UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA
UNAN-Managua
Recinto Universitario Rubén Darío
Facultad de Ciencias e Ingeniería
Departamento de Tecnología

Seminario de Graduación

TEMA DEL PROYECTO

Implementar Untangle como herramienta gráfica para la configuración y gestión de los servicios de red en la empresa EDISA (empresa de desarrollo de ingeniería S.A) Managua.

Autores

Br. Rolando Javier Muñoz Vanegas

Br. Allam Humberto Hernández Conto

Tutor: Msc. Álvaro Noel Segovia Aguirre

Asesor Tecnológico: Ing. Harry Martínez

Dedicatoria

A Dios: Por darme la vida y la sabiduría y poder llegar a finalizar mis estudios superiores.

A mis padres: En especial a mi madre porque sé que ella siempre estuvo pendiente de mi formación profesional y personal, ella está conmigo en todo momento y ha guiado mis pasos para que pudiera finalizar este trabajo.

A mi familia: En especial a mi hermana (Marlene) que me ha apoyado con sus consejos, con su paciencia y su tiempo, además me ha motivado para lograr llegar a la meta profesional.

Dedicatoria

A Dios, por brindarnos la dicha de la salud y bienestar físico y espiritual.

A nuestros padres, como agradecimiento a su esfuerzo, amor y apoyo Incondicional, durante nuestra formación tanto personal como profesional.

A nuestros docentes, por brindarnos su guía y sabiduría en el desarrollo de este Trabajo.

Agradecimiento

Le damos las gracias a la empresa EDISA especialmente a su gerente general la Lic. Mireya Escobar por la confianza de permitirnos que se pudiera realizar las pruebas del proyecto en sus instalaciones.

A los profesores que desde las aulas de clases nos transmiten sus conocimientos y experiencias para brindarnos una formación de primera calidad y que seamos buenos profesionales para desempeñarnos en todas las áreas que la carrera de Ing. Electrónica posee.

A nuestro tutor y guía Ing. Álvaro Noel Segovia Aguirre por brindarnos todas las pautas y conocimientos para poder elaborar el proyecto y así culminar la carrera.

Al Ing. Harry Martínez nuestro asesor tecnológico por estar siempre a disposición para todas las consultas que requerimos.

A la Universidad Nacional Autónoma de Nicaragua Por ser la que con voz de lucha ha forjado hombres de servicio a la sociedad. Con amor.

Índice

Capítulo VIII

Capitulo IX

Capitulo X

Capítulo XI

Capítulo I

Introducción

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura de la red y a la información de la empresa. En la actualidad el principal problema que presentan las redes locales en las empresas y organizaciones, son las contantes invasiones de una gran cantidad de elementos dañinos para los equipos de cómputo como: virus, hackers, spam, etc, que perjudican el buen funcionamiento de nuestro sistema de red. La protección de la información y el control de acceso se ha convertido en uno de los elementos más importante dentro de una organización por lo que dicha seguridad informática debe ser administrada de acuerdo a los criterios establecidos por administradores y supervisores, evitando que usuarios tanto internos como externos puedan acceder a ella sin autorización.

En Internet, hay múltiples amenazas que pueden afectar el buen funcionamiento de la red de una empresa. Muchas veces se aprovecha la imprudencia de algunos empleados al utilizar la Web, el correo electrónico o la mensajería instantánea. La solución es establecer Políticas de uso en el manejo de la red y hacerlas cumplir. Por tal motivo diversas empresas se han dado a la tarea de desarrollar una diversidad de equipos para lograr la máxima protección de la red, nuestros equipos computacionales y la información que estos poseen, varias de estas tecnologías protectoras son: cortafuegos, sistemas de detección de intrusos, llaves para protección de software, etc.

Retomando esos aspectos, hemos considerado realizar nuestro trabajo basado en la implementación de un sistema de protección sobre la plataforma **Debían/Linux** que permitirá solo el acceso de los contenidos que la empresa estime conveniente, respetando las políticas de uso, la propuesta de seguridad a emplear es Untangle un paquete de software creado para la protección perimetral de la red, esta herramienta ofrece módulos de aplicación integrados que pueden ser empleados por usuarios con conocimientos básicos en informática, ya que su interfaz es grafica.

Open Source y Free Apps (Lite Package): El servidor UNTANGLE y 13 de las aplicaciones que se ejecutan en él, son de código abierto y libre bajo la Licencia General Publica (GNU General Public License v2) (GPLv2). La plataforma de Untangle ofrece la interfaz gráfica de usuario, registro, notificación y canalización virtual, con tecnología para hacer que todas las aplicaciones se ejecuten juntas sin problemas.

Apps Pagado. Estas son diseñadas para redes con necesidades avanzadas. ***Paid Apps*** incluye soporte técnico en vivo, funciones avanzadas de gestión y las aplicaciones de seguridad adicionales y acceso remoto.

En definitiva, con éste programa se pretende proteger y controlar el acceso a internet en la red de manera fácil y con muy poco esfuerzo. Para obtener un mejor manejo del sistema éste software será instalado en un ordenador que actuará como servidor dedicado al que tendrá acceso solamente el administrador de la red.

Todas estas características positivas que brinda Untangle es la razón principal que nos ha llevado a efectuar el estudio y la implementación de dicho sistema en la empresa EDISA.

Capítulo II

Justificación

Los principales problemas que las empresas y microempresas presentan al momento de la utilización de sus sistemas de red son las frecuentes invasiones de grandes cantidades de elementos informáticos dañinos en las PC de los usuarios como: spam y virus que causan perdida de información, así como el acceso y descarga de aplicaciones en sitios webs con contenido no deseado los cuales perjudican el buen funcionamiento y desempeño de la red.

El presente proyecto tiene como objetivo implementar un sistema de protección nuevo en el mercado que será instalado en la red y resolverá problemas de filtración de elementos no deseados, así como la restricción de acceso a sitios webs a los que ingresan empleados de la empresa.

La empresa EDISA nos abre las puertas para la implementación del servidor Untangle un programa de alto nivel, éste software es una herramienta integrada con grandes aplicaciones, una de las aplicaciones importante es la de Reports la que nos permitirá, a través de reportes diarios o semanales que se realice un monitoreo de cuantos elementos nocivos así como sitios web no deseados han sido bloqueados.

Otro punto a favor de Untangle es que posee una galería de aplicaciones de uso amigable para cualquier persona que cuente con conocimientos básicos en informática, por su interfaz gráfica con que está diseñado el programa.

Realmente hay que reconocer que nada en el mundo es perfecto, en el mundo de la informática, muchos nos hemos topado con aplicaciones o productos en general que fallan constantemente, Untangle por su parte tiene 5 años de experiencia en el mercado y a escalado posiciones hasta convertirse en una de las mejores soluciones de muro de fuego, forjando un nombre en el ambiente de la tecnología, garantizando confianza y seguridad.

Capítulo III

Objetivo General:

- Implementar Untangle sobre la plataforma Debían/Linux para la administración de los servicios de red en EDISA (Empresa de Desarrollo de Ingeniería S.A).

Objetivos Específicos:

- Identificar los aspectos generales de la red de área local de la empresa (topología, estructura, direccionamiento IP).
- Instalar Untangle en un servidor dedicado, en la red de la empresa EDISA, para la administración de los servicios.
- Configurar el paquete de aplicaciones Untangle, para obtener un alto nivel de seguridad en la red de la empresa EDISA.
- Administrar y monitorear la red local controlando el acceso a sitios webs, descargas de aplicaciones, bloqueo de virus, spam entre otros**.**

Capítulo IV

Antecedentes

Untangle fue fundada en 2003 como Metavize, Inc. por John Irwin y Dirk Morris, Metavize se lanzó oficialmente en 2005 en Demo@15! En el año 2006 cambio su nombre a Untangle, Inc. En el 2007, Untangle lanzo la plataforma Untangle Gateway de código abierto (open source) bajo la licencia GPL (versión 2). Posteriormente Dirk Morris anuncio el lanzamiento de Untangle Gateway en versión 8.0, el cual es una distribución Linux basada en Debían o puerta de enlace con módulos agregables para aplicaciones de red.

La misión principal que tiene Untangle es ser utilizada en la práctica de ingeniería abierta. Para acelerar el desarrollo y hacer que la base de código resultara más accesible, implementaron *Java*, y para hacerlo funcionar sobre un servidor de bajo costo solo inventaron y patentaron una nueva manera de racionalizar la sobrecarga de comunicaciones entre los módulos, nombrando a su solución canalización virtual.

Revisando los diferentes trabajos monográficos que se encuentran en la biblioteca central de la Universidad Nacional Autónoma de Nicaragua (UNAN-Managua) en las áreas de computación, informática e Ing. Electrónica, así como diversos sitios webs nacionales y revistas tecnológicas empresariales en Nicaragua, no se ha encontrado ningún tipo de trabajo acerca de la implementación de un Servidor Untangle por lo que hemos recopilado información de diferentes sitios webs con contenido técnico, provenientes de la experiencia en el manejo del sistema en otros países, para de esta manera completar la investigación y llevar a cabo el proyecto.

Capitulo V

Planteamiento del problema

El presente proyecto se basa en la implementación de un software, el que estará instalado en una PC y actuará como un servidor dedicado para proteger y controlar el área perimetral de la red de la empresa EDISA, la que actualmente presenta diversos problemas en cuanto a la filtración de elementos no deseados en sus equipos de computo, lo que ha provocado gastos en mantenimiento, pérdida de información, baja en su productividad, etc.

Al igual que muchas empresas, EDISA no cuenta con personal experto trabajando dentro y a tiempo completo para garantizar que su negocio se encuentre protegido frente a ataques informáticos, Por lo antes expuesto presentamos esta propuesta seguridad para la red de la empresa llamada Untangle, el cual contribuirá a tener un mejor control de la red y reducir los ataques de elementos informáticos dañinos a la misma.

Capítulo VI

Hipótesis

Si la empresa EDISA llegase a implementar éste software mejoraría la seguridad en la red, ofreciendo mejor protección a los equipos usuarios que la conforman ya que la información de cada uno estaría segura y se tendría un mejor control de los recursos de la red, bloqueando virus, spyware y phishing impidiendo que lleguen hasta los equipos y puedan afectarlos. Sin embargo es necesario mencionar que éste software no elimina ningún virus, simplemente impide su entrada en el sistema de red de la empresa. Se tendría un mejor control de los sitios a los que accedan los trabajadores de la empresa .La estructura de su red no sufriría ningún cambio por lo que la empresa no incurriría en gastos de otros equipos.

Capítulo VII

7.1 Conceptos básicos de sistemas de redes

Para efectos de la realización del trabajo en la implementación de Untangle como herramienta gráfica para la administración y gestión de los sistemas de red en la empresa EDISA consideramos de mucha importancia dar a conocer los conceptos más utilizados en nuestra investigación.

7.1.1 Software

Se conoce como **software** al equipamiento lógico o soporte lógico de un sistema informático, 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.

Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas; tales como el *procesador de texto*, que permite al usuario realizar todas las tareas concernientes a la edición de textos; ***el software*** *de sistema*, tal como el sistema operativo, que básicamente permite al resto de los programas funcionar adecuadamente **(http://www.solinux.es, 2010).**

7.1.2 Código abierto

Es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales las cuales destacan en el llamado ***software libre*** **(http://es.wikipedia.org/wiki/C%/C3%B3digo_abierto, 2011).** El código abierto ha marcado lo que será el futuro del software. Los clientes pagarán por los servicios y el soporte, pero el software será gratuito. Con cientos de clientes de pequeño y mediano tamaño como referencia Untangle ha decidido extender su mercado objetivo ofreciendo su software por tiempo ilimitado y dando a los usuarios la oportunidad de actualizar la

solución a la versión empresarial de la plataforma; pero en este caso tendría que ser remunerado.

Su uso nació por primera vez en 1998 de la mano de algunos usuarios de la comunidad del software libre, tratando de usarlo como reemplazo al ambiguo nombre original en inglés del software libre (free software). «Free» en inglés significa dos cosas distintas dependiendo del contexto: gratuidad y libertad.

7.1.3 Internet: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET.

Uno de los servicios que más éxito ha tenido Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto (**http://es.wikipedia.org/wiki/Internet, 1990)**. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia telefonía (VoIP), televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

7.1.4 Malware

Malware (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

7.1.5 Virus informático

Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, remplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir de manera intencionada los datos almacenados en un ordenador, aunque también existen otros más inofensivos que solo se caracterizan por ser molestos.

Los virus informáticos tienen básicamente la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático que son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones por desconocimiento del usuario (**http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico**). El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.

El virus toma entonces el control de los servicios básicos del sistema operativo, infectando de manera posterior archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

7.1.6 Filtro de contenido WEB

Un filtro de contenido se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web (**http://www.salixnetworks.com/filtrado_web.html, 2008)**. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable.

7.1.7 Firewall

Cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear o denegar el acceso a personas no autorizadas a una PC, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuego a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

7.1.8 Red WAN: Una red de área amplia, con frecuencia denominada **WAN**, de la expresión en idioma inglés *wide area network*, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de internet (ISP) para proveer de conexión a sus clientes.

Hoy en día, Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente, mientras que las ***redes privadas virtuales*** que utilizan ***cifrado*** y otras técnicas para hacer esa red dedicada, aumentan continuamente.

Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

7.1.9 **Pasarela o Puerta de Enlace**: Su significado (del inglés Gateway) es un dispositivo, con frecuencia una computadora, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red, al protocolo usado en la red de destino. La puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (Network Address Translation).

Esta capacidad de traducción de direcciones permite aplicar una técnica llamada "enmascaramiento de IP", usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de una puerta de enlace normalmente se parece a ó y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.16.x.x a 172.31.x.x, 192.168.x.x, que engloban o se reservan a las redes de área local. Además se debe notar que necesariamente un equipo que cumpla el rol de puerta de enlace en una red, debe tener 2 tarjetas de red **(http://www.todo-redes.com/gateway-puerta-de-enlace.html, 2011).**

En entornos domésticos se usan los enrutadores ADSL o cable módem como pasarelas para conectar la red local doméstica con la red que es Internet, si bien esta puerta de enlace no conecta 2 redes con protocolos diferentes, sí hace posible conectar 2 redes independientes haciendo uso del NAT.

La configuración en los enrutadores domésticos, consiste en escribir la dirección IP de la puerta de enlace en un navegador web, el cual solicitará usuario y contraseña del Administrador, y en caso de ser correctos abrirá una página web donde se muestra la información del módem, WAN y LAN, permitiendo su edición.

7.1.10 Router: También conocido como **enrutador** o **encaminador de paquetes** es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un Router (mediante bridges), y que por tanto tienen prefijos de red distintos.

7.1.11 Switch: Un ***conmutador*** o ***switch*** es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

7.1.12 Fibra óptica: Las fibras ópticas son conductos, rígidos o flexibles, de plástico o de vidrio (sílice), que son capaces de conducir un haz de luz inyectado en uno de sus extremos, mediante sucesivas reflexiones que lo mantienen dentro de sí para salir por el otro. Es decir, es una guía de onda y en este caso la onda es de luz.

Los dos *tipos de fibra óptica* son:

- Monomodo (single mode)
- Multimodo (multimode)

La *fibra óptica monomodo* es utilizada para las conexiones interurbanas, básicamente son instaladas por las prestadoras de servicios públicos, ya que permite el uso de amplificadores a una distancia entre sí de 40 Km. o más, mientras que las líneas de transmisión de cobre necesitan más de tres amplificadores cada 10 Km. En cambio la *fibra óptica multimodo* es instalada dentro de edificios comerciales, oficinas, bancos y dependencias donde la distancia entre centros de cableado es inferior a los 2 Km.

Los *conectores de fibra óptica* más usuales comercialmente son:

- ST, metálico, con ferrule de cerámica, sujeción a bayoneta, usado en multimodo, con pulido convexo PC. Puede conectarse por crispado mecánico, soldadura por material epoxi.
- SC, plástico, con ferrule de cerámica, sujeción push-pull, simple o dúplex, usado tanto en multimodo como en monomodo, con pulido convexo PC y APC, en tres colores diferenciados: azul, para monomodo; beige para multimodo y verde para larga distancia.
- FC, similar al ST pero roscado.
- FDDI
- D4
- Biconic
- SMA
- ESCON

7.1.13 Transceiver: Son equipos que son una combinación de transmisor - receptor de información. El transceiver transmite paquetes de datos desde el controlador al bus y

viceversa. En una Ethernet, los transceivers se desconectan cuando el equipo al que están conectados no está funcionando, sin afectar para nada al comportamiento de la red.

El transceiver tiene internamente un circuito electrónico que le permite transmitir y recibir los datos a través del cable y proteger el cable principal contra fallas que se presentan en el computador. El cable que va del transceiver al computador tiene cinco pares de cable trenzado, uno para alimentar los circuitos del transceiver dos para enviar y recibir datos y los otros dos para realizar funciones de control, este cable tiene en cada extremo un conector AUI.

7.1.14 UTP: (unshielded twisted pair) o UTP en español "par trenzado no blindado es un tipo de cable de par trenzado que no se encuentra blindado y se utiliza principalmente para comunicaciones. Se encuentra normalizado de acuerdo a la norma estadounidense TIA/EIA-568-B y a la internacional ISO/IEC 11801. A continuación se presenta un gráfico donde podemos ver una de las características que posee este cable el empleo de un código de colores para la conexión con los diferentes equipos.

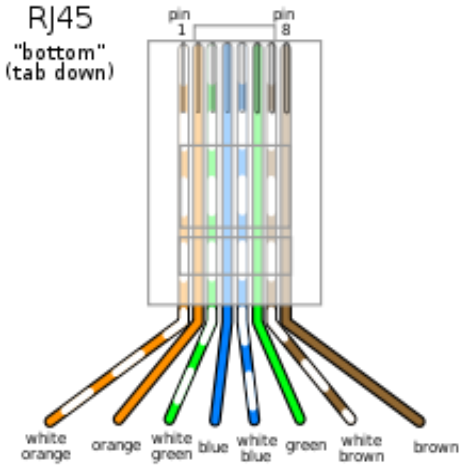

Figura 1. Colores del cableado en un conector RJ-45 según la norma 568B (http://www.es.wikipedia.org).

7.1.15 Patch Cord: Se usa en una red para conectar un dispositivo electrónico con otro**.** En cuanto a longitud, los cables de red pueden ser desde muy cortos (unos pocos centímetros) para los componentes apilados, o tener hasta 100 metros máximo. A medida que aumenta la longitud los cables son más gruesos y suelen tener apantallamiento para evitar la pérdida de señal y las interferencias.

7.1.16 Topología de Red en Estrella: Una topología *Estrella* es una arquitectura LAN en la cual los puntos finales de una red son conectados a un hub o switch central por enlaces dedicados, en una configuración con forma de estrella, los mensajes de cada nodo individual pasan directamente a la computadora central, que determinará, en su caso, hacia dónde debe encaminarlos, es de fácil instalación y si alguna de las instalaciones falla las demás no serán afectadas.

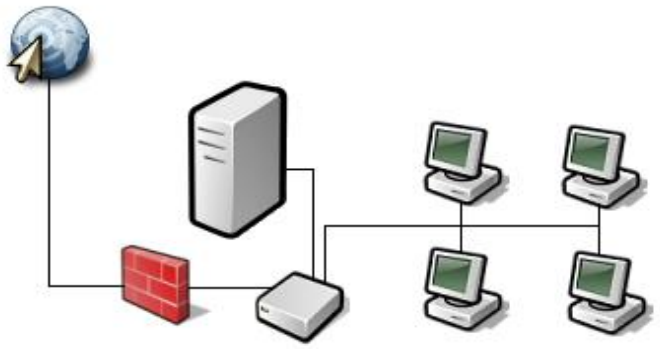

Figura 2. Diagrama topología estrella (http://www.solinux.es)

7.1.17 Red LAN: Una red de área local, red local o **LAN** (del inglés *local area network*) es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

7.1.18 Protocolos De Comunicación

7.1.18.1 Protocolo IMAP (Internet Message Access Protocol)

Internet Message Access Protocol, o su acrónimo IMAP, es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP, que es el otro protocolo empleado para obtener correo desde un servidor. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

IMAP y POP3 (Post Office Protocol versión 3) son los dos protocolos que prevalecen en la obtención de correo electrónico. Todos los servidores y clientes de email están virtualmente soportados por ambos, aunque en algunos casos hay algunas interfaces específicas del fabricante típicamente propietarias. Por ejemplo, los protocolos propietarios utilizados entre el cliente Microsoft Outlook y su servidor Microsoft Exchange Server o el cliente Lotus Notes de IBM y el servidor Domino. Sin embargo, estos productos también soportan interoperabilidad con IMAP y POP3 con otros clientes y servidores. La versión actual de IMAP, IMAP versión 4 revisión 1 (IMAP4rev1), está definida por el RFC 3501.

7.1.18.2 Protocolo POP (Post Office Protocol)

En informática se utiliza el Post Office Protocol (POP3, Protocolo de la oficina de correo) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI. Las versiones del protocolo POP (informalmente conocido como POP1) y POP2 se,

han hecho obsoletas debido a las últimas versiones de POP3. En general cuando uno se refiere al término POP, nos referimos a POP3 dentro del contexto de protocolos de correo electrónico.POP3 está diseñado para recibir correo, no para enviarlo; le permite a los usuarios con conexiones intermitentes o muy lentas (tales como las conexiones por módem), descargar su correo electrónico mientras tienen conexión y revisarlo posteriormente incluso estando desconectados. Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta. En contraste, el protocolo IMAP permite los modos de operación conectado y desconectado.

7.1.18.3 Protocolo SMTP (Simple Mail Transfer Protocol)

Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

7.1.18.4 Protocolo TCP/IP: **TCP/IP** es un conjunto de protocolos. La sigla TCP/IP significa "**Protocolo de control de transmisión/Protocolo de Internet**" y se pronuncia "T-C-P-I-P". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- Dividir mensajes en paquetes
- Usar un sistema de direcciones
- Enrutar datos por la red
- Detectar errores en las transmisiones de datos.

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental, espacialmente de ciertos criterios como:

- **Capa de acceso a la Red**: Especifica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.
- **Capa de Internet**: Es responsable de proporcionar el paquete de datos (datagrama).
- **Capa de Transporte**: Brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.
- **Capa de Aplicación**: Incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

7.1.18.5 Protocolo DHCP: El protocolo de configuración dinámica de Host o DHCP es un protocolo que permite a los administradores de red automatizar y gestionar de manera centralizada la asignación de direcciones del protocolo Internet (IP) en una red de una organización o de un proveedor de servicios de Internet (ISP). Usando el conjunto de protocolos de Internet (TCP/IP), cada ordenador que puede conectarse a Internet necesita una dirección IP exclusiva. Cuando una organización configura los ordenadores de diferentes usuarios para que éstos se conecten a Internet, debe asignar una dirección IP.

Sin DHCP, la dirección IP debe entrarse manualmente en cada ordenador, y si los ordenadores cambian de sitio a otro lugar de la red, hay que introducir una nueva dirección IP. El DHCP permite al administrador de la red supervisar y distribuir las direcciones IP de forma centralizada enviando automáticamente una nueva dirección IP cada vez que un ordenador se conecta en un lugar diferente de la red o cuando llama al ISP.

7.1.18.6 Protocolo HTTP: HTTP de ***HyperText Transfer Protocol*** (Protocolo de transferencia de hipertexto) es el método más común de intercambio de información en la World Wide Web, el método mediante el cual se transfieren las páginas web a un ordenador. Todas las páginas web están escritas en lenguaje de hypertexto (hyper-text markup language (**HTML**)), por lo que el hipertexto es el contenido de las páginas web.

El protocolo de transferencia es el sistema mediante el cual se transfiere información entre los servidores y los clientes (por ejemplo los navegadores).Hay una versión de ***http*** para la transferencia segura de información llamada ***https*** que puede utilizar cualquier método de cifrado siempre que sea entendido tanto por el servidor como por el cliente.

7.1.18.7 Protocolo DNS: Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en

números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet. El Domain Name System (DNS), o Sistema de Nombres de Dominio, comprende personas, instituciones reguladoras, archivos, máquinas y software trabajando conjuntamente. El servicio de DNS es indispensable para que un nombre de dominio pueda ser encontrado en Internet.

7.1.19 Servidor

En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. También se suele denominar con la palabra servidor a una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Sin embargo, de acuerdo al rol que asumen dentro de una red se dividen en:

7.1.19.1 Servidor dedicado: Son aquellos que le dedican toda su potencia a administrar los recursos de la red, es decir, atender las solicitudes de procesamiento de los clientes.

7.1.19.2 Servidor no dedicado: Son aquellos que no dedican toda su potencia a los clientes, sino también pueden jugar el rol de estaciones de trabajo al procesar solicitudes de un usuario local.

