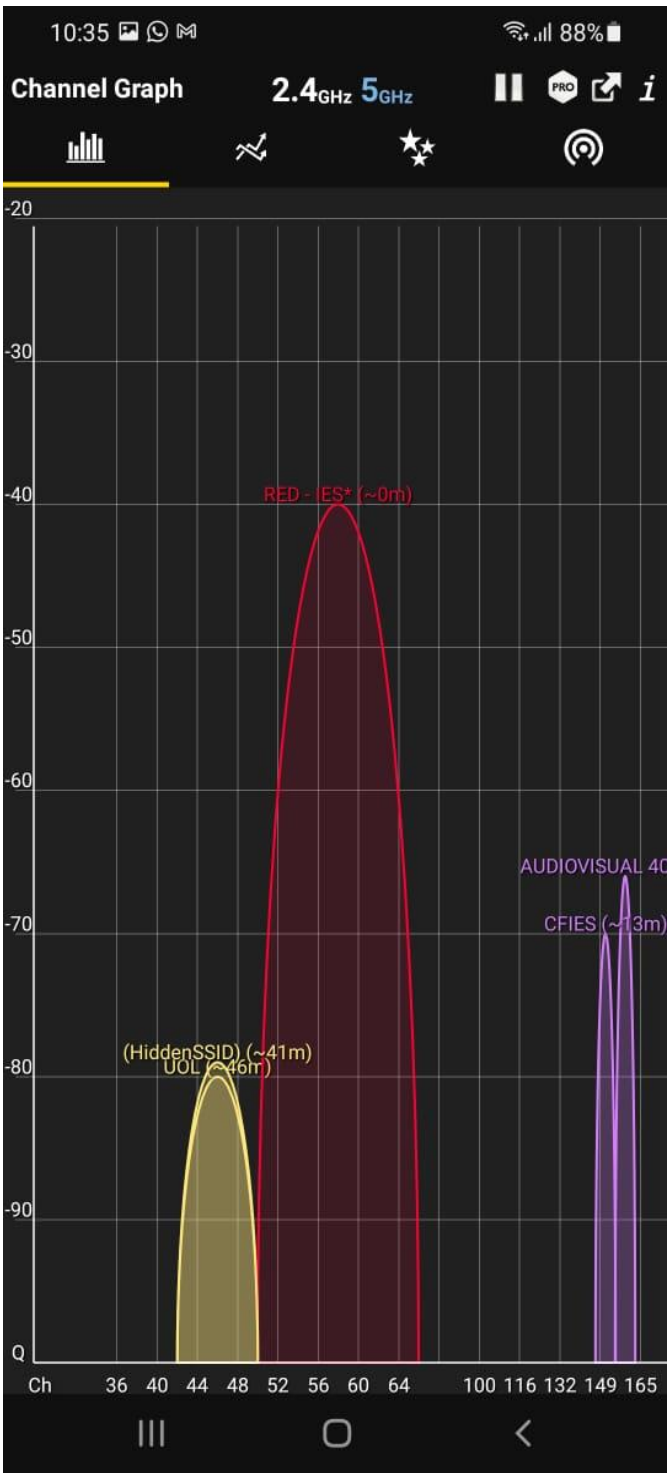
AP “RED-IES” (5GHz) a 6 metros.



Nota: Desde APP wifi analyzer.

Figura 30.

