UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

FACULTAD DE INGENIERÍAS

CARRERA DE SISTEMAS

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

"AUDITORIA FÍSICA Y LÓGICA A LAS REDES DE COMUNICACIONES DE COMPUTADORES DE LA FÁBRICA PASAMANERÍA S.A"

AUTORES:

NORMA CUMANDA ARCE CUESTA.

ANDRÉS FERNANDO TACURI JAPA.

DIRECTOR:

ING. RODOLFO BOJORQUE.

2010

CUENCA – ECUADOR.

Ing. Rodolfo Bojorque

Certifica

Que el presente informe de monografia fue desarrollado por los estudiantes Norma Cumanda Arce Cuesta y Andrés Fernando Tacuri Japa, bajo mi supervision ,en base a ello, autorizo la presentación de la misma.

Cuenca, Septiembre del 2010

Ing. Rodolfo Bojorque
Director de tesis

Responsabilidad de Autoría

El análisis de los conceptos y las ideas vertidas en la presente tesis son de total responsabilidad de los autores.

Cuenca, 18 de Septiembre del 2010

Norma Arce

Andrés Tacuri

Dedicatorias

Este proyecto de tesis está dediado de manera especial a la persona mas importante en mi vida , mi madre Esthela, quien ha sabido darme todo su apoyo incondicional para la culminación de mi carrera profesional.

Norma Cumanda Arce Cuesta.

Agradecimientos

A Dios por brindarme la sabiduria para cumplir mis metas en la vida. De manera especial a mi madre, hermanos y hermanas, por la confianza y su apoyo en todo momento.A mi compañero de tesis por su apoyo y comprensión a lo largo de estos años de estudio universitario. A las personas que me extendieron una mano cuando lo necesite.

Norma Cumanda Arce Cuesta.

Dedicatorias

Esta tesis la dedico con todo el cariño y amor a mis padres, en especial a mi madre Gladys que siempre me brinda su cariño, amor y apoyo en todo momento, a mi padre Oswaldo por todo el apoyo que me brindas, les agradezco de todo corazón, por darme la oportunidad de culminar una carrera profesional para mi futuro.

GRACIAS LES QUIERO MUCHO.

Andrés Fernando Tacuri Japa.

Agradecimientos

A DIOS por enseñarme el camino correcto de la vida, por levantarme en los momentos más difíciles y guiarme con su sabiduría para poder cumplir mis metas en la vida.

A mi madre, a mis dos hermanos, por siempre haberme dado su fuerza, confianza y apoyo incondicional en todo momento.

A mi compañera, de tesis por brindarme su apoyo, ánimo y colaboración en todos estos años de estudios, por darme la iniciativa de entrar a realizar este proyecto de tesis, gracias por todo.

A todos mis amigos de la universidad que siempre estuvieron cuando más los necesitaba, por brindarme su apoyo y ayuda.

A la Fábrica la Pasamanería S.A por habernos abierto las puertas para poder realizar nuestra tesis, en especial al Tnlg. Oswaldo Vivar administrador de la red, por darnos todas las facilidades y ayudarnos en cada una de nuestras preguntas.

GRACIAS A TODOS.

Andres Fernando Tacuri Japa.

Índice General

Índice de Figuras

Índice de Tablas

CAPITULO 1

DESCRIPCIÓN DE LA FÁBRICA PASAMANERÍA S.A.

1.1 Reseña Histórica

En el año de 1926 el fundador Sr. Carlos Tosi Siri inicia sus actividades comerciales en la ciudad de Cuenca, creando su almacén llamado "Almacén de Carlos Tosí". Como se puede observar en las fotografías de la figura 1.1.

Figura 1.1. ***Fotografías de la fábrica en sus inicios.***[5]

Para el año de 1935 instalan una fábrica para la producción de artículos textiles, ya que tenían una buena demanda en el mercado nacional, por lo que para este año llegan las tres primeras máquinas trenzadoras y en el patio de la casa de la familia Tosi comienzan la producción un 11 de abril de 1935, fecha que es reconocida como el inicio de la actividad de PASAMANERIA S.A.

En 1949, adquieren parte de la maquinara de la que fue la Textil Azuaya y es así como la Pasamanería inicia la fabricación de su propio hilo de algodón. En este mismo año se

[5] Imágenes obtenidas del manual de inducción Pasa.

crea el departamento de Confecciones, para la producción de ropa, que son comercializados con la marca PASA.

Hoy la fábrica Pasamanería S.A se encuentra ocupando un lugar preferencial en la actividad industrial a nivel nacional. En las figura 1.2 se muestran las fotografías actuales de la misma.

Figura 1.2. ***Fotografías actuales de la fábrica*****.**[6]

A continuación se indica la misión y visión que tiene la fabrica.

- **Misión**

Somos una Empresa Industrial Textil. Fundada en 1935, dedicada a la fabricación y comercialización de confecciones dirigidas al comercio y consumidor final, y de insumos textiles orientados a las industrias afines, con calidad garantizada, bajo el amparo de la marca PASA, operando bajo criterios de rentabilidad sustentable.

- Visión

Mantener el liderazgo competitivo por medio de una gestión transparente, creativa e innovadora. Lograr la fidelidad del cliente para ampliar y garantizar el mercado. Generar rentabilidad sustentable para beneficio de nuestros accionistas y colaboradores y para el desarrollo del país.

[6] Imágenes obtenidas del manual de inducción Pasa.

1.1.1 Ubicación Geográfica

La Pasamanería S.A está ubicada en Ecuador, en la provincia del Azuay, en la ciudad de Cuenca, en la Av. Huayna Capac 1-97 y Pio Bravo. En la figura 1.3 se muestra un mapa de la Ubicación de la fábrica.

Figura 1.3. ***Mapa de la ubicación física de la Pasamanería S.A.***[7]

1.1.1.1 Distribución de espacios.

La fábrica se encuentra implantada en 36.014 m2 de área total. Sin embargo la fábrica está distribuida de la siguiente manera:

- En áreas de producción 22.342 m2.
- En área de oficinas 862 m2.
- En áreas libres 6.868 m2
- Areas verdes 2.250 m2
- En viviendas 3.692 m2.

[7] www.pasa.ec

1.1.2 Estructura Organizacional

La estructura organizacional se indica en el Anexo1, el cual representa el organigrama de la fábrica.

1.2 Línea de confecciones, insumos textiles, hilos.

Todas las prendas elaboradas en la Pasamanería S.A, tienen una mezcla de fibra de 65% algodón 35% poliéster.

La línea de confecciones esta subdividida de la siguiente manera:

- Ropa de bebé.
- Ropa infantil masculina y femenina.
- Ropa interior femenina y masculina.
- Ropa casual femenina y masculina.
- Ropa deportiva.
- Ropa de dormir femenina y masculina.
- Calcetines.
- Línea de mantelería.

La línea de pasamanerías o insumos textiles:

- Cintas y cintillos.
- Elásticos.
- Trenzados.
- Encajes.
- Cordones torcidos.
- Reatas.
- Metalizados (dorados y plateados).
- Hilos de seda.
- Mallas (telas).

Línea de hilos:

- Hilo de costura industrial.
- Hilo de bordado.
- Hilo de tejido.
- Piolas.

1.3 Situación actual.

Pasamanería S.A., es manejada por su Gerente General el Sr. Pietro Tosí, y por la Subgerencia General que es presidida por el Ing. Augusto Tosi.

La empresa cuenta con diferentes departamentos que son los siguientes:

- Gerencia de Proyectos.
- Departamento de Compras
- Departamento de Diseño
- Departamento de Auditoría Interna
- Gerencia de Sistemas
- Gerencia de Producción.
- Gerencia de Ventas.
- Gerencia de Mercadeo.
- Gerencia Financiera de la Comercializadora
- Gerencia de Finanzas
- Gerencia de Recursos Humanos.
- Mantenimiento General.

La Gerencia de Proyectos, los Departamentos de Compras, Diseño, Auditoría Interna y la Gerencia de Sistemas, funcionan en la fábrica como áreas de staff, esto quiere decir de apoyo para todas las secciones de la organización.

La Gerencia de Producción, se encuentra dirigida por el Ing. Manuel Espinoza, la cual es la responsable de lograr la mayor producción, de la mejor calidad, con el menor

tiempo y desperdicio optimizando recursos. Este departamento comprende toda el área de planta.

La Gerencia de Mercadeo, es manejada por el Ing. Juan Tosi y es el departamento encargado del control y manejo de las ventas, políticas de mercado para optimizar las ventas; bajo su dependencia se encuentran las Gerencias de Producto tanto para la línea de insumos como para la línea de confecciones, así como el manejo de los almacenes de la empresa.

La Gerencia Financiera de la comercializadora, realiza el manejo y control tanto administrativo como financiero del área de la comercialización en operaciones de venta, que va desde el pedido del cliente hasta la cobranza. Esta área es manejada por el Econ. Lucila Palacios.

La Gerencia de Finanzas, este departamento es manejado por el Econ. Edmundo Pauta y es el que administra el área contable, financiera y económica de la empresa, procurando el uso eficiente de los recursos financieros para generar la mejor rentabilidad económica y financiera posible.

La Gerencia de Recursos Humanos, este departamento está bajo el cargo de la Ing. Diana Feicán, cuyas principales funciones se puede mencionar las de atraer, mantener y desarrollar los recursos humanos necesarios para el funcionamiento de la organización.

El área de Mantenimiento General, vela por el buen mantenimiento tanto de la maquinaria como de la infraestructura general de la empresa. Abarca áreas como las de mecánica, electromecánica, carpintería y limpieza.

CAPITULO 2

REVISIÓN DE CONCEPTOS DE INTERNETWORKING

2.1 Revisión de los conceptos de red.

2.1.1 Red

Una red informática, es un conjunto de computadoras conectadas por medio de cables, señales, ondas con el objetivo de compartir información o recursos, los mismos que pueden ser Cd-Rom, impresoras, programas, y también servicios como acceso a internet, e-mail, chat, juegos, etc., además da la posibilidad de creación de grupos de trabajo, gestión centralizada, acceso a otros sistemas operativos. En la figura 2.1 se muestra la estructura de una red.

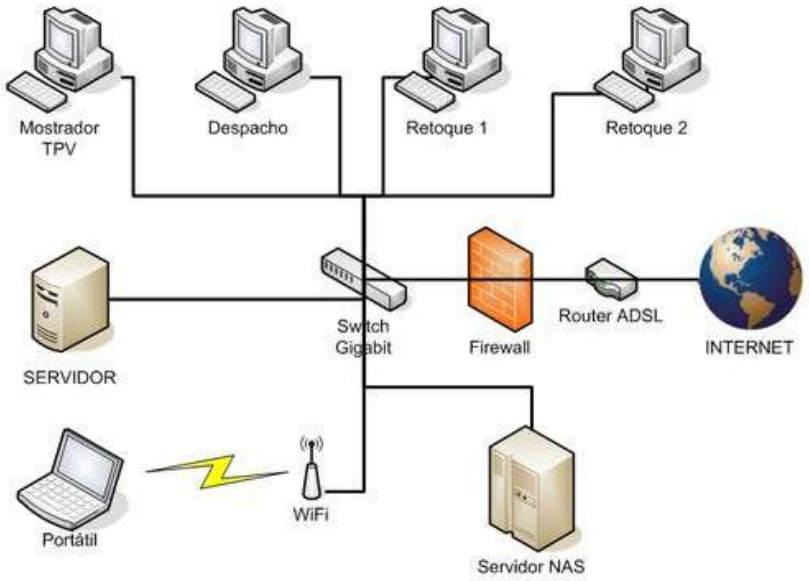


Figura 2.1. ***Estructura de una Red.***[8]

[8] http://topicosusscez.wordpress.com/2009/10/28/

A continuación se explicara los diferentes dispositivos de redes, los más comunes y utilizados.

2.1.2 Dispositivos de Red.

2.1.2.1 Cableado.

Una red está compuesta por un sistema de cableado, que conecta las estaciones de trabajo con los servidores de archivos y otros periféricos. Existen varios tipos de cableados, cada uno con sus propias características en cuanto al costo, velocidad y capacidad.

2.1.2.1.1 Cable de par trenzado.

Un cable de par trenzado consta de dos hilos de cobre aislados y entrelazados. Hay dos tipos de cables: cable de par trenzado sin apantallar (UTP) y par trenzado apantallado (STP).

- **UTP o trenzado sin apantallar**: Se utilizan para redes locales, son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal, sin embargo este tipo de cable es el más usado en los últimos años en las redes. En la figura 2.2 se muestra este tipo de cable.

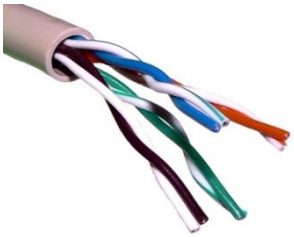


Figura 2.2. *Cable UTP*.[58]

- **STP o Par trenzado apantallado:** Este cable utiliza una envoltura con cobre trenzado, más protectora y de mayor calidad que la usada en el cable UTP.

[58] http://tics-garcia2.blogspot.com/2008/10/211-medios-de-transmisin.html

STP también utiliza una lámina rodeando cada uno de los pares de hilos. Esto ofrece un excelente apantallamiento en los STP para proteger los datos transmitidos de ruidos, lo que permite soportar mayores tasas de transmisión que los UTP a distancias mayores, este tipo de cable es más caro que el UTP. En la figura 2.3 se muestra este tipo de cable.

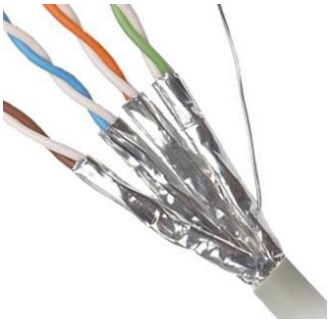


Figura 2.3. *Cable STP*.[59]

2.1.2.1.2 Cable coaxial

Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas.

A inicios fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive. Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos. En la figura 2.4 se muestra este tipo de cable y sus partes.

Este cable se puede utilizar en diferentes aplicaciones como:

- Entre la antena y el televisor.
- En las redes urbanas de televisión por cable e Internet.
- En las redes de transmisión de datos como Ethernet

[59] http://sincables.com.ve/blog/?p=273

- En las redes telefónicas interurbanas y en los cables submarinos.

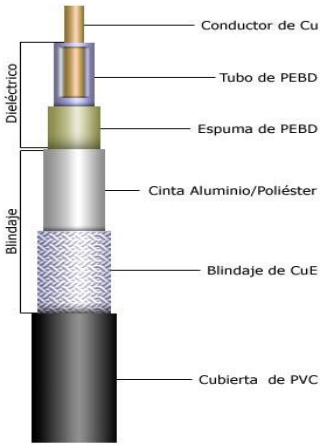


Figura 2.4. *Cable Coaxial*.[60]

2.1.2.1.3 Cable de fibra óptica

El cable de fibra óptica es habitualmente utilizado en redes de datos, el cual está compuesto de un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Las fibras son utilizadas en su mayoría en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia siendo inmune a la interferencia de frecuencias de radio; además las fibras son utilizadas para redes locales, en donde se necesite una alta confiabilidad y fiabilidad, teniendo así un costo mayor que los cables de transmisión anteriormente mencionadas. En la figura 2.5 se muestra una imagen de la fibra óptica.

