Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

TEMA:

``SISTEMA DE MONITOREO PARA DE REDES COMPUTACIONALES BASADO EN SOFTWARE LIBRE Y HARDWARE DE BAJO COSTO``.

TRABAJO DE GRADUACIÓN PRESENTADO POR:

RAÚL ALFREDO CORNEJO SOSA

RAÚL OSVALDO CRUZ PACHECO

MÓNICA FABIOLA PORTILLO GUARDADO

PARA OPTAR AL GRADO:

TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

ABRIL,2018

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AUTORIDADES ACADÉMICAS

ING. NELSON ZARATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA

VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

OSCAR RODRÍGUEZ

PRESIDENTE

SALVADOR ALCIDES FRANCO

PRIMER VOCAL

OMAR OTONIEL FLORES CORTEZ

SEGUNDO VOCAL

ABRIL 2018

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Ing. Salvador Alcides Franco, Ing. Omar Otoniel Flores, Ing. Oscar Ernesto Rodríguez, a las 12:30m del día Viernes, 1 de Diciembre de dos mil diecisiete.
Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1-Raúl Alfredo Cornejo Sosa Carnet 26-0408-2013
2-Raúl Osvaldo Cruz Pacheco Carnet 26-4999-2014
3-Monica Fabiola Portillo Guardado Carnet 26-4044-2014

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Sistema de monitoreo para redes computacionales basado en Software libre y Hardware de bajo costo"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 1 de Diciembre de dos mil diecisiete.

F._____
PRIMER VOCAL
Ing. Salvador Alcides Franco

F._____
SEGUNDO VOCAL
Ing. Omar Otoniel Flores

F._____
PRESIDENTE
Ing. Oscar Ernesto Rodríguez

Calle Arce No. 1020, San Salvador, El Salvador, C.A. Apdo. Postal 1770
Centro de llamadas: (503) 2275-8888. Fax: (503) 2271-4764
Email: contactanos@utec.edu.sv

Indice

Introducción

Actualmente en la Universidad Tecnológica de El Salvador (UTEC) se tienen muchos laboratorios adecuados para impartir diferentes materias del ámbito informático, pero no se posee una herramienta de monitoreo de redes computacionales la cual permitiría hacer un buen análisis de lo que ocurre en la red, ver por donde está fluyendo la mayor cantidad de datos y así evitar un colapso de las redes existentes en la Universidad. Viendo esta necesidad se ha optado por implementar un sistema de monitoreo de redes basado en software y hardware de bajo costo.

En el presente documento hacemos referencia a lo que es el sistema de monitoreo de redes (Netpi) el cual se implementara en el laboratorio que está ubicado en el edificio Francisco Morazán (Cisco) se dará una explicación detallada de lo que es el monitoreo de redes, todos los detalles de lo que es el sistema netpi y se brindara un manual de uso de este programa para su uso en diferentes laboratorios de la Universidad Tecnológica

Capítulo I

Planteamiento del Problema

1.1 Antecedentes

En la Universidad Tecnológica de El Salvador (UTEC) cuenta con muchos laboratorios para que sus alumnos practiquen y refuercen los conocimientos adquiridos en las clases lo cual cada uno de ellos están comunicados entre sí y como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo de operación.

En toda red de computadoras es necesario tener un sistema de monitoreo basado en el enfoque del Marco Lógico, con lo que se está logrando unificar criterios de monitoreo y recojo de información, usar herramientas tecnológicas que reduzca el tiempo del proceso de recojo, análisis y gestión de información para la generación de informes y reportes y, finalmente, gestionar el conocimiento en función a la sistematización de experiencias identificadas en el proceso.

Esto conlleva a la necesidad de institucionalizar una cultura del monitoreo distinta, dinámica, moderna y con un enorme valor para la toma de decisiones y alto sentido de responsabilidad con el manejo y gestión de información y de recursos económicos

1.2 *Planteamiento del Problema*

En la Universidad Tecnológica de El Salvador (UTEC) está el laboratorio de cisco que cuenta con 21 ordenadores con su respectivo CPU, teclado, mouse.

Este laboratorio es utilizado para impartir diferentes materias las cuales son:

- Tecnología certificada en redes
- Administración de redes
- Certificación de Cisco
- Soporte técnico de redes

También se cuentan con lo que son switches de marca cisco 2960 con una cantidad de 24 ethernet y 2 giga Ethernet y routers de marca cisco 1941 2 puertos seriales 2 puertos gigaetherneth 1 puerto auxiliar 1 puerto de consola 2 y dos puertos USB y 1841 2 puertos fast Ethernet 1 de consola 1 auxiliar y 2 seriales que eso nos hace obtener acceso a red

No obstante, no cuentan con un sistema de monitoreo de red que sirva para analizar el estado de la red que se está utilizando y poder ver si es una red confiable para poder trabajar, pero lamentablemente en el laboratorio de cisco que se encuentra en la universidad tecnológica de el salvador no cuenta con un buen sistema que cumpla esa tarea; que los alumnos y catedráticos puedan resolver más fácilmente cuando la red tiene algún problema

1.3 Objetivos

General

Implementar una herramienta computacional para el monitoreo del rendimiento de redes de computadora como apoyo en las labores verificación y control del uso de estas.

Específicos

- Construir un prototipo de un sistema de monitoreo basado en plataforma de hardware Raspberry Pi y Linux
- Implementar el sistema de monitoreo en la red de datos del Laboratorio de Cisco de la Utec.
- Diseñar un manual para el uso correcto del dispositivo NETPI

.

1.4 Justificación

Netpi es la solución ideal para la Universidad Tecnológica de El Salvador por ser una herramienta muy completa que se puede utilizar para hacer diagramas de topología de la red, análisis de velocidad, LLDP (Link Layer Discovery Protocol) y CDP (Cisco Discovery Protocol), administración remota por VNC (Virtual Network Computing) o SSH (Secure Shell) y hasta hacer un escaneado de todo tráfico en la red.

Con Netpi evitaríamos muchos problemas que se dan muy común mente en la red como los ataques de red, sobrecarga de tráfico de red y muchos otros. Esta herramienta brindara un mejor monitoreo de lo que serían las redes existentes en la Universidad y con esto se tendría una mejor funcionabilidad de dicha red.

Los beneficios al utilizar Netpi serían:

- Administración remota con VNC (Virtual Network Computing) y SSH (Secure Shell).
- Prueba de Ping / Trace / Speed.
- Servidor Syslog para recopilar los resultados de las pruebas y poder analizarlos después.
- CDP (Cisco Discovery Protocol) / LLDP (Link Layer Discovery Protocol) para obtener los resultados obtenidos a través del puerto RJ-45.
- DIA como software para crear diagramas de topologías de redes.
- Wireshark, Wireless Scanner y Zen Map para análisis forense de una red local y pruebas de seguridad y pentesting.

1.5 Limitaciones del Estudio

Delimitación geográfica:

A realizarse en laboratorio de Cisco de la Universidad Tecnológica de El Salvador del departamento de San Salvador, El Salvador C.A.

Delimitación temporal:

Con un tiempo estimado de 6 meses a partir de julio a diciembre.

Capítulo II.

Marco Teórico

2.1 Redes Computacionales

Una red de ordenadores (también llamada red de comunicaciones de datos o red informática) es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un ejemplo es Internet, el cual es una gran red de millones de ordenadores ubicados en distintos puntos del planeta interconectados básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red

en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares

Descripción básica

La comunicación por medio de una red se lleva a cabo en dos diferentes categorías: la Capa física y la capa lógica.

La capa física incluye todos los elementos de los que hace uso un equipo para comunicarse con otros equipos dentro de la red, como, por ejemplo, las tarjetas de red, los cables, las antenas, etc.

La comunicación a través de la capa lógica se rige por normas muy rudimentarias que por sí mismas resultan de escasa utilidad. Sin embargo, haciendo uso de dichas normas es posible construir los denominados protocolos, que son normas de comunicación más complejas (mejor conocidas como de alto nivel), capaces de proporcionar servicios que resultan útiles.

Los protocolos son un concepto muy similar al de los idiomas de las personas. Si dos personas hablan el mismo idioma, es posible comunicarse y transmitir ideas.

La razón más importante (quizá la única) sobre por qué existe diferenciación entre la capa física y la lógica es sencilla: cuando existe una división entre ambas, es posible utilizar un número casi infinito de protocolos distintos, lo que facilita la actualización y migración entre distintas tecnologías.

Componentes básicos de las redes

Para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (hosts) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es la de interconectar los componentes hardware de una red , y por tanto, principalmente, los ordenadores individuales, también denominados hosts, a los equipos que ponen los servicios en la red, los servidores, utilizando el cableado o tecnología inalámbrica soportada por la electrónica de red y unidos por cableado o radiofrecuencia. En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea parte de un ordenador, de un conmutador, de una impresora, etc. y sea de la tecnología que sea (ethernet, Wi-Fi, Bluetooth, etc.)

Software

Sistema operativo de red: Permite la interconexión de ordenadores para acceder a los servicios y recursos. Al igual que un equipo no puede trabajar sin un sistema operativo,

una red de equipos no puede funcionar sin un sistema operativo de red. En muchos casos el sistema operativo de red es parte del sistema operativo de los servidores y de los clientes.

Software de aplicación: En última instancia, todos los elementos se utilizan para que el usuario de cada estación, pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que puede incluir procesadores de texto, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados, correos electrónicos, etc. El software adecuado en el sistema operativo de red elegido y con los protocolos necesarios permiten crear servidores para aquellos servicios que se necesiten.

Hardware

Para lograr el enlace entre los ordenadores y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red (NIC, Network Card Interface), con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras ordenadores, empleando un protocolo para su comunicación y convirtiendo a esos datos a un formato que pueda ser transmitido por el medio (bits, ceros y unos). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (Media Access Control), que consta de 48 bits (6 bytes). Dicho

identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

El trabajo del adaptador de red es el de convertir las señales eléctricas que viajan por el cable (p.e.: red Ethernet) o las ondas de radio (p.e.: red Wi-Fi) en una señal que pueda interpretar el ordenador.

Estos adaptadores son unas tarjetas PCI que se conectan en las ranuras de expansión del ordenador. En el caso de ordenadores portátiles, estas tarjetas vienen en formato PCMCIA o similares. En los ordenadores del siglo XXI, tanto de sobremesa como portátiles, estas tarjetas ya vienen integradas en la placa base.

Adaptador de red es el nombre genérico que reciben los dispositivos encargados de realizar dicha conversión. Esto significa que estos adaptadores pueden ser tanto Ethernet, como wireless, así como de otros tipos como fibra óptica, coaxial, etc. También las velocidades disponibles varían según el tipo de adaptador; estas pueden ser, en Ethernet, de 10, 100, 1000 Mbps o 10000, y en los inalámbricos, principalmente, de 11, 54, 300 Mbps.

Almacenamiento en red

En las redes medianas y grandes el almacenamiento de datos principal no se produce en los propios servidores sino que se utilizan dispositivos externos, conocidos como disk arrays (matrices de discos) interconectados, normalmente por redes tipo SAN o Network-

Attached Storage (NAS). Estos medios permiten centralizar la información, una mejor gestión del espacio, sistemas redundantes y de alta disponibilidad.