7.1.19.3 Servidor de Seguridad: Tiene software especializado para detener instrucciones maliciosas, normalmente tienen antivirus, antispyware, antiadware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques, los servidores de seguridad varían dependiendo de su utilización e importancia.

7.1.19.4 Servidor Proxy

Es el intermediario entre tu computadora y el internet, este hace registros sobre las páginas que visitas en internet pero también sirve para bloquear el acceso a otras páginas web **(http://www.alegsa.com.ar/dic/servidor.php, 1998).**

También bloquea unas páginas por si misma esto también lo hace con el fin de aumentar la velocidad de acceso a estas páginas web que han sido visitadas con frecuencia y al mismo tiempo, libera la carga de los enlaces de internet. En otras palabras se puede decir que este intercepta la navegación de los clientes por páginas web, por distintos motivos como los de seguridad, rendimiento, anonimato etc. No nada más existe el Proxy web si no También existen proxys para otros protocolos, como el proxy de FTP.

El proxy ARP puede hacer de enrutador en una red, ya que la hace de intermediario entre ordenadores. El Proxy (patrón de diseño) también es un patrón de diseño (programación) con la misma forma del el proxy de red.

Un ejemplo de ello lo tenemos en nuestra vida cotidiana es cuando vamos a un centro comercial los proxys vendrían siendo los trabajadores de caja ellos son los intermediarios entre el dueño del centro comercial y nosotros al comprar un artículo. También puede existir un proxy cuando conectamos un plug de USB con varias entradas de

USB este está amplificando las entradas de USB por medio de una y sirve de intermediario entre nosotros y la computadora, no hay que ir muy lejos también el Sistema Operativo que usamos sirve como intermediario para comunicarnos con la computadora.

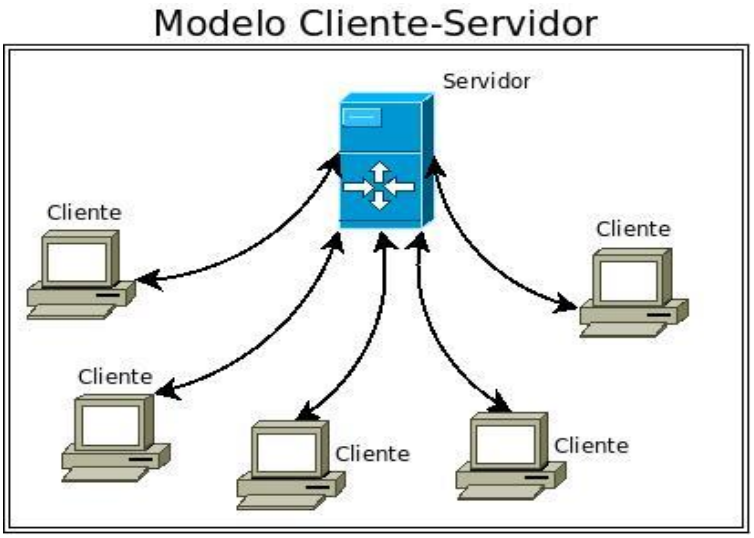

Figura3. Esquema de modelo cliente servidor (http://www.solinux.es).

7.1.20 Untangle

Untangle es una empresa privada que ofrece una pasarela de red (Network Gateway) de código abierto para pequeñas empresas. Untangle ofrece muchas aplicaciones como el bloqueo de correo electrónico no solicitado (spam), bloqueo de software malicioso (malware), filtrado de web, protección contra robo de información sensible (phishing), prevención de intrusiones y más **(http://.es.wikipedia.org, 2010)** sobre la Plataforma Untangle Gateway.

Para José M. Cestero, encargado de informática de la empresa PYME la definición de este software es la siguiente: "Más que un programa, ***Untangle*** es en realidad una recopilación de programas de seguridad unificados bajo una interfaz común que nos permite configurar y manejar la suite de forma sencilla. Podemos instalarlo en un equipo que actúe como servidor independiente que únicamente ejecuta esta solución o utilizarlo como un programa en un ordenador de escritorio con Windows XP" **(Cestero M. 2009 Untangle, *software para la protección perimetral de la red)***, Untangle es un servidor (Debían) de seguridad multi-función.

Untangle puede descargarse directamente del sitio web www.untangle.com en formato ISO, lo cual permite una grabación rápida y sencilla en un CD o en un dispositivo pendrive. No necesita ningún sistema operativo sobre el cual debe ir montado porque posee su propio sistema.

Capítulo VIII

8.1. Descripción de Untangle

8.1.1 Aplicaciones gratis de Untangle (Lite package)

Untangle es una solución bastante completa que podemos bien descargar gratuitamente además posee uno de los métodos de instalación más sencillos que existe entre las herramientas de red. Toda su interfaz es muy amigable, desde el principio de la instalación hasta el último paso de su configuración.

Las diferentes aplicaciones disponibles en Untangle pueden encontrarse en otras soluciones similares, pero la forma de activarlas es muy interesante. Cada aplicación es un módulo, sobre el cual debes hacer doble click sobre el botón on/off para activarlo y desactivarlo. Este nivel de flexibilidad te permitirá "armar" tu propia configuración, y dejar activas sólo las aplicaciones que creas necesarias. A continuación presentamos cada una de ellas con sus definiciones:

- ***Web Filter Lite***: Es un filtro de contenido para internet. Además de proteger la red del malware de internet, ofrece al administrador una lista de sitios web bloqueados totalmente personalizable agrupados en categorías. También permite bloquear la descarga de archivos para evitar que se pueda saturar la red con descargas, además de filtrar las descargar por extensión de archivo.
- ***Protocol Control***: Esta aplicación sirve para bloquear puertos dentro de nuestra red y así limitar a los usuarios la capacidad para usar determinadas aplicaciones de red. Permite añadir nuevos protocolos no soportados a las listas.
- ***Virus Blocker* Lite:** Esta aplicación analiza todo el tráfico proveniente de páginas web (HTTP), servidores ftp y correos electrónicos (IMAP, POP, SMTP). Permite detectar malware dentro de Zip, RAR, Tar y otros archivos comprimidos o compactos. Sus bases de datos son actualizadas periódicamente mediante actualizaciones automáticas.

- ***Spyware Blocker***: Es una buena opción para proteger a los usuarios del malware instalado desde el navegador, aunque no substituye a un spyware instalado en el sistema. Escanea todo el tráfico de la red en busca de malware. Dispone de registro de eventos en tiempo real y lista personalizable de excluidos.
- ***Phish Blocker***: Esta aplicación ayuda a proteger los intentos de suplantación de identidad de correos electrónicos y páginas web. Algunos de los protocolos soportados son HTTP, SMTP, POP e IMAP. Dispone de un registro de eventos donde se especifican todas las incidencias.
- ***Intrusion Prevention:*** Esta aplicación bloquea los intentos de hackeo antes de los servidores internos así como las PC de los usuarios, con firmas pre configuradas basadas en IPS hacen fácil al administrador.
- ***Firewall:*** Esta aplicación dibuja una línea que separa la red interna de la red externa, además filtra el tráfico basado en una dirección IP, Protocolo y Puerto.
- ***OpenVPN:*** esta aplicación habilita al administrador a proporcionar acceso remoto y seguro a la red interna para realizar configuraciones básicas.
- ***Reports*****:** Proporciona a los administradores la visibilidad y los datos necesarios para investigar incidentes de seguridad, monitorea la conducta de los usuarios y se encarga de conocer el flujo del tráfico y el uso de la red.
- ***Spam Blocker*** **Lite**: Como su nombre indica es un bloqueador de SPAM incluido en las aplicaciones gratuitas de Untangle, soporta SMTP, POP e IMAP, además también soporta cuarentenas individuales para cada bandeja de correo entrante. Tiene un buen filtro de SPAM basado en las mejores técnicas de detección en tiempo real.
- ***Ad Blocker*****:** Esta aplicación elimina los anuncios molestos y disminuye el tiempo de carga de una página WEB, reduciendo el tráfico en la red.

8.1.2 Aplicaciones de pago

- ***Web Filter*:** Bloqueo de 100 millones de sitios en 57 categorías, además de otras nuevas a tiempo real
- ***Kaspersky Virus Blocker***: Su funcionamiento es parecido al módulo Virus Blocker, por no decir que es igualito, pero con las bases de virus y el motor heurístico de Karspersky Labs. Evita que el malware infecte los PCs y servidores de la red protegiéndolos en tiempo real.
- ***Virus blocker*: Ver virus blocker lite**
- ***Spam Blocker:* Ver spam blocker lite**
- ***Web Cache*:** Se llama **caché web** a la cache que almacena documentos web(es decir, paginas, imágenes, etc) para reducir el ancho de banda consumido, la carga de los servidores y el retardo en la descarga. Un caché web almacena copias de los documentos que pasan por él, de forma que subsiguientes peticiones pueden ser respondidas por el propio caché, si se cumplen ciertas condiciones.
- ***Bandwith Control*:** Esta aplicación permite el control del tráfico de la red, se pueden asignar cuotas a los usuarios y asignar el uso que se le va a dar al ancho de banda seleccionado. Con esta aplicación es posible garantizar ancho de banda para una aplicación o usuario de la red, también permite priorizar servicios. Se puede encontrar más información acerca de esta aplicación en la siguiente dirección
- ***Policy Manager*:** Se trata de una aplicación para personalizar el acceso a la red filtrando por franja horaria y por usuario. Permite crear políticas de acceso totalmente personalizables asignando permisos a los usuarios de la red. Se puede encontrar más información acerca de la aplicación en la página de Untangle.
- ***Directory Connector*:** Esta aplicación permite explotar todo el potencial del Active Directory de Microsoft. Permite autentificación mediante usuario y mediante servidor RADIUS. Dispone de sistema de reporte de estadísticas en PDF y HTML..
- ***WAN Failover*** – Cambiar automáticamente el tráfico a una conexión alternativa.

- ***WAN Balancer*** - Asigna el tráfico a través de hasta seis conexiones a Internet por separado.
- ***Branding Manager*** – Use su propio logo y mensajes en el servidor y bloqueos las pantallas.
- ***Live Support*** – Personas reales, con un conocimiento real para ayudar cuando haga falta.
- ***Commtouch Spam Booster*** – Una capa de protección extra para contener el SPAM.
- ***Policy Manager*** - Crear varios usuarios y sesiones basadas en la web y acceso remoto.
- ***AD Connector*** – Utiliza tu servidor de Microsoft Active Directory para simplificar la gestión de políticas y presentación de informes.
- ***PC Remote*** - Permite acceso directo in situ y la solución de problemas.
- ***Remote Access Portal*** – Proporcionar acceso seguro a los servidores internos y servicios.
- -***QoS:*** Permite la priorización del tráfico.

Capítulo IX

9.1 Plataforma Debían/Linux

9.1.1 Debían

El proyecto debían es una asociación de personas que han hecho causa común para crear un sistema operativo (SO) libre. Este sistema operativo que fue creado se llama ***Debían GNU/Linux***, o simplemente **Debían** para acortar.

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.

Debían GNU/Linux es un sistema operativo libre, desarrollado por más de mil voluntarios alrededor del mundo, que colaboran a través de Internet. Nació en el año 1993, de la mano del proyecto Debían, con la idea de crear un sistema GNU usando Linux como núcleo ya que el proyecto Debían, organización responsable de su mantenimiento en la actualidad, también desarrolla sistemas GNU basados en otros núcleos (Debían GNU/Hurd, Debían GNU/NetBSD y Debían GNU/kFreeBSD).

Debían funcionará en casi todos los ordenadores personales, incluyendo la mayoría de los modelos más antiguos. Cada nueva versión de **Debían** generalmente soporta un mayor número de arquitecturas de ordenadores. Lo que más distingue a **Debían** de otras distribuciones GNU/LINUX es su sistema de gestión de paquetes. Estas herramientas otorgan al administrador de un sistema Debían total control sobre los paquetes instalados.

Capitulo X

10.1 Administración de la red con Untangle

10.1.1 Generalidades de la red

La visibilidad del administrador Untangle es el primer paso en el control de su red. Los módulos están optimizados para una sencilla administración, cada aplicación tiene un aspecto similar permitiendo un manejo simplificado. La tecnología de Untangle asegura una alta protección, sin disminuir la velocidad del acceso a Internet, actualizaciones automáticas para el control de virus, filtros anti-Spam y módulos del sistema, servicios avanzados de red: QoS, manejo de fallas, DNS y mucho más. Untangle proporciona reportes para todas las actividades del sistema, generados de forma automática y que están disponibles. El software Untangle se ejecutará en cualquier tipo de hardware genérico de Intel/AMD. El siguiente grafico (fig. 4) muestra los módulos en que está estructurada la red de Untangle.

Figura4. Aplicaciones de administrador Untangle (http://www.tecnologiapyme.com).

10.1.2 Características del administrador Untangle

1-***Accesible*** - Menor costo total de propiedad de cualquier solución de Gateway de la red en el mercado de hoy.

2-***Integral*** - Maneja filtrado web, spam, control de redes, gestión de usuarios, gestión de ancho de banda.

3-***Flexible*** - Añadir aplicaciones en cualquier momento para satisfacer las necesidades cambiantes de su negocio con tan sólo arrastrar y soltar.

4-***Probado*** - Protege 1,7 millones de personas en más de 30.000 organizaciones en todo el mundo.

10.1.3 Hardware Requerido

Lo primero que necesitamos es un ordenador dedicado que realice la tarea de cortafuegos o firewall. Los requisitos recomendados para el manejo del tráfico de una red de 1 a 50 usuarios son de un procesador P4, 1GB de memoria RAM, 80GB en disco duro y 2 tarjetas de red. El software no necesita de un sistema operativo, ***Untangle*** instala su propio sistema operativo. El software ***Untangle*** borra por completo cualquier contenido o información que pueda existir en el disco duro del PC. El software ***Untangle*** requiere un equipo específico instalado en la puerta de entrada a la red. La tabla 1 muestra las características que el servidor ***Untangle*** debe tener, tomando en cuenta la cantidad de usuarios a los que tiene que dar servicios.

Recomendaciones de Hardware

Número de usuarios	Procesador	Memoria	Disco Duro	Tarjetas de Red	Notas
Mínimo	Intel / AMD compatible con el procesador (800 + MHz)	512 MB	20 GB	2	32-bits
1-50	Pentium 4 equivalente o superior	1 GB	80 GB	2 o más	32-bits
51-150	Dual Core	2 GB	80 GB	2 o más	32- bits
151-500	2 o más núcleos	2 o más GB	80 GB	2 o más	32-bits
501-1500	4 núcleos	4 GB	80 GB	2 o más	64-bits
1501-5000	4 núcleos o mas	4 GB o mas	80 GB	2 o más	64-bits

Tabla 1. Características recomendadas para instalar Untangle en un servidor.

10.1.4 Implementación en la red.

Por último, tendrás que decidir cómo deseas ejecutar Untangle en tu red. Se puede ejecutar ***Untangle como un Router***, aprovechando nuestras potentes herramientas de red, o como un ***puente transparente Bridge*** dejándolo caer sin problemas detrás del ***Router*** existente. Untangle es un dispositivo en línea, es decir, sólo el tráfico que fluye a través de él se filtró. Hay dos modos disponibles con Untangle: modo Router y modo Puente.

10.1.4.1 *Modo Router*

En Modo ***Router*** , Untangle será el dispositivo de borde en la red y servira como un Router y Firewall. En este caso, tendrá que configurar las interfaces externas e internas correctamente para que el tráfico fluya, esto se deberá hacer durante la instalación.

La figura 5 muestra esta disposición.

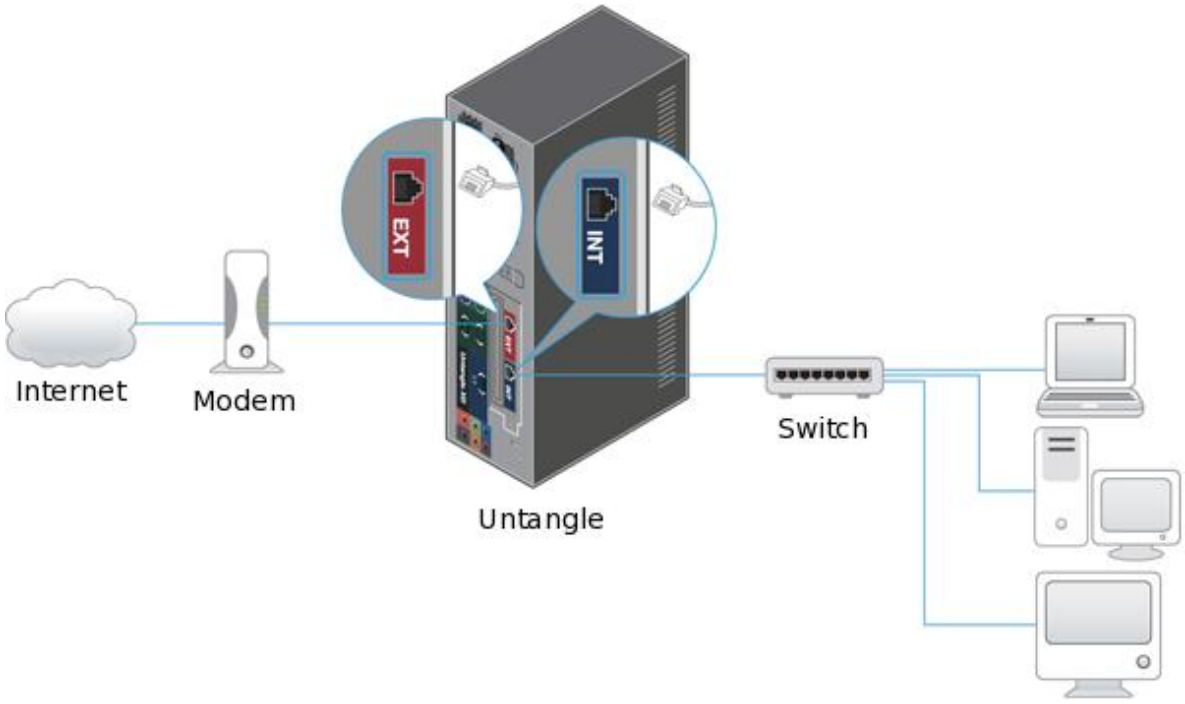

Figura 5. Modo Router (www.untangle.com).

10.1.4.2 *Modo Puente Transparente Bridge*

En modo ***Puente transparente Bridge*** Untangle está situado entre el firewall existente y el Switch principal. Cuando está en modo de puente Untangle es transparente, lo que significa que no tendrá que cambiar la puerta de enlace predeterminada de los ordenadores en la red o las rutas en el servidor de seguridad, sólo hay que poner el Untangle entre el cortafuegos y el Switch principal. Usted tendrá que dar a Untangle una IP externa a la interfaz en la subred del servidor de seguridad, establezca la interfaz interna para salvar de cualquier intruso del exterior. Como se observa en la figura siguiente.

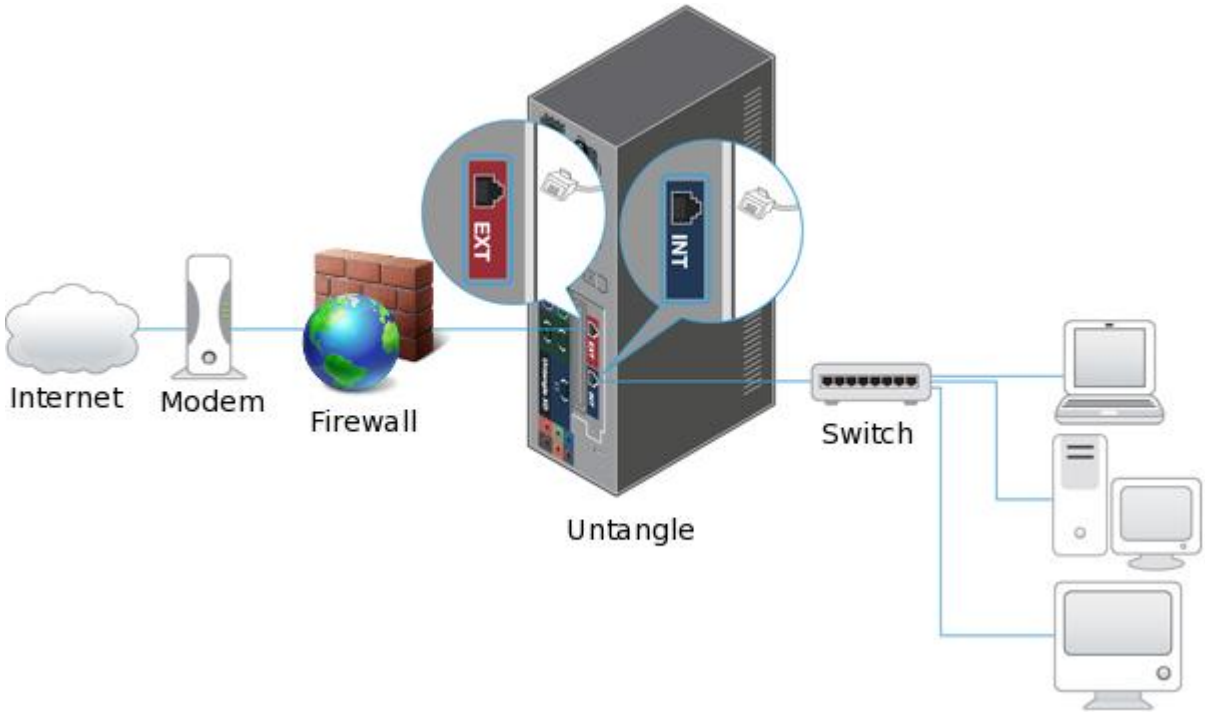

Figura 6. Modo puente bridge (www.untangle.com)

Capitulo XI

Desarrollo

11.1 Área de Estudio

El presente trabajo de desarrollo tecnológico experimental se llevó a cabo en la empresa EDISA, ubicada de la CST 1c sur, 2c al este calle 27 de Mayo.

11.2 Tipo de Estudio

En lo que respecta al tipo de trabajo se enfoca en la implementación de un equipo tecnológico es decir que cuenta con carácter experimental, porque en él se llevan a cabo procesos de instalación tanto de hardware como software y se pretende brindar un mejor funcionamiento de la red de la empresa así como mejorar su seguridad.Para lograr el desarrollo del proyecto se ha dividido en dos etapas importantes, en la primera parte se efectuó un análisis general de la red de la empresa. Obtuvimos la siguiente información:

- El servicio de internet lo provee ENITEL garantizando un ancho de banda de 2 Mbps por medio de fibra óptica SM 4 hilos.
- El cable de fibra óptica es conectado posteriormente a un transceiver el cual sirve como un convertidor SC de fibra óptica a Ethernet (RJ-45).
- Este transceiver sirve como puente por medio de UTP cobre Cat 5e 100 Mbps Hacia el Router Marca: Cisco Modelo: 827
- El Router proporciona conectividad con un Switch Marca: TRENDNET, Modelo: TEG-S24DG de 24 puertos.
- El Switch interconecta por medio de UTP cobre Cat 5e 100 Mbps a los usuarios, sirviendo como conmutador.
- La empresa EDISA cuenta con una red de área local (LAN) privada, compuesta por 8 computadoras de diversas marcas, con el objetivo de compartir recursos e intercambiar información.

La tabla número 2 muestra las características detalladas que posee cada una de las computadoras de la empresa EDISA, sus sistemas operativos, memorias, velocidad, etc.

Ítem	Sistema Operativo	Memoria RAM	Tipo y Velocidad del Procesador	Marca
1	Microsoft Windows XP Profesional	2 Gb	Intel Pentium 4 - 2.8 GHz	COMPAQ
2	Microsoft Windows XP Profesional	1 Gb	Intel Celeron 1.8 GHz	SIN MARCA
3	Microsoft Windows XP Profesional	1 Gb	Intel Pentium 4 - 1.5 GHz	HP
4	Microsoft Windows XP Profesional	512 Mb	Intel Pentium 4 - 2.66 GHz	HP
5	Microsoft Windows XP Profesional	1 Gb	Intel Celeron 1.8 GHz	SIN MARCA
6	Microsoft Windows XP Profesional	1 Gb	Intel Celeron 2.8 GHz	DELL
7	Microsoft Windows XP Profesional	1 Gb	AMD SEMPRON 1.8 GHz	DELL
8	Microsoft Windows XP Profesional	2 Gb	Intel Pentium 4 - 3 GHz	COMPAQ
9	Microsoft Windows XP Profesional	2 Gb	AMD Opteron 2.2 GHZ	SUN

Tabla 2. Características de los recursos que disponen las PC de la empresa.

11.3 Topología de Red

- El diseño de la topología de red empleado en EDISA es de tipo estrella, la cual se caracteriza por contar con un punto central o más propiamente conocido como nodo central al cual se conectan todos los equipos, como podemos observar en la figura 7, este diagrama fue tomado antes de la instalación del servidor Untangle posteriormente presentaremos el nuevo diseño con el servidor ya incorporado a la red.