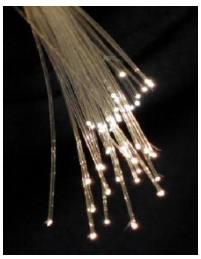


Figura 2.5. *Cable de Fibra Óptica*.[61]

[60] http://www.qsl.net/xe3rn/coaxiales.htm

[61] http://upload.wikimedia.org/wikipedia/commons/4/49/Fibreoptic.jpg

A continuación, en la tabla 2.1, se indica los estándares que plantea la IEEE para la utilización de *Fast Ethernet*[62].

Nombre	Cable	Segmento Máx.	Nodos/seg	Ventajas
10Base5	Coaxil Grueso	500 m	100	Bueno para backbone. Ethernet Grueso.
10Base2	Coaxil Delgado	200 m	30	Sistema más barato. Ethernet Delgado
10Base-T	Par Trenzado	100 m	1024	Fácil Mantenimiento
10Base-F	Fibra Optica	2000 m	1024	Mejor entre edificios. Cara.

Tabla 2.1. ***Estándares de cable planteado por la IEEE para la utilización en Fast Ethernet (tarjetas de red).***

2.1.2.2 Tarjetas de red.

Este es el dispositivo más utilizado en la actualidad para conectar un equipo a la red, es de tamaño estándar que puede venir de forma integrada en las placas base o individualmente, se coloca en ranuras de ampliación de las PC, a diferencia en las computadoras portátiles ya vienen incorporadas.

Las tarjetas de red actúan como la interfaz entre un ordenador y el cable de red. La función de la tarjeta de red es la de preparar, enviar y controlar los datos en la red. En la figura 2.6 se muestra una tarjeta de red.

Figura 2.6 ***Tarjeta de Red.***[63]

2.1.2.3 Modem.

El modem es usado para la transmisión de datos vía telefónica, el cual convierte señales o pulsaciones en información, comunicándose con el *ISP*[64] mediante una

[62] Fast Ethernet. Estándares IEEE de redes Ethernet de 100Mbps.
[63] http://www.monografias.com/trabajos37/tarjetas-red/tarjetas-red.shtml

línea telefónica, con un modem se puede descargar información, enviar y recibir datos, también existen algunos módems que pueden enviar y recibir faxes y llamadas telefónicas , etc.

2.1.2.3.1 Funcionamiento del Módem

La computadora es un dispositivo digital, a diferencia de las líneas telefónicas son dispositivos análogos. La función del modem es unir el espacio entre estos dos tipos de dispositivos. Debe enviar los datos digitales de la computadora a través de líneas telefónicas análogas.

Logra esto modulando los datos digitales para convertirlos en una señal análoga, es decir, el módem varía la frecuencia de la señal digital para formar una señal análoga continua y cuando el módem recibe señales análogas a través de la línea telefónica, hace el opuesto: demodula, o quita las frecuencias variadas de la onda análoga para convertirlas en impulsos digitales. De estas dos funciones, MODulación y DEModulación es el nombre del módem. En la figura 2.7 se muestra un modem con sus partes principales.

Figura 2.7. ***Modem ADSL FAQS.***[65]

2.1.2.4 Hub.

Un Hub es un dispositivo que permite conectar entre sí otros equipos o dispositivos ya que tiene varios puertos, a cada uno de estos puertos se conecta un dispositivo que

---

[64] ISP. Proveedor de Servicios de Internet.

[65] http://articulo.mercadolibre.com.ec/MEC-7005995-modem-internet-motorola-sb5101-sb5100-nunca-abierto-sin-caja-_JM

puede o no transmitir datos, cuando lo hace el Hub transmite el mensaje a todos los puertos menos al que lo envió.

Este dispositivo en la actualidad no es muy redes grandes por su velocidad, sin embargo es bastante útil en redes pequeñas de pocas computadoras, pero su utilización se debe realizar con cuidado ya que podemos colisionar o saturar a la red dejando totalmente inoperable a la misma. En la figura 2.8 se muestra un HUB y un ejemplo de red con este dispositivo.

(a) (b)

Figura 2.8. ***Representación de un HUB: (a) HUB NETGEAR[66] y (b) Esquema de red con HUB[67].***

2.1.2.5 Switch

Este es un dispositivo de interconexión de redes de computadoras, opera en la capa 2 del modelo *OSI*[68] es decir el nivel de enlace de datos, estos tienen la particularidad de aprender y almacenar las direcciones de dicho nivel, por lo que siempre irán desde el puerto de origen directamente al de llegada.

La función de este dispositivo a más de interconectar computadoras, sirve para expandir la red conectando múltiples dispositivos dentro de un edificio o campus, por ejemplo puede conectar los ordenadores, impresoras y servidores, creando una red de recursos compartidos.

Cabe recalcar que este dispositivo permite ahorrar dinero y aumentar la productividad.

Existen dos tipos básicos de switch los cuales son los gestionados y no gestionados.

[66] http://www.alegsa.com.ar/Dic/hub.php

[67] http://www.taringa.net/posts/apuntes-y-monografias/5291084/Administracion-de-redes.html

[68] OSI. Modelo de interconexión de sistemas abiertos, divide las tareas de red en 7 niveles.

- **Los switch gestionados:** Permiten acceder a ellos para programarlos, se puede monitorizar y ajustar local o remotamente, para proporcionarle al switch el control de cómo transmite el tráfico en su red y quien tiene acceso a su red.
- **Los switch no gestionados:** Funcionan de forma automática y no permiten realizar cambios. Un ejemplo de quienes utilizan estos tipos de switch son los equipos de redes domésticas.

Además el switch se encarga de encaminar la conexión hacia el puerto requerido por una única dirección y de esta manera reduce el tráfico y disminuye las colisiones notablemente. En la figura 2.9 se muestra un switch.

Figura 2.9. *Switch.*[69]

2.1.2.6 Router.

El Router es un dispositivo que sirve para la interconexión de redes informáticas que opera en la capa tres perteneciente al nivel de red, trabajan con direcciones IP[70], el cual nos permitirá el enrutamiento de paquetes de datos entre redes, lee cada paquete y lo envía atreves del camino más eficiente al destino, toma en cuenta factores como líneas más rápidas, líneas menos saturadas, etc.

A continuación se dará una explicación de lo que anteriormente llamamos paquete de datos.

Es la unidad fundamental de transporte de información en todas las redes de computadoras, el mismo que está compuesto por tres elementos:

[69] http://wakon.nirewiki.com/listado+de+los+equipos+utilizados+en+la+red+de+datos+

[70] Direcciones IP. Es un número que identifica lógica y jerárquica a una computadora.

- **Una cabecera:** Contiene la información necesaria para transportar el paquete desde el emisor hasta el receptor.
- **Área de datos:** Contiene los datos que se trasladarán.
- **Cola:** Comúnmente incluye código de detección de errores.

2.1.2.6.1 Enrutadores inalámbricos.

Tradicionalmente los routers o enrutadores solían tratar con redes fijas como Ethernet[71], actualmente se utilizan en la mayoría de casos enrutadores que permiten realizar una conexión entre redes fijas y móviles es decir inalámbricamente.

La diferencia al tradicional es que este permite la conexión de dispositivos inalámbricos a las redes a las que el enrutador está conectado mediante conexiones por cable, una clara diferencia es la potencia que alcanza, las frecuencias y los protocolos que trabajan.

2.1.2.6.2 Router ADSL.

Es un dispositivo que permite conectar uno o varios equipos o incluso una LAN[72], este router trata de varios componentes en uno solo, el cual realiza las funciones de:

- **Puerta de enlace:** Es decir proporciona salida hacia el exterior a una red local.
- **Router:** Dirige el paquete procedente de internet hacia el destino por medio del camino correspondiente, es decir es capaz de encaminar paquetes IP.
- **Módem ADSL:** Este es el que modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos.

[71] Ethernet. Es un estándar de redes de computadoras de área local.

[72] LAN. Red de área local.

- **Punto de acceso wireless:** Esto es lo más común que se utiliza ya que algunos router ADSL permiten la comunicación vía Wireless es decir sin cables con los equipos de la red local.

En la actualidad los avances tecnológicos son muy interesantes, ya que han conseguido introducir la funcionalidad de cuatro equipos en uno solo como se explico anteriormente. En la figura 2.10 se muestra un Router.

Figura 2.10. *Router.*[73]

2.1.2.7 Microonda.

Es un tipo de red inalámbrica que utiliza microondas como medio de transmisión, generalmente transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps.

2.1.2.7.1 Funcionamiento.

El servicio utiliza una antena que se coloca en un área despejada sin obstáculos que pudieran entorpecer una buena recepción en el edificio o la casa del receptor y se coloca un módem que interconecta la antena con la computadora. La comunicación entre el módem y la computadora se realiza a través de una tarjeta de red, que deberá estar instalada en la computadora.

La tecnología inalámbrica trabaja bien en ambientes de ciudades congestionadas, ambientes suburbanos y ambientes rurales. En la figura 2.11 se muestra un ejemplo de red Microonda.

[73]http://www.comprawifi.com/routers-aps-switch/routers-y-aps/belkin/belkin-router-adsl-802-11g-54mbps-4-puertos-rj45/prod_1430.html

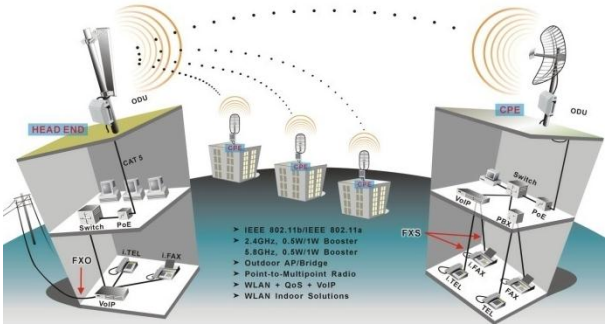


Figura 2.11. ***Microonda.***[74]

2.1.2.8 Red por infrarrojos.

Las redes por infrarrojos permiten la comunicación entre dos nodos, se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, con la desventaja que cada dispositivo necesita ver al otro para realizar la comunicación por ello es escasa su utilización a gran escala, además de que el rango de velocidad y el tamaño de los datos a enviar/recibir es pequeño. Existen tres tipos de redes infrarrojas:

- Punto a punto: Requiere una línea de visión entre emisor y receptor para comunicarse.
- Cuasi-difuso: No es necesaria la línea-de-visión entre dos estaciones, ya que se comunican por medio de superficies reflectantes, es el más recomendable y el más fácil de incrementar.
- Difuso: Es el más flexible y no necesita la línea-de-visión.

[74] http://comunicacionredes.wordpress.com/category/informatica/comunicacion-y-redes/

Figura 2.12. ***Infrarrojos.***[75]

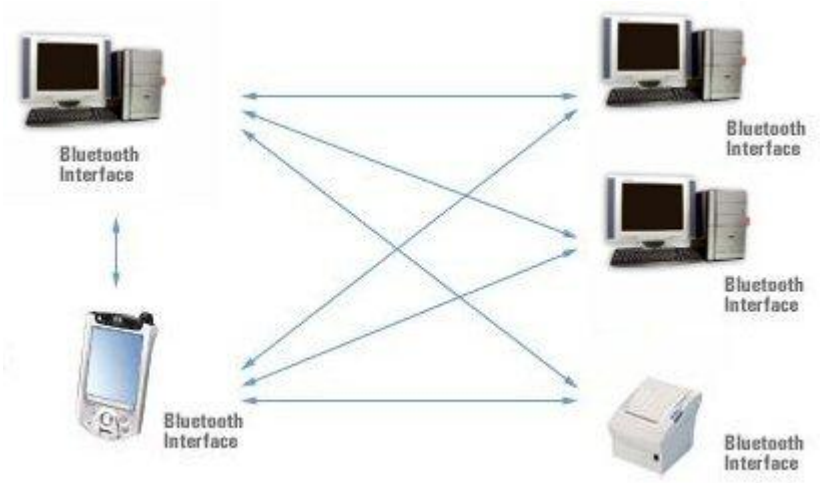
2.1.2.9 Bluetooth.

El bluetooth es un sistema de transmisión de datos y voz, que funciona por ondas de radio para transmitir, la frecuencia del bluetooth está abierta globalmente, esto significa que se puede utilizar sin mediar un pago por estar ocupando esta banda del espacio radioeléctrico.

Este protocolo de transmisión nació para facilitar la conexión entre diferentes aparatos, sin necesidad de cables, para poder crear pequeñas redes entre ellos como móviles, pdas, ordenadores portátiles, etc. En la figura 2.13 se muestra un ejemplo de dispositivos bluetooth.

Las funciones principales del bluetooth son las siguientes:

- Eliminación de la necesidad de conexiones por cable entre los productos y accesorios electrónicos.
- Intercambio de archivos, tarjeta de visitas, citas del calendario, etc. entre usuarios del bluetooth.
- Sincronización y transferencia de archivos entre dispositivos.



[75] http://manolo10-victor.blogspot.com/2009_05_01_archive.html.

Figura 2.13. *Bluetooth.*[76]

2.1.2.10 Red Satelital.

Son redes que utilizan como medios de transmisión satélites artificiales localizados en órbita alrededor de la tierra.

2.1.2.10.1 Elementos de las redes satelitales:

- **Transponders.** Es un dispositivo que realiza la función de recepción y transmisión. Las señales recibidas son amplificadas antes de ser retransmitidas a la tierra. Para evitar interferencias les cambia la frecuencia.
- **Estaciones terrenas.** Las estaciones terrenas controlan la recepción con el satélite y desde el satélite, regula la interconexión entre terminales, administra los canales de salida, codifica los datos y controla la velocidad de transferencia.

Consta de 3 componentes:

- **Estación receptora:** Recibe toda la información generada en la estación transmisora y retransmitida por el satélite.
- **Antena:** Capta la radiación del satélite y concentrarla en un foco donde está ubicado el alimentador, ignorando las interferencias y los ruidos en la mayor medida posible.
- **Estación emisora:** Esta compuesta por el transmisor y la antena de emisión. La potencia emitida es alta para que la señal del satélite sea buena. Esta señal debe ser captada por la antena receptora.

El funcionamiento de la red satelital se puede observar en la figura 2.14

[76] http://articulo.mercadolibre.com.ec/MEC-7107895-red-bluetooth-antena-router-pc-laptop-nokia-lg-sony-samsung-_JM

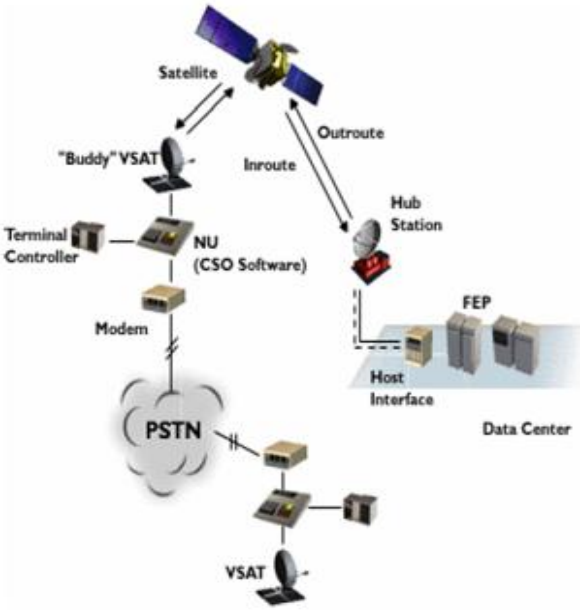


Figura 2.14 Red Satelital.[77]

2.1.2.11 Servidor.

Los servidores forman parte de una red y se lo visualiza desde dos puntos diferentes, de tipo software y hardware pero a la final ambos proveen servicios a otras aplicaciones llamados clientes.