Los medios de copia de seguridad suelen incluirse en la misma red donde se alojan los medios de almacenamiento mencionados más arriba, de esta forma el traslado de datos entre ambos, tanto al hacer la copia como las posibles restauraciones, se producen dentro de esta red sin afectar al tráfico de los clientes con los servidores o entre ellos.

Dispositivos de red

Los equipos informáticos descritos necesitan de una determinada tecnología que forme la red en cuestión. Según las necesidades se deben seleccionar los elementos adecuados para poder completar el sistema. Por ejemplo, si queremos unir los equipos de una oficina entre ellos debemos conectarlos por medio de un conmutador o un concentrador, si además hay un varios portátiles con tarjetas de red Wi-Fi debemos conectar un punto de acceso inalámbrico para que recoja sus señales y pueda enviarles las que les correspondan, a su vez el punto de acceso estará conectado al conmutador por un cable. Si todos ellos deben disponer de acceso a Internet, se interconectarán por medio de un router, que podría ser ADSL, ethernet sobre fibra óptica, broadband, etc.

Los elementos de la electrónica de red más habituales son:

- Conmutador de red (switch),
- Enrutador (router),
- Puente de red (bridge),
- Puente de red y enrutador (brouter),

- Punto de acceso inalámbrico (Wireless Access Point, WAP).

Protocolos de redes

Existen diversos protocolos, estándares y modelos que determinan el funcionamiento general de las redes. Destacan el modelo OSI y el TCP/IP. Cada modelo estructura el funcionamiento de una red de manera distinta. El modelo OSI cuenta con siete capas muy definidas y con funciones diferenciadas y el TCP/IP con cuatro capas diferenciadas pero que combinan las funciones existentes en las siete capas del modelo OSI. Los protocolos están repartidos por las diferentes capas pero no están definidos como parte del modelo en sí sino como entidades diferentes de normativas internacionales, de modo que el modelo OSI no puede ser considerado una arquitectura de red

Modelo OSI

El modelo OSI (Open Systems Interconnection) fue creado por la ISO y se encarga de la conexión entre sistemas abiertos, esto es, sistemas abiertos a la comunicación con otros sistemas. Los principios en los que basó su creación eran: una mayor definición de las funciones de cada capa, evitar agrupar funciones diferentes en la misma capa y una mayor simplificación en el funcionamiento del modelo en general.

Este modelo divide las funciones de red en siete capas diferenciadas:

#	Capas	Unidad de intercambio
7.	Capa de aplicación	APDU
6.	Capa de presentación	PPDU
5.	Capa de sesión	SPDU
4.	Capa de transporte	TPDU
3.	Capa de red	Paquete de red
2.	Capa de enlace de datos	Trama de red (Marco / Trama)
1.	Capa física	Bit

2.1.1 Modelo OSI

Modelo TCP/IP

Este modelo es el implantado actualmente a nivel mundial: fue utilizado primeramente en ARPANET y es utilizado actualmente a nivel global en Internet y redes locales. Su nombre deriva de la unión de los nombres de los dos principales protocolos que lo conforman: TCP en la capa de transporte e IP en la capa de red. Se compone de cuatro capas:

#	Capas	Unidad de intercambio
4.	Capa de aplicación	*no definido*
3.	Capa de transporte	Paquete de red
2.	Capa de red (red / interred)	*no definido* (Datagrama)
1.	Capa de enlace de datos (enlace / nodo a red)	*??*

2.1.2 Modelo TCP/IP

Existen otros estándares, más concretos, que definen el modo de funcionamiento de diversas tecnologías de transmisión de datos. La siguiente lista no es completa, solo muestra algunos ejemplos:

Tecnología	Estándar	Año de primera publicación	Otros detalles
Ethernet	IEEE 802.3	1983	-
Token Ring	IEEE 802.5	1970[6]	-
WLAN	IEEE 802.11	1997[7]	-
Bluetooth	IEEE 802.15	2002[8]	-
FDDI	ISO 9314-x	1987	Reúne un conjunto de estándares.
PPP	RFC 1661	1994[9]	-

Tipos de redes

RED WAN

Una red de área amplia, o RED WAN, (Wide Área Network en inglés), es una red de computadoras que une varias redes locales, (LAN), aunque sus miembros no están todos en una misma ubicación física. Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de Internet (ISP) para proveer conexión a sus clientes. Hoy en día, internet brinda conexiones de alta velocidad, de manera que un alto porcentaje de las redes WAN se basan en ese medio,

reduciendo la necesidad de redes privadas WAN, mientras que las virtuales que utilizan cifrado y otras técnicas para generar una red dedicada sobre comunicaciones en internet, aumentan continuamente.

RED LAN

Una RED LAN significa Red de área local. Es un grupo de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña a través de una red, generalmente con la misma tecnología (la más utilizada es Ethernet). Una red de área local es una red en su versión más simple. La velocidad de transferencia de datos en una red de área local puede alcanzar hasta 10 Mbps (por ejemplo, en una red Ethernet) y 1 Gbps (por ejemplo, en FDDI o Gigabit Ethernet). Una red de área local puede contener 100, o incluso 1000, usuarios.

RED MAN

Una red de área de metropolitana MAN, siglas del inglés Metropolitan Area Network) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50 ms), gran estabilidad y la carencia de interferencias radioeléctricas,

las redes MAN BUCLE, ofrecen velocidades de 10 Mbit/s ó 20 Mbit/s, sobre pares de cobre y 100 Mbit/s, 1 Gbit/s y 10 Gbit/s mediante fibra óptica.

RED WLAN

Una Red de Área Local Inalámbrica, más conocida como WLAN, es básicamente un sistema de transferencia y comunicaciones de datos el cual no requiere que las computadoras que la componen tengan que estar cableadas entre sí, ya que todo el tráfico de datos entre las mismas se realiza a través de ondas de radio. A pesar de que son menos seguras que su contrapartida cableada, ofrecen una amplia variedad de ventajas, y es por ello que su implementación crece día a día en todos los ámbitos. Sin embargo, la característica más destacada de este tipo de red es el ahorro en el tendido de los cables para la interconexión de las PC.

RED WMAN

La RED WMAN en términos muy básicos o Red Metropolitana Inalámbrica por su traducción al español, es una versión inalámbrica de MAN, la cual puede llegar a tener un rango de alcance de decenas de kilómetros. Esta tecnología utiliza técnicas basadas en el estándar de comunicaciones WiMAX (Worldwide Interoperability for Microwave Access). Una de sus principales ventajas es notable en los costos, ya que se elimina el cableado Ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

RED PAN

Una Red PAN, abreviatura del inglés Personal Area Network, y cuya traducción al español significa Red de Área Personal, es básicamente una red integrada por todos los dispositivos en el entorno local y cercano de su usuario, es decir que la componen todos los aparatos que están cerca del mismo. La principal característica de este tipo de red que le permite al usuario establecer una comunicación con sus dispositivos de forma sencilla, práctica y veloz. Estas tecnologías permitieron una altísima transferencia de datos dentro de las soluciones de sistemas o redes inalámbricas. La ventaja de las comunicaciones inalámbricas es que con la terminal la persona se puede mover por toda el área de cobertura, lo que no ocurre con las redes de comunicaciones fijas.

RED SAN

Una red de área de almacenamiento, en inglés Storage Area Network (SAN), es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

• Una red de alta velocidad de canal de fibra o iSCSI.

• Un equipo de interconexión dedicado (conmutadores, puentes, etc).

• Elementos de almacenamiento de red (discos duros).

Una SAN es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía. Además de contar con interfaces de red tradicionales, los equipos con acceso a la SAN tienen una interfaz de red específica que se conecta a la

SAN. El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza.

2.2 Monitoreo de Redes

El término Monitoreo de red (Monitorización de red) describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Monitorización de red

Mientras que un sistema de detección de intrusos monitoriza una red por amenazas del exterior (externas a la red), un sistema de monitorización de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u tros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web, software de monitorización que puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (Protocolo de Transferencia de Correo Simple), para luego ser retirados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3 (Protocolo Post Office).

Comúnmente, los datos evaluados son tiempo de respuesta y disponibilidad (o uptime), aunque estadísticas tales como consistencia y fiabilidad han ganado popularidad. La generalizada instalación de dispositivos de optimización para redes de área extensa tiene un efecto adverso en la mayoría del software de monitorización, especialmente al intentar medir el tiempo de respuesta de punto a punto de manera precisa, dado el límite visibilidad de ida y vuelta.

Las fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, el tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitorización. Estas acciones pueden variar: una alarma puede ser enviada al administrador, ejecución automática de mecanismos de controles de fallas, etcétera.
Monitorizar la eficiencia del estado del enlace de subida se denomina Medición de tráfico de red.

Ejemplos de Aplicaciones utilizadas

TCPDump

Tcpdump es una excelente herramienta que nos permite monitorizar a través de la consola de Linux todos los paquetes que atraviesen la interfaz indicada. A su vez, los múltiples filtros, parámetro y opciones que tcpdump nos ofrece, nos permite infinidades de combinaciones, al punto de poder monitorizar todo el tráfico completo que pase por la interfaz, como el tráfico que ingrese de una ip, un host o una página especifica, podemos

solicitar el tráfico de un puerto especifico o pedirle a esta magnífica herramienta que nos muestre todos los paquetes cuyo destino sea una dirección MAC específica.

Wireshark.

Wireshark es un sniffer que te permite capturar tramas y paquetes que pasan a través de una interfaz de red. Cuenta con todas las características estándar de un analizador de protocolos. Posee una interfaz gráfica fácil de manejar, permite ver todo el tráfico de una red (usualmente en una red Ethernet, aunque es compatible con algunas otras).

Hyperic

Aplicación open source que nos permite administrar infraestructuras virtuales, físicas y nube este programa auto-detecta muchas tecnologías.Cuenta con dos versiones una open source y una comercial Algunas de las características de esta aplicación son:

Optimizado para ambientes virtuales que integran vCenter y vSphere

Construido para funcionar en 75 componentes comunes tales como: base de datos, dispositivos de red, servidores de red, etc.

Detecta automáticamente todos los componentes de cualquier aplicación virtualizada

Nagios.

Nagios es un sistema de monitorización que permite a cualquier empresa identificar y resolver cualquier error critico antes de que afecte los procesos de negocio. Esta aplicación monitoriza toda infraestructura de la información para asegurarse de que sistemas, aplicaciones, servicios y procesos de negocios estén funcionando correctamente. En el

caso de un error la aplicación se encarga de alertar al grupo técnico para que rápidamente resuelvan el problema sin que afecte a los usuarios finales.

Pandora FMS

Pandora FMS es un software de monitorización que otorga a cualquier empresa la posibilidad de monitorizar en un mismo panel redes, sistemas, servidores, aplicaciones y procesos de negocio. Debido a la posibilidad de monitorización bottom-up de Pandora FMS, el panel de monitorización permite personalizar los accesos por rol para que cada rol vea la información que le interesa.