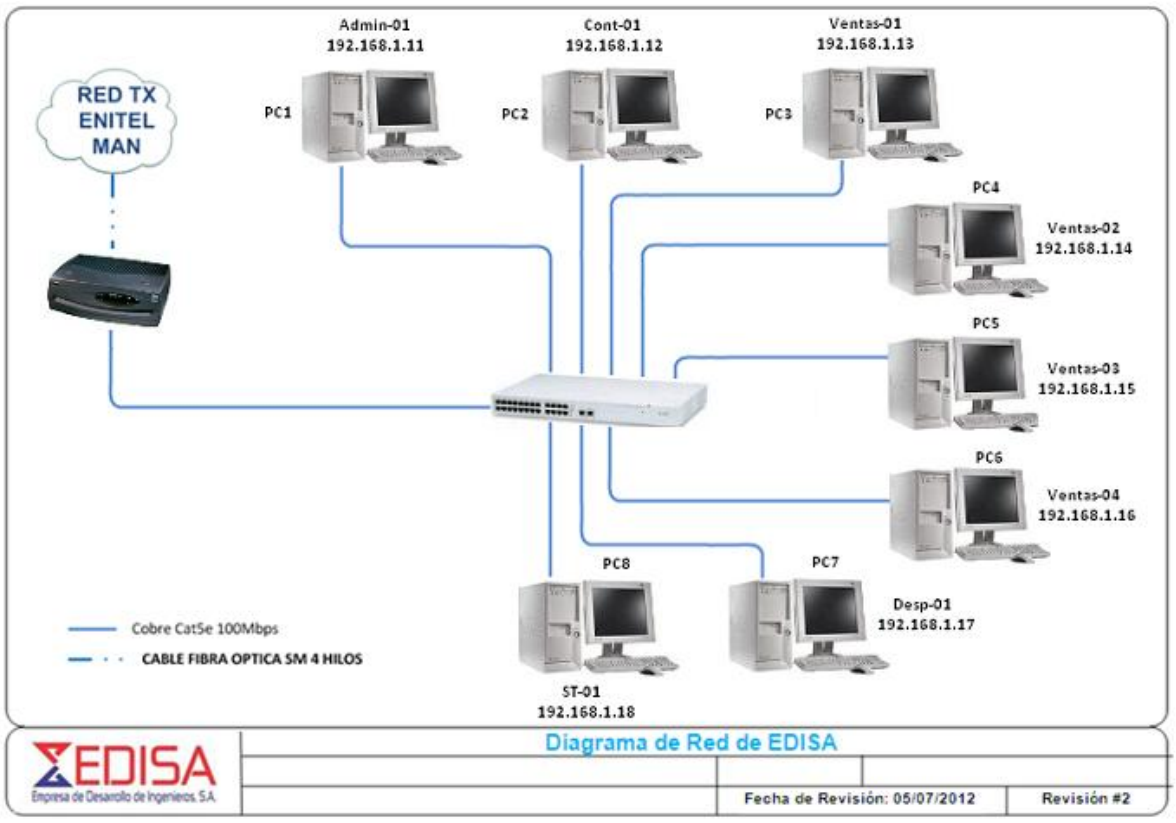

Figura 7. Topología estrella de la empresa EDISA.

11.4 Estructura de la Red: La tabla 3 muestra las ubicaciones de cada máquina en la red de la empresa al igual que las diferentes direcciones IP, los puertos de ubicación y la distancia entre ellas.

PISO	UBICACION	NOMBRE DEL EQUIPO	IP (192.168.1.0/24)	MAC-ADDRESS (eth0)	GRUPO DE TRABAJO	No PUERTO SW24	DIST EN Mts
1	Administración	Admin-01	192.168.1.11/24	00-24-5A-93-80-DC	Edisa	11	10
1	Contabilidad	Cont-01	192.168.1.12/24	00-42-2C-35-E1-CA	Edisa	12	7
1	Sala de Ventas	Ventas 01	192.168.1.13/24	00-16-E6-1B-84-34	Edisa	13	3
1	Sala de Ventas	Ventas 02	192.168.1.14/24	12-DF-60-5A-F8-87	Edisa	14	5
1	Sala de Ventas	Ventas 03	192.168.1.15/24	00-EB-84-09-IE-23	Edisa	15	7
1	Sala de Ventas	Ventas 04	192.168.1.16/24	34-05-00-AA-E3-85	Edisa	16	9
1	Despacho	Desp 01	192.168.1.17/24	00-20-2A-D0-FD-76	Edisa	17	11
2	Soporte Técnico	ST01	192.168.1.18/24	87-60-ET-98-00-E0	Edisa	18	15
1	Servidor Untangle	Server 01	192.168.1.2/24	00-02-B3-AL-CA-3E	Edisa	2	3

Tabla 3. Estructura de la red

11.4.1 Ubicación de las computadoras dentro de la empresa Edisa

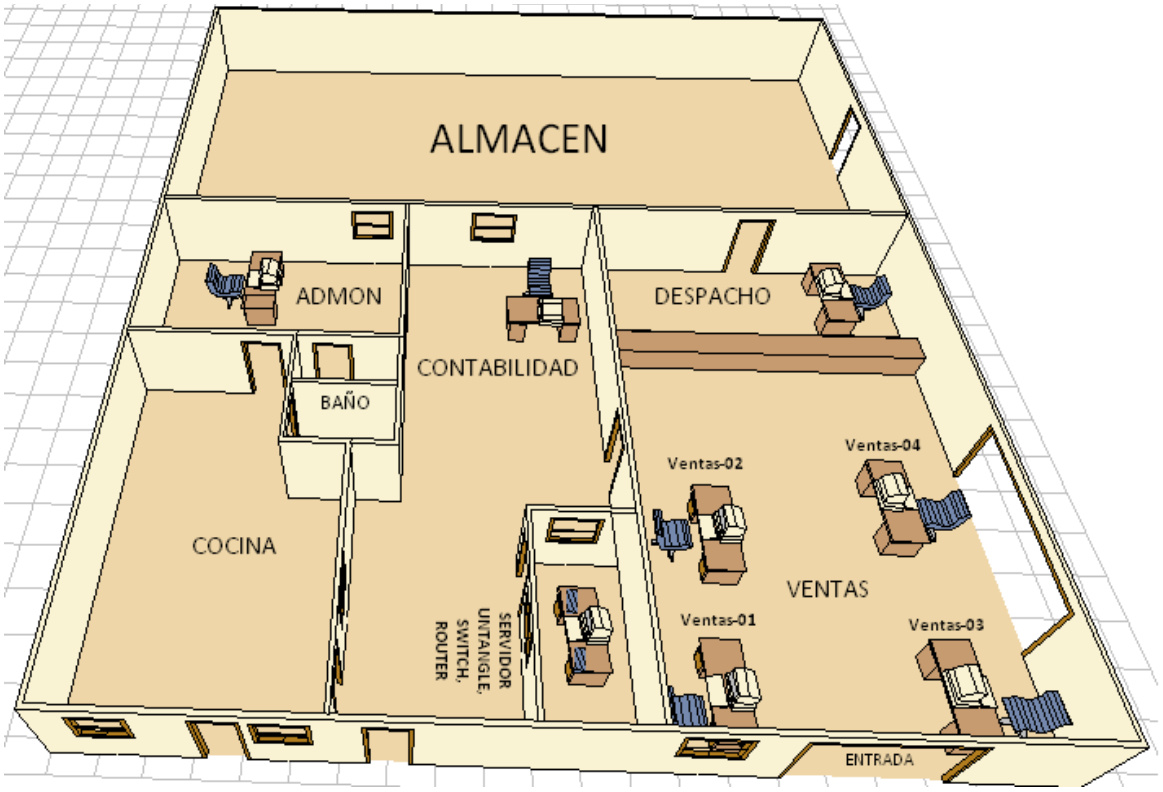

Figura 8. Esquema de la localización de cada computadora en el edificio de la empresa Edisa.

11.4.2 Estructura donde se Localiza las áreas de mantenimiento y reparación de Edisa.

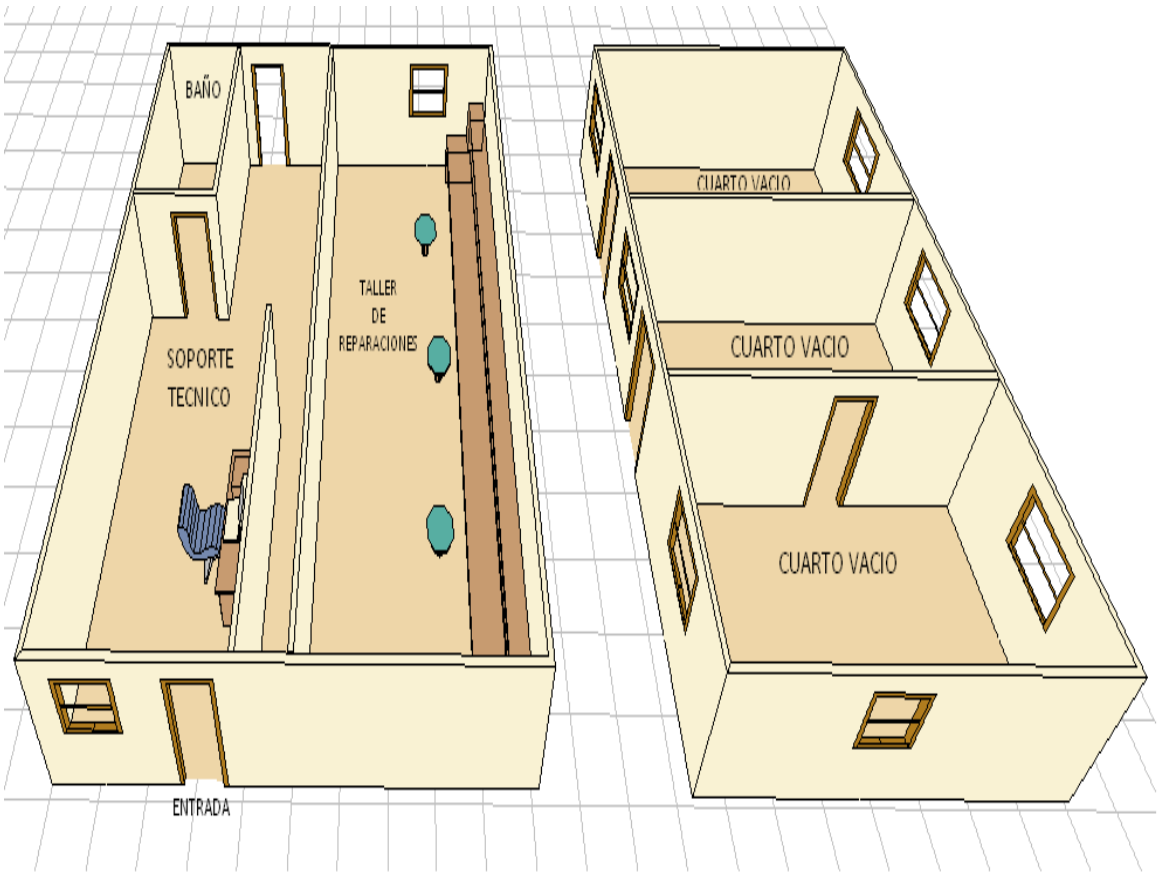

Figura 9. Áreas de mantenimiento y reparación

11.4.3 Estructura de Red Workgroups:

La red de la empresa EDISA funciona como una red Workgroups que le permite a las computadoras actuar como clientes y servidores al mismo tiempo. Los sistemas Workgroups garantizan menos costos que los sistemas basados en servidores, pero poseen más restricciones, especialmente en el aspecto del desempeño y del número de usuarios. La red de EDISA está formada por un pequeño número de computadoras 8 en total, en contraposición a los sistemas basados en servidores que normalmente conectan más de 20 computadoras.

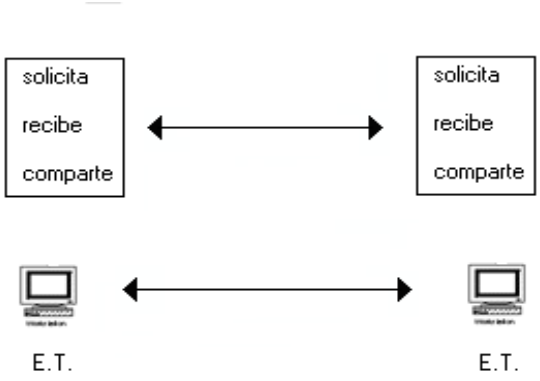

Figura 10. Modo de intercambio de información en una red Workgroups

11.4.4 Sistema operativo empleado para este grupo de trabajo:

El sistema operativo actualmente empleado en los ordenadores de la red es Microsoft Windows XP Profesional. El uso del ancho de banda bajo este sistema es optimizado por medio de la conectividad entre los usuarios, pueden compartir archivos de cualquier tipo (audio, video y software, etc.).

11.4.5 Servidor Untangle Instalado en Edisa:

Debido que el servidor proporciona centralización de la gestión de la información y la separación de responsabilidades, lo que facilita y clarifica el diseño del sistema. Como sabemos por medio del servidor Untangle podemos manejar diversos protocolos tales como SMTP, POP, IMAP, etc.

Cuando hablamos de la centralización nos referimos a los accesos, recursos y la integridad de los datos controlados por el servidor Untangle de forma que un programa de un cliente defectuoso o no autorizado pueda dañar el sistema. Además con el uso del servidor en la red se puede aumentar la capacidad de los clientes, puesto que solamente se usa para las tareas relacionadas directamente con la red y se elimina la sobrecarga adicional que se produce al emplearla como grupo de trabajo, en consecuencia se puede optimizar su rendimiento. Esto significa que todas las gestiones que se hagan en la red se concentraran en nuestro servidor Untangle, de manera que en él se disponen los requerimientos provenientes de los clientes, los archivos que son de uso público para la empresa, los que son de uso restringido, los archivos que son de solo lectura y los que, por el contrario, pueden ser modificados. El tipo de red con topología en estrella utilizado realiza funciones que están bien definidas. Para verificar la tasa de transferencia de datos disponible antes y después de instalar el servidor Untangle en la red se ha recurrido a la utilización de un test de velocidad online el cual nos proporcionará la velocidad de transferencia en Mbps disponible, así como la velocidad de respuesta del servidor a la petición del usuario.

Después del análisis de la red el siguiente paso a seguir fue la obtención del software la que se descargo del sitio web de Untangle y se creó el archivo siguiente:

Nombre archivo (disco): untangle_920_x32.ISO
Nombre Del Equipo: Proyecto Untangle
Sistema Operativo: DEBIAN Linux (32-bit)

En la tabla 4 se especifica las características del hardware que se implemento, este tipo de hardware puede variar dependiendo de la cantidad de usuarios a los que se quiera brindar atención con este servidor, en nuestro caso la cantidad de computadoras que se pretende dar servicio son 8.

Información Hardware del Servidor utilizado en este proyecto:

Número de Usuarios	Procesador	Memoria RAM	Disco Duro	Tarjetas de RED
1 a 50	Intel Pentium 4 – 2.4 GHz	1 GB	80 GB	2

Tabla 4

11.5 Topología de la Red EDISA con el servidor Untangle Incorporado

El siguiente paso en el trabajo fue la instalación del servidor en la red de la empresa como se señalo anteriormente el modo de instalación será el de Router haciendo las conexiones respectivas del modem a la interfaz externa del servidor y la interfaz interna del servidor conectada al switch desde donde ahí se controlara la red LAN de la empresa Al incorporar el servidor a la red podemos observar que la estructura no sufre ninguna modificación

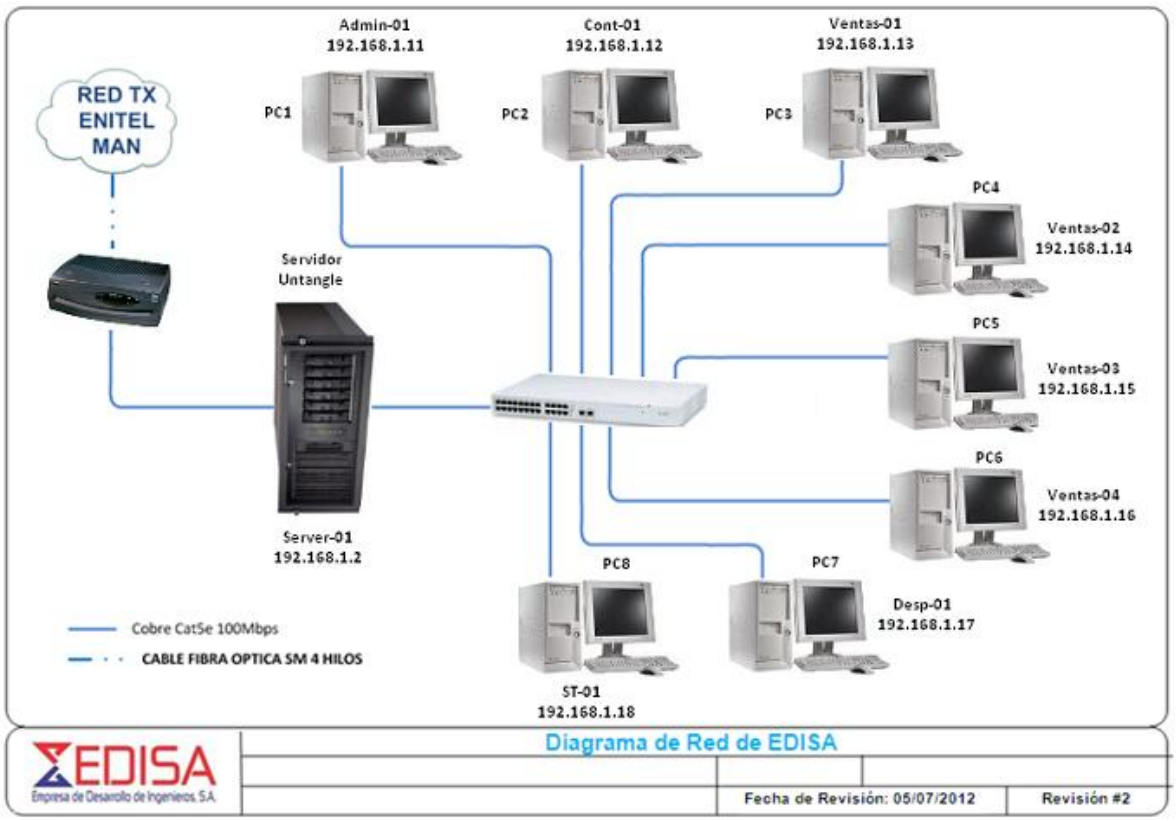

Figura 11. Topología de la red con el servidor Untangle.

11.6 Pasos para la instalación de Untangle

Para hacer más claro y detallado la investigación en el proceso de instalación del programa Untangle en la computadora o servidor dedicado, se ha recurrido a utilizar imágenes o links que se han recopilados de diferentes fuentes con ellos se tendrá una mejor explicación de cada paso que se está llevando a cabo,

A continuación presentamos las figuras respectivas de la instalación del programa.

11.6.1 Primer paso: De las cuatro opciones que observamos tomaremos la primera, instalar en modo gráfico damos Enter y continuamos.

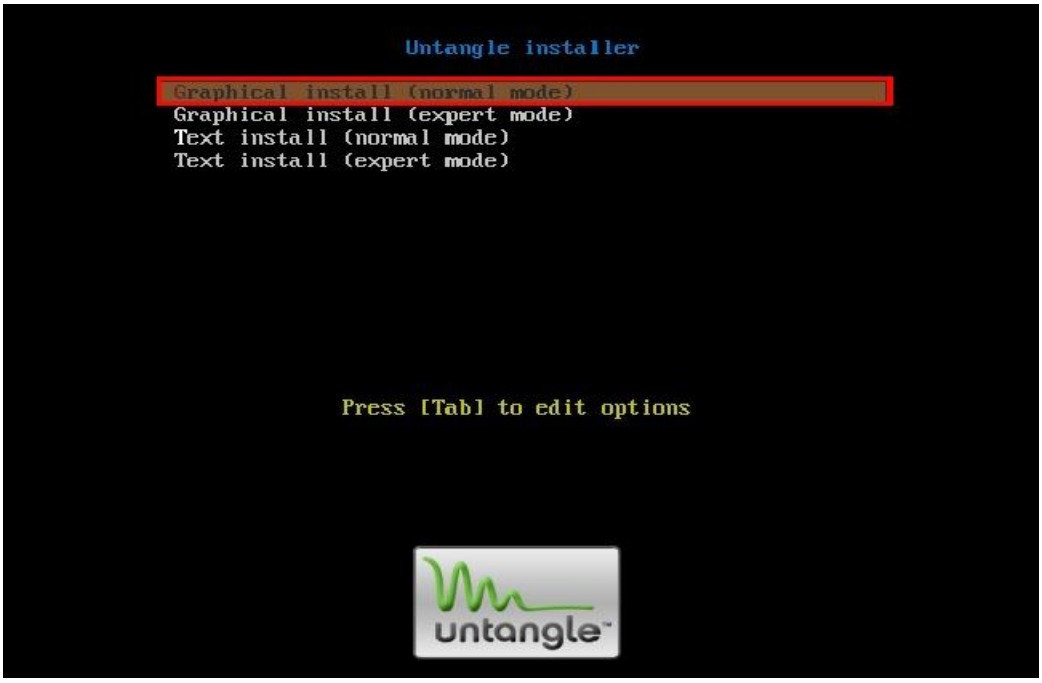

Figura 12. Interfaz gráfica para instalar Untangle (http://gnunick.blogspot.com/2011/08/).

11.6.2 Segundo paso: Aquí nos aparece la opción que dice que por favor escojamos el lenguaje a usar en el proceso de instalación. Este lenguaje no puede ser omitido porque es el lenguaje final del sistema, damos continuar y nos aparece la siguiente opción que informa que basándose en el idioma que ha elegido es probable que se encuentre en algunos de los siguientes países o regiones. Se eligira un país, territorio o área y continuamos.

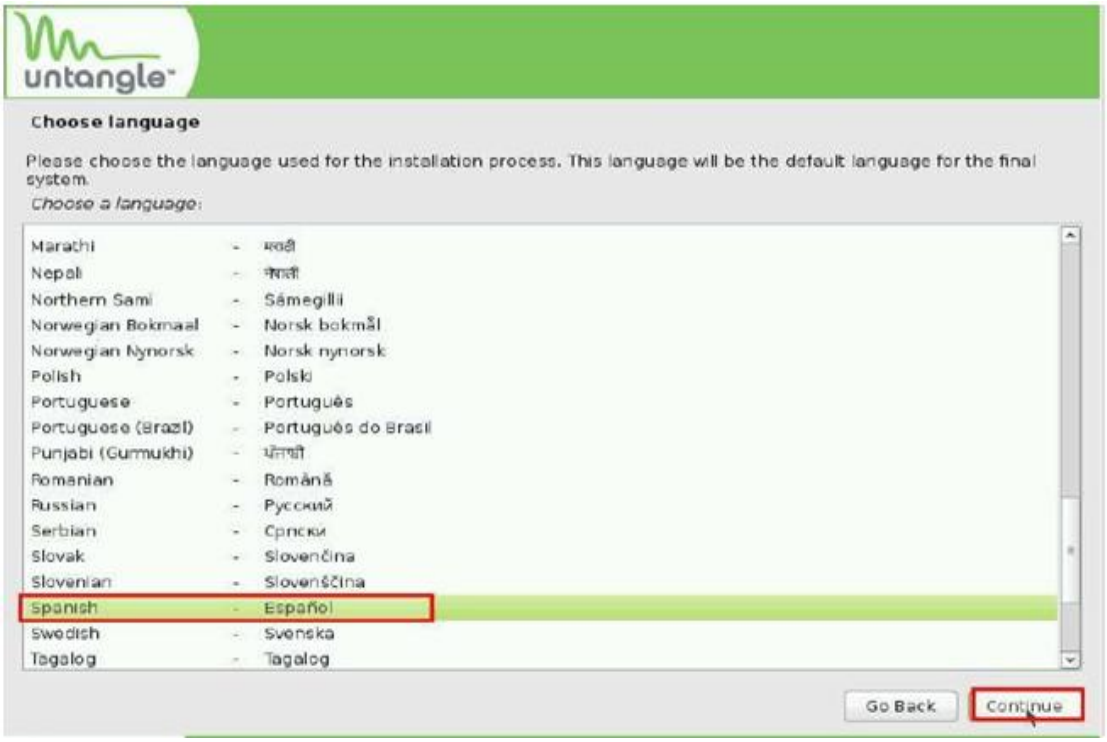

Figura 13. Idioma y país en la configuración (http://gnunick.blogspot.com/2011/08/).

11.6.3Tercer paso: Aquí podemos observar el total de memoria y la velocidad del procesador que es grande, continuamos y nos traslada a la ventana donde podemos observar mapas de teclado a usar, elegimos la distribución del teclado que vamos utilizar y le damos continuar.