Algunos servicios habituales son, los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final, es decir el propósito de estos servidores es proveer datos que otras maquinas puedan utilizar.

2.1.2.11.1 Tipos de servidores:

- **Servidor web:** Es un ordenador que usa el protocolo http para enviar páginas web cuando el usuario lo solicita.
- **Servidor de archivo**: Este servidor es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.
- **Servidor de correo**: Este servidor almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.

[77] **http://www.mailxmail.com/curso-introduccion-comunicaciones-satelite/diagrama-tipico-2**

- **Servidor de fax**: Este servidor almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiada de fax.
- **Servidor de Base de Datos**: Este servidor provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor.

Los servidores web, servidores de correo y servidores de bases de datos son a lo que tiene acceso la mayoría de la gente al usar Internet.

2.1.2.12 Firewall.

Firewall trata de un dispositivo o conjunto de dispositivos configurados para bloquear el acceso no autorizado a la red, un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial a más de virus o de algún archivo malicioso del Internet, ya que todos los mensajes que entren o salgan de la intranet pasan a través de los firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. En la figura 2.15 se muestra un ejemplo de la implementación de firewall.

El firewall presenta las siguientes ventajas:

- **Protege de intrusiones:** El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- **Protección de información privada:** Un punto muy importante es que permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tenga acceso sólo a los servicios e información que le son estrictamente necesarios.

- **Optimización de acceso:** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

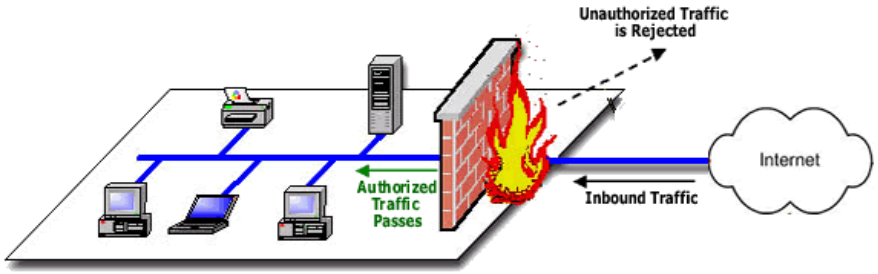


Figura 2.15. ***Firewall.***[78]

2.1.3 Topologías de Red.

La topología de red se refiere a la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que la conectan. Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de las topologías es buscar la forma más económica y eficaz de conectarlas.

2.1.3.1 Topologías físicas.

Es la forma en la que el cableado se realiza en una red. Existen tres topologías físicas puras:

2.1.3.1.1 Topología en bus.

Todas las computadoras están conectadas a un cable central, llamado el bus. Las redes de bus lineal son las más fáciles de instalar y son relativamente baratas. La ventaja es su simplicidad. En la figura 2.16 se muestra un esquema de topología de bus.

[78] https://www.esbroker.com/in/como-funciona/faq/6-Inform%C3%A1tica%20y%20Comunicaciones/16-Firewall.html

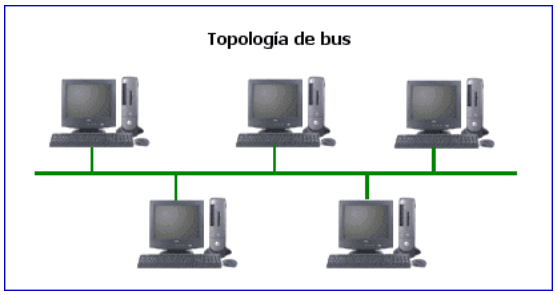


Figura 2.16. ***Topología de bus.***[79]

2.1.3.1.2 Topología en estrella

Las redes de esta topología tienen una caja de conexiones llamada *hub* o concentrador en el centro de la red. Todas las PC se conectan al concentrador, el cual administra las comunicaciones entre computadoras. En la figura 2.17 se muestra un esquema de topología de estrella.

Figura 2.17. ***Topología de estrella.***[80]

2.1.3.1.3 Topología en anillo.

El cableado y la disposición física son similares a los de una topología de estrella, con la diferencia que en lugar de que la red de anillo tenga un concentrador en el centro, tiene un dispositivo llamado MAU.

La MAU realiza la misma tarea que el concentrador, pero en lugar de trabajar con redes Ethernet lo hace con redes *Token Ring*[81] y maneja la comunicación entre computadoras de una manera ligeramente distinta.

---

[79] http://verdirame.blogspot.com/2010/04/proponer-topologia-de-red-de-area-local.html

[80] http://verdirame.blogspot.com/2010/04/proponer-topologia-de-red-de-area-local.html

[81] Token Ring. Usa una topología donde cada computadora está conectada a la siguiente formando un anillo.

Todas las computadoras o nodos están conectados el uno con el otro, formando una cadena o círculo cerrado. En la figura 2.18 se muestra un esquema de la topología de anillo.

Figura 2.18. ***Topología de anillo*****.**[82]

2.1.3.1.4 Topología en estrella extendida.

Conecta los dispositivos centrales de varias topologías en estrella simple a un dispositivo de red central.

Figura 2.19. ***Topología en estrella extendida***.[83]

2.1.3.1.5 Topología jerárquica.

Conecta los host a un dispositivo de red principal y luego se va expandiendo hacia afuera con ayuda de los equipos de red.

[82] http://verdirame.blogspot.com/2010/04/proponer-topologia-de-red-de-area-local.html
[83] http://topologiadered-kelvin.blogspot.com/2009/05/topologia-en-estrella.html

Figura 2.20. ***Topología Jerárquica***.[84]

2.1.3.1.6 Topología de malla.

Interconecta todos los host y es una topología muy costosa y además confiada y generalmente es utilizada cuando no se puede interrumpir las comunicaciones.

Figura 2.21. ***Topología de malla.***[85]

2.1.3.2 Topologías lógicas.

Estas topologías se refieren a la forma de cómo la red reconoce a cada conexión de estación de trabajo.

De las más comunes son las siguientes:

[84] http://members.fortunecity.es/infokmas/index/memorias/memorias.htm

[85] http://long-way-short-life.blogspot.com/2010/03/topologia-malla.html

2.1.3.2.1 La topología Broadcast.

Se refiere cuando un host envía sus datos a todos los equipos conectados al medio, la transmisión no es controlada.

2.1.3.2.2 Topología de transmisión de Tokens.

Se refiere que para controlar las transmisiones, mediante el envió de un token, un host puede transmitir solo cuando ah aceptado la señal del token.

2.2 Modelo Jerárquico

El modelo jerárquico fue creado para describir la red, con el fin de simplificar el diseño, implementación y administración de las redes.

De esta menara, tenemos un diseño fácilmente entendible, este modelo separa la red en 3 niveles. Cada capa tiene funciones específicas asignadas y no se refiere necesariamente a una separación física, sino lógica.

La figura 2.22 muestra la representación jerárquica de la red, dividida en sus 3 capas lógicas.

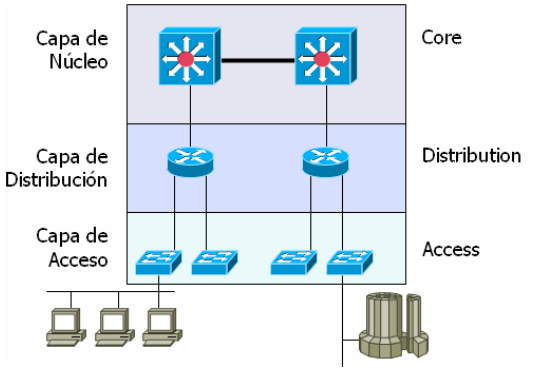


Figura 2.22. ***Modelo Jerárquico.***[86]

2.2.1 Capa de acceso.

[86] http://www.ipref.info/2008/11/el-modelo-jerarquico-de-3-capas-de.html

A esta capa de acceso corresponde el punto en el que cada usuario se conecta a la red. Por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario.

Los recursos más utilizados por los usuarios en esta capa son switch, hub, access point, bridges y usuarios finales.

2.2.2 Capa de distribución

Esta capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red y permite a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web, a mas de realizar funciones como enrutamiento, filtrado y acceso a WAN.

La capa de distribución abarca una gran diversidad de funciones tales como:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Traducir los diálogos entre diferentes tipos de medios, como Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución determina la forma más rápida para que la petición de un usuario pueda ser remetida al servidor.

Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo, y la capa de núcleo podrá entonces transportar la petición al servicio apropiado.

2.2.3 Capa de núcleo

La capa del núcleo se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados de una manera confiable y veloz.

Algunos servicios de esta capa son e-mail, el acceso a Internet o la videoconferencia.

El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado.

2.3 Panorámica del modelo de referencia OSI

El modelo OSI fue creado por la *ISO*[87] con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes, así todo dispositivo de computo y telecomunicaciones podrá ser referenciado a este modelo con características muy precisas en cada nivel.

Este modelo es considerado una arquitectura de redes, ya que especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes, el mismo que está dividido en siete como se muestra en la figura 2.23.

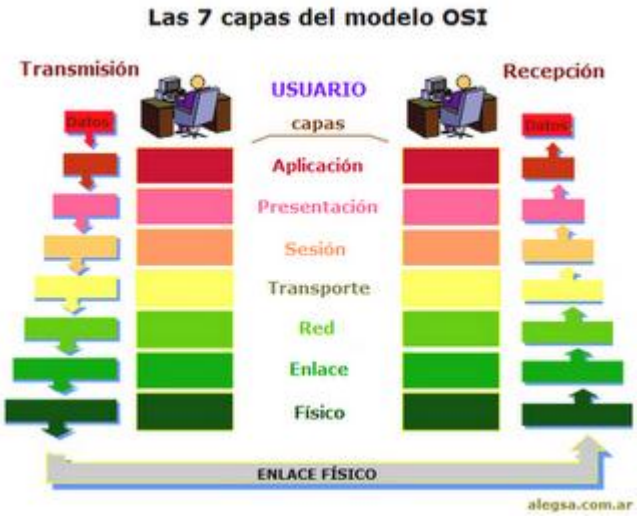


Figura 2.23. ***Modelo de referencia OSI.***[88]

[87] ISO. Organización Estándar Internacional.
[88] http://gruppo9.blogspot.com/2009/07/funcion-de-dispositivos-se-encuentran.htm

2.3.1 Nivel Físico (Capa 1).

El nivel físico, corresponde a la primera capa del modelo de referencia OSI y básicamente es la que se encarga de las conexiones físicas de la computadora hacia la red, pudiendo ser:

- **Medios guiados:** Cable coaxial, cable de par trenzado, fibra óptica, etc.
- **Medios no guiados:** Radio, infrarrojos, microondas, láser y otras redes inalámbricas.

2.3.1.1 Funciones de la capa física

Esta capa se encarga de las siguientes funciones:

- Son los que transmiten el flujo de bits a través del medio.
- Son los que manejan las señales eléctricas y electromagnéticas.
- Define si la trasmisión es uni o bidireccional (símplex, dúplex o full-dúplex).
- Características del medio físico de trasmisión, es decir tipo de cable o calidad del mismo, tipo de conectores normalizados o a su vez tipo de antena.
- Definen las características de los materiales como componentes, conectores mecánicos y eléctricas, de este ultimo los niveles de tensión que se van a usar en la transmisión de los datos por los medios físicos.
- Definen las características funcionales de la interfaz, el establecimiento, mantenimiento y liberación del enlace físico.
- Son los que garantizan la conexión, aunque no la fiabilidad de ésta.

2.3.1.2 Medio físico y conectores

2.3.1.2.1 Conectores.

- Los RS-232 consiste en un conector tipo DB-25 de 25 pines, aunque es normal encontrar la versión de 9 pines DE-9, más barato e incluso más extendido para cierto tipo de periféricos como el ratón serie del PC, como se muestra en la figura 2.24.

Figura 2.24. *RS-232.*[89]

- Los v.24 son adaptadores y con ayuda de un microcontrolador con el software respectivo puede reproducirse por partes una interfaz RS232, como se muestra en la figura 2.25. Este adaptador pone a disposición algunas señales de modem estándar.

Figura 2.25. Adaptador V.24.[90]

- Los conectores RJ 45 es básicamente una interfaz física para conectar redes de cableado estructurado, el mismo que posee 8 pines y que generalmente es usado en los extremos de cables de par trenzado.

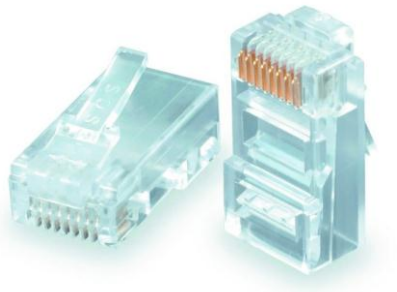


Figura 2.26 Conector RJ-45.[91]

- Sistemas satelitales, microondas, radio enlaces, canales digitales y líneas privadas.

[89] CISCO
[90] http://www.mcls-modular.de/espaniol/hardware/hw_v24.htm
[91] http://compuescazu.com/tienda/product_info.php?cPath=38&products_id=493

- Además, la capa física también se encarga de dispositivos pasivos y activos que permiten la conexión de los medios de comunicación como repetidores de redes LAN, repetidores de microondas, concentradores de cableado (HUB), conmutadores de circuitos físicos de telefonía o datos, equipos de modulación y demodulación (módems) y hasta los aparatos receptores telefónicos convencionales.

2.3.2 Capa de enlace de datos (Capa 2).

El nivel de la capa de enlace de datos corresponde al segundo nivel del modelo de referencia OSI y es una capa lógica adicional sobre el nivel físico para controlar y gestionar el intercambio de información. El objetivo del nivel de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente.

En Resumen la capa de Enlace de Datos hace lo siguiente:

- Direccionamiento en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que el ordenador debe seguir para transmitir y recibir mensajes.
- Realizar la transferencia de datos a través del enlace físico.
- Distribución ordenada de tramas las mismas que son pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

Esta capa se subdivide en 2 subcapas las cuales se verá a continuación.

- Control de acceso al medio (MAC 802.3)
    - Como transmitir tramas en el cable físico.
    - Gestiona direccionamiento físico.
- Control de enlace Lógico (LLC 802.2)
    - Identificación de protocolos y encapsulación.

2.3.2.1 Subcapa Mac (802.3)

La subcapa de control de acceso al medio (MAC), administra el protocolo de acceso al medio físico de red. Cabe recalcar que las direcciones MAC son definidas por la IEEE y son únicas a nivel mundial puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación de esta manera varios dispositivos se identifiquen sin repetición, en la capa de enlace de datos.

La subcapa MAC tiene dos principales propósitos que son:

- **Encapsulado/Desencapsulado de datos. Se refiere al** ensamblado de las tramas después de su transmisión, y la detección de errores en la trama durante la recepción de la misma.
- **Control de acceso al medio,** incluyendo la inicialización de la transmisión de la trama y la recuperación de transmisiones fallidas.