Puntos a tener en cuenta a la hora de evaluar un monitor de red

A continuación se muestran las principales características que debe tenerse en cuenta a la hora de evaluar un software de monitorización de red:3

- Comunicación de las alertas.
- Integraciones con servidores externos.
- Usabilidad y presentación de los datos en el panel.
- Flexibilidad a la hora de adaptarse a herramientas o software particulares.
- API de acceso desde sistemas externos.
- Detección de dispositivos de forma automática.
- Integraciones con Bases de Datos
- Multidispositivo
- Escalado
- Soporte del mayor número de protocolos de adquisición de datos posible

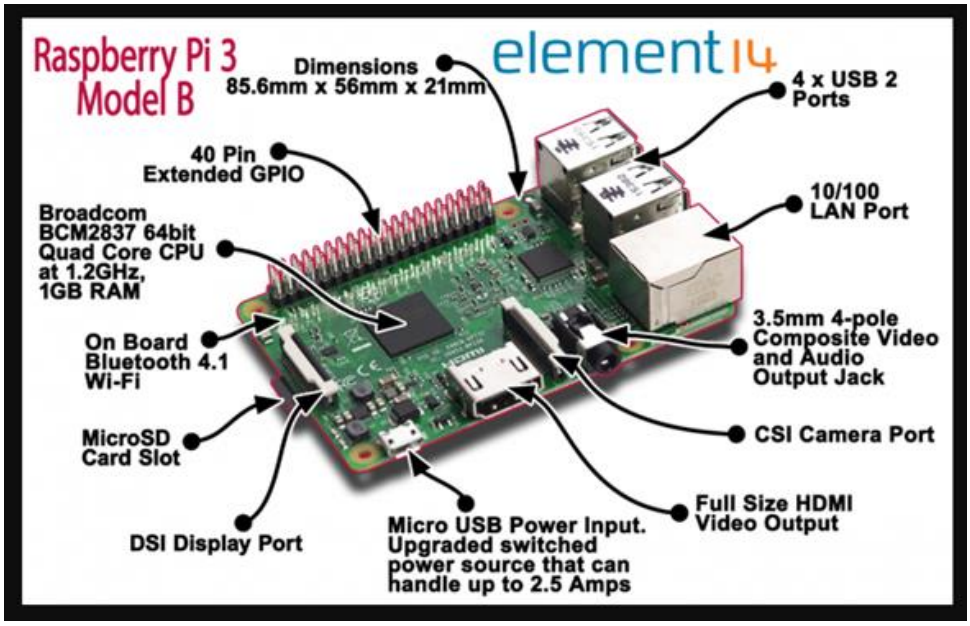
- Seguridad
- Integración con máquinas virtuales
- Integraciones hardware
- Control remoto
- Inventario de Hardware y Software
- Gelocalización
- Monitorización de la nube

2.3 Plataforma Computacional Raspberry PI.

El Raspberry Pi es una serie de pequeñas computadoras de un solo tablero desarrolladas en el Reino Unido por la Fundación Raspberry Pi para promover la enseñanza de la informática básica en las escuelas y en los países en desarrollo. El modelo original llegó a ser mucho más popular que anticipado, vendiendo fuera de su mercado de blanco para los usos tales como robótica .

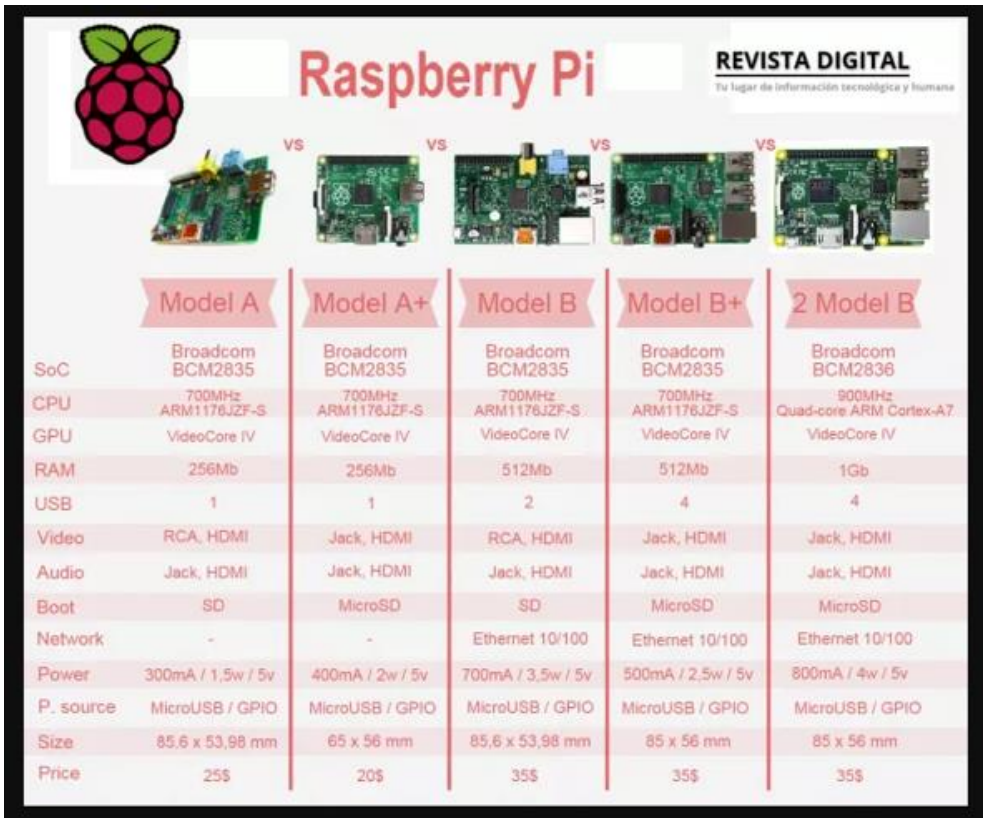
Periféricos (incluidos teclados , ratones y estuches) no se incluyen con la frambuesa Pi. Sin embargo, algunos accesorios han sido incluidos en varios paquetes oficiales y no oficiales

El hardware de Raspberry Pi ha evolucionado a través de varias versiones que presentan variaciones en la capacidad de memoria y soporte de dispositivos periféricos.



Raspberrypi función de bloque v01.svg

Este diagrama de bloques representa los modelos A, B, A + y B +. Los modelos A, A + y Pi Zero carecen de los componentes de concentrador Ethernet y USB . El adaptador Ethernet está internamente conectado a un puerto USB adicional. En el modelo A, A + y el Pi Zero, el puerto USB se conecta directamente al sistema en un chip (SoC). En el Pi 1 Modelo B + y modelos posteriores el chip USB / Ethernet contiene un concentrador USB de cinco puntos, de los cuales hay cuatro puertos disponibles, mientras que el Pi 1 Modelo B sólo proporciona dos. En el Pi Zero, el puerto USB también está conectado directamente al SoC, pero usa un puerto micro USB (OTG).

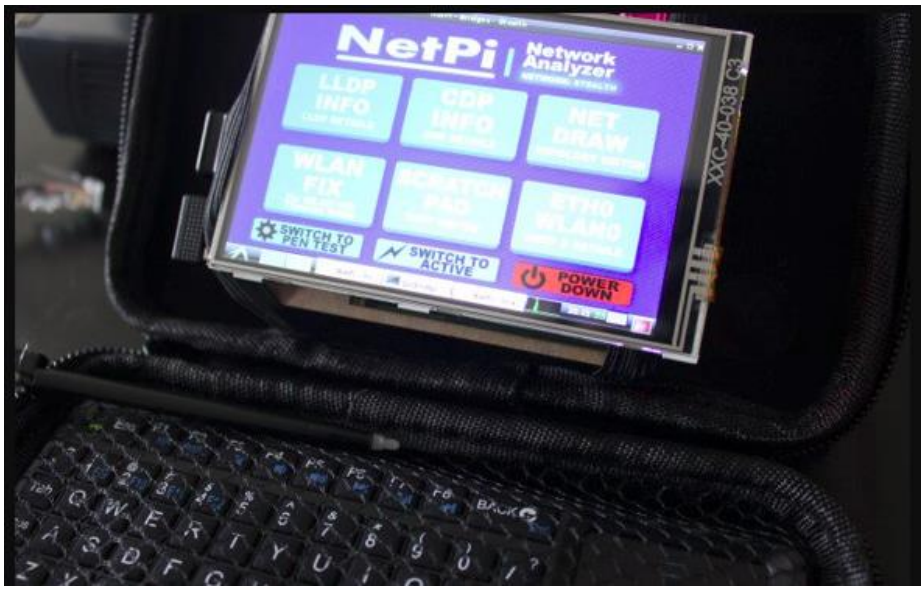


	Model A	Model A+	Model B	Model B+	2 Model B
SoC	Broadcom BCM2835	Broadcom BCM2835	Broadcom BCM2835	Broadcom BCM2835	Broadcom BCM2836
CPU	700MHz ARM1176JZF-S	700MHz ARM1176JZF-S	700MHz ARM1176JZF-S	700MHz ARM1176JZF-S	900MHz Quad-core ARM Cortex-A7
GPU	VideoCore IV	VideoCore IV	VideoCore IV	VideoCore IV	VideoCore IV
RAM	256Mb	256Mb	512Mb	512Mb	1Gb
USB	1	1	2	4	4
Video	RCA, HDMI	Jack, HDMI	RCA, HDMI	Jack, HDMI	Jack, HDMI
Audio	Jack, HDMI	Jack, HDMI	Jack, HDMI	Jack, HDMI	Jack, HDMI
Boot	SD	MicroSD	SD	MicroSD	MicroSD
Network	-	-	Ethernet 10/100	Ethernet 10/100	Ethernet 10/100
Power	300mA / 1,5w / 5v	400mA / 2w / 5v	700mA / 3,5w / 5v	500mA / 2,5w / 5v	800mA / 4w / 5v
P. source	MicroUSB / GPIO	MicroUSB / GPIO	MicroUSB / GPIO	MicroUSB / GPIO	MicroUSB / GPIO
Size	85,6 x 53,98 mm	65 x 56 mm	85,6 x 53,98 mm	85 x 56 mm	85 x 56 mm
Price	25$	20$	35$	35$	35$

2.4 Sistema de Monitoreo: NETPI

Es un pequeño proyecto en el que se ha conseguido crear un completo dispositivo de análisis de redes alternativo a las principales herramientas comerciales de más de 1.500 dólares aunque utilizando sólo software libre y hardware económico como un Raspberry Pi. Estos dispositivos de análisis de red son utilizados para comprobar el estado de una red (generalmente local y de cable, para la fibra óptica hay que utilizar otros dispositivos), así como para poder encontrar diferentes problemas que pueda haber en ella (cuellos de botella, ordenadores que envían paquetes masivos, fallos de seguridad, etc)

Este pequeño sistema operativo para Raspberry Pi, que además es de código abierto, nos va a permitir disponer de una completa herramienta de análisis de red de bajo coste y totalmente funciona, tanto a nivel personal como profesional. NetPi aún sigue en desarrollo implementando nuevas funciones, sin embargo, por el momento es posible disponer de las siguientes herramientas y funciones:



✓ *Netpi*

- CDP / LLDP para obtener los resultados obtenidos a través del puerto RJ-45.
- DIA como software para crear diagramas de topologías de redes.
- Test de Ping, ruta (tracert) y velocidad para analizar el rendimiento de la red.
- Wireshark, Wireless Scanner y Zen Map para análisis forense de una red local y pruebas de seguridad y pentesting.

- VNC y SSH para control remoto del dispositivo.
- Servidor Syslog para recopilar los resultados de las pruebas y poder analizarlos después.