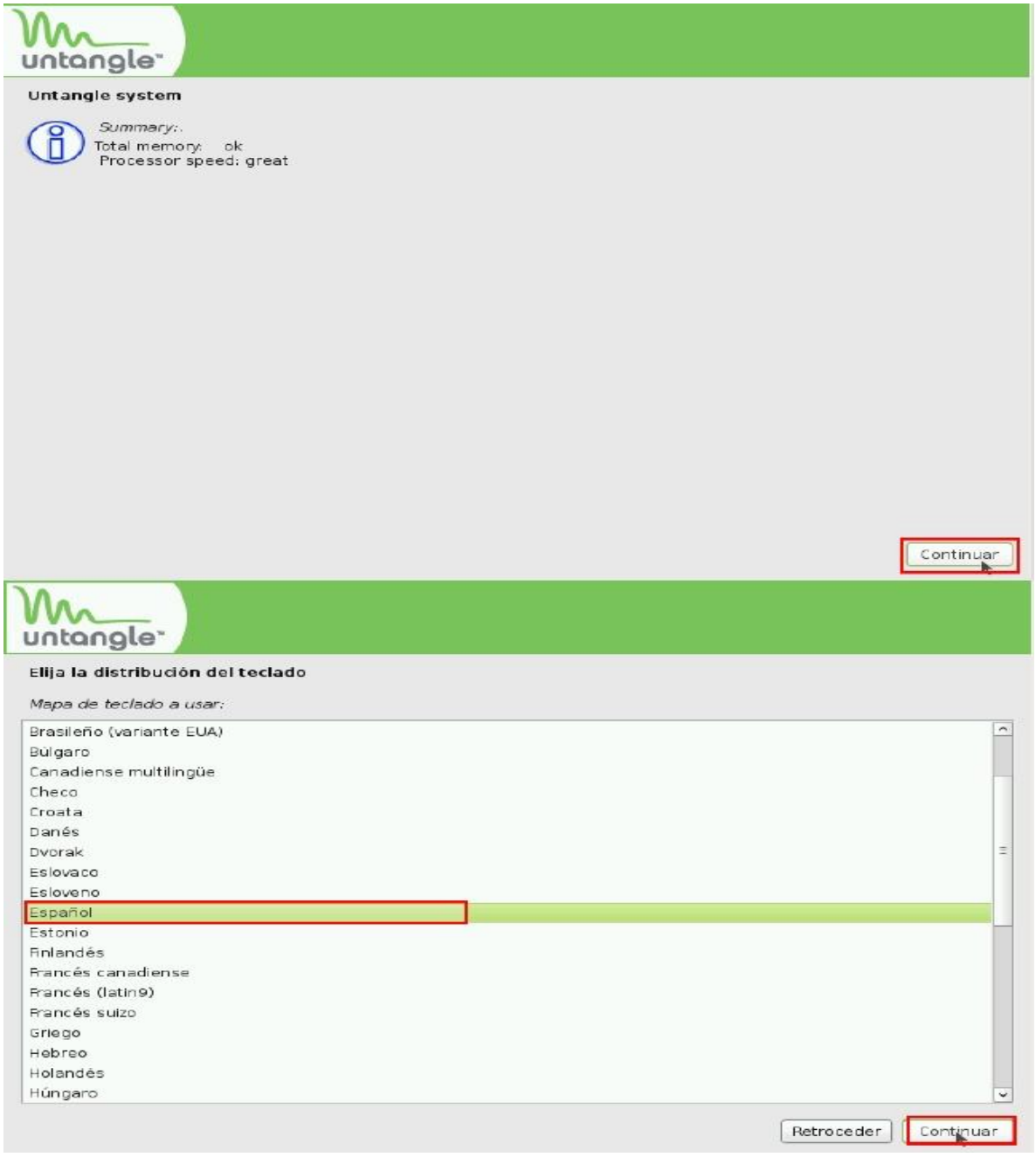

Figura 14. Distribución de teclado y total de memoria (http://gnunick.blogspot.com/2011/08/).

11.6.4 Cuarto paso: A continuación Untangle debe formatear el disco. Advirtiendo que los datos en su disco se perderán se tomara la opción que si y continuaremos. La siguiente pantalla nos informa que la instalación ha terminado. Asegúrese de extraer el disco de instalación (CD-ROM) para que el sistema arranque del disco en lugar de reiniciar la instalación.

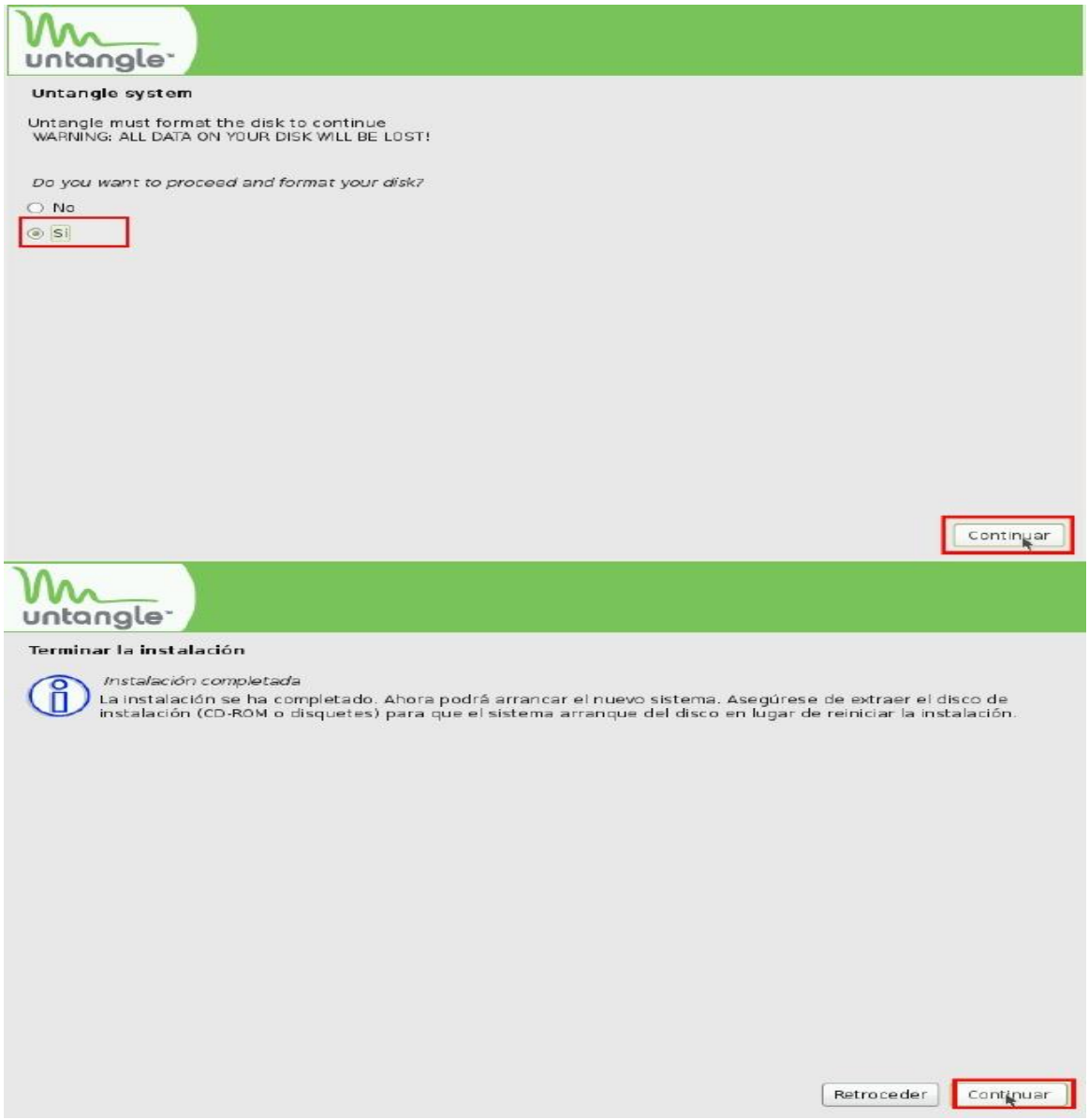

Figura 15. Formateado del disco y fin de la instalación (http://gnunick.blogspot.com/2011/08/).

11.6.5 Quinto paso: Efectuaremos las configuraciones básicas. El sistema tardara unos minutos en cargarse por ser la primera vez y aparecerá la siguiente pantalla de presentación con el logotipo de Untangle

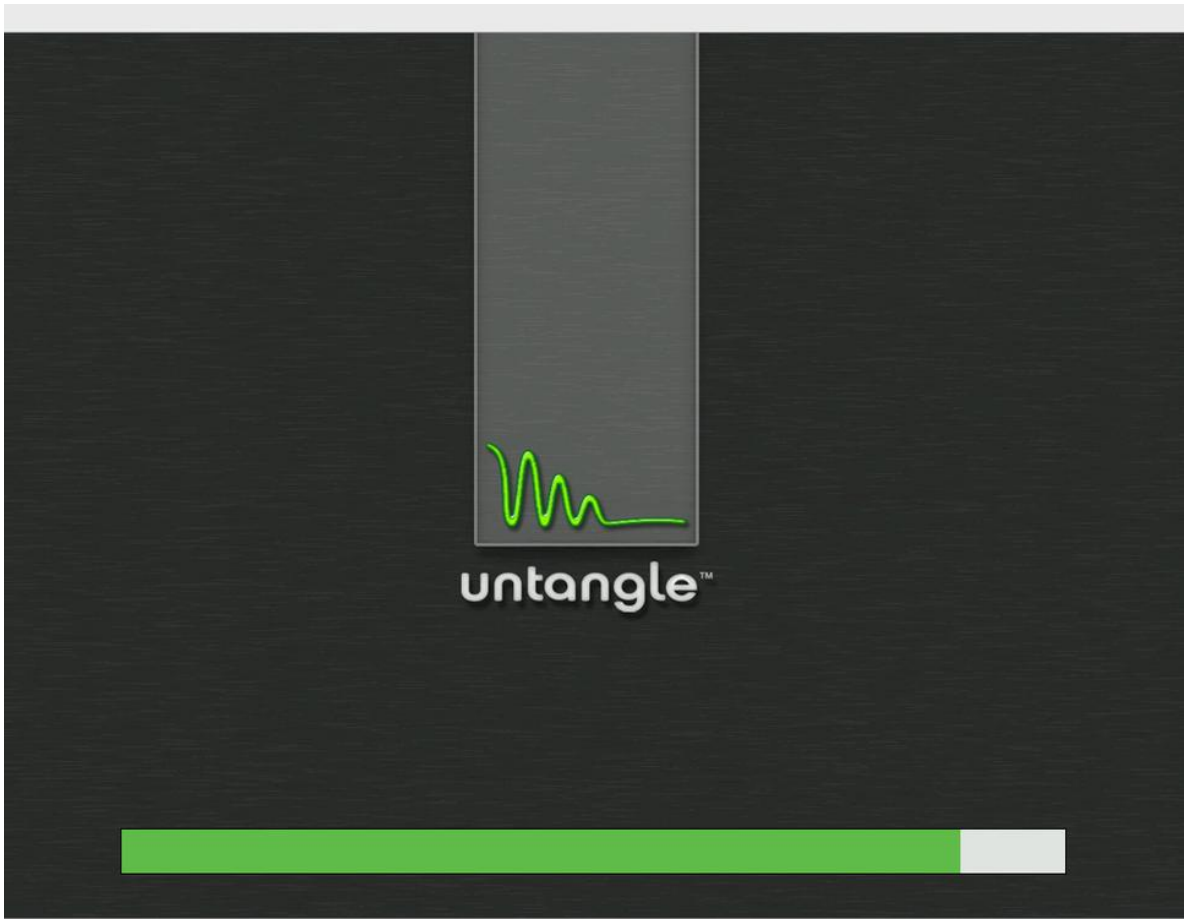

Figura 16. Presentación inicial de Untangle (http://gnunick.blogspot.com/2011/08/).

11.6.6 Sexto paso: Esta pantalla nos pide que por favor nuevamente seleccionemos el lenguaje damos siguiente. Y nos traslada a la opción, que brinda la bienvenida al Untangle. Existen varias opciones que nos guiaran atreves de la correcta instalación y configuración del servidor comenzaremos dando click en la pestaña continuar.

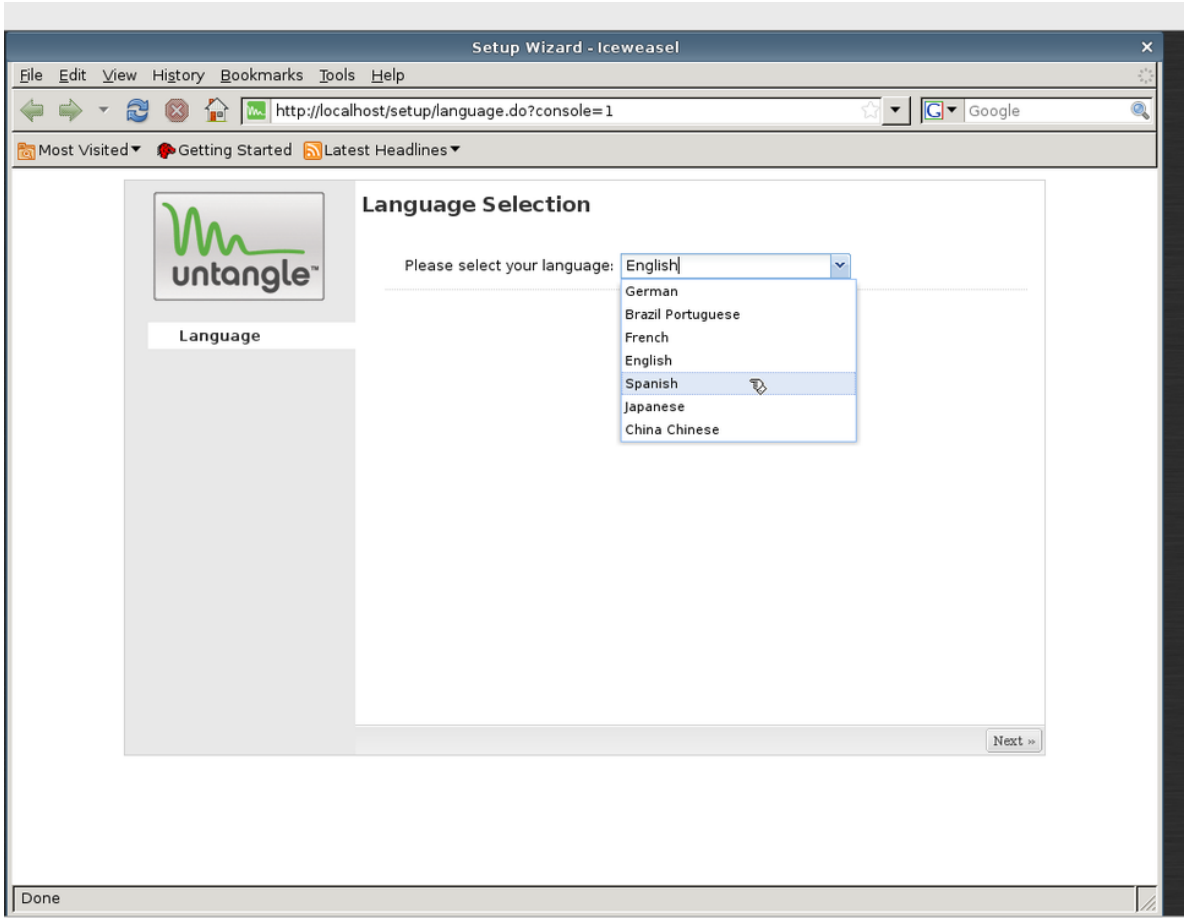

Figura 17. Lenguaje y configuraciones básicas de Untangle (http://gnunick.blogspot.com/2011/08/).

11.6.7 Séptimo paso: El asistente muestra como configurar el servidor, se escoge una contraseña para la cuenta de administrador, por defecto el inicio de sesión nos dará admin se pide una contraseña y también una confirmación por último se escogerá la zona horario y continuamos.

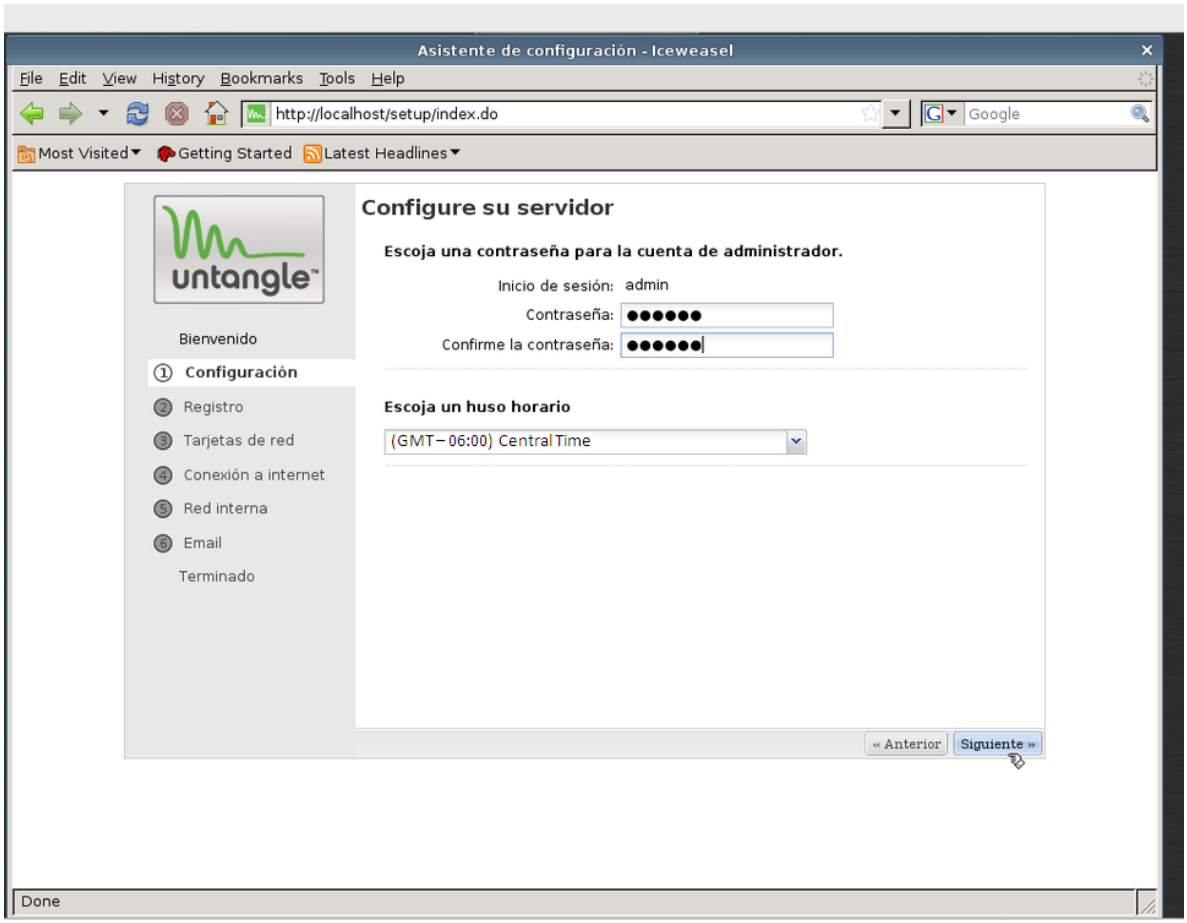

Figura 18. Configurando el servidor (http://gnunick.blogspot.com/2011/08/).

11.6.8 Octavo paso: Identificar las tarjetas de red. Este paso identifica las tarjetas de red externa e interna además de otras, conecte y active el cable en cada una de las tarjetas de red y al mismo tiempo determine cada una de las tarjetas de red a utilizar.

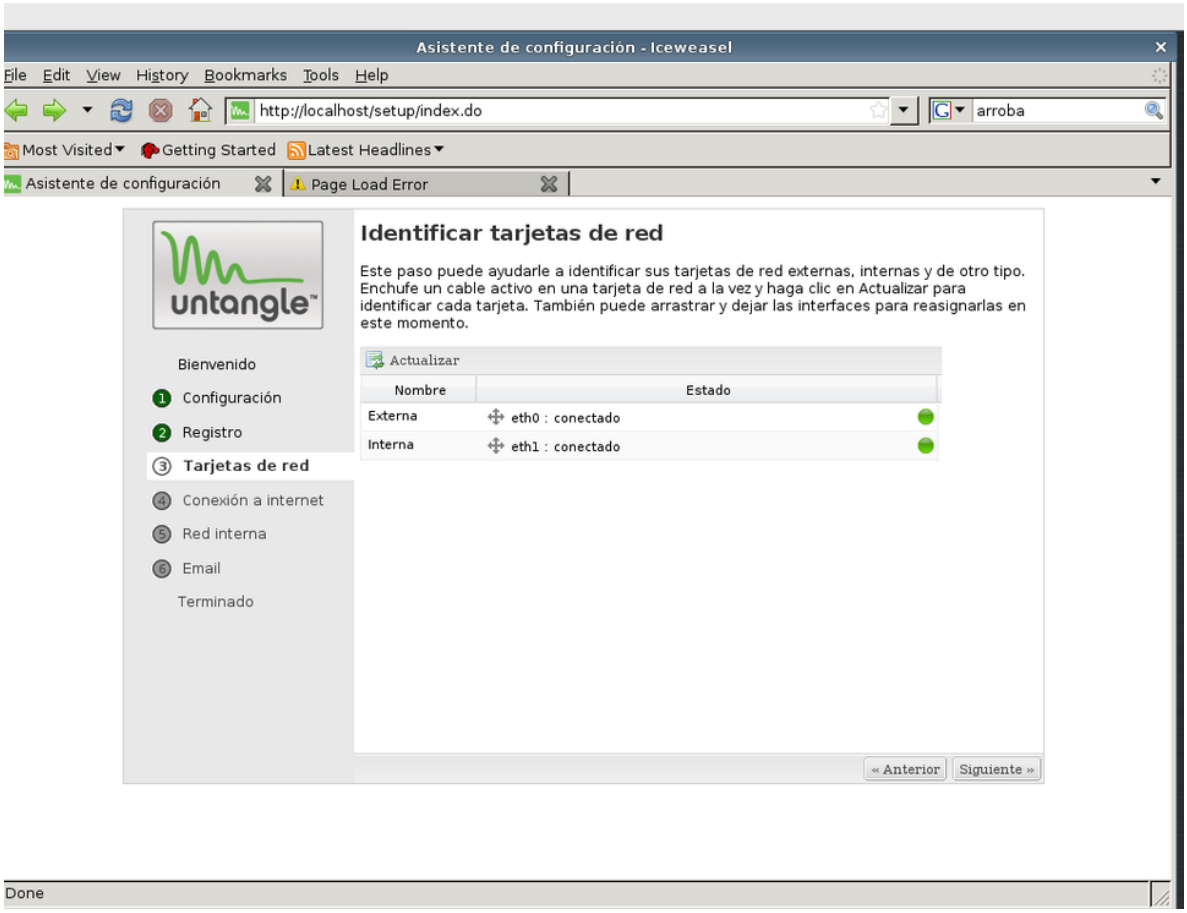

Figura 19. Identificar las tarjetas de red (http://gnunick.blogspot.com/2011/08/).

11.6.9 Noveno paso: Configure su conexión de internet. Esta pantalla nos muestra el tipo de configuración a internet, el estado del DHCP su dirección IP de mascara de red, la IP de la pasarela, del servidor DNS primario y también se probará la conectividad a internet, damos siguiente y pasamos a otro paso.