2.3.2.2 Subcapa LLC (802.2)

Esta es la más alta de las dos subcapas de enlace de datos definidas por el IEEE y la responsable del control de enlace lógico.

Las principales funciones de esta subcapa LLC son:

- Agrupar los bits a transmitir en forma de tramas.
- Se ocupa de los errores de transmisión.
- Regula el flujo de las tramas.
- Administra la capa de enlace.
- Traduce las tramas de redes diferentes.
- Direccionamiento de la subcapa MAC.

En esta subcapa LLC se contemplan dos aspectos bien diferenciados los cuales son los Protocolos y las Interfaces.

2.3.2.2.1 Los protocolos.

Los protocolos LLC: Es para la comunicación entre entidades de la propia subcapa LLC, estos definen los procedimientos para el intercambio de tramas de información y de control entre cualquier par de puntos de acceso al servicio del nivel de enlace LSAP es decir a los protocolos de nivel superior.

2.3.2.2.2 Las interfaces.

En este punto se hablara de la interfaz con la subcapa inferior MAC y de la interfaz con la capa superior de Red.

- **Interfaz LLC – MAC:** Se refiere a los servicios que la subcapa de LLC requiere de la subcapa MAC, independientemente de la topología de la subred y del tipo de acceso al medio.
- **Interfaz LLC – Capa de Red:** Servicios que la Capa de Red del Modelo OSI obtiene de la Capa de Enlace de datos.

2.3.3 Capa de red (Capa 3).

La capa de red, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Para realizar la transferencia de archivos de extremo a extremo la Capa 3 utiliza cuatro procesos básicos: direccionamiento, encapsulamiento, enrutamiento y desencapsulamiento. El funcionamiento se puede observar en la figura 2.27.

2.3.3.1 Direccionamiento.

La Capa de red debe proveer un mecanismo para direccionar los dispositivos finales, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

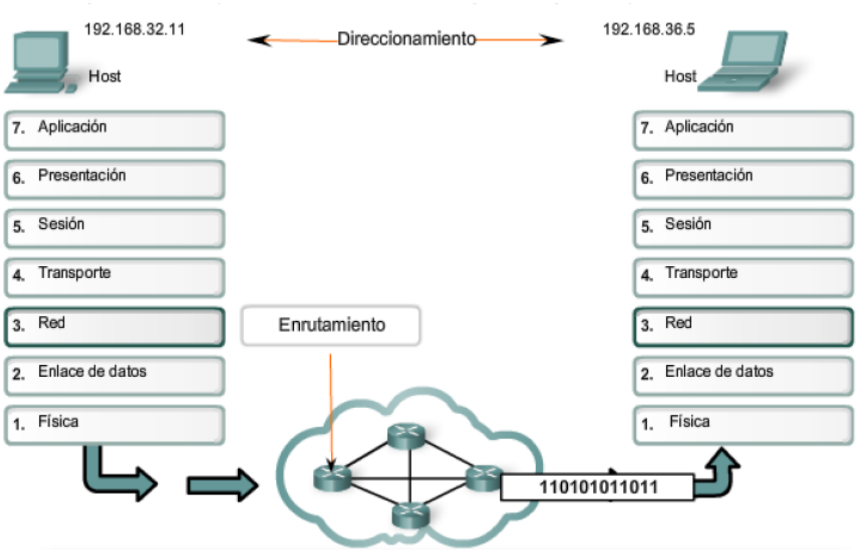


Figura 2.27 ***Procesos básicos de la capa de red.***[92]

2.3.3.2 Encapsulación.

El encapsulamiento trata de un proceso que envuelve los datos con la información de protocolo necesaria antes de transitar por la red, la información se mueve hacia abajo por las capas del modelo OSI, para que cada capa añada un encabezado, antes de pasarla a una capa inferior. Los encabezados contienen información de control para los dispositivos de red y receptores para asegurar la apropiada entrega de de los datos y que el receptor interprete correctamente lo que recibe.

2.3.3.3 Enrutamiento.

El proceso de enrutamiento consiste en proveer los servicios para que a lo largo de la ruta, cada paquete pueda ser guiado a través de la red para que llegue a su destino final, los mismos que no siempre están conectados a la misma red, esto se logra mediante los dispositivos intermediarios que conectan las redes, es decir los routers, cuya función es seleccionar las rutas y dirigir paquetes hacia su destino.

2.3.3.4 Desencapsulamiento.

[92] CISCO

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red, para luego pasar al servicio adecuado en la capa de Transporte.

El propósito de esta capa es el de formar una interface entre los usuarios de una máquina y la red, ya que la red es controlada por esta capa y las 2 primeras.

2.3.3.5 Direcciones de la capa de red

Las direcciones de la capa de red, también se las conoce como direcciones virtuales, las mismas que son de tipo jerárquico.

Una dirección de red virtual está conformada por dos partes: La primea corresponde a cada una de las redes de internetwork, y la otra parte corresponde a los hosts en cada una de las redes.

La parte de la red, identifica cada red dentro de la estructura de la internetwork, permitiendo que los routers identifiquen las rutas de conexión ya que el router utiliza esta dirección para determinar el host destino de los paquetes de red.

La parte del host identifica los dispositivos o un puerto de ese dispositivo.

2.3.3.5.1 Estructura de una dirección IP.

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo que utilice el protocolo Internet Protocol y está dividida en cuatro secciones de 8 bits llamados octetos, los mismos q identifican una red especifica y un host en particular dentro de la red. En la tabla 2.2 se muestran las clases de direcciones IP.

Clase	Cantidad de redes posibles	Cantidad máxima de equipos en cada una
A	126	16777214
B	16384	65534
C	2097152	254

Tabla 2.2. *Clases de direcciones IP*.

2.3.3.5.2 Direcciones IP reservadas.

ICANN[93] ha reservado una cantidad de direcciones, para evitar conflictos de direcciones IP en la red de redes. Estas direcciones son las siguientes:

- Direcciones IP privadas de clase A: 10.0.0.1 a 10.255.255.254; hacen posible la creación de grandes redes privadas que incluyen miles de equipos.
- Direcciones IP privadas de clase B: 172.16.0.1 a 172.31.255.254; hacen posible la creación de redes privadas de tamaño medio.
- Direcciones IP privadas de clase C: 192.168.0.1 a 192.168.0.254; para establecer pequeñas redes privadas.

2.3.3.6 Operativa del router en la capa de red.

Los routers operan en la capa de red registrando y grabando las diferentes redes y eligiendo la mejor ruta para las mismas. En la figura 2.28 se muestra un ejemplo de la operativa del Router en la capa de Red. Los routers colocan esta información en una tabla de enrutamiento, que incluye los siguientes elementos:

Dirección de red. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.

Interfaz. Se refiere a la interfaz usada por el router para llegar a una red dada.

Ésta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.

Métrica. Se refiere al coste o distancia para llegar a la red de destino. Se trata de un valor que facilita al router la elección de la mejor ruta, para llegar al host destino. Esta métrica cambia en función de la forma en que el router elige las rutas.

[93] ICANN. Institución responsable de asignar direcciones IP

Entre las métricas más habituales están las siguientes:

- El número de redes que han de ser cruzadas para llegar al destino (conocido también como saltos).
- El tiempo que se tarda en atravesar todas las interfaces hasta una red dada (conocido también como retraso).
- Valor asociado con la velocidad de un enlace (conocido también como ancho de banda).

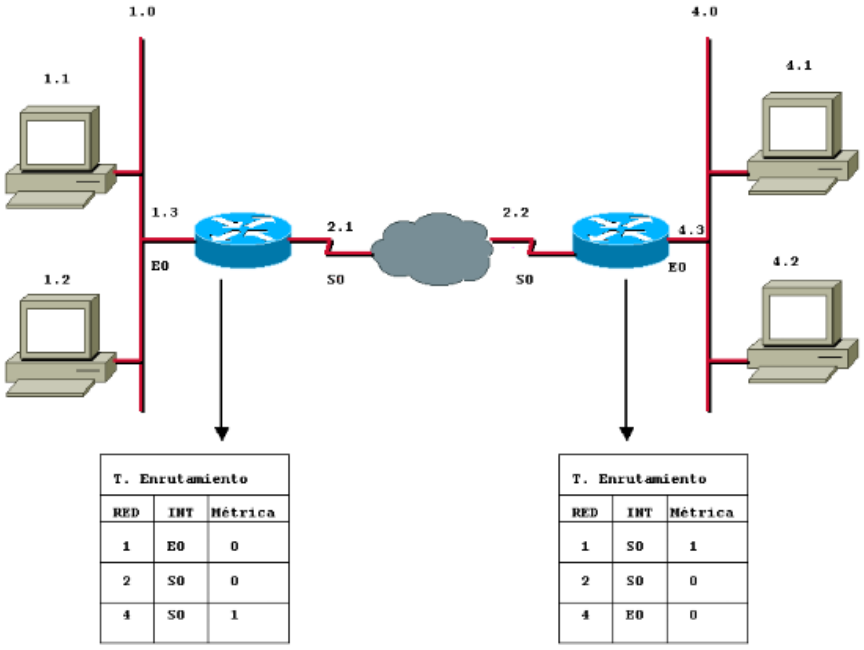


Figura 2.28. ***Operativa del router en la capa de red.***[94]

Para que los routers puedan operar en una red, es necesario que cada tarjeta esté configurada en la red. El router utiliza la información de configuración de la tarjeta para determinar la parte de la dirección correspondiente a la red, a fin de construir una tabla de enrutamiento.

Además de identificar redes y proporcionar conectividad, los router deben proporcionar las siguientes funciones:

[94] CISCO.

- Los routers separan las *tramas*[95] de Capa 2 y envían paquetes basados en direcciones de destino Capa 3.
- Los routers asignan una dirección lógica de Capa 3 individual a cada dispositivo de red por tanto, los routers pueden limitar o asegurar el tráfico de la red basándose en atributos identificables con cada paquete ya que pueden incluir o sacar paquetes.
- Los routers pueden ser configurados para realizar funciones tanto de puenteado como de enrutamiento.
- Los routers proporcionan conectividad entre diferentes LAN virtuales (VLAN) en entornos conmutados.
- Los routers soportan una gran variedad de estándares de conectividad al nivel de la capa física, lo cual ofrece la posibilidad de construir WAN.
- Además, pueden proporcionar controles de acceso y seguridad, que son elementos necesarios cuando se conectan ubicaciones remotas.

2.3.4 Capa de transporte (Capa 4).

La capa transporte es el cuarto nivel del modelo OSI, encargado del transporte de paquetes confiable y eficiente de la máquina origen a la destino, independientemente del tipo de red física que se esté utilizando.

Para lograr este objetivo, la capa de Transporte, hace uso de los servicios proporcionados por la capa de red. El hardware o software que se encarga del trabajo se llama entidad de transporte que puede estar:

- En la Tarjeta de interfaz de red
- En el núcleo del sistema operativo
- En un proceso de usuario independiente
- En un paquete de biblioteca que forma parte de las aplicaciones de la red

Parámetros de la calidad del servicio de la capa de transporte, se observa en la tabla 2.3.

[95] Trama. Es una unidad de envió de datos.

Retardo de Establecimiento de Conexión	Tiempo que transcurre entre la solicitud de una conexión y la confirmación del usuario
Probabilidad de falla de establecimiento de Conexión.	Posibilidad de que una conexión no se establezca en un lapso máximo de tiempo.
Rendimiento	Mide la cantidad de bytes de datos transferidos pos segundo
Retardo de tránsito	Mide el tiempo entre el envío de un mensaje y su recepción por el destino.
Tasa de errores residual	Mide la cantidad de mensajes perdidos o alterados como una fracción del total enviado.
Protección	Mecanismo por el cual el usuario indique su interés en que la capa de transporte, proporcione protección contra terceros no autorizados
Prioridad	Mecanismo para que un usuario indique que conexiones son más importantes.
Tenacidad	Probabilidad de que la capa de transporte termine por sí misma una transmisión debido a problemas interno o congestionamiento.

Tabla 2.3. ***Parámetros de la calidad del servicio de la capa de transporte*****.**

2.3.4.1 Funciones de la capa de transporte.

- La capa de transporte establece las reglas para conectar dos dispositivos remotos.
- Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas unidades si es necesario, y pasarlos a la capa de red.
- Permite que las estaciones finales ensamblen múltiples segmentos del mismo flujo de datos, mediante identificadores llamados números de puerto.
- Permite además que las aplicaciones soliciten transporte fiable entre los sistemas, asegurando que los segmentos distribuidos serán confirmados al remitente.
- Proporciona la retransmisión de cualquier segmento que no sea confirmado.

- Proporciona control de flujo regulando el tráfico de datos.
- En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.
- Establece conexiones punto a punto sin errores para el envío de mensajes

2.3.5 Capa de sesión (Capa 5).

La capa de sesión es el quinto nivel del modelo de referencia OSI, la misma que organiza y sincroniza el diálogo y controla el intercambio de datos, además de controlar el diálogo entre las aplicaciones de los sistemas finales.

Permite a los usuarios de máquinas diferentes establecer sesiones entre ellos, permitiendo el transporte ordinario de datos, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

2.3.5.1 Función.

La capa de sesión tiene las siguientes funciones.

- **Control del Diálogo**: Quién habla, cuándo, cuánto tiempo, este puede ser simultáneo en los dos sentidos (full-duplex) o alternado en ambos sentidos (half-duplex).
- **Agrupamiento**: El flujo de datos se puede marcar para definir grupos de datos.
- **Recuperación**: La capa de sesión puede proporcionar un procedimiento de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación y no desde el principio.

- **Establecer sesión:** Permite a usuarios en diferentes máquinas establecer una sesión la cual puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas.

2.3.6 Capa de presentación (Capa 6)

La capa de presentación es el sexto nivel del modelo de referencia OSI, se podría definir como un protocolo de paso de la información desde las capas adyacentes , a diferencia de todas las capas inferiores que se interesan solo en mover bits de manera confiable de la maquina origen a la maquina destino, la capa de presentación se ocupa de la sintaxis y la semántica de la información que se transmite, además de ser necesario esta capa puede traducir entre distintos formatos de datos y de ordenar, organizar los datos antes de su transferencia.

2.3.6.1 Función de la Capa de Presentación.

- Está a cargo de la presentación de los datos en una forma que el dispositivo receptor pueda comprender.
- Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta una de sus funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión.

  Para comprender esto mejor maneja dos sistemas:

  El primer sistema utiliza el Código de caracteres decimales codificados en binario (EBCDIC) para representar los caracteres en la pantalla.

  El segundo sistema utiliza el Código (ASCII) para el intercambio de la información, la capa de presentación opera como traductor entre estos dos tipos diferentes de códigos.
- Comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos.

2.3.6.2 Cifrado y compresión de datos

La capa de presentación, protege la información durante la transmisión, ya que utiliza una clave de cifrado para cifrar los datos en el lugar origen y luego descifrarlos en el lugar destino.

La capa de presentación también se ocupa de la compresión de los archivos, es decir reducir el tamaño de los archivos, esto se realiza mediante el uso de algoritmos.

2.3.7 Capa de aplicación (Capa 7).

La capa de aplicación es el séptimo nivel del modelo de referencia OSI, ofrece la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros.

Cabe aclarar que el usuario no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, un ejemplo claro es, cuando chateamos con el messenger no es necesario que codifiquemos la información y los datos del destinatario para entregarla a la capa de Presentación para que esta a su vez realice el envió del paquete.