Ventajas

- Soporte para protocolos de descubrimiento de redes CDP y LLDP.
- Software de diagrama DIA para construir topologías de red.
- Generación de informes de estadísticas de Ping, Trace y test de velocidad.
- Posee un kit de herramientas de red constituido por: Wireshark, escaner Wifi y ZenMap.
- Administración remota via VNC y SSH.
- Servidor Syslog, para recoger mensajes Syslog de los dispositivos de red para un posterior análisis.

En el proyecto se describe un hardware para construir este analizador de redes

- Raspberry Pi B+.
- MicroSD HC 16 GB Samsung, No necesariamente este modelo de tarjeta, y el tamaño puede variar, pero debe ser soportado por la Raspberry Pi B+. Se han detectado problemas de compatibilidad con otras MicroSD en Debian (Wheezy).
- JBtek 4in LCD Touch Panel, Una pantalla táctil para visualizar y manejar los datos. Tabien se pueden utilizar dispositivos HDMI y optar por una pantalla que no sea táctil en función de su uso.

- Edimax USB WiFi, Puede ser usado para la gestión remota mediante interfaz inalámbrica, muy práctico para consultar los archivos de registro
- Cargador USB, Para alimentar el dispositivo. En general, cualquier bloque de alimentación USB debería funcionar.
- Teclado FAVI Micro USB, Este teclado es perfecto por su reducido tamaño, para introduccir algún comando. La configuración de NetPI es mas practica realizara por consola.
- Funda HDE 5.2in, para facilitar su transporte y mantener el teclado, la pantalla y la Raspberry Pi todo junto.

Capítulo III.

Metodología

3.1 Enfoque Metodológico

La investigación fue desarrollada usando el método experimental, el cual es “un método empleado en caso donde la investigación tiene por objeto el provocar determinados fenómenos que no se presentan usualmente en la naturaleza y cuyo conocimiento puede ser interesante o importante en el avance de la ciencia y la tecnología”

Específicamente en esta investigación y a partir de la revisión teorica, se seleccionaron diversas herramientas y componentes electrónicos para el diseño de un prototipo electrónico que se apegara a los objetivos del estudio.

3.1.1 Tipo de estudio

Este estudio fue del tipo de investigación aplicada tecnológicamente o investigación técnica ste tipo de investigación “tiende la resolución de problemas o al desarrollo de ideas a corto o mediano plazo dirigidas a conseguir innovaciones mejoras en procesos o productos incrementos de calidad y/o productividad, etc

3.2 Implementación de Sistema de Monitoreo de Red

Mientras que un sistema de detección de intrusos monitoriza una red por amenazas del exterior (externas a la red), un sistema de monitorización de red busca problemas causados

por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web, software de monitorización que puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (Protocolo de Transferencia de Correo Simple), para luego ser retirados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3 (Protocolo Post Office).

3.2.1 ¿Que es el sistema de monitoreo?

El uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Cuando se da un determinado servicio en este caso a una Universidad, las redes son uno de los elementos más importantes a tener en cuenta. Si la red deja de funcionar por el motivo que sea, y no llegan a transmitirse los datos necesarios, si la Universidad deja de prestar servicio a sus alumnos durante el tiempo que dure la caída. Todo esto puede causar grandes problemas,

Por estas razones, un sistema de monitoreo de red, puede marcar la diferencia Elegir una herramienta de monitoreo de red adecuada, nos va a ayudar a detectar posibles problemas

antes de que se provoque un colapso o una caída de las redes. Para poder centrarnos y saber qué es lo que debes tener en cuenta para la monitorización de red, es importante saber diferenciar entre el monitoreo de red y la gestión de red.

El monitoreo de red te va a permitir analizar y ver el estado de tus redes a un nivel básico. Mientras que la gestión de red, va más allá, no sólo permite tomar acciones para la gestión, sino que te va a permitir tomar acciones para paliar los problemas de nuestras redes, dando una visión global de todos nuestros sistemas.

3.2.2 Sistema NETPI

Las grandes ventajas de una Raspberry Pi como arquitectura hardware son: su reducido tamaño, su alta capacidad de proceso en relación a su tamaño y su escaso costo. Estas son las características ideales para usar este hardware para utilidades de redes y seguridad informática.

ScoutBot una herramienta de reconocimiento de red que automatiza completamente el proceso de recolección de datos. es posible pre-configurar los parámetros de exploración antes de conectarse a la red, y una vez conectado, esperar a que finalice la exploración para recoger los resultados del análisis. Estos resultados pueden ser recuperados mediante la conexión al servidor FTP interno de ScoutBot

es una aplicación ideal para realizar test de penetración de manera que la recopilación de información en la red se haga de forma fácil y discreta. Construido para Raspberry Pi

3.3 NETPI

NetPi es un pequeño proyecto en el que se ha conseguido crear un completo dispositivo de análisis de redes alternativo a las principales herramientas comerciales de más de 1.500 dólares aunque utilizando sólo software libre y hardware económico como un Raspberry Pi.

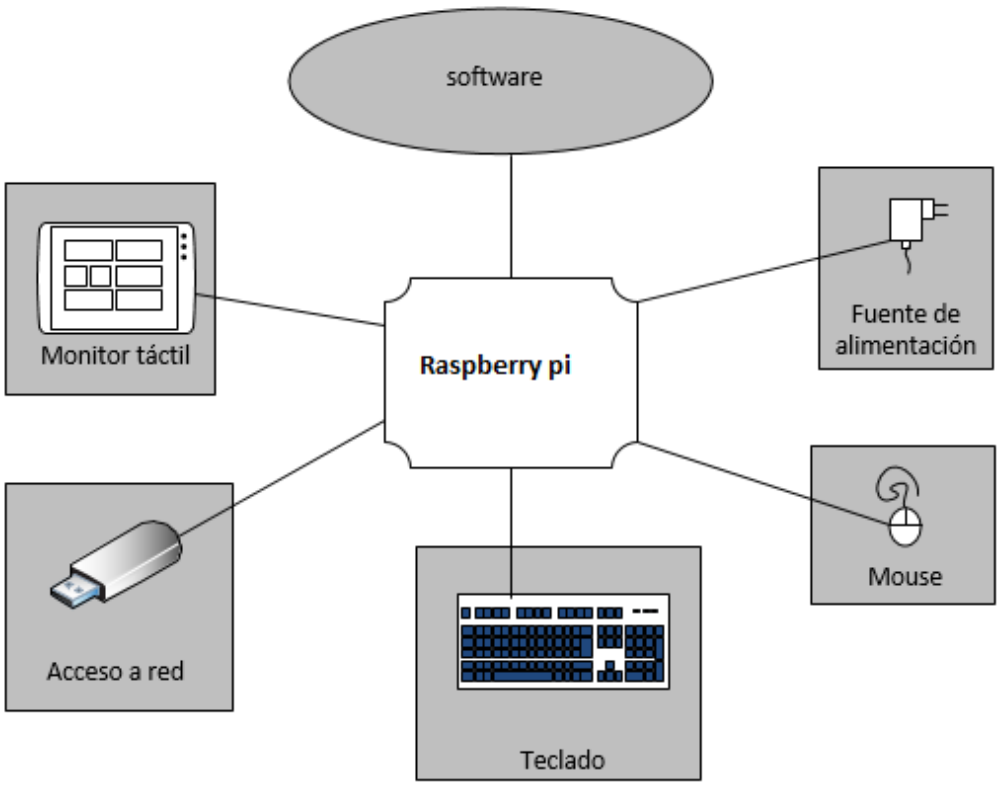
3.3.1 Ventajas / usos

- Un inventario completo de la red.
- Detección de dispositivos con SNMP.
- Servidores DHCP y alcance.
- Dirección IP exterior.
- Capturas de paquetes.
- Informe filtrado de tráfico hacia la WWW.
- Identifica el ISP utilizado por la red.
- Realiza un traceroute hacia el exterior.
- Chequea el estado del filtrado de salida.
- Identifica los protocolos de enrutamiento dinámico.
- se puede configurar en tres modos diferentes de trabajo:
- Realizar Scan:

  Realiza un escaneo rápido de la red e intenta enumerar cualquier dispositivo conectado a la red.

Realizar captura de paquetes:
ScoutBot también tiene la capacidad de realizar una captura de paquetes de la red.
Recuperar resultados del escaneo:
Una vez terminada la exploración para recuperar los resultados del análisis, simplemente eligiendo este modo en la configuración, arranca un servidor FTP en una dirección IP predeterminada.

3.3.2 Estructura de NETPI



3.3.3 Componentes de NETPI

Raspberry Pi es un computador de placa reducida, computador de placa única o computador de placa simple (SBC) de bajo costo desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.

Aunque no se indica expresamente si es hardware libre o con derechos de marca, en su web oficial explican que disponen de contratos de distribución y venta con dos empresas, pero al mismo tiempo cualquiera puede convertirse en revendedor o redistribuidor de las tarjetas RaspBerry Pi, por lo que se entiende que es un producto con propiedad registrada, manteniendo el control de la plataforma, pero permitiendo su uso libre tanto a nivel educativo como particular.

En cambio el software sí es open source, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian, aunque permite usar otros sistemas operativos, incluido una versión de Windows 10. En todas sus versiones incluye un procesador Broadcom, una memoria RAM, una GPU, puertos USB, HDMI, Ethernet (El primer modelo no lo tenía), 40 pines GPIO y un conector para cámara. Ninguna de sus ediciones incluye memoria, siendo esta en su primera versión una tarjeta SD y en ediciones posteriores una tarjeta MicroSD

Una pantalla táctil (en inglés, touch screen) es una pantalla que mediante un toque directo sobre su superficie permite la entrada de datos1y órdenes al dispositivo, y a su vez muestra los resultados introducidos previamente; actuando como periférico de entrada y salida de datos, así como emulador de datos interinos erróneos al no tocarse efectivamente. Este contacto también se puede realizar por medio de un lápiz óptico u otras herramientas similares. Actualmente hay pantallas táctiles que pueden instalarse sobre una pantalla

normal, de cualquier tipo o denominación (LCD, monitores y televisores CRT, plasma, etc.).

En electrónica, la fuente de alimentación o fuente de potencia es el dispositivo que convierte la corriente alterna (CA), en una o varias corrientes continuas (CC), que alimentan los distintos circuitos del aparato electrónico al que se conecta (computadora, televisor, impresora, router, etc.)

Módem USB otra forma de conectarse a internet es por medio de un módem USB. Este tipo de conexión también es inalámbrica y te permite acceder a internet desde cualquier lugar.

En informática, un teclado es un dispositivo o periférico de entrada, en parte inspirado en el teclado de las máquinas de escribir, que utiliza una disposición de botones o teclas, para que actúen como palancasmecánicas o interruptores electrónicos que envían información a la computadora.

El ratón o mouse (en inglés, pronunciado [maʊs]) es un dispositivo apuntador utilizado para facilitar el manejo de un entorno gráfico en una computadora. Generalmente está fabricado en plástico, y se utiliza con una de las manos. Detecta su movimiento relativo en dos dimensionespor la superficie plana en la que se apoya, reflejándose habitualmente a través de un puntero, cursor o flecha en el monitor. El ratón se puede conectar de forma alámbrica (puertos PS/2 y USB) o inalámbricamente (comunicación

inalámbrica o wireless, por medio de un adaptador USB se conecta a la computadora y esta manda la señal al ratón, también pueden ser por medio de conectividad bluetooth o infrarrojo).