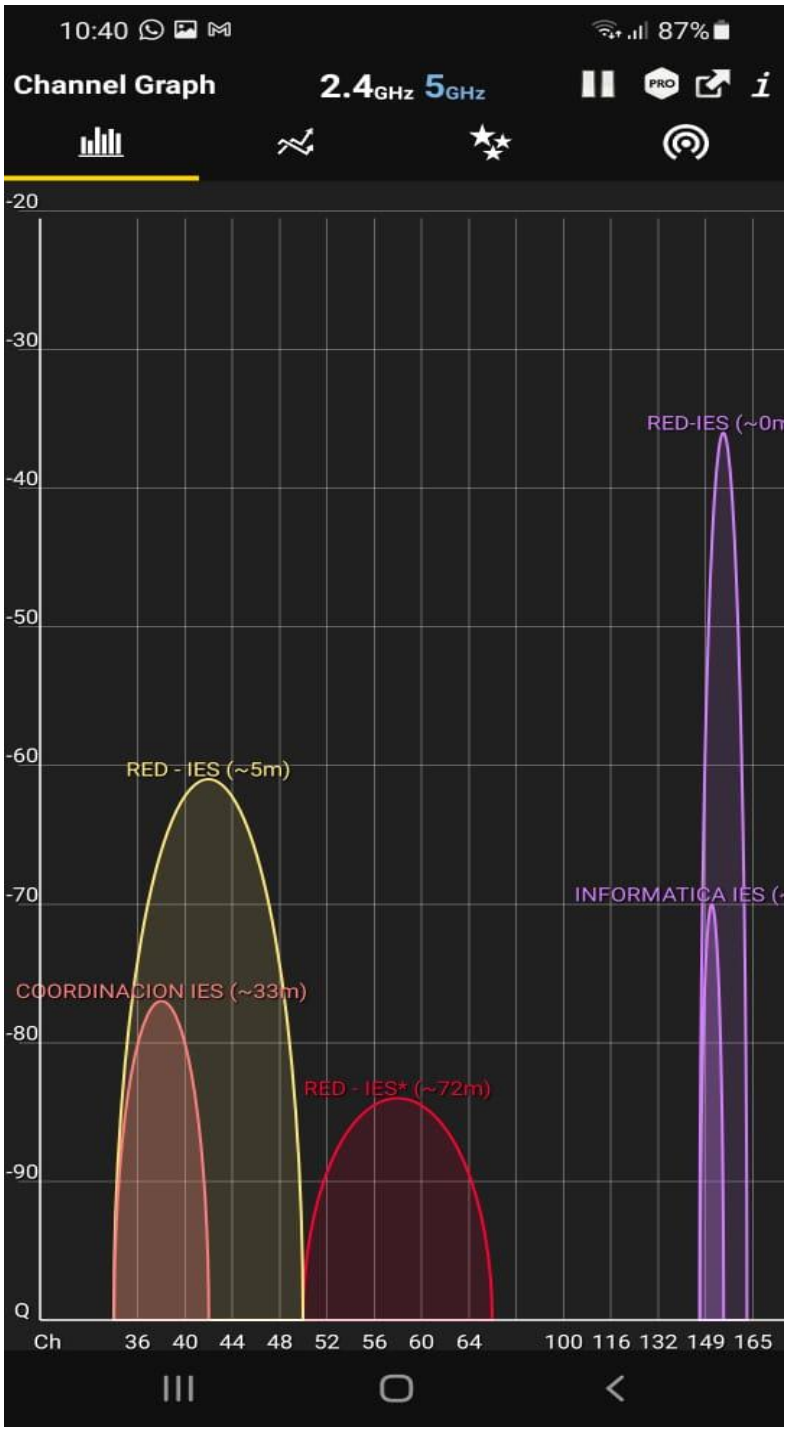
AP “RED-IES” (5GHz) localizado.



Nota: Desde APP wifi analyzer.

Figura 31

Centro de la UNI-IES, se muestran múltiples redes.



Nota: Desde APP wifi analyzer.

Figura 32.

Ancho de banda regulado por monowall a 2 Mbps de descarga, 1 Mbps de subida.

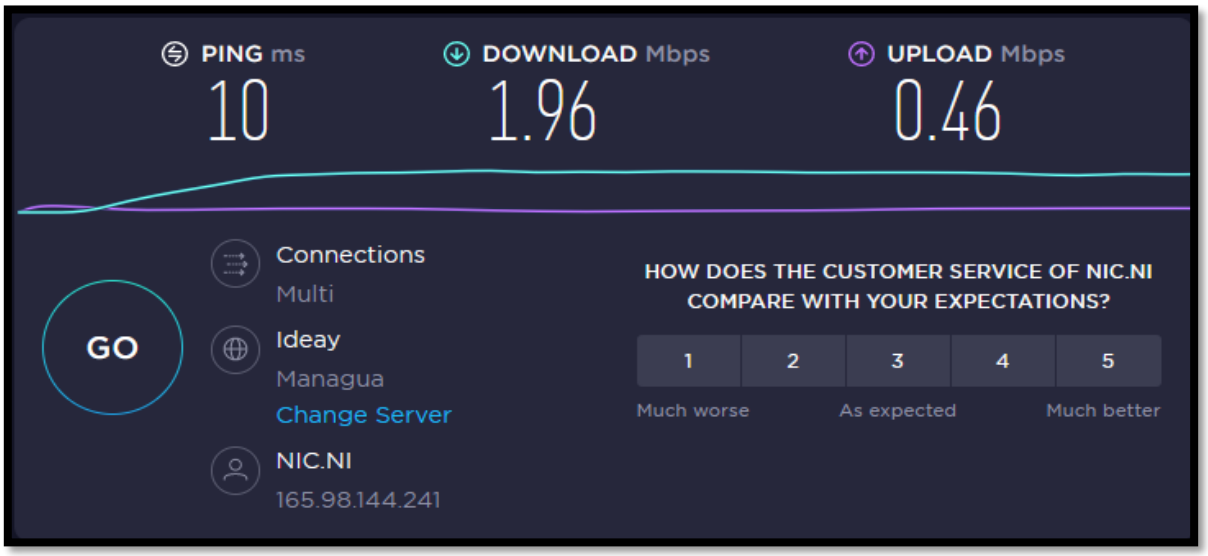


Figura 33.