Protocolos que intervienen en esta capa, se exponen en la tabla 2.4.

Protocolo	Uso
HTTP (HyperText Transfer Protocol)	Para acceso a páginas web
FTP (File Transfer Protocol)	Transferencia de archivos.
SMTP (Simple Mail Transfer Protocol)	Envío y distribución de correo electrónico.
POP (Post Office Protocol)	Correo electrónico.
SSH (Secure Shell)	Cifra casi cualquier tipo de transmisión.
Telnet	Para acceder a equipos remotos.
DNS (Domain Name Service)	Servicio de nombres de dominio.

Tabla 2.4. ***Protocolos que intervienen en esta capa de aplicación*****.**

2.3.7.1 Función de la capa de aplicación.

La capa de aplicación es responsable de lo siguiente:

- Identifica y establece la disponibilidad de los socios de comunicación deseados.
- Sincroniza las aplicaciones que cooperan.
- Establece acuerdos con respecto a los procedimientos para la recuperación de errores.
- Controla la integridad de los datos.

2.4 Comunicación entre capas de referencia del modelo OSI.

Las 7 capas correspondientes al modelo de referencia OSI muestran el flujo de información sobre el que navegan los mensajes que se envían de emisor a receptor y la forma en que pasan por cada uno de las capas de tal forma que, cada uno, codifica y decodifica según su protocolo los datos necesarios para enviar la información hacia arriba o abajo en la estructura jerárquica.

Las comunicaciones parten de un origen conocido como emisor y deben llevar a un destino llamado receptor y la información que viaja a atreves de la red se denomina datos o paquetes de datos.

Cuando se da el envió de datos desde el emisor al receptor, se empaquetan los datos a través del proceso encapsulamiento, la misma que es incluir a los datos, la información de protocolo necesario antes de que este en el trafico de la red. Por lo que cuando los datos circulan atreves de las capas del modelo OSI, reciben encabezados e información adicional en cada capa.

Cada capa realiza sus funciones para permitir a los datos desplazarse atreves de la red. Intercambiando información. Para realizar esta comunicación se utiliza las denominadas PDU (Unidad de datos del protocolo), las mismas que controlan la información añadida a los datos del usuario, esta información es la que se agrega en los campos llamados cabecera.

Finalmente, el paquete llega al host destino y se da el proceso de desencapsulado.

2.5 Dominios de colisión y difusión.

En el diseño de una red se debe tener especial cuidado con los llamados Dominios de Colisión y Dominio de difusión (Broadcast).

2.5.1 Dominio de colisión.

Los dominios de colisión son un conjunto de dispositivos que comparten el mismo medio físico, esto se da generalmente mas en un hub, ya que si dos dispositivos acceden al mismo tiempo existirá la colisión entre estas dos, pero esta colisión de señales se puede eliminar con un switch debido a que cada puerto tiene su propio dominio de colisión.

Como resultado de estas colisiones se produce un consumo inadecuado de recursos y de ancho de banda.

A partir de las capas del modelo OSI es posible determinar qué dispositivos extienden o componen los dominios de colisión.

- Dispositivos de la capa 1 OSI (concentradores y repetidores) reenvían todos los datos transmitidos en el medio y por lo tanto extienden los dominios de colisión.
- Dispositivos de la capa 2 y 3 OSI (Conmutadores) segmentan los dominios de colisión.
- Dispositivos de la capa 3 OSI (routers) segmentan los dominios de colisión y difusión.

Cuando la colisión es detectada, ambos equipos dejan de trasmitir, e intentaran trasmitir de nuevo en un tiempo aleatorio. En la figura 2.29 se muestra un ejemplo de dominio de colisión.

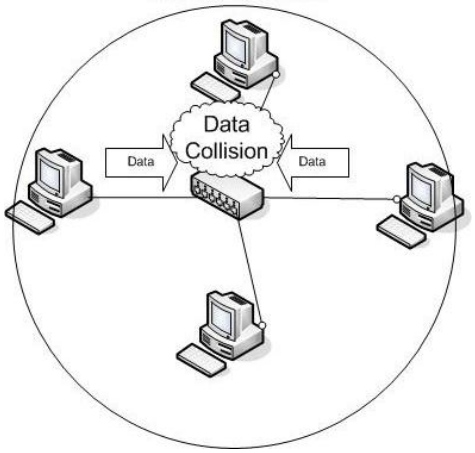


Figura 2.29. ***Dominio de colisión.***[96]

2.5.2 Dominio de difusión.

Un dominio de Difusión, o Broadcast es un área lógica en una red de hosts, ya que son grupos de dispositivos que envían y reciben mensajes de difusión entre ellos sin precisar ningún dispositivo de encaminamiento, pero una cantidad exagerada de estos mensajes de difusión provocara un mal funcionamiento de la red hasta al punto de dejarla completamente congestionada.

2.6 VLAN

Las redes virtuales (VLAN), es una red de área local que agrupa un conjunto de equipos de manera lógica y permite liberarse de las limitaciones de la arquitectura física es decir limitaciones geográficas, limitaciones de dirección. La configuración de las VLAN se hace en los switches mediante software.

Las VLAN funcionan a nivel de Capa 2 y Capa 3 del modelo de referencia OSI ya que la comunicación entre las VLAN es implementada por el enrutamiento de la capa de red.

Además se podría decir que las VLAN proporcionan un método para controlar los *broadcasts*[97] de red y también aumentar la seguridad de la red, definiendo cuáles son los nodos de red que se pueden comunicar entre sí. En la figura 2.30 se muestra un ejemplo de una VLAN.

[96] http://www.thebryantadvantage.com/CCNACCENTCertificationTrainingHubsCollisionDomains.htm

[97] Broadcast. Transmisión de un paquete que será recibido por todos los dispositivos en una red

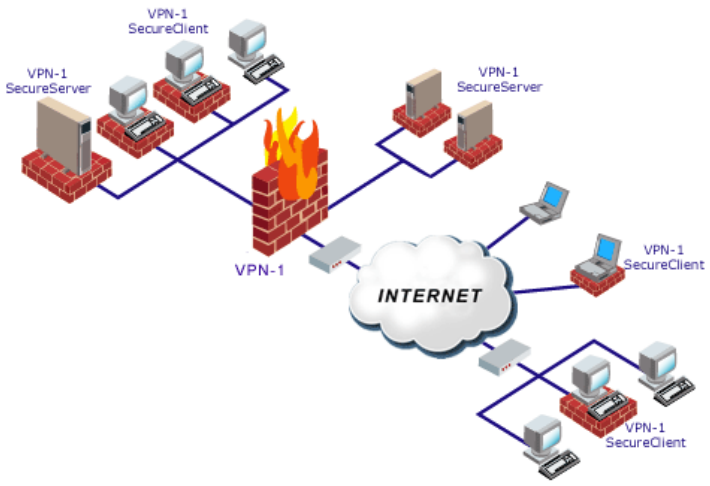


Figura 2.30. *VLAN*.[98]

Las VLANs pueden ser:

Estáticas. En este tipo de VLAN es posible configurar puerto por puerto, es decir realizar asignaciones entre los puertos y las VLANs.

Dinámicas. Aquí los puertos pueden calcular dinámicamente, se usa una base de datos de software que contiene un mapeo de direcciones MAC a las VLAN.

2.6.1 Tipos de VLAN

- La **VLAN de nivel 1 o** VLAN basada en puerto, define una red virtual según los puertos de conexión del switch.
- La **VLAN de nivel 2** o VLAN basada en la dirección MAC, define una red virtual según las direcciones MAC de las estaciones, y la red es independiente de la ubicación de la estaciones.
- La **VLAN de nivel 3**: conlleva lo siguiente:
    - **VLAN basada en la dirección de red,** conecta subredes según la dirección IP de origen de los datagramas (fragmento de paquete) y es de gran ayuda, ya que la configuración de los switch cambia automáticamente cuando se mueve una estación.

[98]http://www.experts-exchange.com/Hardware/Networking_Hardware/Q_23698769.html

- La **VLAN basada en protocolo,** permite crear una red virtual por tipo de protocolo por ejemplo, TCP/IP, IPX, AppleTalk. Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Tener configurado VLANs significa tener los siguientes beneficios en la red:

- Una computadora puede ser trasladada físicamente y seguirá permaneciendo a la misma VLAN sin ningún tipo de reconfiguración, ya están configurados como dominios lógicos.
- Control y conservación del ancho de banda, ya que las redes virtuales tienen la posibilidad de restringir los broadcast a los dominios lógicos q se desee.
- Conectividad, porque se puede conectar diferentes switch y expandir las redes virtuales atreves de los mimos, aunque este situados en lugares geográficamente distintos.
- Aumento de la seguridad en la red, ya que los accesos desde y hacia los dominios lógicos pueden ser restringidos de acuerdo a las necesidades de cada red.
- Disminución de tráfico en la red.
- Ahorro de dinero, al utilizar conmutadores existentes**.**
- Grupos de Trabajo Virtuales.

CAPITULO 3

AUDITORIA DE COMUNICACIONES

3.1 Consideraciones.

3.1.1 Gestión de red: los equipos y su conectividad.

En principio se definirá a lo que hace referencia gestión de red, para posteriormente dar a conocer como se gestiona la red en la Pasamanería.

La *Gestión de red* se refiere a todo el conjunto de actividades dedicadas al control y vigilancia de los recursos de la red, esto se logra empleando una variedad de herramientas, aplicaciones o dispositivos. Cuyo principal objetivo es garantizar un buen nivel de servicio en los recursos gestionados.

Las funciones de gestión de red se basan en dos procedimientos:

3.1.1.1 Monitoreo

El monitoreo es un proceso pasivo, el mismo que se encarga de observar y obtener datos acerca del estado y del comportamiento de configuración de los recursos de la red, analizando las seguridades, fallos en el sistema de la red, con la ayuda de herramientas o equipos.

3.1.1.2 Control

A diferencia del monitoreo, el control es un proceso activo, el cual se basa en obtener información del monitoreo y actuar sobre el comportamiento de los recursos de la red administrada. Además abarca la configuración y seguridad de la red.

La gestión de la red en la pasamanería está administrada de la siguiente manera: se centraliza en un centro de gestión, donde se controla y vigila el correcto funcionamiento de todos los equipos integrados a la red de la fábrica.

Dispone de dos tipos de recursos:

3.1.1.3 Recursos humanos.

El Personal encargado del correcto funcionamiento del centro de gestión de red, corresponde a dos personas, Ing. Marco Orellana y el Ing. Oswaldo Vivar.

3.1.1.4 Herramientas de apoyo.

Las herramientas que facilitan las tareas de gestión a los operadores humanos, corresponde a las siguientes.

3.1.1.4.1 NetOp

NetOp es una herramienta que ayuda al administrador de la red al control y vigilancia constante de la red, accediendo remotamente a todos los puntos de red conectados.

NetOp consta de dos módulos: el módulo Administrador, que está instalado en el equipo del administrador de la red, y el módulo Cliente, que está instalado en todos los equipos que forman parte de la red.

3.1.1.4.2 Team Viewer 5

Con esta herramienta el administrador de la red establece conexión a cualquier ordenador a través de Internet, mediante un Id y una clave que genera Team Viewer, sin tener que preocuparse por cortafuegos, direcciones IP, de esta manera controla a distancia los equipos conectados a la red.

3.1.1.4.3 WebMin

En el centro de gestión de red de la fábrica, hacen uso de la herramienta Webmin, el cual es una interfaz que permite administrar el servidor de correo externo, el mismo que está en el sistema operativo Linux Centos 5.4.

WebMin se ejecuta en el servidor web apache y se compone de un cierto número de módulos que actúan directamente sobre los ficheros de configuración.

La herramienta Webmin en la fabrica está configurado para que funcione con el protocolo https.

Permite por ejemplo administrar las cuentas de usuario, el servidor Apache, el DNS, permisos sobre directorios, crear y borrar usuarios y grupos, controlar qué procesos se están ejecutando.

3.1.2 Equipos y su conectividad.

3.1.2.1 Equipos

La Fábrica tiene estructurado la red de computadoras de la siguiente manera.

Cuenta con dos servidores HP:

- **Servidor de Aplicaciones ¨Pasamanería¨.**

Características:

Modelo: HP ProLiant ML370 G5 E5430 2.66GHz Quad Core Base Tower Server.

Procesador Intel CEON serie E5335QUOD 2GHZ

Memoria Ram: 4GB

2 Disco Duro 200 GB

Windows Server 2003

Direcciones Ip:

Dirección pública: 200.110.77.254/ 255.255.255.252

Dirección privada: 192.168.1.1/255.255.255.0

En este servidor están las aplicaciones de la fábrica, Sistema de Producción Pasa SPP, la misma que está en el lenguaje de programación visual fox 6 y Sistema de transacción de negocio SBT la cual es manejada para el control de roles.

Además en este servidor se administran los usuarios y los respectivos permisos asignados a cada uno.

- **Servidor de Correo Externo.**

Características:

HP ProLiant ML150

Linux Centos 5.4

Direcciones Ip:

Dirección pública: 201.218.4.190/ 255.255.255.252

Dirección privada: 192.168.1.3/255.255.255.0

En este servidor está la página web y se maneja como el servidor proxy de la fábrica, ya que sirve para permitir el acceso a Internet a los equipos de la misma.

- **Servidor correo Pasa Interno.**

Características:

Centos 5.4

Mainboard ASOS

Disco Duro 1 Samsung 120 GB

Disco Duro 2 Samsung 120 GB

Memoria Ram 1G

Es una PC, la cual utilizan como servidor para correo interno, tanto dentro de la fábrica como para las 16 sucursales a nivel nacional.

Direcciones IP:

Dirección pública: 201.218.4.189/ 255.255.255.252

Dirección privada: 192.168.1.200/255.255.255.0

- **Servidor telefonía IP**

Direcciones IP:

Dirección privada: 192.168.1.251/255.255.255.0

Al igual que el servidor de correoPasa Interno, utilizan una PC como servidor, para la telefonía IP.

- **Servidor Central telefónica**

Direcciones IP:
Dirección privada: 192.168.1.76/255.255.255.0

Es una PC, la misma que es utilizada como servidor para registrar todas las llamadas entrantes y salientes de la fábrica además de tiempos de uso a detalle.

- **Servidor Reloj**

Direcciones IP:
Dirección privada: 192.168.1.92/255.255.255.0

Al igual que las anteriores es una PC, que se utiliza como servidor de control de asistencia para todos los empleados de la fábrica. Se registra horarios de entrada, de salida, incluso permisos de salida durante el horario de trabajo.

- **Router Cisco**

Cisco de 8 puertos. Este router Cisco, tiene conexión con el proveedor de internet Telconet, el cual distribuye internet para toda la fabrica.

Direcciones IP:
Dirección privada: 192.168.1.11

- **Router Linksys (Wireless)**

Direcciones IP:
Direcciones privadas: 192.168.1.6 **Rango:** 192.168.1.160 – 192.168.1.177
Dirección pública: 200.110.77.251

- **Switch**

En la tabla 3.1 se muestra la descripción del switch.

Departamentos	**Marca**	**Numero de puertos**
Servidores	3Com	8
Ventas Principal	3Com	24

Sistemas, Contabilidad	3Com	24
Secretaria General	3Com	24
Supervisión General	3Com	24
Mecánica	3Com	24
Corte	3Com	24
Diseño	3Com	24
Almacén	3Com	8

Tabla 3.1. ***Descripción de switch.***

- **Máquinas:**

Siete laptos.