Se conoce como software1 al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

3.3.4 Implementación de NETPI

Este dispositivo de análisis de red es utilizado para comprobar el estado de una red (generalmente local y de cable, para la fibra óptica hay que utilizar otros dispositivos), así como para poder encontrar diferentes problemas que pueda haber en ella (cuellos de botella, ordenadores que envían paquetes masivos, fallos de seguridad, etc).

Capítulo IV

Análisis de Resultado

Durante las pruebas realizadas en cisco se tuvieron resultados positivos en la red demostrando que este sistema es el más apropiado para una monitorización.

En la red de cisco se hicieron pruebas de ping pruebas de velocidad pruebas de puertos las cuales salieron con éxito y pudimos observar todas las maquinas conectadas que existen en la red con la herramienta LLDP

Así queda demostrado tanto la efectividad del sistema Netpi para una buena monitorización como el excelente desempeño de la red de cisco.

4.1 Ensamblaje de Raspberry

Para el ensamblaje de raspberry necesitamos las siguientes piezas que se muestran en la imagen siguiente:

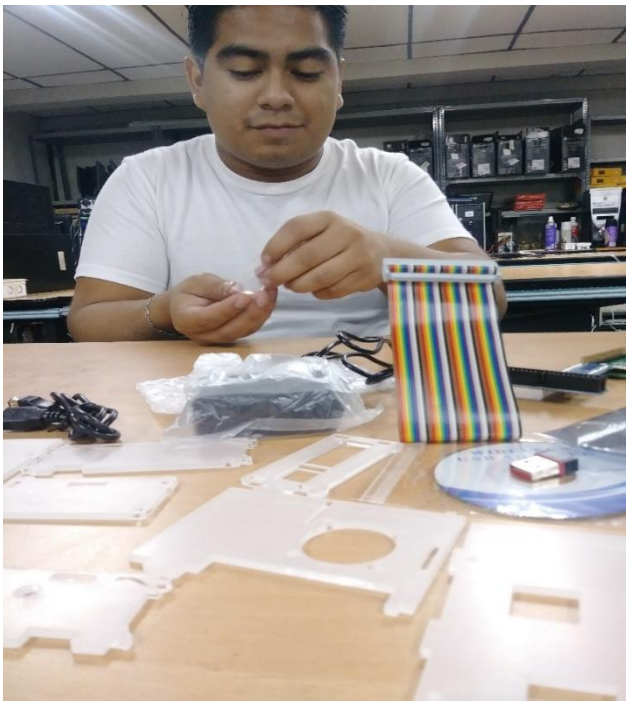
- ✓ *Piezas*

- ✓ *Piezas*

En las siguientes imágenes observamos su ensamblaje

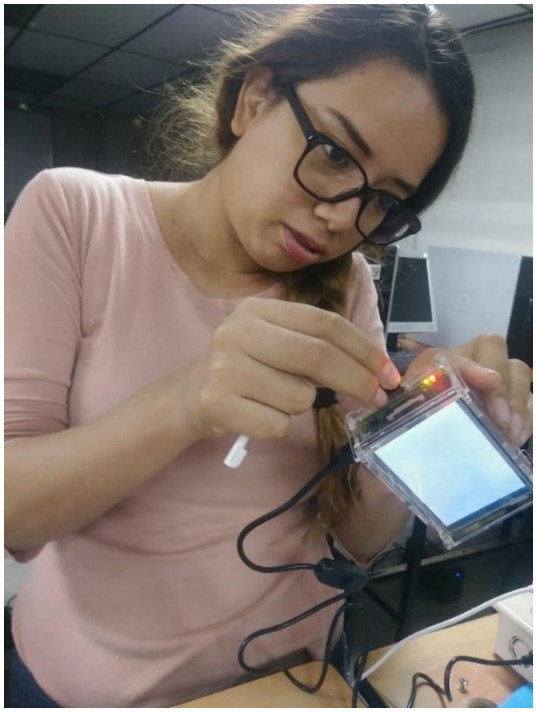
- ✓ *Ensamblaje*

- ✓ *Ensamblaje*



- ✓ *Ensamblaje*

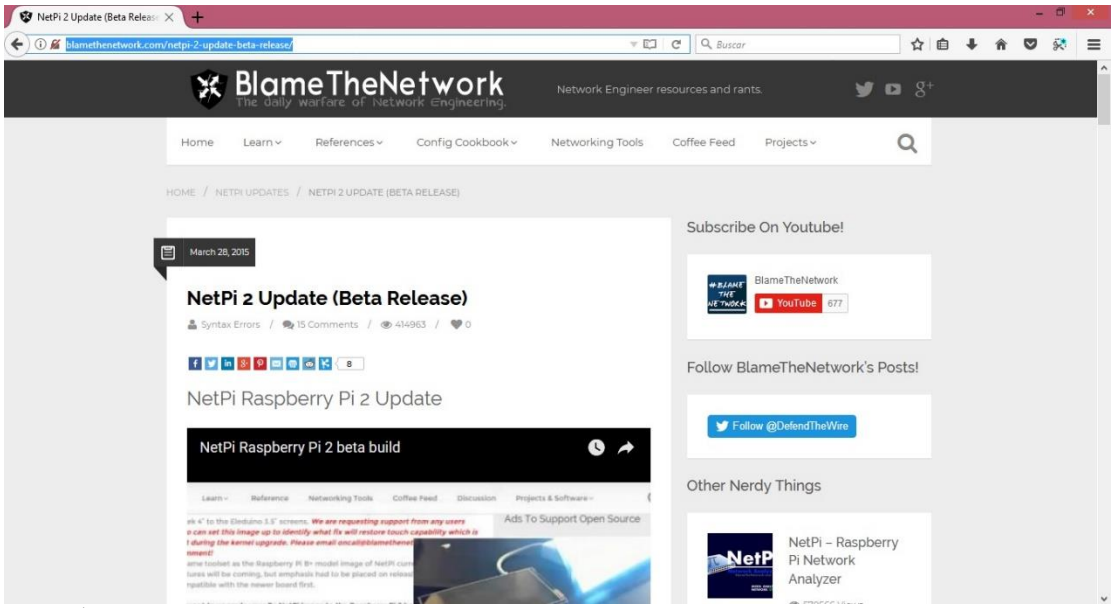
- ✓ *Ensamblaje*



- ✓ *Ensamblaje*

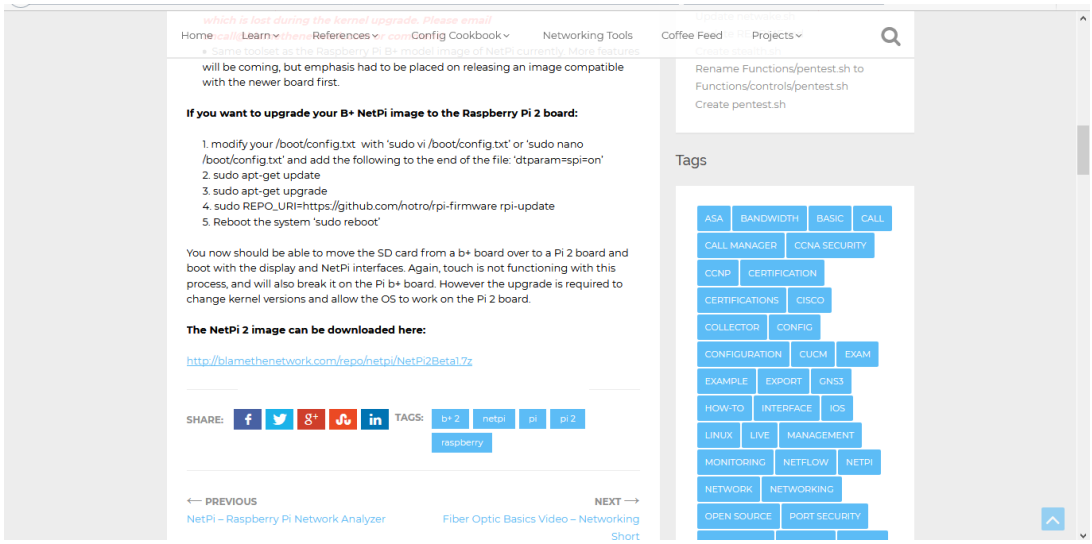
4.2 Instalación del Sistema NETPI para el Monitoreo de Redes.

Primer nos vamos a la página siguiente: http://blamethenetwork.com/netpi-2-update-beta-release/

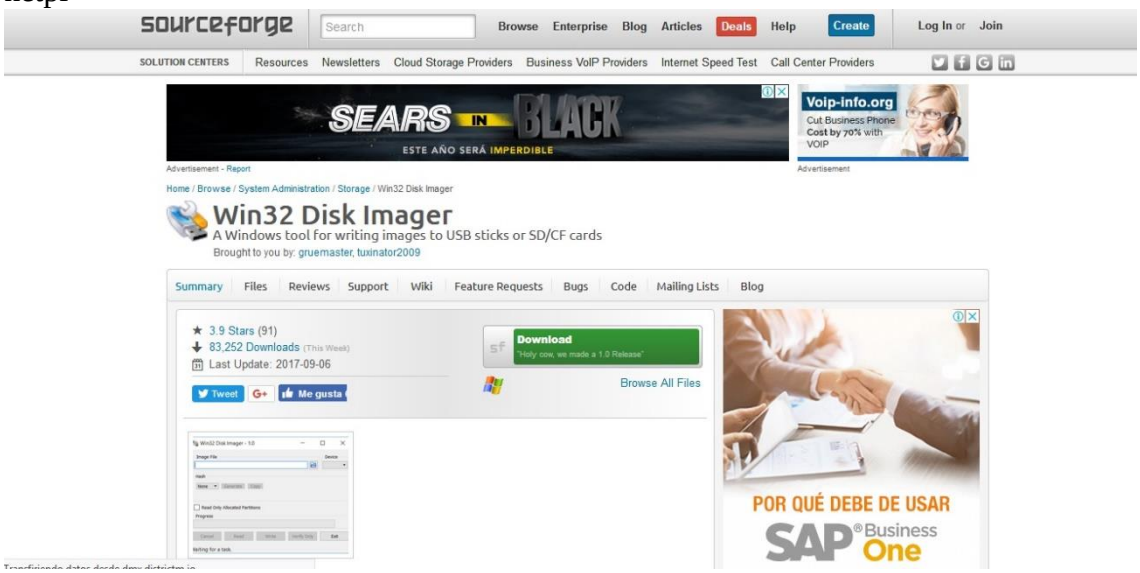


✓ *Instalación*

Nos vamos hasta el final de la página y nos encontraremos un enlace el cual nos permitirá descargar el archivo el cual contiene el sistema netpi para nuestra Raspberry