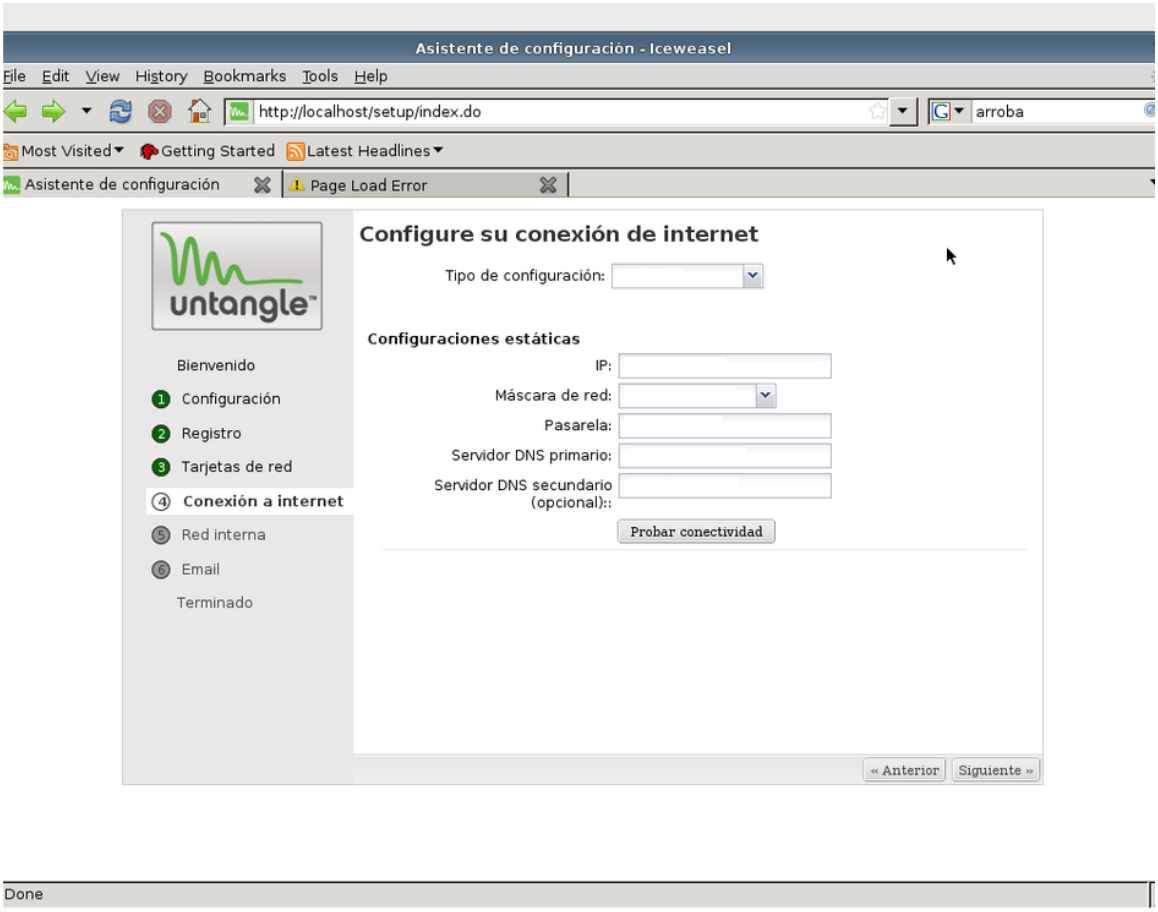

Figura 20. Configurando la conexión de internet (http://gnunick.blogspot.com/2011/08/).

11.6.10 Decimo paso: La siguiente pantalla muestra la configuración de la interfaz de la red interna, aquí nos mostrara dos opciones de configuración, uno es el puente transparente aquí se recomienda que el puerto externo esté conectado a un cortafuegos o Router. Esto establece un puente entre externo e interno desactivando el DHCP. Dos es la opción Router la que será escogida. Se recomienda que el puerto externo esté conectado a la fuente de internet, esto activa el NAT en la interfaz interna y el DHCP.

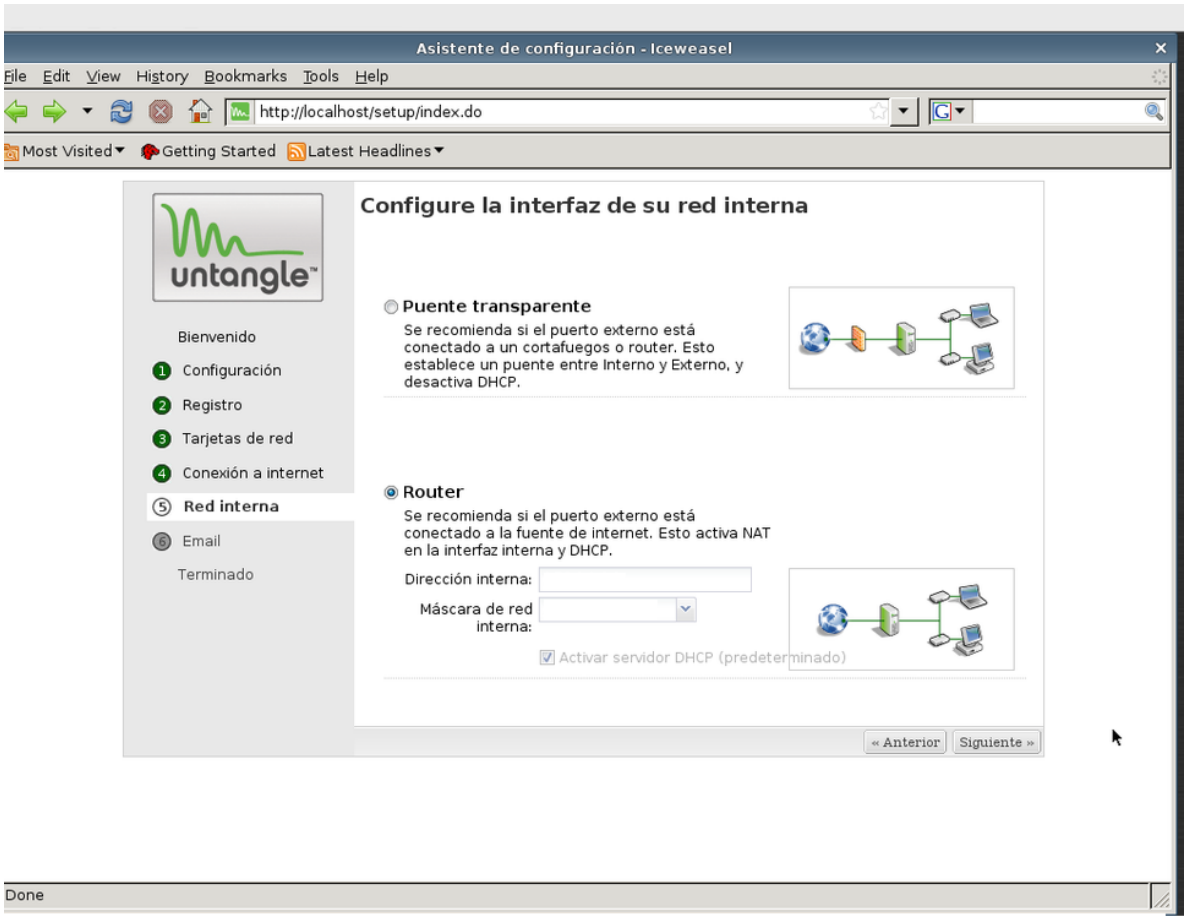

Figura 21. Configurando la red interna y asignación de las ip (http://gnunick.blogspot.com/2011/08/).

11.6.11 Decimo primer paso: Configuración de email el servidor Untangle enviara notificaciones de reportes a través de correos, luego damos click a la opción continuar.

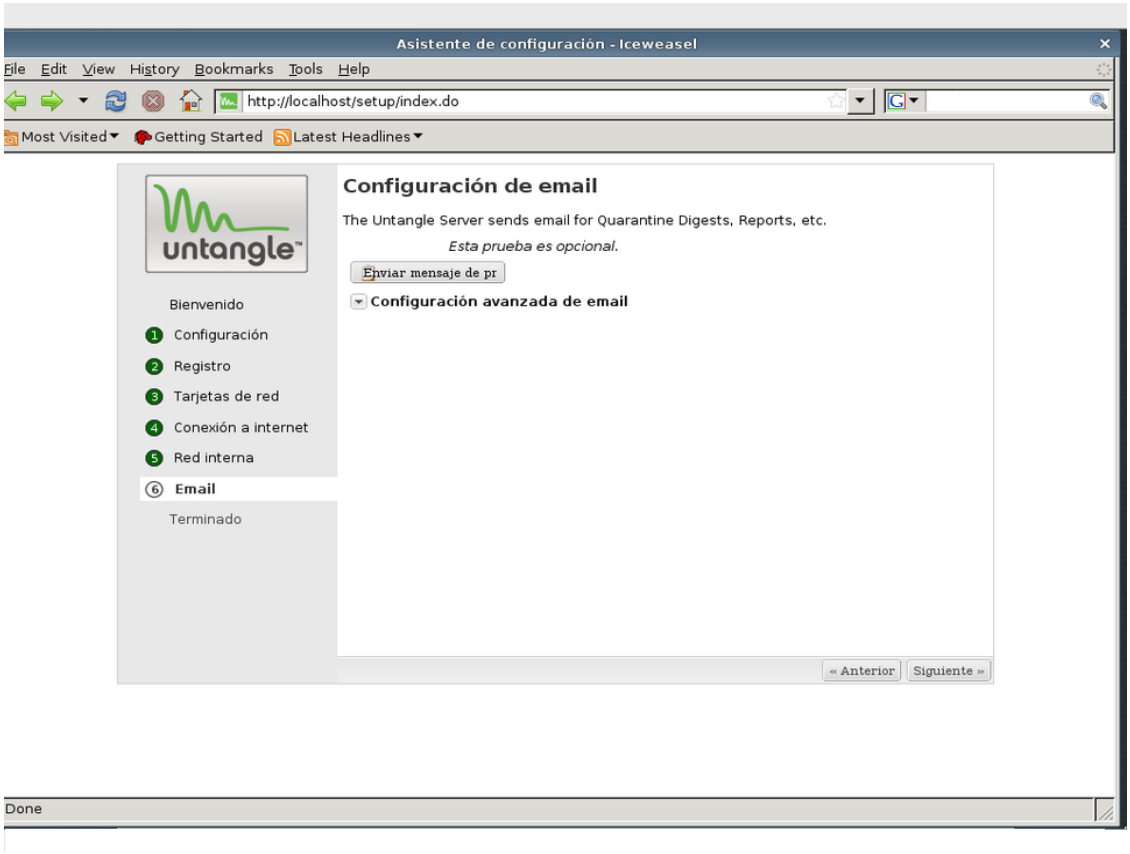

Figura 22. Configuración de email (http://gnunick.blogspot.com/2011/08/).

.

11.6.12 Decimo segundo paso: Su servidor Untangle ahora está configurado. Ahora usted está listo para descargar algunas aplicaciones.

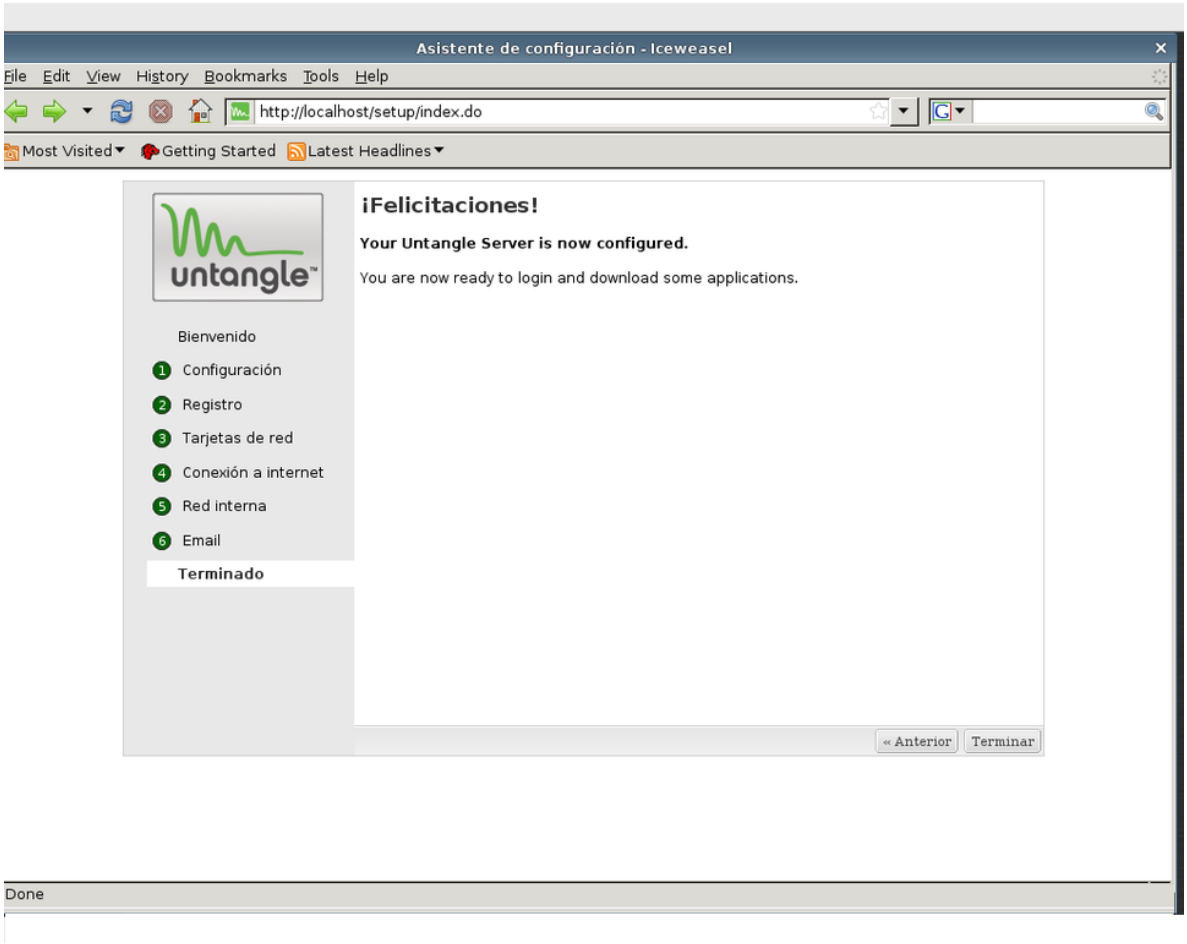

Figura 23. Finalización del proceso de instalación (http://gnunick.blogspot.com/2011/08/).

Finalizada la instalación procedemos a descargar 13 aplicaciones del paquete lite utilizando la cuenta con que descargamos el software untangle de la página, de esta forma se instalara de manera automática el ***web filter lite*** y el ***protocol control*** que son muy necesario en el proceso de configuración y de bloqueo de páginas, de diversos sitios web y puertos dentro de la red. Posteriormente se descargaran las demás aplicaciones.

Una vez realizado este proceso pasaremos a la configuración de la aplicación ***web filter lite*** que se utiliza para bloquear las páginas, los archivos y las extensiones que deseamos que el usuario no abra. Cuando entremos al botón de configuración en el ***web filter lite*** del rack podremos observar 4 pestañas que son las listas de bloqueos, listas permitidas, log de eventos y log desbloqueados, en la primera pestaña seleccionaremos la opción de páginas especiales en el cual escribiremos el nombre de paginas especificas que deseamos bloquear agregamos un comentario guardamos y continuamos con la siguiente categoría.

Editar Categorías: Muestra un listado de las categorías de páginas web a filtrar como pornografía, redes sociales y proxys en internet.

Editar Sitios: permite agregar de forma manual un sitio web para filtrar, esto mediante URL o dirección IP.

Editar tipos de archivos: Permite un filtrado de extensiones a descargar como .mp3, .exe, .mov, entre otras.

Si alguien intenta acceder a uno de los sitios web que fueron bloqueados la aplicación de reporte del Untangle registrara la IP de la computadora donde se quiso acceder a dicha página, también el reporte mostrara la cantidad de virus que han sido bloqueados. Una vez configurado el ***web filter lite*** se procedió a realizar la prueba conectando una máquina al switch la que automáticamente nos dará una IP, intentaremos entrar al sitio web que había sido bloqueado, al querer acceder a dicha pagina nos aparece un mensaje que indica que dicha sitio a sido bloqueado lo cual indica que la prueba realizada resulto positivo y el servidor está trabajando de forma correcta.

11.7 Pruebas de ancho de banda:

Se realizaron pruebas de ancho de banda en los siguientes escenarios:

1. La siguiente medición se realizó antes de la incorporación del servidor Untangle.

   - Se tomó 01 muestra de velocidad en el usuario 01 de ventas.
   - El ancho de banda suministrado por el ISP es de 2Mbps.
   - La medición fue realizada a través del sitio web: **http://www.bandwidthplace.com**

Resultados de la medición:

Figura 24. Test de velocidad antes del instalar el servidor

Como podemos observar la velocidad de bajada o descarga es de 1.8 Mbps y la velocidad de subida o carga es de 1Mbps, el tiempo de respuesta es de 31 ms.

2. La siguiente medición se realizó luego de la incorporación del servidor Untangle, con todas las aplicaciones *lite* en ejecución.

   - Se tomó 01 muestra de velocidad en el usuario 01 de ventas.
   - El ancho de banda suministrado por el ISP es de 2Mbps.
   - La medición fue realizada a través del sitio web:

http://www.bandwidthplace.com

Resultados de la medición:

Figura 25. Test de velocidad después de instalar el servidor Untangle

Con el servidor instalado podemos ver que la velocidad de bajada o descarga es de 1.6 Mbps y la velocidad de subida es de 1 Mbps

Como podemos observar en la primera medición sin el servidor Untangle, hay una pequeña pérdida de 0.2Mbps, esto se debe a que generalmente el ancho de banda que ofrece el ISP o la velocidad que la empresa contrató, no es completamente exacta, es muy común que hayan perdidas, debido a la atenuación e interferencias que perjudican la señal.Como podemos observar en la segunda medición una vez incorporado el servidor Untangle, con todas las aplicaciones *lite* en ejecución logramos apreciar un mínimo de pérdida de 0.2Mbps, el cual no es muy significativo con respecto a la primera medición.

La medición realizada antes de la incorporación del servidor Untangle a la red, comparada con la segunda medición una vez incorporado el servidor Untangle, no es muy significativa, ya que hay una diferencia de 0.2 Mbps antes y después, con los resultados antes obtenidos logramos corroborar que el ancho de banda se mantiene bastante estable y que la incorporación del servidor y la ejecución de las aplicaciones no afectan significativamente el ancho de banda en la red.

Las mediciones antes expuestas (primera y segunda) son muestras que se tomaron fuera de horario laboral, se realizaron a esta hora con el objetivo de obtener un resultado más preciso, cabe señalar que estas mediciones tienden a sufrir cambios de acuerdo a las aplicaciones de trabajo que estén siendo ejecutadas por el usuario.

Capitulo XII

Conclusiones

- El presente trabajo se efectuó de forma práctica en la empresa EDISA donde se instalo por un corto periodo de tiempo de 72 horas el servidor.
- Se realizo un análisis general de la red de la empresa, donde se pudo determinar el tipo de topología, la cantidad de usuarios así como las características de los equipos.
- Se logro incorporar el servidor a la red, la estructura de la red no sufrió grandes cambios ya que el servidor Untangle se utilizo en modo Router colocado entre el modem y el switch.
- Se realizo la debida instalación y configuración del software Untangle, también se utilizaron las aplicaciones de filtrado sin costo.
- Para lograr la implementación del servidor Untangle utilizamos un ordenador personal con las características recomendadas por el fabricante del software Untangle, sus aplicaciones Lite fueron descargados gratuitamente desde la página principal.
- Mediante el reporte generado por Untangle se lograron recopilar datos los cuales nos ayudaron a conocer la cantidad de incidencias en la red.
- Logramos efectuar las mediciones de la transferencia de datos mediante un test de velocidad de carga y descarga de información para conocer los cambios que sufre el ancho de banda de la red antes y después de la instalación del servidor. Se observa una diferencia de 0.2 Mbps.

Capitulo XIII

Recomendaciones

- El periodo de tiempo para la práctica tiene que ser mayor para verificar más detalladamente el funcionamiento del servidor y observar el máximo rendimiento de todas las aplicaciones.
- Este software también trae una versión para Windows el que se puede instalar como una aplicación más, soporta todas las versiones de XP y vista. Para la versión sistema operativo es como instalar una distribución Debían.
- El servidor empleado en el proyecto opera con dos tarjetas de red, pero si queremos añadir un servidor mas como el DMZ podemos agregarle otra tarjeta.
- Para el proyecto fue empleado una computadora con características mínimas que exige el los fabricante en cuanto hardware, pero se pueden utilizar computadoras con mayores recursos para satisfacer necesidades de empresa mas grandes.
- Para que la empresa pueda obtener todos los beneficios de seguridad y fácil manejo administrativo recomendamos la instalación pronta del servidor.

Bibliografía

- **Sitios de internet**

http://www.es.wikipedia.org

http://www.tecnologiapyme.com

www.untangle.com

http://www.solinux.es

http://www.es.wikipedia.org/wiki/C%/C3%B3digo_abierto,2011

http://www.es.wikipedia.org/wiki/Virus_inform%C3%A1tico

http://www.todo-redes.com/gateway-puerta-de-enlace.html

http://www.salixnetworks.com/filtrado_web.html

http://www.alegsa.com.ar/dic/servidor.php

http://www.solinux.es/2011/untangle-seguridad-para-redes

http://gnunick.blogspot.com/2011/08/untangle-configurando-proxy-web-filter.html

Anexos

Tabla de Costos

- **Compra de Equipo**:

ITEM	PRODUCTO	CANTIDAD	PRECIO
1	Equipo Dual Core 2.6 GHz/2GB RAM/500GB DD/DVDRW/CARD	1	7,169.82
2	Monitor LED AOC 18.5" 1366X768 E950SWN	1	2,668.02
3	Encore Tarjeta de RED 10/100 ENL832-TX-RE	1	108.72
4	UPS FPC Full Power 600VA 1050DS	1	920.4
5	CAP Escritorio "Z"C/TOP Negril CAP-0D-210CY	1	516.29
6	New Link Patch Cord CAT 6A, 50 UM, 7 FT Blue 16607BL	1	184.37
		Precio Bruto:	11,567.62
		Descuento:	285.86
		Impuesto de Venta:	1,692.27
		Precio Neto:	12,974.03

- **Otros Costos:**

ITEM	SERVICIO	CANTIDAD	PRECIO
1	Instalación y Configuración del Servidor	1	3995 CS
1	Mantenimiento Preventivo (Cada 3 Meses)	1	587.5.00 CS
		Precio Bruto:	4582.5 CS
		Impuesto	687.375 CS
		Precio Neto:	5269.875 CS

Beneficios que ofrece Untangle:

- Evitar amenazas que provienen de Internet como virus, Spam, Spyware o intentos de conexiones fraudulentas no autorizadas, etc.
- Aumentar la productividad de sus empleados restringiendo el acceso a sitios web con contenido no deseado tales como: redes sociales, juegos online, pornografía, etc.
- Evitar el uso y descarga de programas que consumen el ancho de banda de la red, tales como: programas de descarga de archivos, descarga de música y videos, etc.
- Favorecer la movilidad del administrador de la red permitiéndole acceder de forma remota mediante Redes Privadas Virtuales a los recursos de su red.
- Monitorear el comportamiento de los usuarios por medio de un reporte de incidentes en la red.
- controlar el tráfico de Internet de su negocio.

Tabla de actividades necesarias para llevar a cabo el proyecto

			Tiempo dado en días		
	Actividad	Precedencia	Tiempo optimista	Tiempo probable	Tiempo pesimista.
A	Evaluar red local		1	2	4
B	Acondicionar el local	A	0.5	1	3
C	Compra de equipos	A,B	1	2	3
D	Ubicación e instalación	B,C	0.5	1	2
E	Configuración del servidor	D	1	2	3
F	Pruebas de configuración	E	1	2	3

CONTROL

MANUAL DEL USUARIO

untangle™

Tabla de Contenidos:

Capitulo 5: Aplicaciones de Untangle

5.1 Tipos de aplicaciones
5.1.2 Aplicaciones de filtro
5.1.3 Aplicaciones de servicios
5.2. Descarga de aplicaciones
5.3. Aplicaciones gratis de Untangle (Lite package)
5.3.1. Web Filter Lite
5.3.2 Protocol Control
5.3.3 Virus Blocker Lite
5.3.4 Spyware Blocker
5.3.5 Phish Blocker
5.3.6 Intrusion Prevention
5.3.7 Firewall
5.3.8 OpenVPN
5.3.9 Reports:
5.3.10 Spam Blocker Lite
5.3.11. Ad Blocker
5.4 Aplicaciones de pago:
5.4.1. Web Filter:
5.4.2. Kaspersky Virus Blocker:
5.4.3. Virus blocker: Ver virus blocker lite
5.4.3 Spam Blocker: Ver spam blocker lite
5.4.5 Web Cache:
5.4.6 Bandwith Control:
5.4.7 Policy Manager:
5.4.8 Directory Connector:
5.4.9 WAN Failover
5.4.10 WAN Balancer
5.4.11 IP sec VPN:
5.4.12 Configuration backup:
5.4.13 Branding Manager
5.4.14 Live Support
5.4.15 Commtouch Spam Policy Manager
5.4.16 AD Connector
5.4.17 PC Remote
5.4.18 Remote Access Portal
5.4.19 QoS

Capitulo 6: Trabajando con Untangle

6.1. Administración de Untangle
6.1.1. Local
6.1.2. En la Re d LAN
6.1.3. Remoto: 6.2. La WebGui

Capitulo 7: Configuración Untangle

7.1. Networking
7.1.2 Port Forwards
7.1.3 Hostname
7.1.4 DHCP Server
7.1.5 DNS Server
7.1.6 Troubleshooting
7.1.7. Advanced
7.1.7.1. General
7.1.7.2. Send ICMP Redirects:
7.1.7.3. Enable SIP Helper:
7.1.7.4. Administration overrides Port Forwards: This setting will cause the current
7.1.7.5. Only NAT WAN traffic:
7.1.7.6. Bypass Rules
7.1.7.7. Packet Filter
7.1.7.8. QoS
7.1.7.9. ARP
7.1.7.10. Routes
7.1.7.11. Local DNS
7.1.7.12. DHCP & DNS
7.1.7.13. Overrides
7.2. Administration
7.2.1. Administration
7.2.2. Public Address
7.2.3. Certificates
7.2.4. Monitoring
7.2.5. Skins
7.3. Email
7.3.1. Outgoing Server
7.3.2. From-Safe List

7.3.2. Quarantine

7.4. Local Directory
7.5. Upgrade
7.6. System
7.6.1 Support
7.6.2 Backup
7.6.3 Restore
7.6.4. Protocol Settings
7.6.5 Regional Settings
7.7. System Info
7.7.1. Version
7.7.2. Registration
7.7.3. Licenses
7.7.4. License Agreement

Capitulo 1: Bienvenido a Untangle:

Gracias por adquirir Untangle, este capítulo ofrece una visión General del proyecto.