Cinco maquinas de marca MAC

Setenta y siete maquinas de escritorio.

3.1.2.2 Conectividad

La Pasamanería S.A trabaja con redes públicas, las mismas que sirven para la conexión a internet, además con una red privada, la cual es para la conexión interna y subredes para las respectivas sucursales a nivel nacional.

Red Privada:
192.168.1.0/24

Direcciones Públicas:
200.110.77.254/255.255.255.252
201.218.4.190/255.255.255.0
201.218.4.189/255.255.255.252
201.218.4.185/255.255.255.0

Sub redes:
Para las sucursales a nivel nacional en las ciudades (Quito, Guayaquil, Cuenca). En la tabla 3.2 se muestran las sub redes con sus respectivas direcciones.

Subred	**Sucursal**
192.168.2.10	Vergel
192.168.3.10	Américas

192.168.4.10	Guayascentro
192.168.5.10	Sanmarino
192.168.6.10	Guayassuradultos
192.168.7.10	Paseo
192.168.8.10	Bosque
192.168.9.10	Quincentro
192.168.10.10	Ip no asignada
192.168.11.10	Granados
192.168.12.10	Recreoplaza
192.168.13.10	Recreosaldos
192.168.14.10	Sanluis
192.168.15.10	Atuntaqui
192.168.16.10	Santodomingo
192.168.17.10	Guyassurchicos
192.168.18.10	Machala
192.168.19.10	Ibarra
192.168.20.10	Ip no asignada

Tabla 3.2. ***Sub Redes.***

3.1.2.3 Conectividad. Explicación de la conexión de la red.

- Router cisco, este equipo está conectado con el proveedor de internet en este caso de la fábrica Telconet y a su vez con el switch que conecta los servidores.
- El Switch que conecta los servidores, está conectado con el Router cisco y a su vez con los servidores de Correo Pasa Externo, Correo Pasa Interno, servidor de Telefonía IP, a la máquina del administrador de la red y al Switch de Sistemas-Contabilidad.
- Servidor de aplicaciones Pasamanería, este servidor se conectada al switch de Ventas (Principal).
- Switch Ventas (Principal), este equipo está conectado con los demás switch Sistema-Contabilidad, Secretaria General, Supervisión General, Corte y Mecánica, excepto el switch de Diseño y del Almacén, además está conectado a las 3 laptops de Gerencia y a una laptop de Ventas y también a

las 5 maquinas de escritorio correspondientes a Ventas y a la de Agente de Ventas.

- Switch de Sistemas-Contabilidad, este equipo está conectado al switch Ventas (Principal) y a las 14 máquinas de escritorio correspondiente al departamento de Sistemas y de Contabilidad.
- Switch de Secretaria General, este equipo está conectado al switch Ventas (Principal) y a su vez con las 16 maquinas de escritorio repartido a Secretaria, Recursos Humanos, Control, y Producción y también a las 3 laptops que pertenecen a Control y a Gerencia.
- Switch de Supervisión General, este equipo está conectado con el switch Ventas (Principal) y a las 11 máquinas de escritorio repartido a Recursos Humanos, Secretaria, Producción, Sistemas-Métodos y a Mecánica.
- Switch de Mecánica, este equipo está conectado con el switch Ventas (Principal) y a las 12 maquinas de escritorio repartido a Bodega, Producción y Mecánica.
- Switch de Corte, este equipo está conectado a las 12 máquinas de escritorio repartidas a producción, bodega, recursos humanos y Producción-Serigrafía.
- Switch de Diseño, este equipo está conectado al switch de Corte y a las 5 maquinas de escritorio, siendo 4 maquinas de marca MAC.
- Switch del Almacén, este equipo está conectado a 3 máquinas de escritorio y al switch de Corte.
- Router de marca Linksys para la conexión vía Wireless, este equipo está conectado al switch de Sistemas-Contabilidad.

3.1.3 Monitorización de las comunicaciones.

Generalmente una monitorización de red se basa en los siguientes puntos:

- Control de usuarios de la red.
- Verificación de cuellos de botella en la red.
- Verificación del Qos.
- Vulnerabilidad de la red.

- Tráfico de la red.

Se verificó en la fábrica el control de los puntos mencionados anteriormente.

3.1.3.1 Control de usuarios de la red.

El administrador de la red, controla los usuarios en el servidor de aplicaciones donde se encuentra instalado el sistema operativo Windows Server 2003, con ayuda de una aplicación Active Directory, el mismo que es un servicio de directorio y permite la creación, eliminación de usuarios y asignación de permisos ya sea de administrador general, usuarios de sistemas, usuarios de ventas, usuarios de bodega, etc.

Además permite crear directorios compartidos y ponerlos a disposición de cada uno los usuarios de la red, dando niveles de acceso a los usuarios según sean los requerimientos para desempeñar su trabajo.

En definitiva el administrador de la red con la aplicación Active Directory controla, administra y consulta todos los elementos lógicos de la red, como pueden ser usuarios, equipos y recursos.

3.1.3.2 Verificación de cuellos de botella.

En la Pasamanería no controlan ni verifican los posibles cuellos de botella que se puedan dar, entendiéndose como cuellos de botella a muchas solicitudes a la vez y no pueden ser atendidas al mismo tiempo quedando en una fila de espera hasta llegar a un punto donde quien está atendiendo las solicitudes no puede más.

Generalmente se da por el acceso a internet, cuando la mayoría de usuarios conectados a internet, se bajan archivos muy grandes todos a la vez, sin embargo este no suele ser el caso en la fábrica, ya que la mayoría de usuarios conectados a la red tienen restricciones de acceso a internet, únicamente tienen acceso a determinadas aplicaciones según su cargo o al departamento que pertenezca.

3.1.3.3 Verificación del QoS.

El administrador de la red no utiliza ninguna herramienta para la verificación del Qos que significa calidad de servicio, es decir controlar la calidad de la transmisión y recepción de la información a través de la red.

Para controlar esto se hace mediante la priorización de los paquetes entre sí, para garantizar la transmisión de los datos que se realice sin interrupciones o pérdida de paquetes, por lo que en la Pasamanería S.A no realizan estas priorizaciones para que los paquetes lleguen a su destino sin ningún problema.

3.1.3.3.1 Parámetros para el control de calidad de transmisión de los datos.

3.1.3.3.1.1 Verificación del Ancho de Banda.

Telconet brinda un servicio que mediante una aplicación MRTG, la fábrica puede verificar el consumo de ancho de banda actual, la cual se puede observar en la figura 3.1.

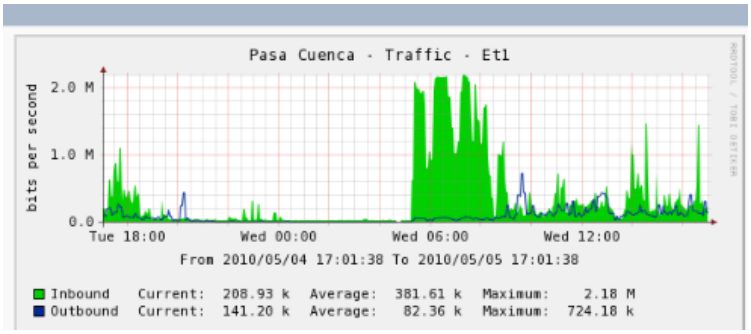


Figura 3.1. ***Consumo de Ancho de Banda Pasamanería*.**

En esta representación grafica se observa la señal de color verde correspondiente al ancho de Banda asignado por Telconet, siendo de 2M y a la señal de color azul correspondiente al consumo de ancho de banda de la fábrica el mismo que no sobrepasa al 1M.

Con la misma aplicación que es proporcionada por Telconet, la fábrica verifica el consumo de ancho de banda de las respectivas sucursales. Esto se representa en la figura 3.2.

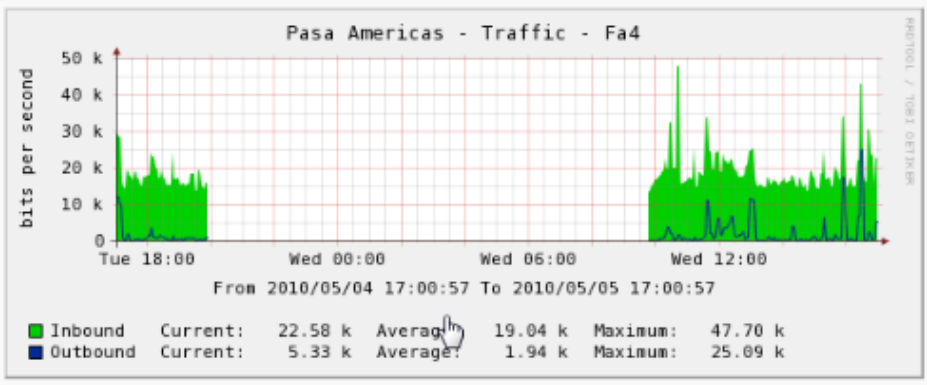


Figura 3.2. ***Consumo Ancho de banda Sucursales de la Pasamanería***.

Se observa en la figura 3.2 que el ancho de banda proporcionado por Telconet es de un máximo de 50Kbps la misma de color verde, y el consumo que tiene la sucursal de las Américas va de de 0kbps hasta un máximo de 25kbps.

Es muy importante tomar en cuenta el ancho de banda, porque se puede priorizar por departamentos, a quienes se les asigna mayor ancho de banda dependiendo de su importancia, por ejemplo no se le puede dar mayor ancho de banda al departamento de mecánica que al departamento de Recursos Humanos.

Cabe recalcar que cuanto mayor sea el ancho de banda más datos podrán circular por ella.

En la fábrica no se realiza este control, porque la red no está segmentada, ya que los datos de todos los departamentos se transmiten por un mismo canal y a la misma velocidad, no se dan prioridades para la transmisión de los datos en la red. En la figura 3.3 se muestra una representación de la segmentación del ancho de banda.

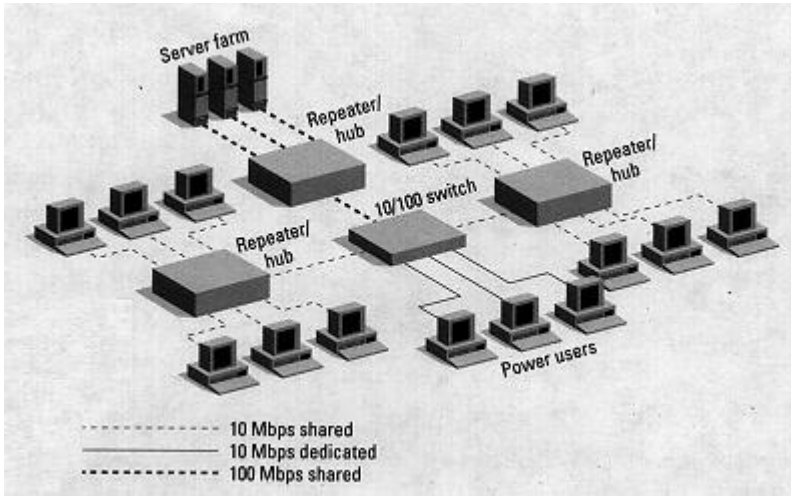


Figura 3.3. ***Segmentación de Ancho de Banda*****.**[99]

Debido a la falta de segmentación de ancho de banda en la pasamanería, suele ocurrir los siguientes inconvenientes:

3.1.3.3.1.2 Paquetes sueltos.

Los paquetes sueltos se dan cuando el router falla en liberar algunos paquetes, si los paquetes llegan cuando los buffers (espacio de memoria) ya están llenos, algunos o todos los paquetes pueden quedar sueltos.

3.1.3.3.1.3 Retardos.

Los retardos son los paquetes que toman un largo periodo en alcanzar su destino, debido a que pueden permanecer en largas colas o toman una ruta menos directa, haciendo a la red muy lenta.

Este es uno de los problemas que se está dando en la pasamanería con los excesivos retardos de los paquetes, por lo que está fallando la telefonía IP que en algún espacio de tiempo la llamada se presenta entrecortada sin poderse comunicar claramente.

La telefonía IP funciona en cada una de las sucursales y actualmente está en funcionamiento en la pasamanería únicamente un teléfono IP, el cual es utilizado por el administrador de la red para dar soporte a los usuarios.

3.1.3.3.1.4 Entrega de paquetes fuera de orden.

Como la telefonía IP funciona mediante internet, cuando un conjunto de paquetes relacionados entre sí son encaminados a Internet, los paquetes pueden tomar diferentes rutas, resultando diferentes retardos. Esto ocasiona que los paquetes lleguen en diferente orden de cómo fueron enviados, provocando fallos en las llamadas telefónicas.

3.1.3.4 Vulnerabilidad de la red.

[99] http://elqui.dcsc.utfsm.cl/util/redes/switch-Router/index.html

El análisis de la vulnerabilidad de la red de la fábrica, consiste en descubrir los puntos débiles de la seguridad de la red, con lo cual evitan que los datos o los equipos se vean afectados en mayor o menor medida por ataques de caballos de Troya, ataques de denegación de servicio, acceso de usuarios no autorizados.

Todo lo anteriormente mencionado el administrador de la red logra controlar mediante el antivirus F-Secure 2010, el mismo que se explicara a continuación.

3.1.3.4.1 Antivirus F-Secure 2010.

Protección del antivirus:

- De virus, gusanos.
- También impide que las aplicaciones de *spyware*[100] y los piratas informáticos accedan al equipo.
- Controla correo electrónico *spam*[101].

Con este antivirus la Pasamanería controla las vulnerabilidades de la red, de los ataques que se les puede presentar, esta aplicación se actualiza automáticamente, pero el administrador lo verifica todos los días para que no ocurra ningún problema.

Se verificó que máquinas están protegidas por el antivirus y cuáles no, mediante un software AutoScan Network 1.42.

- Primero se listó todas las máquinas y servidores conectados actualmente a la red.

Como podemos visualizar en la figura 3.4 con ayuda del software AutoScan Network podemos mostrar a cada uno de los grupos de computadoras según su categoría:

[100]Spyware. Programa para recopilar información sobre las actividades realizadas en el computador.
[101] Spam. Correo Basura.

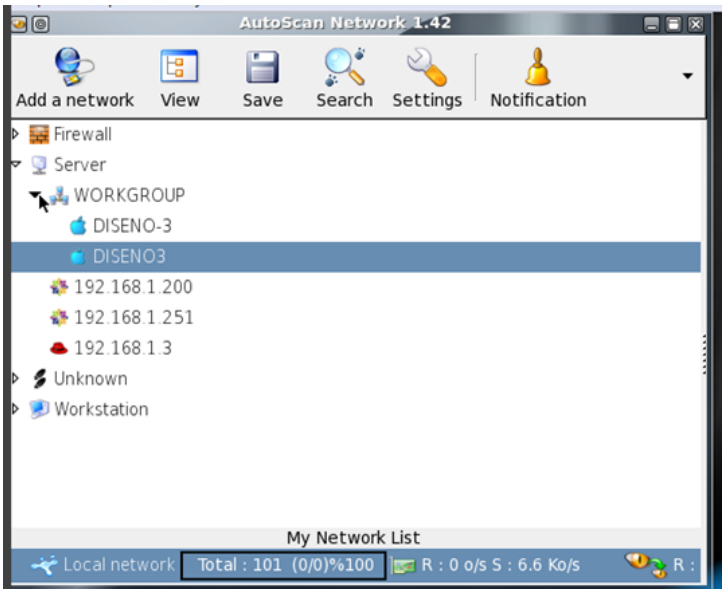


Figura 3.4. ***Grupos de computadoras conectadas a la red.***

- Se verificó las máquinas que tienen protección mediante el antivirus, ya que no todas las máquinas cuentan con esta protección.