Ancho de banda usual de la red inalámbrica actual, irregular a como se puede observar.

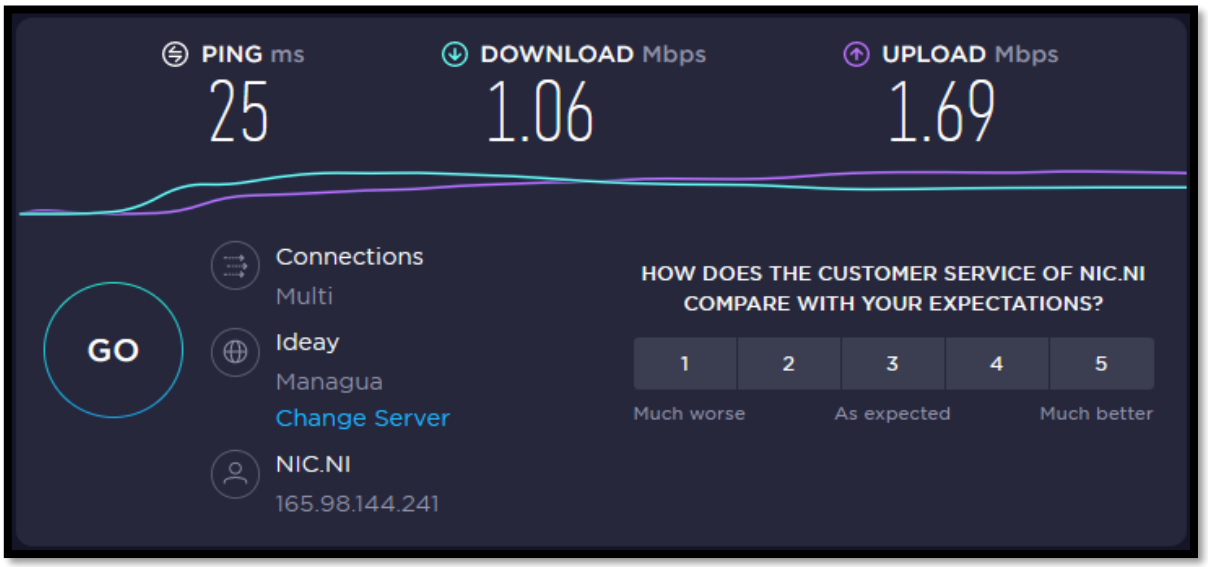


Tabla 4.

Unidades de tasa de transmisión.

Unidad de ancho de banda	Abreviatura	Unidad	Equivalencia	Notación científica
Bits por segundo	bps	1 bps.	Unidad base.	-
Kilobits por segundo	Kbps	1 Kbps.	1,000 bps	10^3 bps
Megabits por segundo	Mbps	1 Mbps	1,000 Kbps	10^6 bps
Gigabits por segundo	Gbps	1 Gbps	1,000 Mbps	10^9 bps
Terabits por segundo	Tbps	1 Tbps	1,000 Tbps	10^{12} bps

Figura 34.

Pre visualización de la página del portal.

Código Html del portal web.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />
<!-- TemplateBeginEditable name="doctitle" -->
<title>:: Portal de Acceso a la Red Inalámbrica, UNI
::</title>
<!-- TemplateEndEditable -->
<!-- TemplateBeginEditable name="head" -->
<!-- TemplateEndEditable -->
<style type="text/css">
<!--
body {
     font: 100% Verdana, Arial, Helvetica, sans-serif;
     background: #666666;
     margin: 0; /* it's good practice to zero the margin and
padding of the body element to account for differing browser
defaults */
     padding: 0;
     text-align: center; /* this centers the container in IE
5* browsers. The text is then set to the left aligned default
in the #container selector */
     color: #000000;
}
.oneColFixCtrHdr #container {
     width: 780px;  /* using 20px less than a full 800px
width allows for browser chrome and avoids a horizontal
scroll bar */
     background: #FFFFFF;
     margin: 0 auto; /* the auto margins (in conjunction with
a width) center the page */
     border: 1px solid #000000;
     text-align: left; /* this overrides the text-align:
center on the body element. */
}
.oneColFixCtrHdr #header {
     background: #213455;
     padding: 0 10px 0 20px;  /* this padding matches the
left alignment of the elements in the divs that appear
beneath it. If an image is used in the #header instead of
text, you may want to remove the padding. */
```