1.1. ¿Qué es Untangle?

Es un sistema que ofrece una pasarela de red (network gateway) de código abierto para pequeñas empresas. Untangle ofrece muchas aplicaciones como el bloqueo de correo electrónico no solicitado (spam), bloqueo de software malicioso (malware), filtrado de web, protección contra robo de información sensible (phishing), prevención de intrusiones y más sobre la Plataforma Untangle Gateway.

1.2 . ¿Qué es Código Abierto?

Es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales las cuales destacan en el llamado software libre.

1.3 . ¿Cómo obtener Untangle?

1. Visitar http:/www.untangle.com/Downloads/Download-ISO
2. Seleccionar la versión 32 o 64 bits e iniciar la descarga
3. Grabar la información descargada en un CD

1.4 . Estructura de este Documento

Este documento se ha elaborado para servir de manual para aquellos que usen Untangle por primera vez. Se intenta hacer la menor cantidad de presunciones posibles acerca de su nivel técnico a nivel de configuración. En cualquier caso, se da por hecho un conocimiento general de uso y también los requerimientos de hardware para llevar a cabo la instalación.

Los usuarios expertos pueden encontrar también interesante la información de referencia de este documento, ya que incluye los requerimientos mínimos de hardware para la instalación del sistema Untangle y sus aplicaciones.

En general, este manual está dispuesto de forma lineal guiando al usuario a través del proceso de instalación de Untangle desde el principio hasta el final.

1.5 . Copyright y Licencias de Software:

Seguramente ha leído las licencias que acompañan a la mayoría del software comercial, generalmente afirman que sólo puede usar una copia del software en un único equipo. La licencia de Untangle Debían GNU/Linux no es como éstas, puede hacer miles de copias aunque con algunas restricciones. Esto es posible gracias a que Untangle trabaja bajo la plataforma de Debían el cual está basado en *software libre*.

Software *libre* no quiere decir que éste carezca de copyright, ni tampoco que el CD con este software se deba distribuir sin costos. Software libre, en parte, significa que las licencias de los programas individuales no requieren de ningún pago por el derecho de distribución o uso de los mismos. También significa que cualquiera puede extender, adaptar y modificar este software, así como distribuir los resultados de su propio trabajo.

1.6 . Copyright de este Documento

El presente documento fue doblado al español en un 70% de su contenido, la información que se muestra en este documento fue tomada en su totalidad de la página oficial de Untangle www.untangle.com , Este manual es software libre, puede redistribuirlo y/o modificarlo bajo los términos de la licencia general pública GNU.

Capitulo 2: Tipos de Configuraciones

2.1. Ubicación de Untangle en su red:

Untangle es un dispositivo en línea, esto significa que únicamente el tráfico que fluye a través de él es filtrado. Existen 2 modos disponibles de operación de untangle:

- ***Modo Router***
- ***Modo Puente (Bridge).***

2.2. Modo Router:

En Modo ***Router,*** Untangle será el dispositivo de borde en la red y servir como un router y firewall. En este caso, tendrá que configurar las interfaces externas e internas correctamente para que el tráfico fluya, que se debería haber hecho durante la instalación, en la Figura 1 podemos apreciar el servidor Untangle instalado en modo Router.

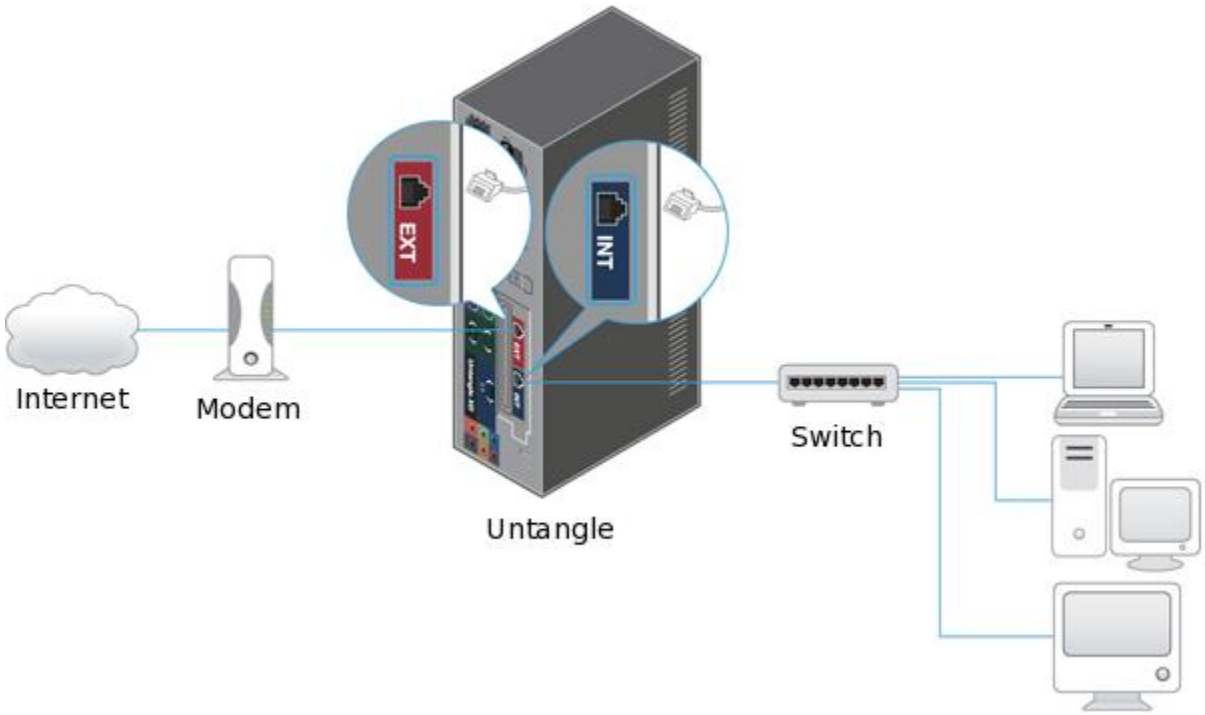

Figura 1: Servidor Untangle en modo Router.

2.3. Modo Puente (Bridge):

En modo Puente, el servidor Untangle es instalado entre el firewall existente y el switch principal, cuando el servidor Untangle está en modo Puente el servidor Untangle es transparente, esto significa que usted no necesitara cambiar la configuración por defecto de la puerta de enlace (Gateway) de las computadoras de su red o las rutas en su firewall, simplemente coloque el servidor Untangle entre su firewall y el switch principal y eso es

todo, usted podría necesitar dar una IP en la interfaz externa en la subred del firewall, ponga la interface interna en el puente y el puente en la externa. Si usted tiene una red compleja, usted puede necesitar agregar rutas estáticas a untangle , para saber donde se envía el trafico para ciertas subred, en la figura 2 podemos apreciar al servidor untangle instalado en modo puente.

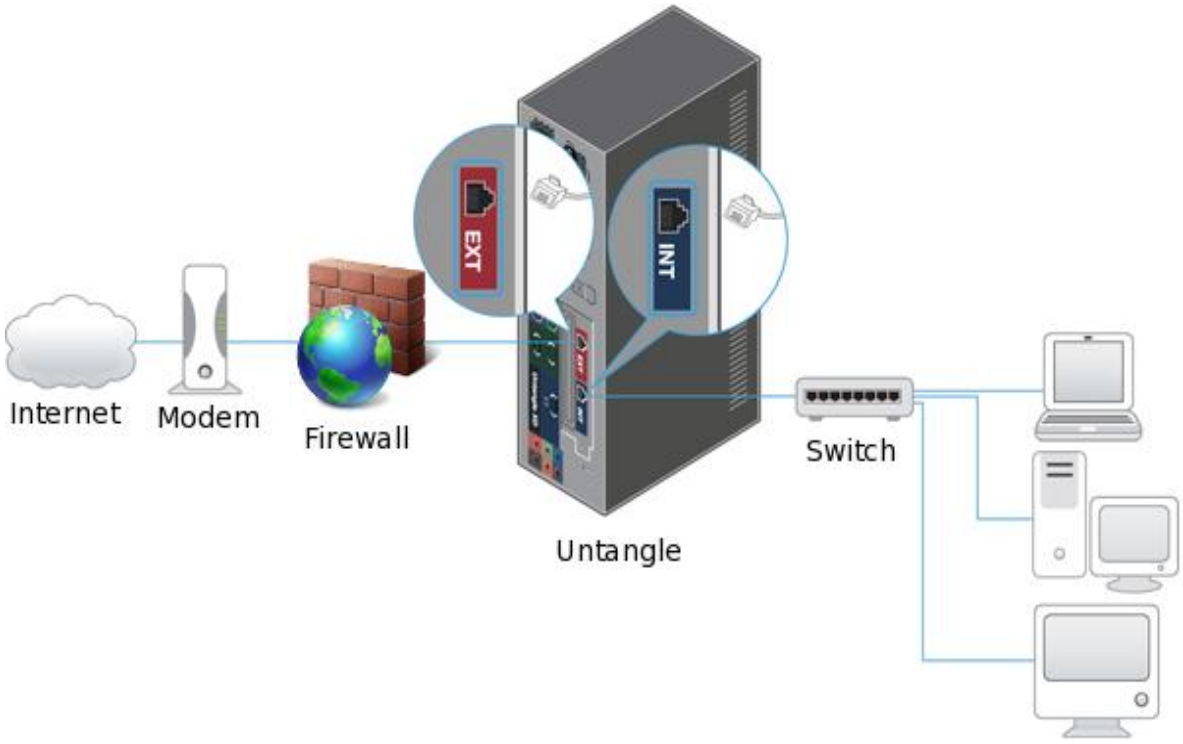

Figura 2: Servidor Untangle en modo Puente.

2.4. Notas Importantes:

- Si usted está teniendo problemas de conectividad, usted puede intentar conectar un cable crossover entre el servidor untangle y el dispositivo, esto es usualmente no necesario con equipos modernos, pero esto es algo que se puede probar si la configuración luce bien pero esto es simplemente si no está trabajando. Si usted no tiene un cable crossover a mano, intente colocar un switch entre el servidor Untangle y el dispositivo.

- Si usted quiere instalar Untangle en una Maquina Virtual, Recomendamos leer esta guía.
- Si usted está en modo de Router y tiene una conexión PPPoE (protocolo punto a punto sobre Ethernet) WAN, contacte a su ISP y vea si el modem puede hacer la autenticación y pase los IPs al servidor Untangle, entonces usted puede configurar la interfaz externa como estática, esta es una situación mucho mejor que estando el servidor Untangle con conexión PPPoE ingresado, desde algunas características (tales como multi-WAN) no podría trabajar con interfaz configurada como PPPoE.
- Si usted está en modo puente es muy probable que usted no quiera tener una doble NAT por lo tanto asegúrese que su interfaz interna este instalado al puente y no al DHCP.

Capitulo 3: Requisitos del Sistema

3.1. Requerimientos de Hardware:

- El servidor Untangle requiere un ordenador dedicado instalado en el GATEWAY de su RED.
- Su hardware no necesita un sistema operativo, el servidor Untangle instala su propio sistema operativo.
- En el proceso de instalación se borra cualquier información almacenada en el disco duro del ordenador.

3.2. Recomendaciones de Hardware:

Número de usuarios	Procesador	Memoria	Disco Duro	Tarjetas de Red	Notas
Mínimo	Intel / AMD compatible con el procesador (800 + MHz)	512 MB	20 GB	2	32-bits
1-50	Pentium 4 equivalente o superior	1 GB	80 GB	2 o más	32-bits
51-150	Dual Core	2 GB	80 GB	2 o más	32- bits
151-500	2 o más núcleos	2 o más GB	80 GB	2 o más	32-bits
501-1500	4 núcleos	4 GB	80 GB	2 o más	64-bits
1501-5000	4 núcleos o mas	4 GB o mas	80 GB	2 o más	64-bits

Tabla Numero 1: Recomendaciones de Hardware

3.3. Notas Importantes:

- **Mínimo**, es el requerimiento mínimo para la instalación. Dependiendo del tráfico en la RED y de las aplicaciones instaladas tus requerimientos pueden variar.
- **Las recomendaciones son basadas en un número de usuario, pero tus requerimientos pueden variar de acuerdo al tráfico en la RED.**
- Los CPU VIA e INTEL ATOM tienen altos rangos de reloj, pero a veces no tienen suficientes caballos de poder.

Capitulo 4: Antes de Instalar Untangle

Este capítulo describe la preparación de la instalación de Untangle paso a paso, esto incluye el efectuar copias de seguridad de su información, reunir información sobre su Hardware y localizar cualquier información necesaria.

4.1. Descripción del proceso de instalación paso a paso:

4.1.1 Primer Paso: Procedemos a instalar en modo gráfico normal.

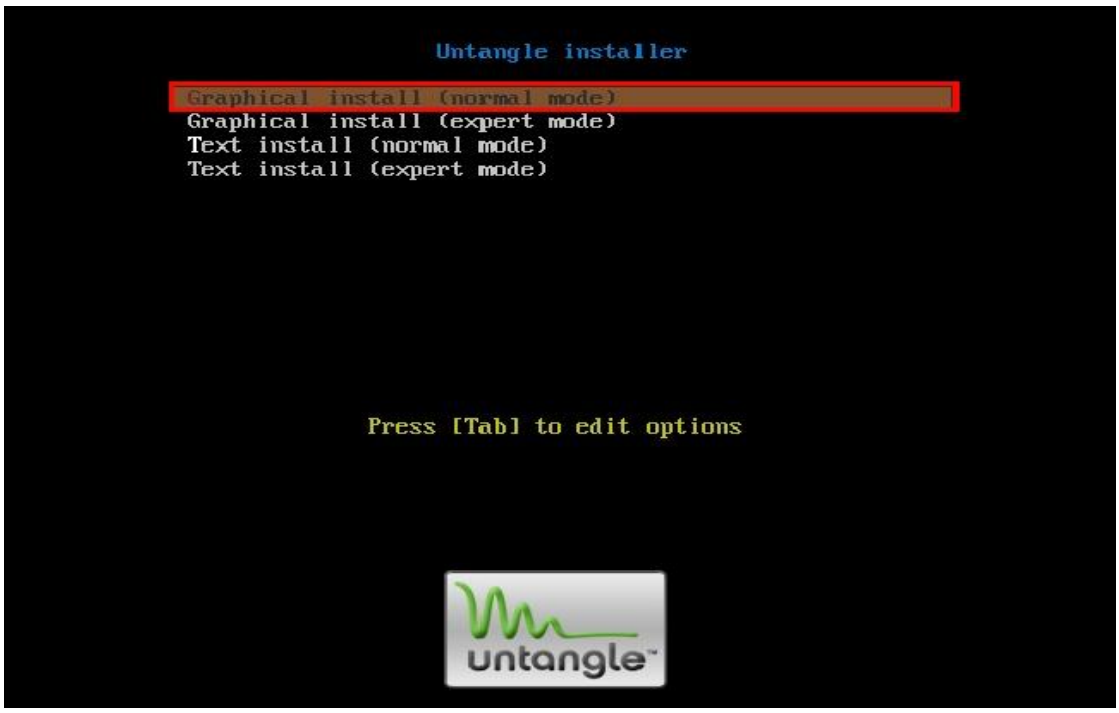

Figura 3: Procedemos a instalar en modo grafico normal

4.1.2 Segundo Paso: seleccionamos el idioma y el país

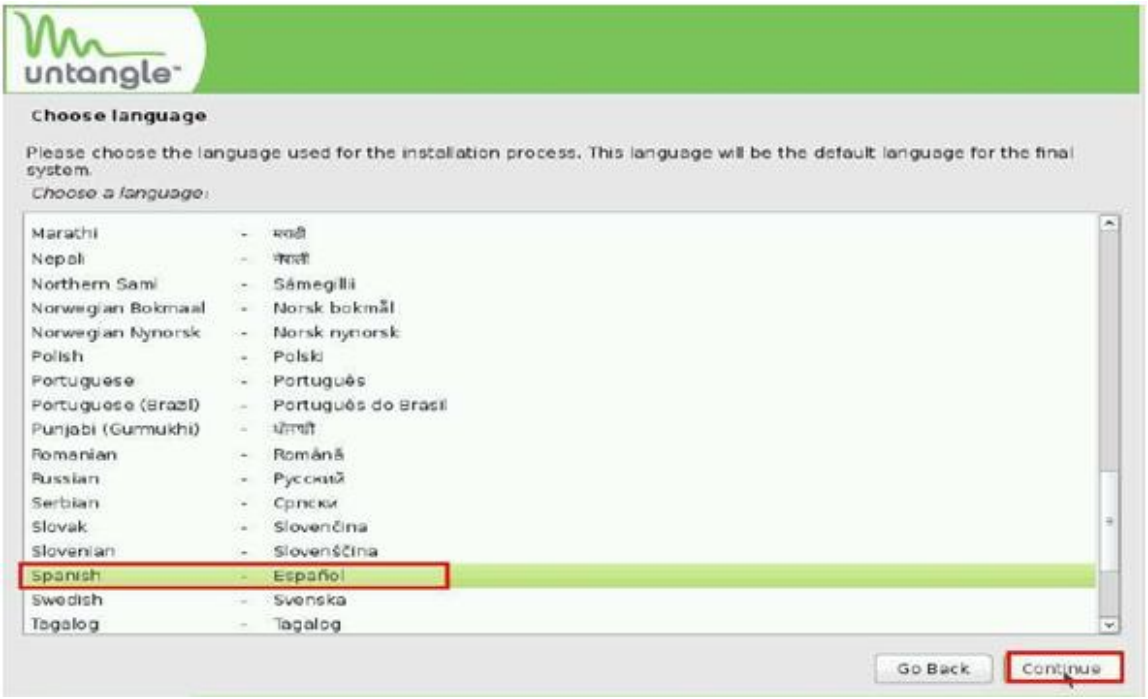

Figura 4: Seleccionamos el idioma y el país

4.1.3 Tercer Paso: El sistema realiza un chequeo de la capacidad de la memoria RAM y la velocidad del procesador luego Elegimos la distribución del teclado y le damos continuar.

Figura 5: El sistema realiza un chequeo de la capacidad de la memoria RAM y la velocidad del procesador luego Elegimos la distribución del teclado y le damos continuar.

4.1.4 Cuarto Paso: Nos pregunta si deseamos formatear el disco le damos que si para finalizar la instalación, luego nos mandara a reiniciar el equipo.

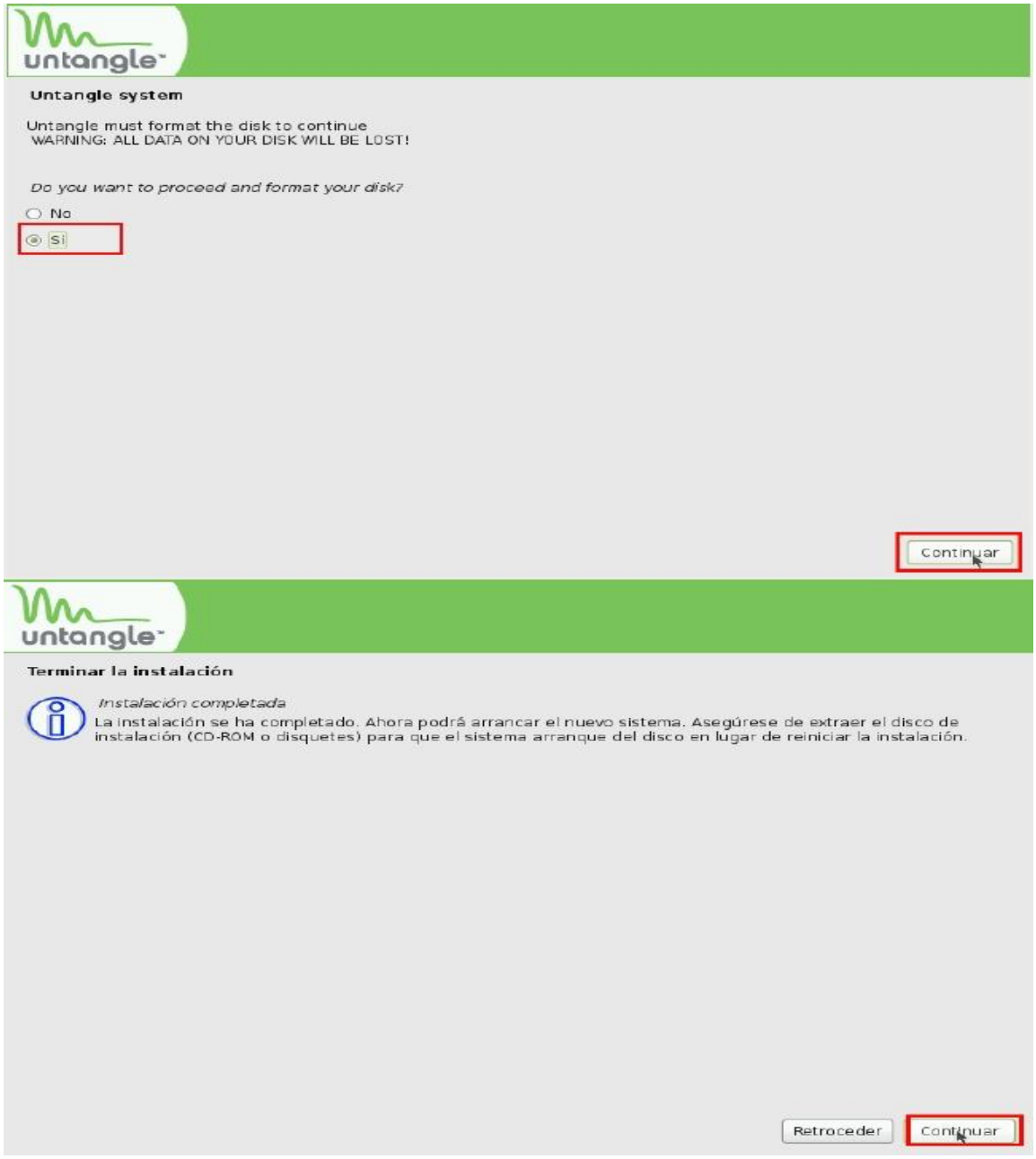

Figura 6: Nos pregunta si deseamos formatear el disco le damos que si para finalizar la instalación, luego nos mandara a reiniciar el equipo.