Firewall: Son las computadoras que utilizan antivirus en este caso el F-Secure 2010, como podemos visualizar en la figura 3.5 se muestran algunas de las 32 computadoras que tienen instalado esta aplicación.

Figura 3.5. ***Maquinas protegidas por el antivirus F-Secure 2010*.**

Cuando se realizó el escaneo de la red se pudo observar una alerta del cortafuego del antivirus F-Secure 2010, inmediatamente bloqueando el escaneo y mostrando un mensaje de intento de intrusión.

La misma alerta mostró la dirección IP de la máquina que está realizando el escaneo de la red en este caso la IP 192.168.1.41 y el puerto por el cual se quiere comunicar 62076.

En este caso la alerta fue en la maquina del administrador de la red la cual tiene la dirección Ip 192.168.1.4, como se puede observar en la figura 3.6

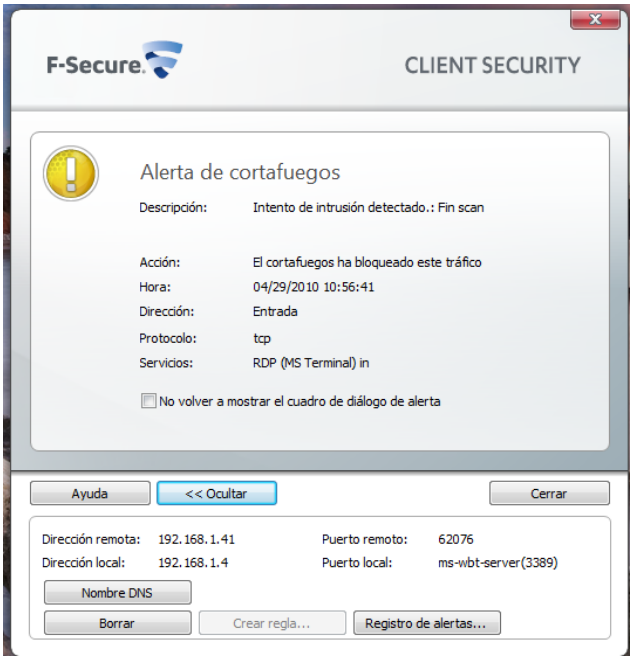


Figura 3.6. ***Alerta del Antivirus de intrusión***.

- De igual forma la alerta del cortafuegos muestra un detalle de los intentos de escaneo de la red, mostrando la hora, la dirección IP de la maquina que ataca y una descripción del intento de ataque. La cual se puede observar en la figura 3.7.

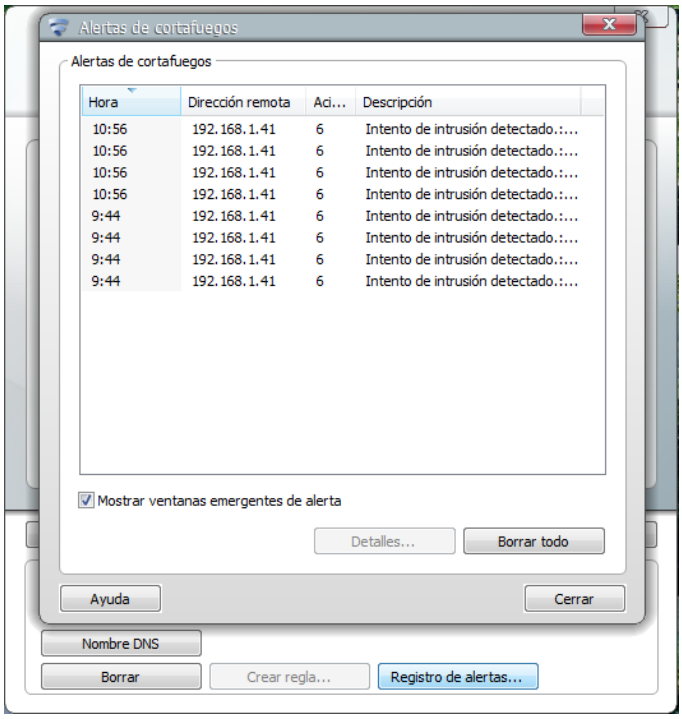


Figura 3.7. ***Detalle de intrusión a la red*.**

- Se verifica las máquinas que no tienen protección del antivirus.

Se puede observar en la figura 3.8 las máquinas que no tienen ninguna protección de antivirus, las mismas se muestran como desconocidas mostrando su dirección IP.

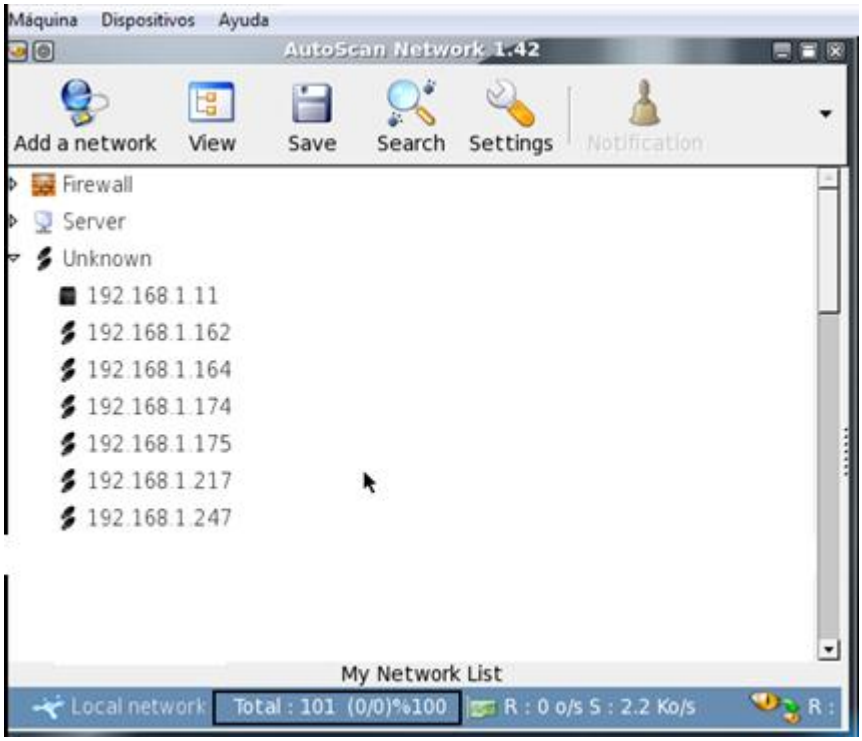


Figura 3.8. ***Maquinas que no tienen la protección del antivirus.***

3.1.3.4.2 Protocolos utilizados en la fábrica

Un protocolo es un estándar que permite la comunicación entre procesos, que potencialmente se ejecutan en diferentes equipos, siendo un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red.

En la pasamanería se utilizan protocolos para la comunicación, los cuales se controlan en el servidor del correo externo, donde está instalado una aplicación llamada Firestarter la cual permite desactivar o activar los protocolos, los mimos se puede observar en la figura 3.12.

La aplicación Firestarter da la posibilidad de permitir o negar la conexión a Internet usando NAT, el mismo que es la Traducción de Dirección de Red, el cual es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

En esta aplicación de puede utilizar la Normativa, donde se muestran las reglas de configuración del cortafuego seleccionando entre las siguientes opciones:

- Normativa para tráfico entrante: sirve autorizar las entradas.
- Normativa para tráfico saliente: sirve para impedir salidas.

Es así como la pasamanería hace uso de la aplicación firestarter para autorizar las entradas y para impedir las salidas de los diferentes protocolos con sus puertos.

Además para crear reglas específicas hay una opción "Anadir reglas" en la cual se llenan los campos con la IP de la red y un comentario identificando a la red. Como se puede ver en la figura 3.9.

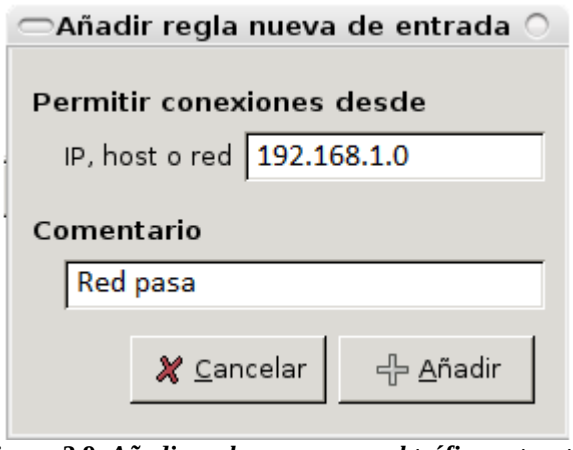


Figura 3.9. ***Añadir regla nueva para el tráfico entrante*****.**

Para que el cambio tenga efecto se selecciona "Añadir", y posteriormente "Aplicar Normativa" como se puede ver en la figura 3.10.

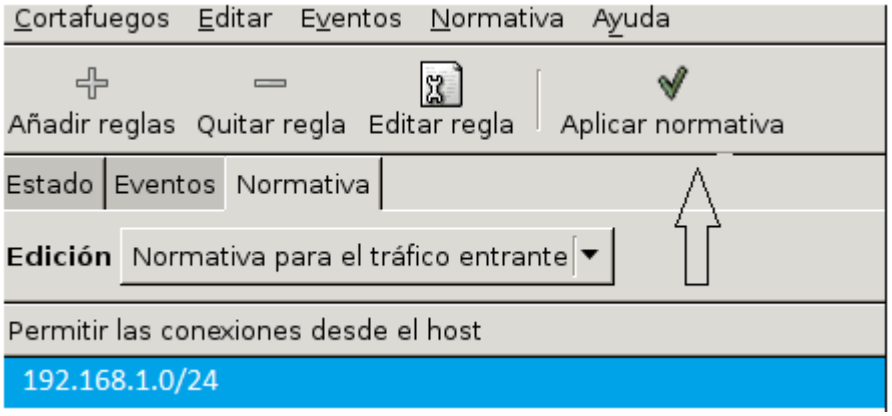


Figura 3.10. ***Normativa para el tráfico entrante*****.**

Para especificar una normativa para el tráfico de entrada y salida se siguen los siguientes pasos.

- Se selecciona Normativa para tráfico entrante, para permitir el acceso a puertos específicos.
- Posteriormente se selecciona Permitir servicio, aquí se selecciona el nombre del protocolo y del puerto que se desea habilitar. Esto se representa en la figura 3.11.

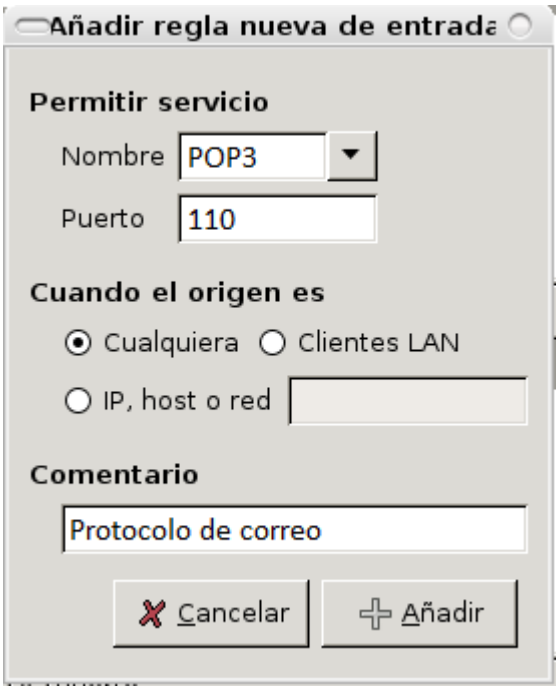


Figura 3.11. ***Habilitar puertos.***

A continuación se indica los protocolos con los que trabaja la fábrica.

SMTP con puerto 25: Protocolo Simple de Transferencia de Correo.

HTTP con puerto 80: Protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción de la World Wide Web (WWW).

HTTPS con puerto 443: Protocolo seguro de transferencia de hipertexto, destinado a la transferencia segura de datos de hipertexto, es la versión segura de HTTP.

VNC con puertos asignados desde 1292 hasta 1242: Es un programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto.

Webmin con puerto 10000: Herramienta de configuración de sistemas vía web, sirve para configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagados del equipo, etc.

FTP con el puerto 20: protocolo de transferencia de archivos.

DNS con puerto 53: Sistema de nombre de dominio

NNTP con puerto 119: Protocolo para la transferencia de noticias en red.

Figura 3.12. ***Interfaz grafica Firestarter pasa*****.**

Con la ayuda del software AutoScan se pudo obtener la siguiente información:

En la figura 3.13 se puede observar los diferentes protocolos y aplicaciones instaladas en el servidor de Aplicaciones con la dirección IP 192.168.1.1 con sus respectivos puertos autorizados.

Figura 3.13. ***Protocolo y aplicaciones instaladas en el servidor de aplicaciones.***

De igual manera se puede observar los protocolos y las aplicaciones permitidas para el tráfico entrante y saliente que están en el servidor de correo externo con la dirección Ip 192.168.1.3. Observar figura 3.14.

Figura 3.14. ***Protocolos y aplicaciones instaladas en el servidor de correo externo*****.**

Con una aplicación NMAP propia del software AuntoScan, se pudo realizar la búsqueda de los puertos que se están abiertos y el total de puertos que están cerrados, en los servidores de aplicaciones, correo interno, correo externo y el servidor de telefonía IP. Podemos observar en la figura 3.15.

Figura 3.15. ***Detalle adquirido por el NMAP del Servidor de aplicaciones con la dirección IP 192.168.1.1.***

3.1.3.4.3 Dispositivo de seguridad firewall.

Uno de los problemas más evidentes que tiene la fábrica, es que no tiene implementado un dispositivo de seguridad firewall que funciona como cortafuegos, permitiendo o denegando las transmisiones de datos.

Por lo que la red esta propensa a recibir ataques, accesos de personas ajenas a la red de la fábrica.

Como se puede visualizar en la figura 3.16 la red de la fábrica, está trabajando de una forma directa con su proveedor de internet Telconet, ya que ingresa el internet directo al router cisco sin ninguna seguridad firewall para evitar cualquier problema que se presente, como ataques, virus, etc., esto se da para la conexión hacia el exterior de la fábrica y de igual forma tampoco manejan seguridad de firewall para la conexión a la red interna de la fábrica, para tener protección de sus trabajadores en caso que intenten entrar a los servidores.

Figura 3.16. ***Diagrama servidores sin firewall*****.**

3.1.3.5 Tráfico de la red.

El tráfico de la red en la Pasamanería S.A no se controla, como anteriormente se mencionó la red trabaja con un mismo ancho de banda para todas las actividades dentro de la fábrica, a una misma velocidad de transmisión de datos, no existe segmentación de la red por prioridades, no se controla la cantidad de datos que se envían por la red, ocasionando problemas a la red por las sobrecargas de datos que se envían, existiendo así las colisiones, retardos de paquetes, etc.