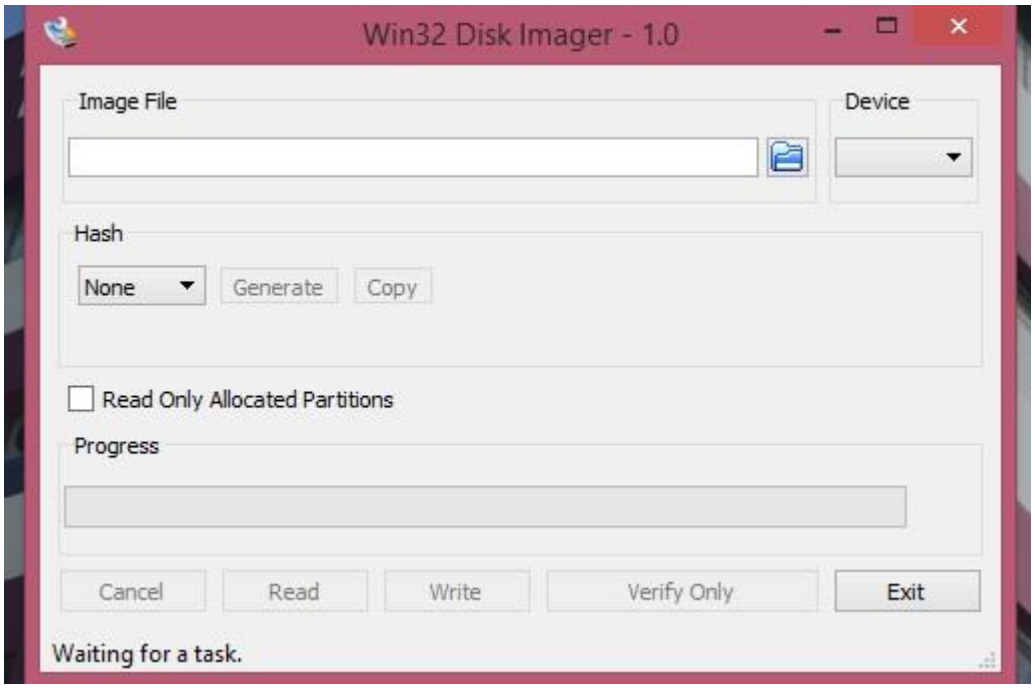


También descargaremos un programa llamado Win32DiskImager para grabar el sistema netpi



- ✓ *Instalación*

Ya con estos 2 archivos descargados abrimos Win32DiskImager para poder grabar el sistema netpi en nuestra micro sd

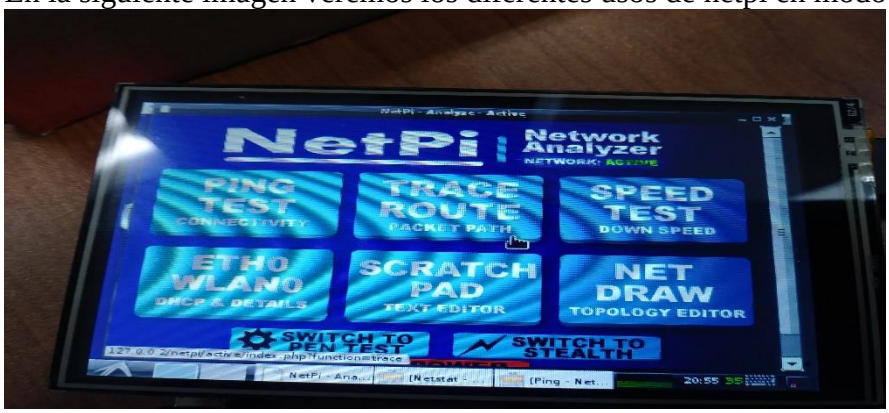


Después de grabar el sistema colocamos la memoria micro sd en nuestra raspberry para que comience la instalación

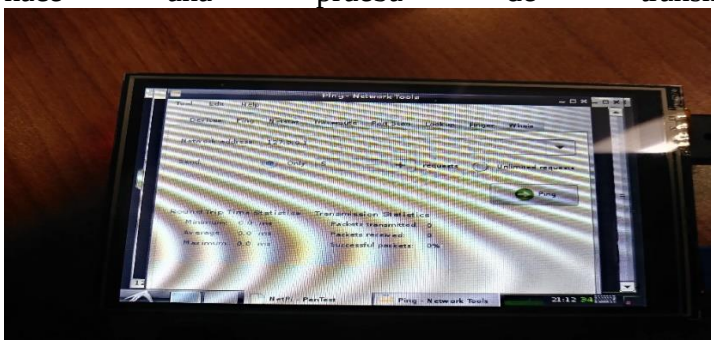
Después de esto ya estará lista nuestra raspberry para utilizar netpi para monitorear redes

4.3 Características de NETPI

En la siguiente imagen veremos los diferentes usos de netpi en modo analyzer:

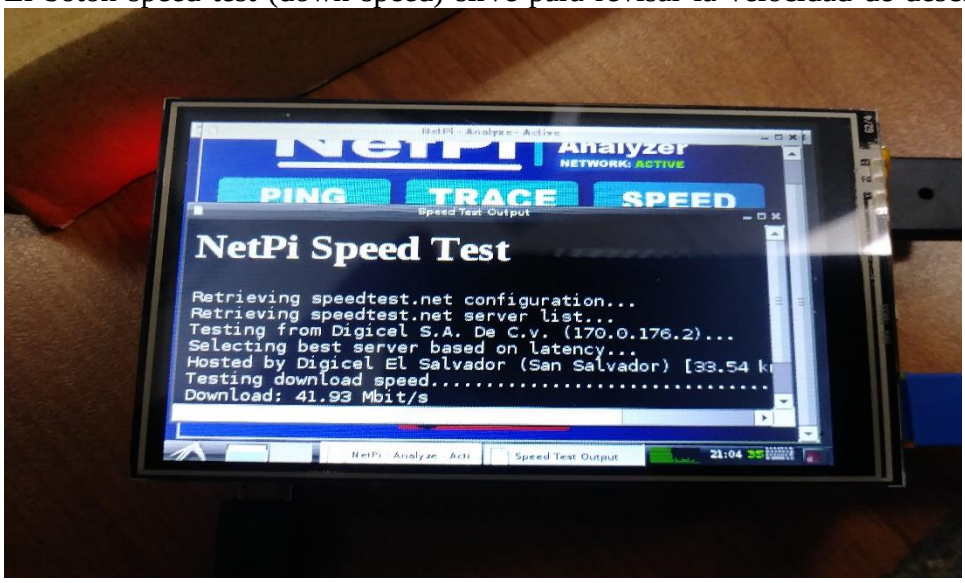


Como podemos el primer botón sirve para hacer un test de ping (conectividad) el cual hace una prueba de transmisión de packetes.

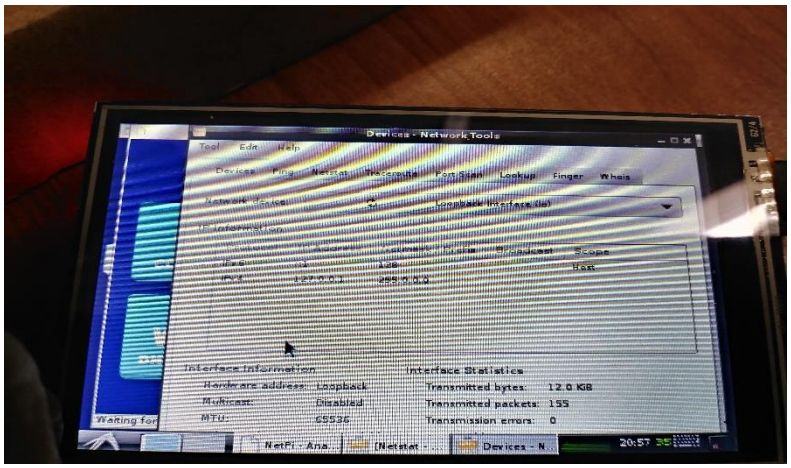


El botón trace router (packet patch) es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red).

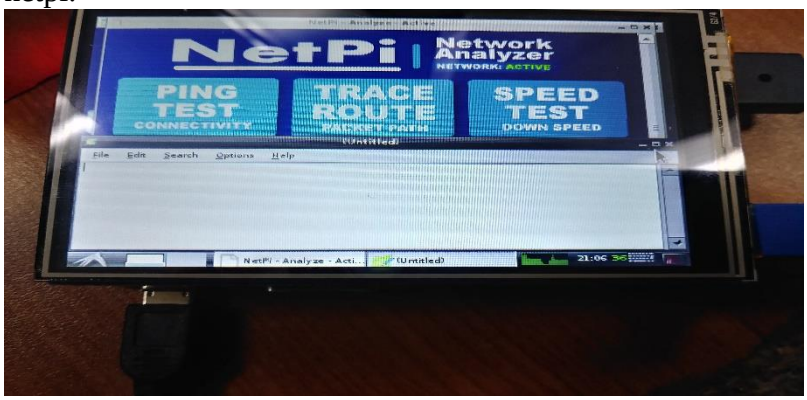
El botón speed test (down speed) sirve para revisar la velocidad de descarga de la red



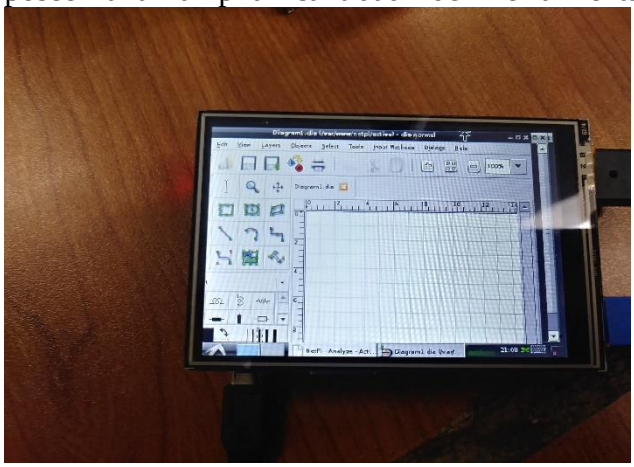
El botón etho wlan0 (dhcp & details) nos brinda información sobre el dhcp y la interface lookback



El botón scratch pad (text editor) es un editor de texto que viene incluido en el sistema netpi.

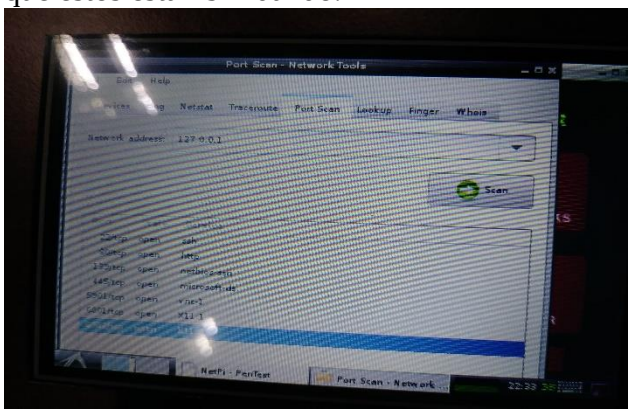


El boton net draw (topology editor) es un programa para realizar topologías de redes y posee una amplia cantidad de herramientas para la creación de topologías

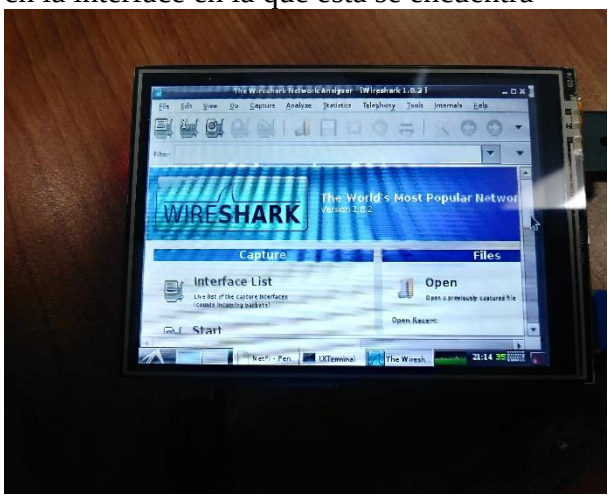


En la siguiente imagen veremos los diferentes usos de netpi en modo pen tester:

El botón port scan (chek open ports) sirve para ver los puertos activados y los servicios que estos están brindando.