4.1.5. Pantalla de inicio de Untangle

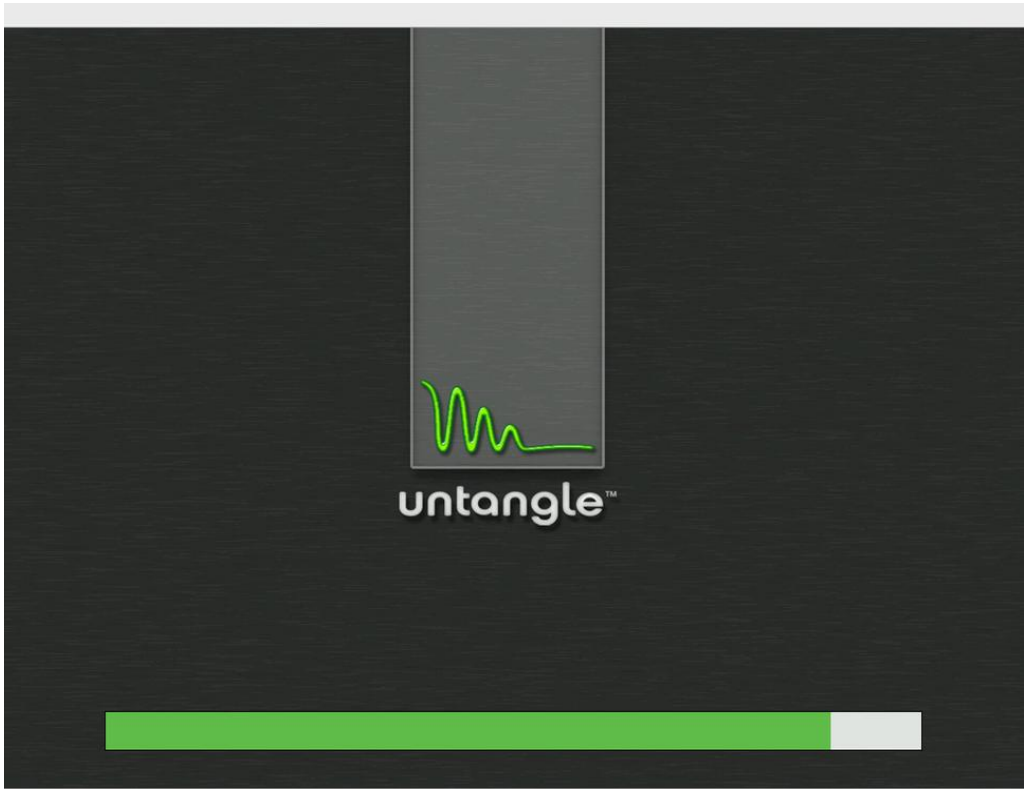

Figura 7: Pantalla de inicio de Untangle

4.1.6. **Quinto paso**: Escogemos el lenguaje

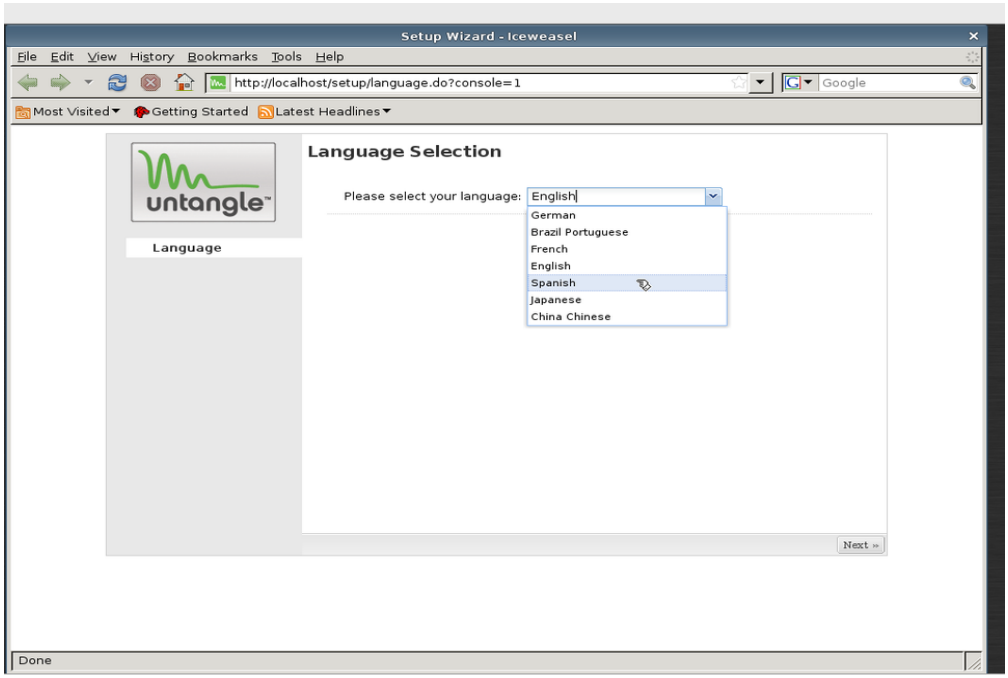

Figura 8: Escogemos el lenguaje

4.1.7 Sexto paso: procedemos a efectuar las configuraciones básicas, asignamos una contraseña al administrador y escogemos la zona horario.

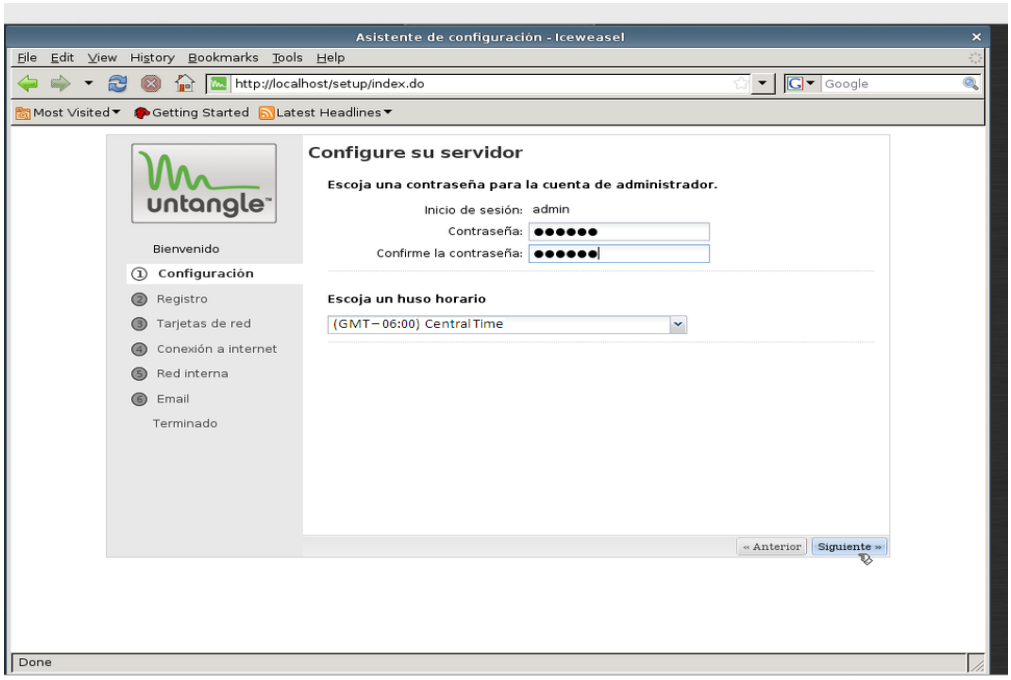

Figura 9: procedemos a efectuar las configuraciones básicas, asignamos una contraseña al administrador y escogemos la zona horario.

4.1.8. Séptimo paso: Identificar las Tarjetas de RED del Equipo.

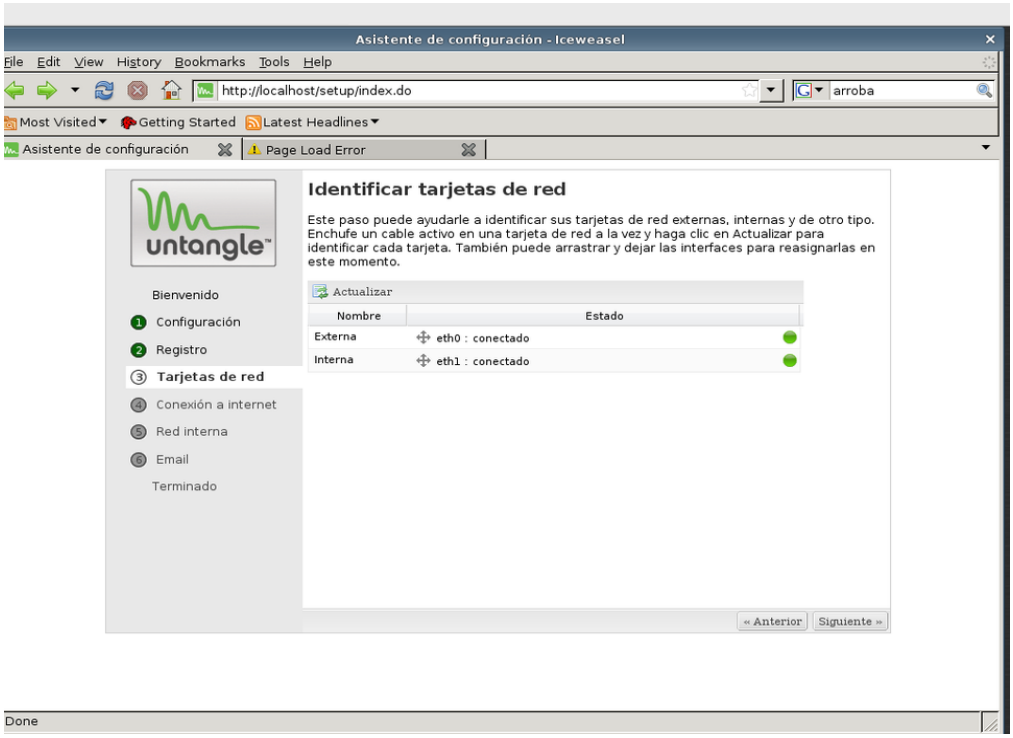

Figura 10: Identificar las Tarjetas de RED del Equipo.

4.1.9. Octavo Paso: configuramos la conexión de Internet y luego realizamos una prueba de conectividad.

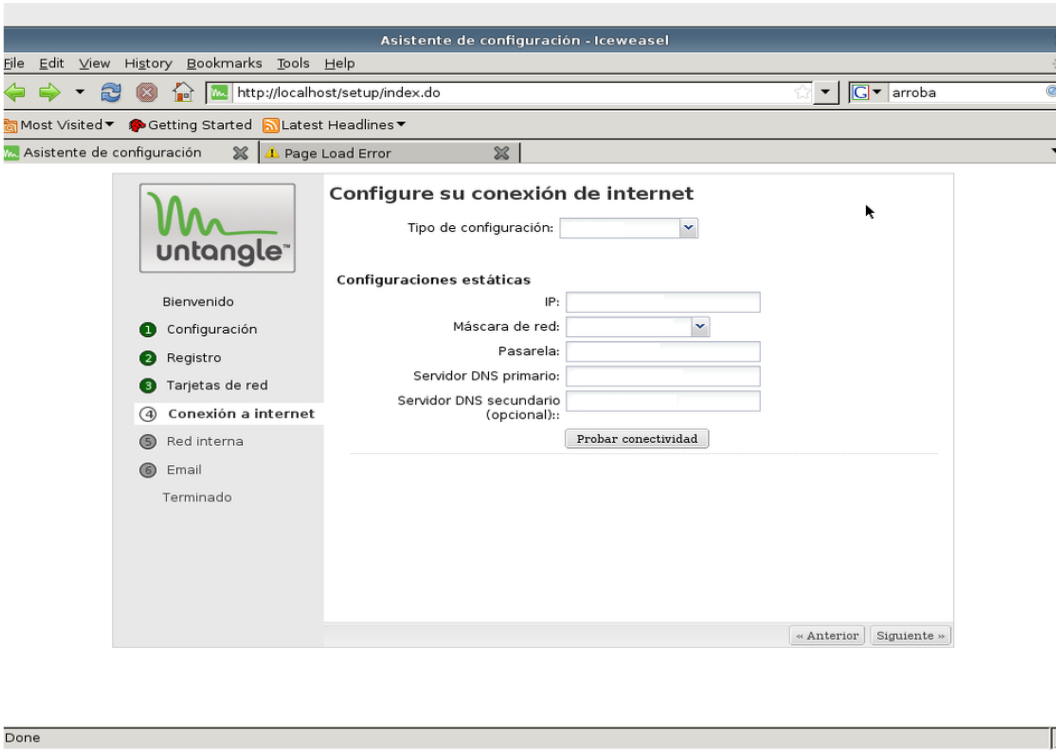

Figura 11: configuramos la conexión de Internet y luego realizamos una prueba de conectividad.

4.1.10. Noveno Paso: Configuramos la interfaz de la Red Interna Modo Router o Modo Puente

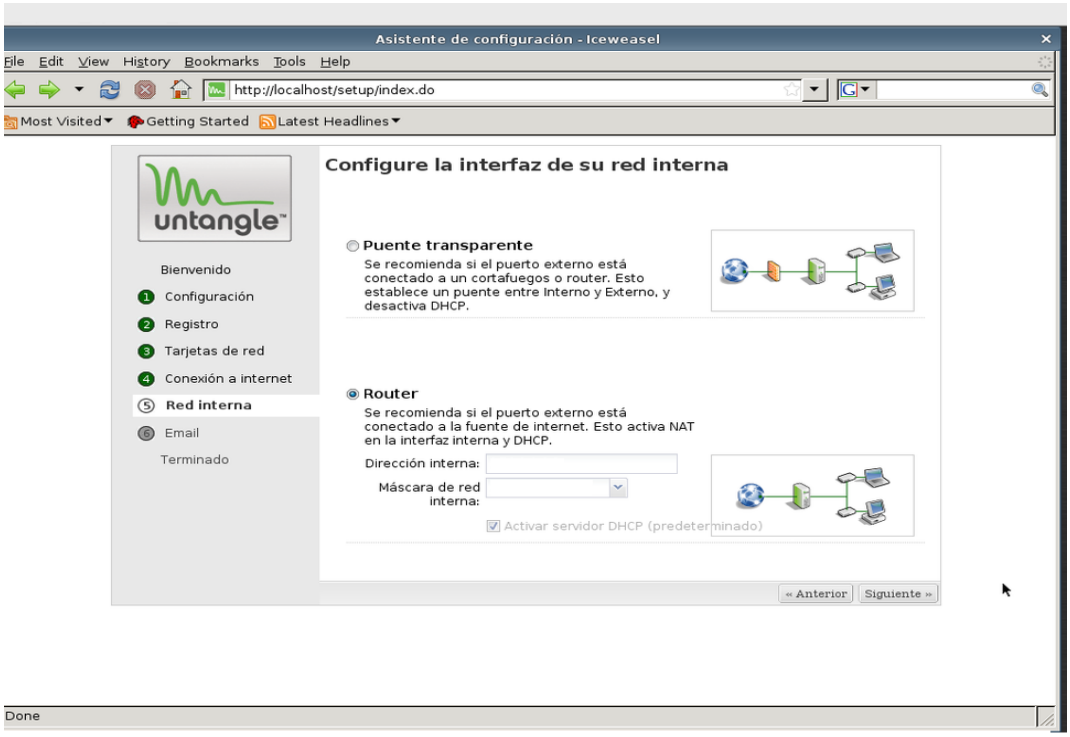

Figura 12: Configuramos la interfaz de la Red Interna Modo Router o Modo Puente

4.1.11. Decimo Paso: Configuración de E-mail, al cual se nos enviara el reporte de incidencias

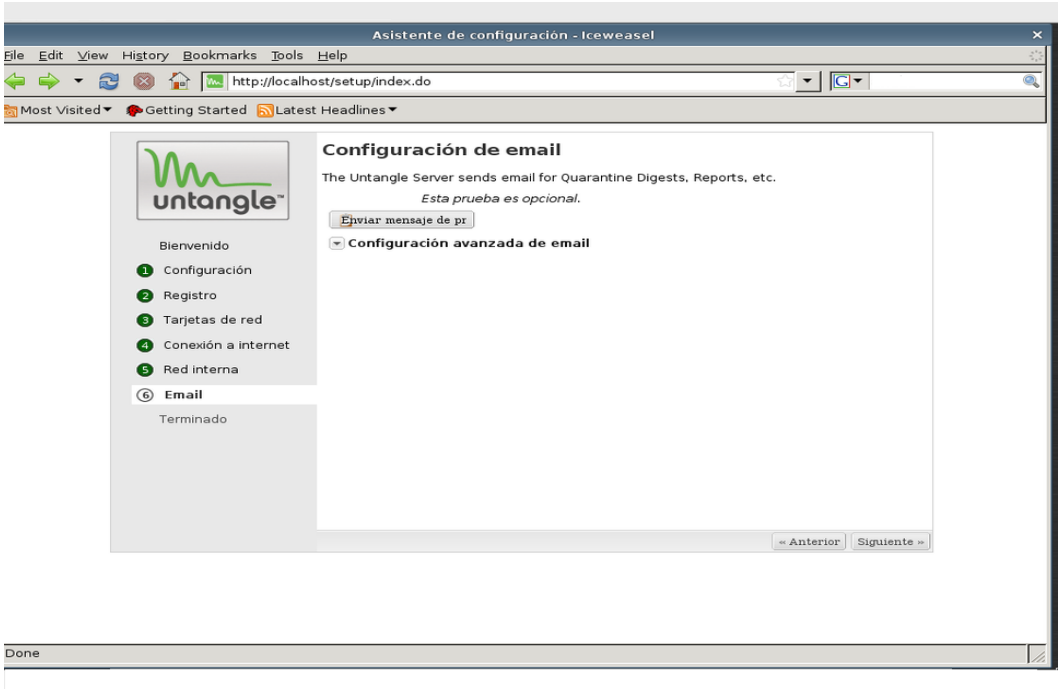

Figura 13: Configuración de E-mail, al cual se nos enviara el reporte de incidencias

4.1.12 Fin de la Instalación

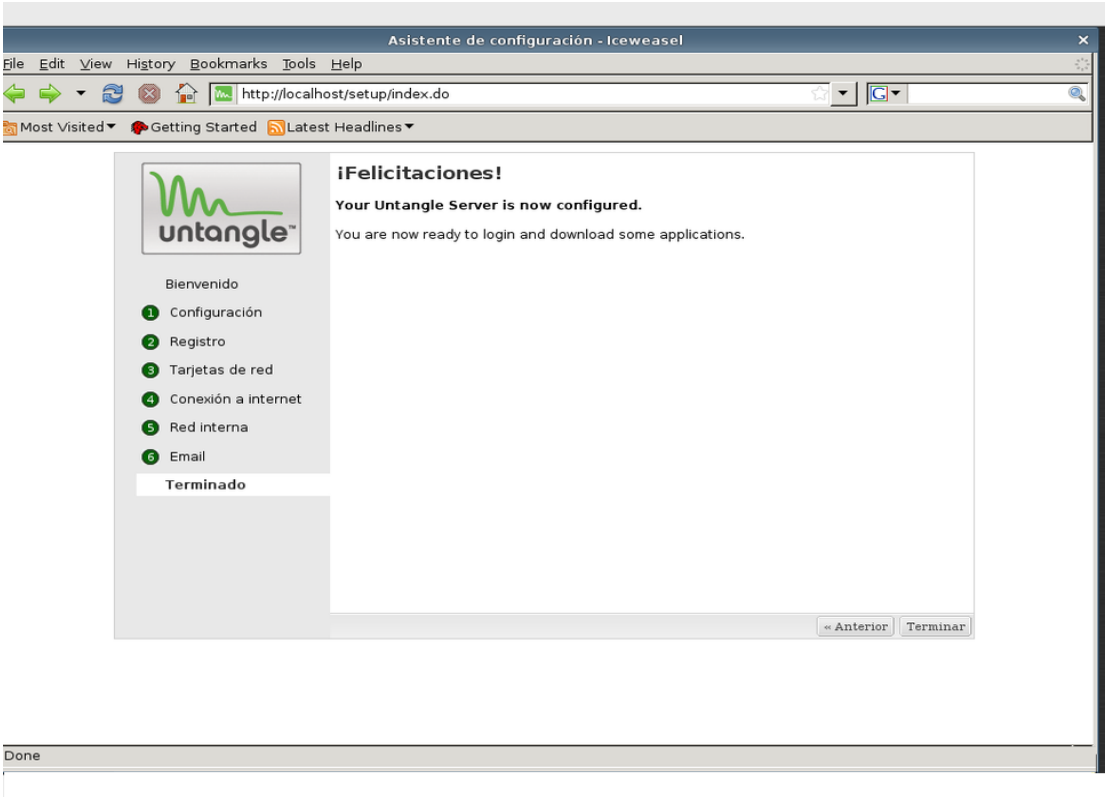

Figura 14: Fin de la Instalación

Capitulo 5: Aplicaciones de Untangle

5.1 Tipos de aplicaciones:

5.1.1 Aplicaciones de filtro: Todas las aplicaciones ubicadas en el Área de Navegación de la WEBgui pueden tener una configuración única el cual puede aplicarse a un rack virtual específico. El rack virtual permite crear políticas para diferentes conjuntos de usuarios.

5.1.2 Aplicaciones de servicios: Todas las aplicaciones bajo el área servicio son servicios y son globales cada uno tiene una configuración que aplica a todas las rack virtuales como si usted eliminara cualquier servicio de cualquier rack usted podría eliminar el servicio de todos los rack.

5.2 Descarga de aplicaciones

Las aplicaciones son descargadas por medio de la WEBgui, simplemente dando click derecho sobre la aplicación que nosotros necesitamos y luego ingresando el correo y la contraseña que se creó en el proceso de instalación de Untangle, todas las aplicaciones ya vienen pre-configuradas una vez que se descarga.

5.3 Aplicaciones gratis de Untangle (Lite package):

5.3.1 Web Filter Lite: Es un filtro de contenido para internet. Además de proteger la red del malware de internet, ofrece al administrador una lista de sitios web bloqueados totalmente personalizable agrupados en categorías. También permite bloquear la descarga de archivos para evitar que se pueda saturar la red con descargas, además de filtrar las descargar por extensión de archivo.

5.3.2 Protocol Control: Esta aplicación sirve para bloquear puertos dentro de nuestra red y así limitar a los usuarios la capacidad para usar determinadas aplicaciones de red. Permite añadir nuevos protocolos no soportados a las listas.

5.3.3 Virus Blocker Lite: Esta aplicación analiza todo el tráfico proveniente de páginas web (HTTP), servidores ftp y correos electrónicos (IMAP, POP, SMTP). Permite detectar malware dentro de Zip, RAR, Tar y otros archivos comprimidos o compactos. Sus bases de datos son actualizadas periódicamente mediante actualizaciones automáticas.

5.3.4 Spyware Blocker: Es una buena opción para proteger a los usuarios del malware instalado desde el navegador, aunque no substituye a un spyware instalado en el sistema.

5.3.5 Phish Blocker: Esta aplicación ayuda a proteger los intentos de suplantación de identidad de correos electrónicos y páginas web. Algunos de los protocolos soportados son HTTP, SMTP, POP e IMAP. Dispone de un registro de eventos donde se especifican todas las incidencias.

5.3.6 Intrusion Prevention: Esta aplicación bloquea los intentos de hackeo antes de los servidores internos así como las PC de los usuarios, con firmas pre configuradas basadas en IPS hacen fácil al administrador.

5.3.7 Firewall: Esta aplicación dibuja una línea que separa la red interna de la red externa, además filtra el tráfico basado en una dirección IP, Protocolo y Puerto.

5.3.8 OpenVPN: esta aplicación habilita al administrador a proporcionar acceso remoto y seguro a la red interna para realizar configuraciones básicas.

5.3.9 Reports: Proporciona a los administradores la visibilidad y los datos necesarios para investigar incidentes de seguridad monitorea la conducta de, los usuarios y se encarga de conocer el flujo del tráfico y el uso de la red.

5.3.10 Spam Blocker Lite: Como su nombre indica es un bloqueador de SPAM incluido en las aplicaciones gratuitas de Untangle, soporta SMTP, POP e IMAP, además también soporta cuarentenas individuales para cada bandeja de correo entrante. Tiene un buen filtro de SPAM basado en las mejores técnicas de detección en tiempo real.

5.3.11 Ad Blocker: Esta aplicación elimina los anuncios molestos y disminuye el tiempo de carga de una página WEB, reduciendo el tráfico en la red.

5.4 Aplicaciones de pago:

5.4.1 Web Filter: Bloqueo de 100 millones de sitios en 57 categorías, además de otras nuevas a tiempo real

5.4.2 Kaspersky Virus Blocker: Su funcionamiento es parecido al módulo Virus Blocker, por no decir que es igualito, pero con las bases de virus y el motor heurístico de Karspersky Labs. Evita que el malware infecte los PCs y servidores de la red protegiéndolos en tiempo real.

5.4.3 Virus blocker: Ver virus blocker lite

5.4.4 **Spam Blocker: Ver spam blocker lite**

5.4.5 **Web Cache:** Se llama caché web a la cache que almacena documentos web(es decir, paginas, imágenes, etc) para reducir el ancho de banda consumido, la carga de los servidores y el retardo en la descarga. Un caché web almacena copias de los documentos que pasan por él, de forma que subsiguientes peticiones pueden ser respondidas por el propio caché, si se cumplen ciertas condiciones.

5.4.6 **Bandwith Control:** Esta aplicación permite el control del tráfico de la red, se pueden asignar cuotas a los usuarios y asignar el uso que se le va a dar al ancho de banda seleccionado. Con esta aplicación es posible garantizar ancho de banda para una aplicación o usuario de la red, también permite priorizar servicios.

5.4.7 **Policy Manager:** Se trata de una aplicación para personalizar el acceso a la red filtrando por franja horaria y por usuario. Permite crear políticas de acceso totalmente personalizables asignando permisos a los usuarios de la red.