```
}
.oneColFixCtrHdr #header h1 {
     margin: 0; /* zeroing the margin of the last element in
the #header div will avoid margin collapse - an unexplainable
space between divs. If the div has a border around it, this
is not necessary as that also avoids the margin collapse */
     padding: 10px 0; /* using padding instead of margin will
allow you to keep the element away from the edges of the div
*/
}
.oneColFixCtrHdr #mainContent {
     padding: 0 20px; /* remember that padding is the space
inside the div box and margin is the space outside the div
box */
     background: #FFFFFF;
}
.oneColFixCtrHdr #footer {
     padding: 0 10px; /* this padding matches the left
alignment of the elements in the divs that appear above it.
*/
     background:#DDDDDD;
}
.oneColFixCtrHdr #footer p {
     margin: 0; /* zeroing the margins of the first element
in the footer will avoid the possibility of margin collapse -
a space between divs */
     padding: 10px 0; /* padding on this element will create
space, just as the the margin would have, without the margin
collapse issue */
}
.style1 {color: #FF0000}
.style2 {font-size: 75%}
.style3 {color: #FFFFFF}
.oneColFixCtrHdr #container #footer h3 strong2 {
     text-align: center;
}
.Estilo1 {color: #0000FF; }
-->
</style></head>

<body class="oneColFixCtrHdr">
<br /><br /><br />
<div id="container">
  <div id="header">
    <!--<img src="wifitop.jpg" width="730" height="140" />
    <h1 align="center" class="style3">Red Inalámbrica -
UNI</h1>
```

```
    <!-- end #header --></div>
  <div id="mainContent">
    <h2 align="center" class="Estilo1"> Ingresar Usuario y
Contraseña:</h2>
    <form method="post" action="$PORTAL_ACTION$">
      <div align="center">Usuario:
        <input name="auth_user" type="text">
        Contraseña:
        <input name="auth_pass" type="password">
        <input name="redirurl" type="hidden"
value="$PORTAL_REDIRURL$">
        <input name="accept" type="submit" value="Acceder">
      </div>
    </form>
    <h2 align="center">Bienvenidos a la Red Inalámbrica de la
UNI.</h2>
    <p align="justify">Se les da la más cordial de bienvenida
a tod@ la comunidad universitaria UNI-IES a la red
inalámbrica para que puedan realizar cada de una de sus
tareas académicas.</p>
    <p align="justify"><em>Con esta herramienta se pretende
<strong>mantener un control de usuarios conectados así como
su uso de ancho de banda</strong> mejorando la experiencia de
navegación.</em></p>
    <p align="justify">Atentamente.</p>
    <p align="justify"><strong>Dirección de
Informática.</strong></p>
    <!-- end #mainContent --></div>
  <div id="footer">
    <h4> </h4>
  <!-- end #footer --></div>
<!-- end #container --></div>
</body>
</html>
```

Referencias

¿Qué es el software libre? - Proyecto GNU - Free Software Foundation. (s.f.). https://www.gnu.org/philosophy/free-sw.es.html

Aoki, O. (28 de Noviembre de 2021). *Guía de referencia de Debian.* [Archivo PDF] https://www.debian.org/doc/manuals/debian-reference/debian-reference.es.pdf

Buechler, C. (Febrero de 2015). *Monowall Handbook. Introduction.* https://doc.m0n0.ch/handbook/intro.html#id11553237

Castro, R. (Septiembre de 2005). *Red Iris Publicaciones, Contenido del boletín No.73.* [Archivo PDF] https://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

CSL. (s.f). *CSL - 300Mbps WiFi PCI Express (PCIe) card / adapter*. https://www.desertcart.ni/products/48569011-csl-300mbps-pci-express-pcie-wlan-card-with-mimo-technology-2x-omni-directional-rsma-antenna-realtek-rtl8192ce-chip-set-2-4-ghz-frequency-range-wep-with-64-128-bit-wpa2-psk-wpa-psk

Debian. (7 de agosto de 2021). *Acerca de Debian*. https://www.debian.org/intro/about

farproc. (7 de junio de 2021). *Wifi Analyzer* (3.7*)* [Aplicación móvil]. Google Play. https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=es_NI&gl=US

Nagios. (s.f.). *Nagios Plugins*. https://www.nagios.org/projects/nagios-plugins/

Portal Cautivo. (24 de Junio de 2020). En *wikipedia* https://es.wikipedia.org/w/index.php?title=Portal_cautivo&oldid=128643529

Sectigo. (10 de junio de 2020). *Embedded Firewalls for IoT Devices*. https://sectigo.com/resource-library/embedded-firewalls-for-iot-devices

Velasco, R. (19 de Julio de 2021). *VMware, VirtualBox o Hyper-V – ¿Qué programa es mejor?* https://www.softzone.es/programas/utilidades/diferencias-vmware-virtualbox-hyper-v/

VMware. (2022). *Maquina virtual. Vmware latam.* https://www.vmware.com/latam/topics/glossary/content/virtual-machine.html