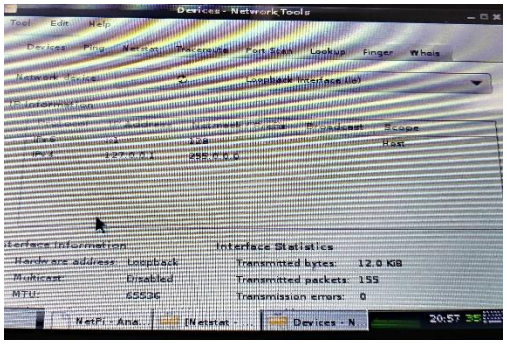


El boton wire shark (test connectivity) es un programa que analiza la conetividad de la red en la interface en la que esta se encuentra

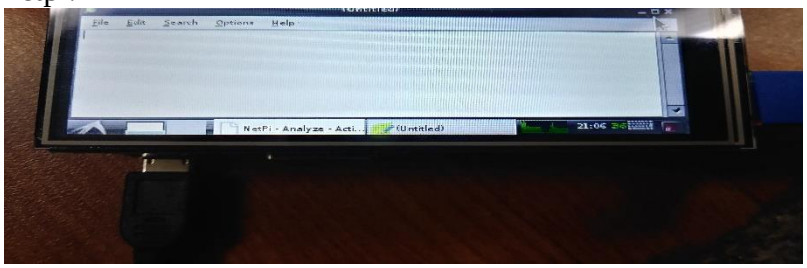


El boton war drive (view networks) es para escanear las redes inalámbricas

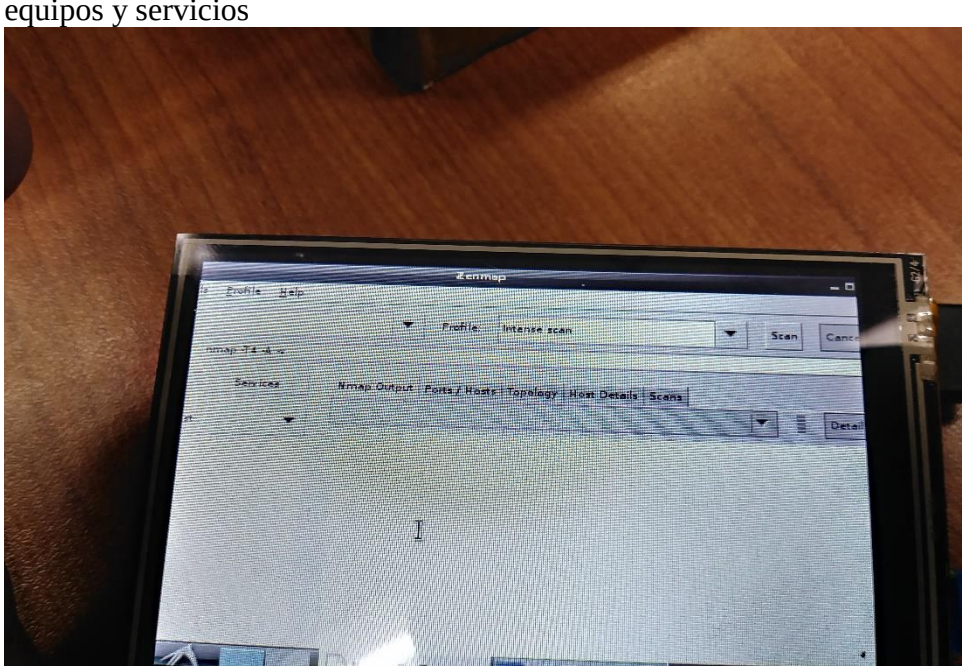
El botón etho wlan0 (dhcp & details) nos brinda información sobre el dhcp y la interface lookback



El botón scratch pad (text editor) es un editor de texto que viene incluido en el sistema netpi.

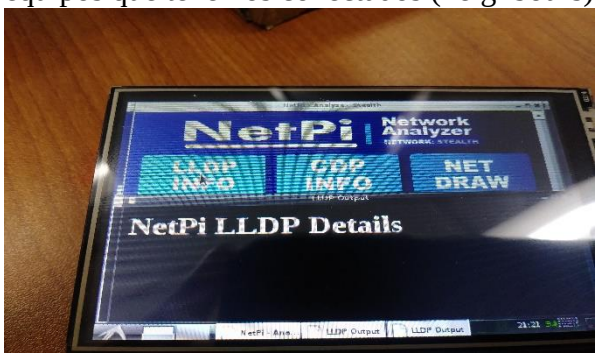


El boton zen map (net scanner) sirve para sondear redes incluyendo la detección de equipos y servicios

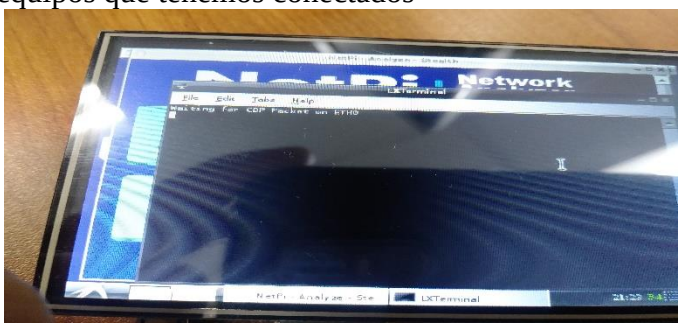


En la siguiente imagen veremos los diferentes usos de netpi en modo stealth:

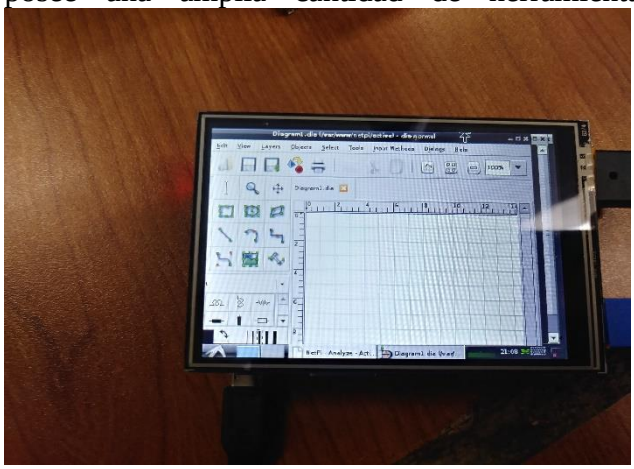
El botón lldp info (lldp details) este boton brinda información sobre el protocolo lldp y los equipos que tenemos conectados (neighbours)



El boton cdp info (cdp details) este boton brinda información sobre el protocolo cdp y los equipos que tenemos conectados



El boton net draw (topology editor) es un programa para realizar topologías de redes y posee una amplia cantidad de herramientas para la creación de topologías



El boton wlan fix (fix wlan nic timeout isssue)

El botón scratch pad (text editor) es un editor de texto que viene incluido en el sistema netpi.

El botón etho wlan0 (dhcp & details) nos brinda información sobre el dhcp y la interface lookback

4.4 Manual de Usuario del Sistema de Monitoreo NETPI

1.-IMPLEMENTACIÓN DEL SISTEMA

a) Requerimientos de hardware

Contar con:

- Monitor táctil
- Raspberry pi modelo B+
- Teclado
- Mouse
- Fuente de alimentación
- Un dispositivo de acceso a red

b) Requerimientos de software

Contar con:

• Sistema operativo NETPI (lo cual se descargó de la siguiente pagina http://blamethenetwork.com/netpi-raspberry-pi-network-analyzer/)

2.- FUNCIONALIDAD GENERAL

Las pantallas del sistema se dividen en tres modos:

- modo analyzer

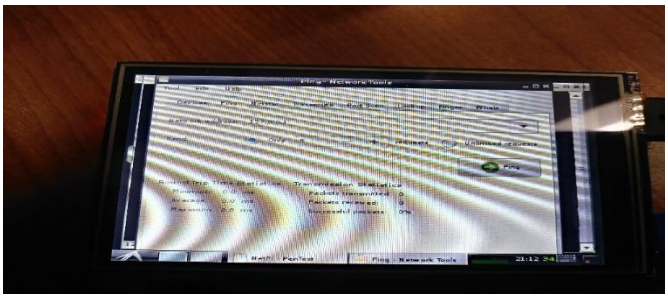
- modo pen tester

- modo stealth

Los 3 modos cuentan con 6 botones, lo cual unos se repiten en los tres modos y tiene la misma funcionabilidad.
A continuación el uso de cada botón.

Modo analyzer active:
El botón:

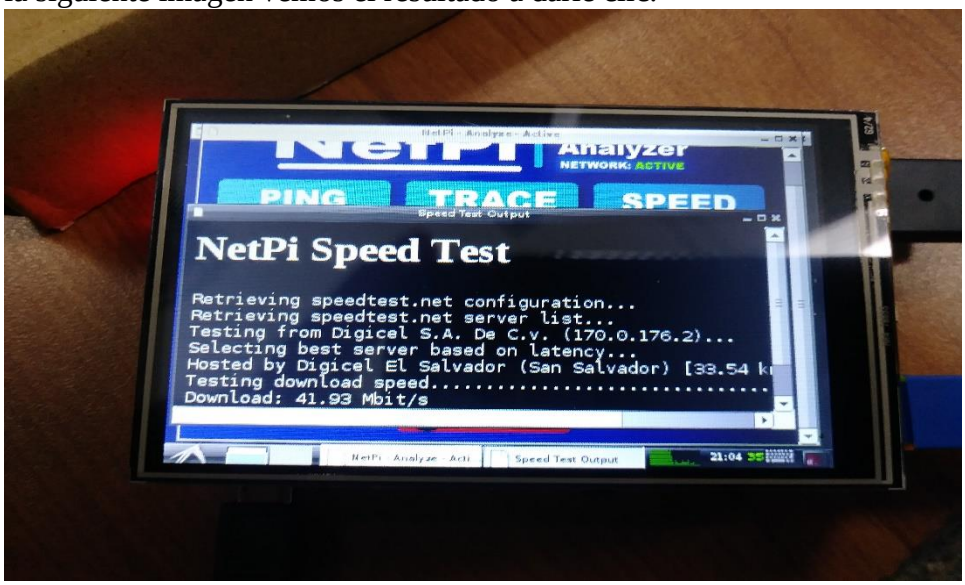
Ping test connectivity : automáticamente el sistema a darle click a este botón hace la prueba de ping, como se puede observar en la siguiente imagen



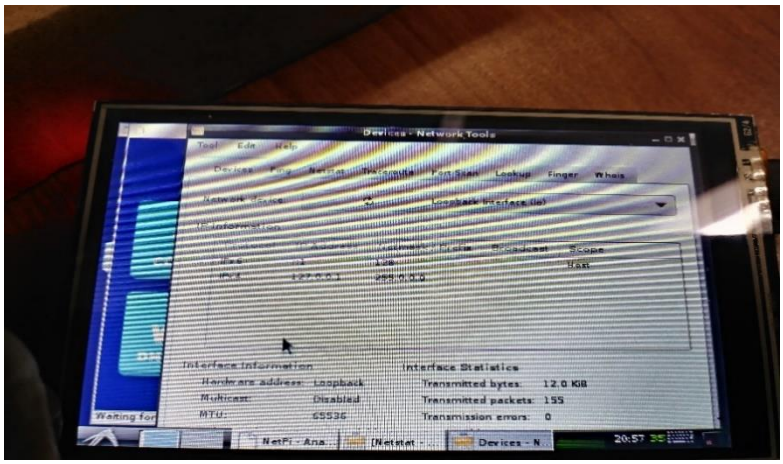
Pero también da la opción del número de paquetes que queremos enviar con los botones más (+) y menos (-) que aparecen en la ventana o está la opción de enviar paquetes ilimitadamente para sí observar él envió y respuesta de paquetes.