5.4.8 **Directory Connector:** Esta aplicación permite explotar todo el potencial del Active Directory de Microsoft. Permite autentificación mediante usuario y mediante servidor RADIUS. Dispone de sistema de reporte de estadísticas en PDF y HTML. Se puede encontrar más información acerca de la aplicación en la dirección.

5.4.9 **WAN Failover** – Cambiar automáticamente el tráfico a una conexión alternativa.

5.4.10 **WAN Balancer** - Asigna el tráfico a través de hasta seis conexiones a Internet por separado.

5.4.11 **Branding Manager** – Use su propio logo y mensajes en el servidor y bloqueos las pantallas.

5.4.12 **Live Support** – Personas reales, con un conocimiento real para ayudar cuando haga falta.

5.4.13 **Commtouch Spam Booster** – Una capa de protección extra para contener el SPAM

5.4.14 **Policy Manager** - Crear varios usuarios y sesiones basadas en la web y acceso remoto.

5.4.15 **AD Connector** – Utiliza tu servidor de Microsoft Active Directory para simplificar la gestión de políticas y presentación de informes.

5.4.16 **PC Remote** - Permite acceso directo in situ y la solución de problemas.

5.4.17 **Remote Access Portal** – Proporcionar acceso seguro a los servidores internos y servicios.

5.4.18 **QoS:** Permite la priorización del tráfico.

Capitulo 6: Trabajando con Untangle

6.1. Administración de Untangle

Usted puede obtener un certificado acerca del aviso, este puede asegurarte la conexión con Untangle creándolo antes y provee su credencial de ingreso el que podría ser presentado a la webgui de Untangle, por defecto, la administración remota es desactivada y puede ser activada desde la Config > Administration

Después que usted reinicie, se le presentara el asistente para las aplicaciones esto lo ayudaría a decidir sobre cuales aplicaciones descargar y usar con Untangle, nosotros proveemos 14 días para utilizar todas las aplicaciones gratuitamente (excepto Branding Manager), siéntase libre de aceptar ciertas aplicaciones y vea cuales le van a ser útil y necesarias para su organización.

Usted puede administrar el servidor Untangle de 3 maneras:

6.1.2 Local: Con un simple clic en Launch Client en la GUI de Untangle y se cargara la Web GUI.

6.1.3 En la Re d LAN: en tu navegador, ingresar la LAN IP de Untangle (por ejemplo http://10.0.0.1)

6.1.4 Remoto: En tu navegador, ingrese la WAN IP de Untangle (por ejemplo http://203.0.113.1)

6.2. La Web GUI

Una vez que las aplicaciones de Untangle han sido descargadas usted podrá ver la webgui en la consola, como podemos apreciar en la figura 3.

Figura 15: Consola webgui de Untangle

Untangle webgui puede ser dividida en 2 partes principales el **Área de Navegación** el cual está ubicada en la parte izquierda y los Racks virtuales en la derecha. El Área de Navegación contiene 2 secciones ***apps*** que es usado para instalar la aplicación dentro del racks y config que es usada para varias configuraciones generales de Untangle. Las aplicaciones son instaladas dentro del rack y filtra el flujo del tráfico hacia ellos, cada aplicación tiene un aspecto grafico con un botón de instalación a configurar, un LED

muestra el corriente estado del Rack (Verde/Apagado) y el botón de encendido y apagado.

En la parte superior de la webgui podemos desplegar, la estadística de la velocidad de la red, una cuenta de sesión abierta, CPU, memoria y información de disco duro.
Por favor note que nuestro paquete libre aparece en la página web y solo incluye la habilidad a usar un rack. Si usted necesita la habilidad de crear múltiples rack usted podría necesitar el policy manager.

Capitulo 7: Configuración Untangle

La tabla de configuración permite modificar el software de Untangle, no a la configuración de las aplicaciones, como por ejemplo interfaces WAN/LAN, puertos, servidor DHCP y más.

7.1 Networking

The **Networking** tab gives you access to the global settings of your Untangle.

7.1.1 Interfaces

On the **Interfaces** tab, you can set up and modify new WAN or LAN interfaces. The table below contains a list of all options; only the applicable options will be displayed depending on your selections for **Config Type** and **is WAN Interface**.

Config Type	This entry controls the type of interface: Use **Static** if you have a static IP. Use **Dynamic** if you have a dynamic IP. Use **Bridge** if you'd like to bridge the interface to another interface. You can use **PPPoE** if your line requires it, but we highly recommend finding out from your ISP if your modem can handle the PPPoE login so you can use **Static** here. PPPoE connections do not

	work with Multi-WAN features and it's generally better to use **Static** if possible.
WAN Interface	Use this checkbox if the interface should be a WAN connection (e.g. pointed towards the Internet)
Primary IP and Netmask	The IP Untangle should use on the interface - for example, 203.0.113.1/28 or 10.0.0.1/24.
IP Address Aliases	These are additional IPs Untangle should hold on that interface. The netmask should (in most cases) match the mask of your primary IP.
NAT Policies	When using a non-WAN interface, these control how machines are NATed to the WAN interface. 0.0.0.0/0 auto will NAT everything to your primary IP.
Default Gateway	The gateway given to you by your ISP.
Primary/Secondary DNS Server	The DNS server info given to you by your ISP. Please note that while you can use public DNS servers such as Google or OpenDNS, using them will stop Spam Blocker's tarpitting feature from working. We recommend against using internal DNS servers.
Override IP Address/Netmask/Gateway/DNS	When using a **Dynamic** interface, you can use these to override the information pulled from the upstream DHCP server.
Username/Password	When using a **PPPoE** interface, this is your Username/Password. As noted above, we recommend having your modem handle the login so you can use a **Static** interface type.
PPPoE Optional Parameters	When using a **PPPoE** interface, these are any optional parameters that the Untangle needs to use. As noted above, we recommend having your modem handle the login so you can use a **Static** interface type.
Bridge to	When using a **Bridge** interface, this is the interface you want to bridge the current interface to.
MTU	The Maximum Transmission Unit of your network. Leave this blank (auto) unless you have a good reason not to.
Ethernet Media	Controls the speed of the interface's NIC. Leave this set to Auto unless you're having duplexing issues. Check to make sure both sides are set to Auto before changing it.

7.1.2 Port Forwards

The **Port Forwards** tab is where you set up your port forwards. More information on Port Forwards can be found here.

7.1.3 Hostname

Using the **Hostname** tab, you can set your hostname, domain name, and configure Untangle to update your Dynamic DNS. There is a dropdown list of supported Dynamic DNS providers. Please note that the **Hostname** entry at the top is for your Untangle while the **Hostname(s)** entry at the bottom is for your Dynamic DNS hostname.

7.1.4 DHCP Server

The **DHCP Server** tab governs the settings for your DHCP Server, allows you to set Static DHCP Entries and see the Current DHCP Entries.

Enabled	Enables or disables the DHCP server. Please note, if the DHCP server is disabled it will not hand out DHCP to **any** interfaces.
Start	Sets the start of the DHCP address pool range, for example 10.0.0.100.
End	Sets the end of the DHCP address pool range, for example 10.0.0.200.
Lease Duration	Sets the duration of DHCP leases in seconds.
Gateway	Sets the Gateway given out to DHCP clients. You can leave this blank and Untangle will hand out the proper gateway on each non-WAN interface you have enabled DHCP on.
Netmask	Sets the Netmask given out to DHCP clients. You can leave this blank and Untangle will hand out the proper netmask on each non-WAN interface you have enabled DHCP on.
Lease Limit	The maximum number of simultaneous DHCP leases.
Authoritative	Makes Untangle's DHCP server the authoritative server on the network. It changes the behaviour from strict RFC compliance so that DHCP requests on unknown leases from unknown hosts are not ignored.

7.1.5 DNS Server

On the **DNS Server** tab you can set your domain name suffix, set Static DNS Entries and see the current Automatic DNS Entries.

Enabled	Enables or disables the DNS server.
Domain Name Suffix	The domain name of your network. This controls, among other things, the suffix pushed out to OpenVPN clients.

7.1.6 Troubleshooting

The **Troubleshooting** tab provides you with tools to assist in problem solving.

Connectivity Test	The Connectivity Test checks that your Untangle can resolve and connect to http://updates.untangle.com This is an important test to establish that your WAN connections is functioning properly.
Ping Test	A simple Ping utility. Enter a hostname or IP and ping away.
DNS Test	A simple DNS utility. Enter a hostname and get an IP.
Connection Test	The Connection Test is a very useful tool that lets you check the status of a port on a remote machine. Enter an IP or Hostname and a Port, click Run Test, and see what happens.
Traceroute Test	A Simple Traceroute utility. Enter a hostname or IP and see what's between your Untangle and the remote machine.
Packet Test	The Packet Test is a very powerful troubleshooting tool. Select an Interface to listen on and a timeout value, then hit Run Test - you'll see all the traffic on that interface. You can filter by IP and/or port to, for example, check if traffic is hitting an interface or if a remote machine is answering a request.

7.1.7. Advanced

Pressing the **Advanced** button allows you to switch in and out of Advanced mode. When in Advanced mode, a dropdown gives you access to additional menus listed below.

7.1.7.1. General

There are four options in the **General** menu:

7.1.7.2. Send ICMP Redirects: Untangle will send updated routing information to hosts if it knows a better path to the destination.

7.1.7.3. Enable SIP Helper: The SIP helper will allow VoIP phones and devices to work through NAT if they can not do NAT traversal themselves - if they are set to do NAT traversal themselves, you may need to disable this setting for them to work. Please note that this requires a reboot to take effect.

7.1.7.4. Administration overrides Port Forwards: This setting will cause the current administration port (443 by default) to override any port forwards you have set up for the port in question.

7.1.7.5. Only NAT WAN traffic: This setting will toggle the NATing of LAN to LAN interfaces on or off.

7.1.7.6. Bypass Rules

You can set up **Bypass Rules** when you don't want traffic scanned by Untangle - scanning will break some types of traffic, such as some times of encryption. Any bypassed traffic will simply be routed to its destination; it will not be scanned and thus will not show up in the Reports. More information on Bypass Rules is available here.

7.1.7.7. Packet Filter

You can use the **Packet Filter** like a Firewall for traffic that does not go through the rack - for example, you can block access to untangle services, such as the administration pages.

Your options are **Pass**, **Drop**, and **Reject**. More information on the Packet Filter is available here. The built-in Packet Filter rules are the following:

Allow DHCP Requests from the internal interface	This rule allows hosts on the Internal interface to grab an IP from Untangle's DHCP server.
Allow DHCP Requests from the DMZ interface	This rule allows hosts on the DMZ interface to grab an IP from Untangle's DHCP server.
Block all DHCP Requests to the local DHCP Server	This rule blocks DHCP requests from all interfaces to Untangle's DHCP server.
Block DHCP Traffic forwarding to internal interface	
Accept DHCP traffic to the local DHCP client	
Accept DNS traffic from the Internal and VPN interfaces to the local DNS Server	This rule allows hosts on the Internal and VPN interfaces to use Untangle's DNS server.
Accept DNS traffic to the local DNS Server from all interfaces	

Accept SNMP traffic from the Internal interface	
Accept SNMP traffic from all interfaces	
Block OpenVPN traffic from the internal interface	
Accept OpenVPN traffic from all interfaces	
Accept SSH traffic from all interfaces	This rule will block or allow incoming SSH connections from all interfaces.
Allow Ping on all interfaces	This rule will block or allow ping replies on all interfaces.
Block traffic to local server processes	
Accept incoming VPN traffic when running as a VPN client	
Route VPN traffic that would go through the Bridge	This rule is for **bridge** mode installations only - it will route VPN traffic over the tunnel that would be passed to the External interface.
Route all bridge traffic	This rule will route all traffic that would pass through the bridge according to Untangle's routing table.

7.1.7.8. QoS

The **QoS** tab contains the Quality of Service settings for Untangle. More information on **QoS** is available here.

7.1.7.9. ARP

You can use the **ARP** tab to statically assign or view the current ARP entries.

7.1.7.10. Routes

Routes will display Untangle's routing table and allow you to set Static Routes.

Target/Netmask	These fields specify the network that will have its traffic routed. Valid values are in IP address/netmask format.
Gateway	This field specifies the host that receives traffic that is routed from the specified network. Valid values are in IP address format.

7.1.7.11. Local DNS

The **Local DNS** tab allows you to have DNS queries for certain domains forwarded to alternate DNS servers - for example, you may want to forward DNS requests for the far side of a VPN tunnel to the DNS server on the other side of the tunnel.

7.1.7.12. DHCP & DNS

The **DHCP & DNS** tab allows you to pass custom options to DNSMASQ, the daemon Untangle uses to handle DHCP and DNS.

7.1.7.13. Overrides

The **Overrides** tab allows you to stop Untangle from modifying certain configuration files if you need to make manual changes.

7.2. Administration

The **Administration** menu controls features of your Untangle including administrative accounts, External Administration, and Certificates.

7.2.1. Administration

From this tab you can add additional administrator accounts to your Untangle and control how Administration behaves.

Admin Accounts	Use this to add, remove or modify administrator accounts.
Enable External Administration	This enables or disables administering Untangle from the WAN.
Enable External Report Viewing	This enables and disables viewing of Untangle Reports from the WAN.
Enable External Quarantine Viewing	This enables and disables viewing of Email quarantines from the WAN.
External HTTP Port	This setting allows you to change Untangle's administration port. This is useful, for example, if you need to forward port 443 from the WAN to a local machine.
Allow/Restrict External Access	This setting lets you switch Untangle administration from any IP to a specific IP or IP range.
Enable/Disable HTTP Administraion from LAN	This settings allows you to disable or enable administration over HTTP from the LAN.

7.2.2. Public Address

You can use this menu to let Untangle know what address it should use when sending out quarantines, OpenVPN clients, and more.

Use External IP address	This will have Untangle use the Primary IP on its External Interface.
Use Hostname	This entry will have Untangle use the Hostname from **Config > Networking > Hostname**.
Use Manually Specified IP	This will have Untangle use the IP and port you specify, for example if you are in bridge mode and port forwarding to the Untagle from your firewall.

7.2.3. Certificates

The **Certificates** tab lets you view Untangle's cert info and create/import certificates. Please note that if you are going to import a certificate, you **must** step through the process: Generate a Certificate, then a CSR, send the CSR to your registrar, and import the certificate they give back to you.

7.2.4. Monitoring

The **Monitoring** tab allows you to enable or disable SNMP and/or Syslog data.

7.2.5. Skins

The **Skins** tab allows you to modify the look and feel of your Untangle with the inbuilt or custom skins. Please note that this only affects the administrative webGUI, if you'd like to change the way user-facing pages are displayed you'll need Branding Manager.

7.3. Email

The Email menu contains settings that pertain to Untangle sending emails as well as whitelists and quarantines.

7.3.1. Outgoing Server

Untangle can be set to either send Email directly or through another server. We recommend using the Email Test to see if test emails go through, if you do not receive them you can switch the settings and try again. Please note that most mail servers will need to be set to allow Untangle to relay through them for Emails to successfully be sent.

7.3.2. From-Safe List

The **From-Safe List** is a whitelist for email addresses. Please note that **all** whitelist entries are **global** in that they will apply to all mailboxes. We provide both a **Global** whitelist so administrators can easily add addresses for all users as well as a **Per-User** list that end users can add to through their quarantines.

7.3.2. Quarantine

The **Quarantine** tab contains settings dealing with quarantines. You can set the **Maximum Holding Time** for emails in the quarantine, the time and sending of daily **Quarantine Digests**, as well as viewing/purging user quarantines. You can also set the quarantinable address list and set email addresses to forward quarantines to.

7.4. Local Directory

On the **Local Directory** menu you can add, delete and edit accounts in Untangle's Local Directory. You can use this for Captive Portal and Policy Manager.

7.5. Upgrade

The Upgrade menu allows you to manually start an Upgrade as well as enable/disable automatic upgrades and set the date/time for automatic upgrade checking.

7.6. System

The **System** tab houses settings for Untangle's secure access to your box, along with Backup/Restore options and reboot/shutdown options.

7.6.1 Support

Allow secure access to your server for support purposes: This joins your Untangle to our secure support channel in the event we need back-end access to the box to fix problems.

Send data about your server for support purposes: This option sends anonymous statistics and error messages to Untangle so we can improve the product. If you're getting email from/to exceptions (at) untangle, you can disable this to stop those.

You can also reboot or restart your Untangle from this tab.

7.6.2 Backup

The **Backup** tab allows you to take a manual configuration backup of your Untangle's settings.

7.6.3 Restore

The **Restore** tab allows you to restore a backup of your Untangle's settings. Please note that racks and individual application settings will not be restored unless the applications have been downloaded to the box, so we recommend installing a trial of the Premium Package before restoring backups when changing hardware.

7.6.4. Protocol Settings

The **Protocol Settings** tab contains options to enable or disable the processing of HTTP/FTP/Email traffic. It is not recommended to modify these options unless instructed to do so by Untangle Support, or if you understand what they do.

7.6.5 Regional Settings

The **Regional Settings** tab allows you to change your timezone and language. You can also upload additional language packs from this menu.

7.7. System Info

The System Info tab displays information about your Untangle and its licenses.

7.7.1. Version

The **Version** tab displays the current revision of Untangle, your UID, and your Java version.

7.7.2. Registration

The **Registration** tab allows you to enter or update registration information on file with Untangle for the UID of your box.

7.7.3. Licenses

This tab allows you to check the current license status of your Untangle and manually sync it with our licensing server if they are outdated.

7.7.4. License Agreement

You can use this tab to view the Untangle License Agreement.

Topología de la Red Edisa

- El diseño de la topología de red empleado en EDISA es de tipo estrella, la cual se caracteriza por contar con un punto central o más propiamente conocido como nodo central al cual se conectan todos los equipos, como podemos observar en la figura 5, este diagrama fue tomado antes de la instalación del servidor Untangle posteriormente presentaremos el nuevo diseño con el servidor ya incorporado a la red.

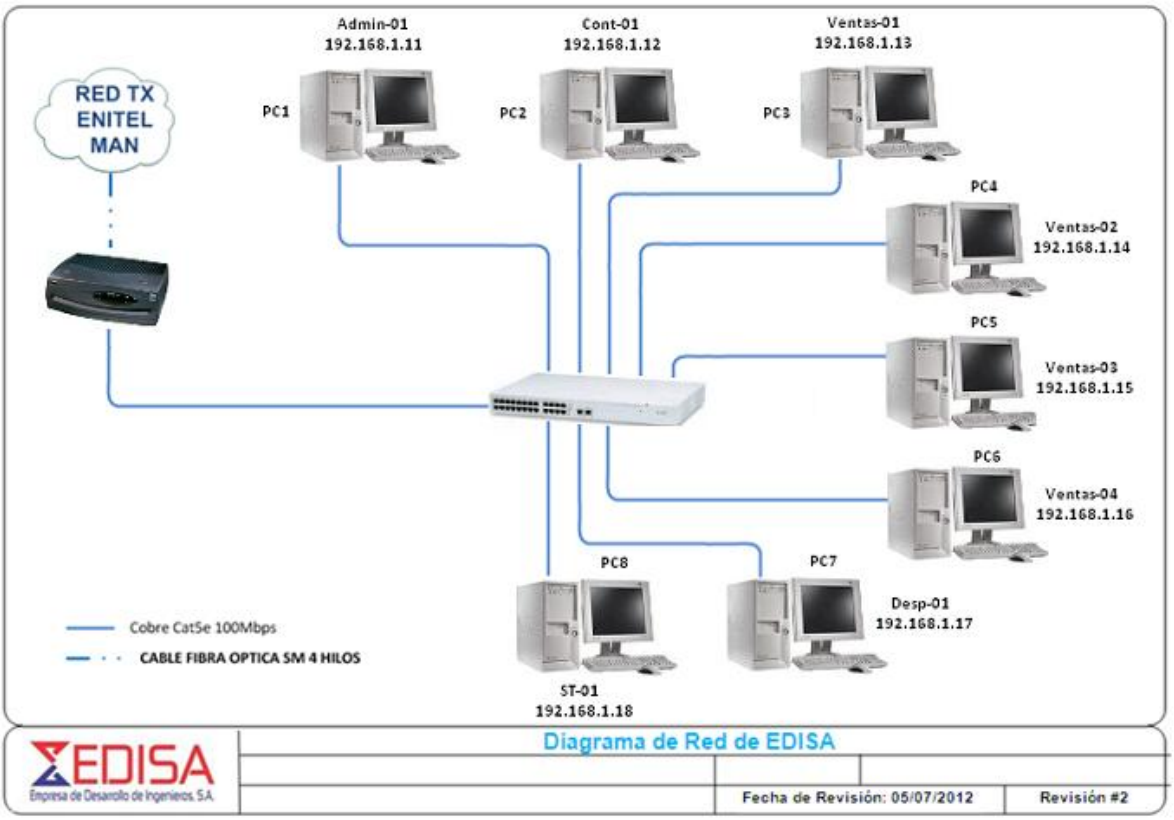

Diagrama de la red de Edisa antes de instalar Untangle

Archivos creados durante la descarga del software Untangle.

Nombre archivo (disco): untangle_920_x32.ISO

Nombre Del Equipo: Proyecto Untangle

Sistema Operativo: DEBIAN Linux (32-bit)

Topología de la Red EDISA con el servidor Untangle Incorporado

El siguiente paso en el trabajo fue la instalación del servidor en la red de la empresa como se señalo anteriormente el modo de instalación será el de Router haciendo las conexiones respectivas del modem a la interfaz externa del servidor y la interfaz interna del servidor conectada al switch desde donde ahí se controlara la red LAN de la empresa Al incorporar el servidor a la red podemos observar que la estructura no sufre ninguna modificación.

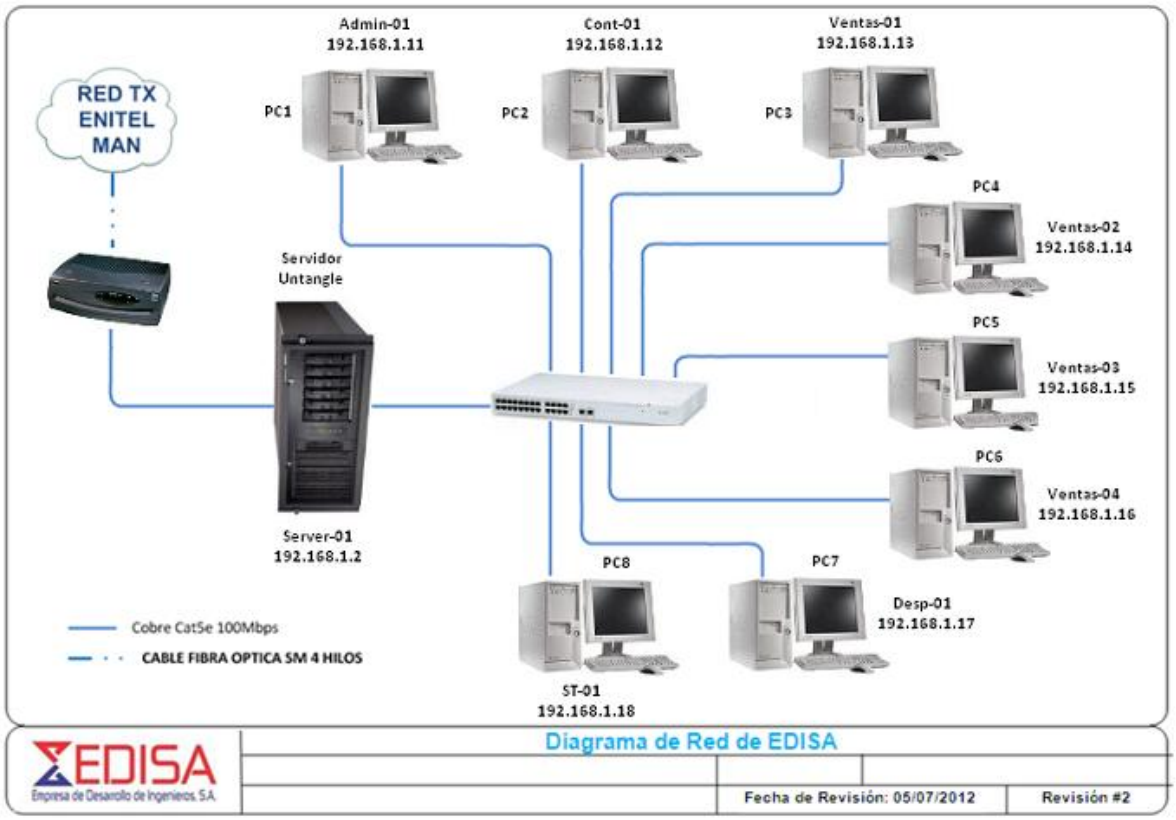

Diagrama de la red con la incorporación del servidor Untangle