Trace raute packet path: a darle clic a este botón nos abra una ventana llamada network tolos este botón sirve para ver los detalles del host la ip del host local y el tiempo que se tarda enviar un rastro, también se puede seleccionar otras opciones de los servidores y hacer la misma prueba.

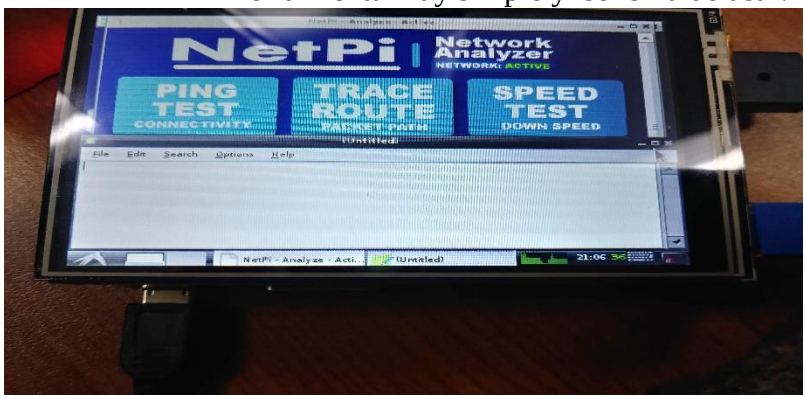
Speed test Down speed: este botón funciona para comprobar la velocidad como de carga y descarga de datos automáticamente a dar clic en este botón comienza hacer una prueba sin necesidad de apretar otro botón, en la siguiente imagen vemos el resultado a darle clic.



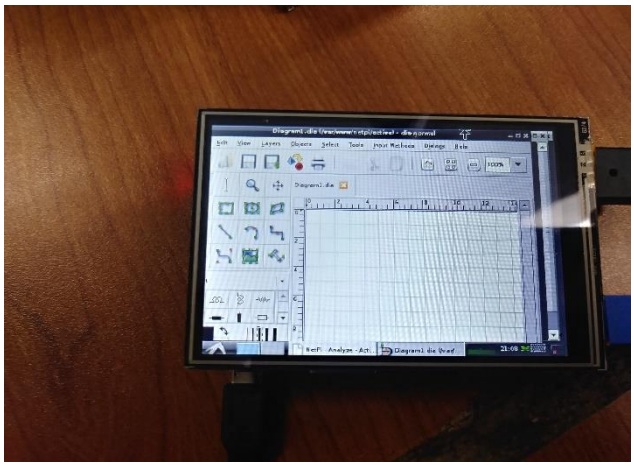
Eth0 wlan: este botón sirve para ver los detalles del servidor DHCP al darle clic nos abre una ventana dándonos información sobre el dhcp cuál es la ipv6 y ipv4 que utiliza, también se puede elegir otro tipo de interface



Scratch pad : este botón es un editor de texto que nos sirve para escribir como un bloc de notas de Windows o como Microsoft Word, es una herramienta muy simple y sencilla de usar.

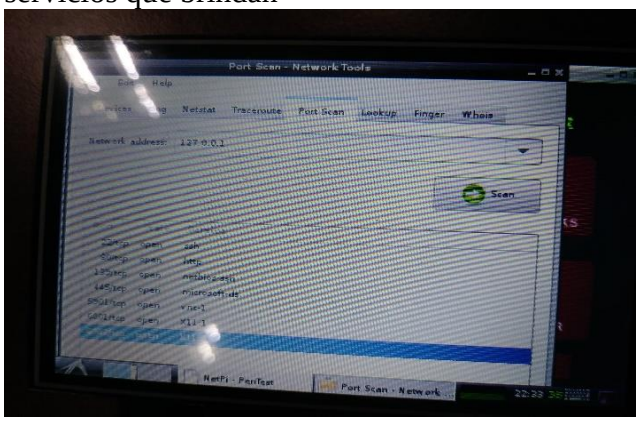


eNet draw: este botón sirve para editar y crear una topología de red, a abrirse la ventana podemos observar que las herramientas para crear la topología se encuentra al lado izquierdo de la pantalla donde se pueden elegir varias opciones.

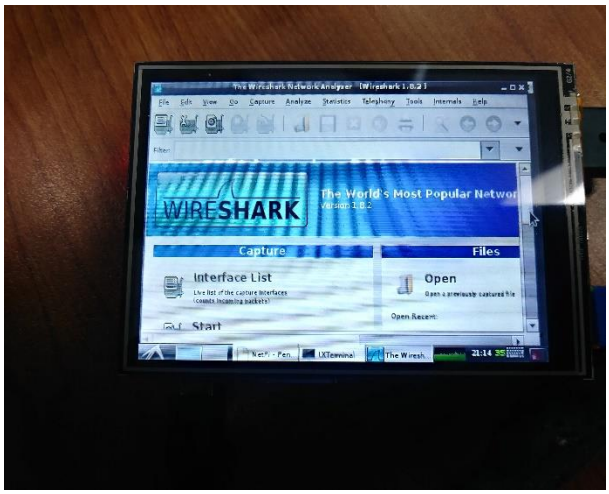


Modo pen tester:
Como observamos en la imágenes anteriores los botones del modo active son azules y las de este modo son rojas.
Botones.

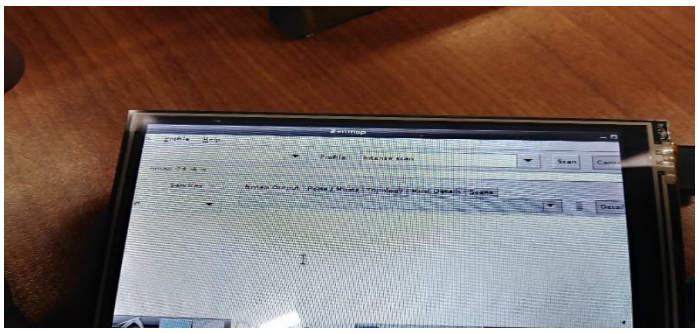
Port scan: este nos da detalles de los servicios que están brindando los puertos que están activados, también se puede seleccionar otras direcciones para saber los puertos que estas tienen habilitados y saber los servicios que brindan



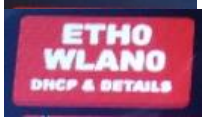
Wire shark: al hacer clic en este botón abre una ventana que nos muestra las interfaces que están conectadas al seleccionar una y apretar el botón de escaneo nos dará un informe de todo lo que está pasando en la red, desde los protocolos el destinatario el tiempo en que se tarda en pedir información y traerla en pocas palabras es un botón que mira la conectividad de la red.



Zen map: este botón tiene como funcionabilidad escanear la red lo cual al darle clic abre una ventana que da a varias opciones de escaneo. Que no brindan los escaneo de ping



boton no funcional.

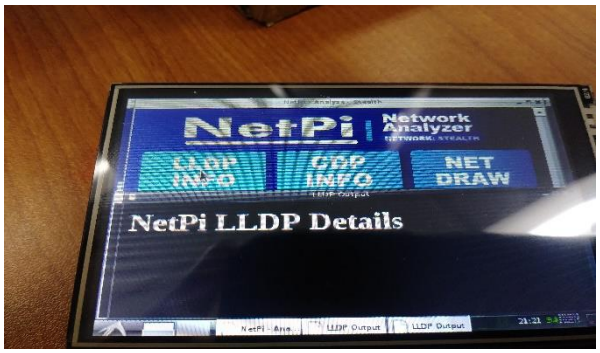


Misma función que el modo active

Modo stealth:

Botones.

LLDP info: este boton nos muestra el descubrimiento de vecinos es alternativo a CDP. Al darle clic automáticamente nos muestra los detalles de los vecinos .



CDP info: tiene la misma funcionabilidad que LLDP solo que este solo sirve con sistema cableado mostrándonos sus detalles de la prueba de protocolo cdp.

Wlan fix: solo funciona con conexiones wifi

Misma funcionabilidad que los otros modos

Nota : netpi es un software que aún se encuentra en desarrollo por ende está la posibilidad que tenga unos márgenes de errores

Capítulo V

Conclusiones

La presente tesis tuvo como objetivo, la implementación de un pequeño proyecto de sistema de monitoreo de redes alternativo a las principales herramientas comerciales, aunque utilizando sólo software libre y hardware económico como un Raspberry Pi. Este dispositivo de monitoreo de red es utilizado para comprobar el estado de una red.

Con este dispositivo se realizó el monitoreo de red del laboratorio de cisco, dando un resultado positivo y esta herramienta permitirá en usos futuros un mejor control de lo que son las redes de la Universidad Tecnológica de El Salvador (UTEC).

Así pues, la aportación principal de este trabajo consiste en dar al estudiante y docentes el material didáctico, y que sea utilizado en las instalaciones universitarias, así también en la biblioteca virtual de la universidad, extendiéndonos también a la posibilidad de que por medio del sistema de préstamo de libros de la universidad tecnológica de El Salvador el alumno pueda llevar el material para trabajarlo en casa y realizar prácticas en los diferentes laboratorios de la universidad.

Referencias

Errors, S. (2015). *NetPi – Raspberry Pi Network Analyzer*. Recuperado de http://blamethenetwork.com/netpi-raspberry-pi-network-analyzer/

Martinez, M. (2016). *NetPi - Raspberry Pi Network Analyzer Monitoriza tu red*. Recuperado de http://raspberryzero.com/index.php/2016/03/04/netpi-raspberry-pi-network-analyzer-monitoriza-tu-red/

Paz, A. (2015). *Aplicaciones de seguridad informática de Raspberry Pi.* Recuperado de http://www.gurudelainformatica.es/2015/10/aplicaciones-de-seguridad-informatica.html

Velasco, R. (2015). *NetPi, Analiza el estado de tu red con un Raspberry Pi*. Recuperado de https://www.redeszone.net/2015/03/23/netpi-analiza-el-estado-de-tu-red-con-un-raspberry-pi/