Por lo que el tráfico de la red se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación y a la velocidad que se transfiere.

Para analizar el tráfico de la red se necesita herramientas, las mismas que son un analizador de protocolos que permite hacer un seguimiento exhaustivo del tráfico de red que pasa por el sistema, permitiendo saber cuál es el estado, identificando rápidamente los problemas, bien para resolver problemas concretos o bien para optimizar la utilización de la red.

3.1.4 Revisión de costes y asignación formal de proveedores.

Actualmente cuenta la fábrica con un único proveedor de servicio de internet, el cual es TELCONET, el mismo que brinda el servicio de Tránsito al Backbone con una de las redes más avanzadas de América Latina, Backbone se refiere a las principales conexiones troncales de Internet, está compuesta de un gran número de routers de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo.

Telconet cuenta con alta velocidad de interconexión al NAP local en Ecuador y al NAP internacional en Miami, siendo el fundamental objetivo de NAP intercambiar tráfico de Internet.

Telconet ofrece sus servicios a la fábrica bajo el siguiente acuerdo de nivel de servicio o también conocido por sus siglas en ingles SLA:

- Disponibilidad de internet: 99.9%
- Packet loss (Perdida de paquetes): cercanos al 0%
- Latencias al backbone en USA: 80 ms
- MTTR(Tiempo medido hasta a ver reparado la avería): 2 horas

Además la fábrica cuenta con algunas herramientas proporcionadas por Telconet:

Medidor de ancho de banda: Longitud medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Este medidor permite verificar el consumo de ancho de banda actual para descargar desde los servidores de Telconet a la fábrica.

TestSpeedtest.net: Es una herramienta de análisis de velocidad de banda ancha que permite probar la conexión a Internet.

Trasmisión de los datos: Telconet proporciona la conexión a internet a la fabrica, mediante la conexión de fibra óptica que posee, la misma que está completamente compuesta por fibra monomodo estándar G.652D del tipo Fibra Corning de la más alta calidad, lo que permite la conexión a grandes distancias y transmitir elevadas tasas de transmisión.

5512 kbps ancho de banda de telconet en la ciudad de cuenca.

El ancho de banda que proporciona telconet a la fábrica es de 2Mbps y de 128 Kbps para las sucursales de las Américas y el Vergel.

3.1.5 Supervisión de aplicabilidad de estándares.

Se supervisó la aplicabilidad de una serie de estándares a la red de la Fábrica, los mismos que se indica a continuación.

Estándares de diseños físicos de LAN y su adecuación a la tipología del lugar.

La red de la fabrica Pasamanería S.A ha ido creciendo a lo largo de los anos, a sus inicios contaba con una red de 4 maquinas conectadas y ha ido creciendo de acuerdo a las necesidades que se han presentando, por esta razón no cuenta con estándares de cableado estructurado.

Sin embargo contar con cableado estructurado, significa el manejo de tráfico heterogéneo y así mismo garantizar el desempeño de la red, una red confiable, rápida y sobre todo contar con puntos de red para el futuro.

La fábrica no ha seguido ningún tipo de estándar para realizar el diseño, adquirir productos, equipos y materiales que cumplan con el estándar ,como por ejemplo estándares de cableado especificados la **EIA/TIA**, ya que siguiendo los estándares mencionados anteriormente se certifica el rendimiento del sistema de cableado.

Y la estructura de la red de la fábrica está basada en los productos más convenientes del momento.

Estándar 607. La fábrica no cuenta con este estándar, el mismo que especifica como deberán proteger los equipos e instalaciones de telecomunicaciones contra descargas eléctricas, además de controlar que tipo de medio, conector y ducto se utilizará, rutas de los cables.

En la fábrica no se cuenta con una documentación del diseño de cableado, sin embargo cabe recalcar que es de mucha importancia, si un diseño de cableado se documenta desde su fase inicial, y si esta documentación se hace siguiendo las indicaciones a estándar, la administración de los servicios y del mismo cableado en un futuro serian muy sencillo.

Estándar 569. Este es un estándar importante a seguir cuando se quiere diseñar el sistema de cableado estructurado de una red, ya que trata de controlar las rutas y espacios donde se instalaran los cables, sin embargo la Pasamanería S.A no ha seguido este estándar por lo que mencionamos anteriormente que la red a ido avanzando según las necesidades.

3.2 Verificaciones.

3.2.1 Nivel de acceso a diferentes funciones dentro de la red.

El servidor de aplicaciones tiene particionado los discos de la siguiente manera:

Cuenta con 4 particiones de 81Gb cada una: Sys, Sys1, Sys2, SBTW.

En la partición Sys Pasamanería esta el directorio de usuarios, el cual contiene a todos los usuarios existentes en la fábrica.

El administrador de la red da permiso de acceso a los usuarios dependiendo de las necesidades para desempeñar su trabajo. En la figura 3.17 se muestran los niveles de acceso a los directorios del servidor de aplicaciones.

Los permisos están de la siguiente manera:

- Administrador de la red. Tiene acceso a absolutamente todos los directorios, es un permiso de administrador.
- Personal de Sistemas. También tienen permiso de administrador.
- Gerencia. Permiso de administrador.
- Mecánica, Contabilidad, Costura, Recursos Humanos. Cada usuario únicamente tiene acceso a sus respectivos directorios los cuales se encuentran en el servidor de aplicaciones.

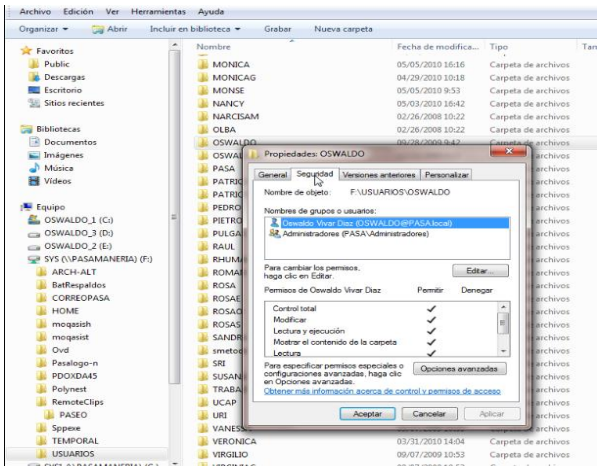


Figura 3.17. ***Niveles de acceso a los directorios del servidor de aplicaciones*****.**

3.2.2 Supervisión de la existencia de normas de comunicación.

Las principales normas para redes locales los emite la IEEE.

Existen dos normas de comunicación de la IEEE que esta implementado en la red de la Pasamanería.

La norma IEEE 802.3u y la IEEE 802.3ab, la diferencia de las dos es que la una FAST ETHERNET y la otra GIGABIT ETHERNET.

3.2.2.1 FAST ETHERNET (IEEE 802.3u).

La norma IEEE 802.3u con la variación física Fast Ethernet (100BASE-T) offers a speed increase ten times that of the 10BaseT Ethernet specification, while preserving such qualities as frame format, MAC mechanisms, an100BASE-T, esta norma tiene un aumento de velocidad diez veces mayor que la especificación 10BaseT Ethernet, siendo su velocidad de transmisión de 100Mbps.

Cuenta con cualidades de Ethernet, tales como el formato de trama, [102]MTU, tamaño máximo de paquetes de datos que van a ser enviados por la red.Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks.

Like Ethernet, 100BASE-T is based on the CSMA/CD LAN access method. Al igual que Ethernet 10BASE-T se basa en el CSMA / CD método de acceso LAN. There are several different cabling schemes that can be used with 100BASE-T, including:

[102] MTU. Unidad máxima de transferencia.

3.2.2.2 GIGABIT ETHERNET (IEEE 802.ab).

La norma IEEE 802.ab con la variación física 1000Base-T es un estándar para redes de área local del tipo Gigabit Ethernet sobre cable de cobre UTP.

Cuando se instalo Fast Ethernet para aumentar el ancho de banda de las estaciones de trabajo, se comenzaron a crear cuellos de botella en la red. 1000BASE-T (IEEE 802.3ab) se desarrolló para proporcionar ancho de banda adicional a fin de ayudar a aliviar estos cuellos de botella.

Proporcionando mayor desempeño a dispositivos tales como enlaces entre los switches, servidores centrales y otras aplicaciones de armarios para cableado así como conexiones para estaciones de trabajo.

Esta norma utiliza el cable UTP de categoría 6 como el cable Cat 5e el cual puede transportar, de forma fiable hasta 125 Mbps de tráfico, obtener 1000 Mbps (Gigabit) de ancho de banda.

El primer paso para lograr una 1000BASE-T es utilizar los cuatro pares de hilos en lugar de los dos pares tradicionales utilizados para 10BASE-T y 100BASE-TX. Esto se logra mediante un sistema de circuitos complejo que permite las transmisiones full duplex en el mismo par de hilos. Esto proporciona 250 Mbps por par. Con los cuatro pares de hilos, proporciona los 1000 Mbps esperados.

La codificación de 1000BASE-T con la codificación de línea *4D-PAM5* [103] se utiliza en UTP de Cat 5e o superior. Esto significa que la transmisión y recepción de los datos se produce en ambas direcciones en el mismo hilo a la vez.

Estas dos normas son utilizadas para las conexiones de los equipos en la red de la Pasamanería.

La norma IEEE 802.3u se utiliza para sus equipos que tienen instalados una tarjeta de red que trabajan a una velocidad de transmisión de 100Mbps.

A diferencia la norma IEEE 802.3ab se utiliza para sus equipos que tienen instalado tarjetas de red que trabaja a una velocidad de transmisión de 1000Mbps, los factores para la utilización de esta norma es por el incremento de las velocidades de los

[103] 4D-PAM5. Modulación de pulsos en amplitud de 5 niveles, este código se usa en redes Gigabit Ethernet que usa como medio de transmisión 4 pares del cable UTP.

procesadores de las máquinas nuevas, a mas de eso el incremento de puntos de red que se han incrementando en la Pasamanería S.A.

Con las dos normas de comunicación mencionadas, es posible trabajar con diferentes topologías de red, la pasamanería trabaja con una topología de árbol, como se puede observar en la figura 3.18.

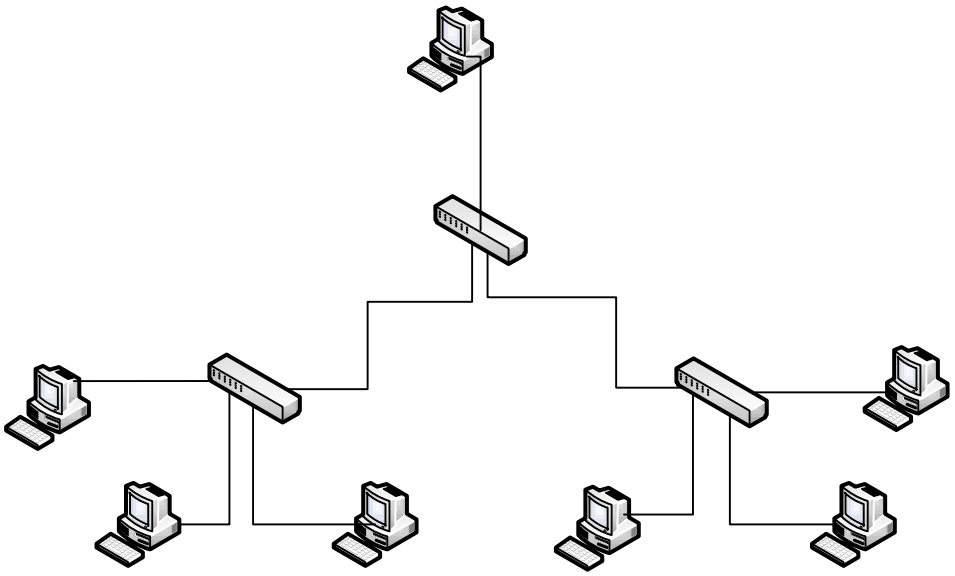


Figura 3.18.*Topologia de árbol de la fábrica*.

Con esta topología la pasamanería ha podido implementar lo siguiente:

- El switch de Ventas (principal) al retransmitir las señales, incrementa la distancia a la que puede viajar la señal.
- Con esta topología pueden conectar más dispositivos gracias a la inclusión de switch secundarios.

Sin embargo esta topología presenta algunos inconvenientes:

- Si se viene abajo el switch de Ventas (principal), todos los demás switch se viene abajo con él.
- Es más difícil su configuración.

3.2.3 Tipos de equipamiento como adaptadores LAN.

3.2.3.1 Norma EIA/TIA 568A y la EIA/TIA-568B.

Estas normas son utilizadas en la fábrica para el armado del los cables de red.

Se diferencian por el orden de los colores de los pares a seguir, para posteriormente ponchar con el conector RJ45.

El uso de las dos normas es diferente, generalmente se utiliza la norma T568B para el cableado directo y el T568A para el cable cruzado. En la figura 3.19 se muestra el uso de las normas de cable T568B y T568A.

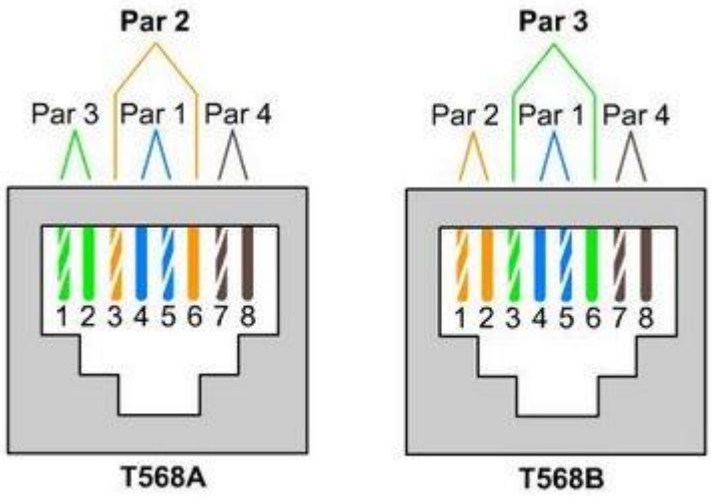


Figura 3.19. ***Normas de cable T568B para el cableado directo y el T568A para el cable cruzado.***[104]

3.2.3.2 Tipos de cable entre dispositivos.

3.2.3.2.1 Cable Directo (Straight Through).

Es el cable cuyas puntas están armadas con la misma norma (T568A - T568A ó T568B-T568B).

Se utiliza entre dispositivos que funcionan en distintas capas del Modelo de Referencia OSI.

- **De PC a Switch/Hub.**
- **De Switch a Router.**

[104] http://www.adslfaqs.com.ar/esquema-de-cables-utp-derecho-y-cruzado-eiatia-568a-eiatia-568b/

3.2.3.2.2 Cable Cruzado (Crossover).

Este cable las puntas están armadas con distinta norma (T568A-T568B).

Se utiliza entre dispositivos que funcionan en la misma capa del Modelo de Referencia OSI.

- **De PC a PC.**
- **De Switch/Hub a Switch/Hub.**
- **De Router a Router.**

La red de la pasamanería tiene conexión entre los siguientes dispositivos:

- **Router a Swicth.**
- **Swicth a pc, para estas conexiones han utilizado el cable directo, utilizando el cable UTP de categoría 5 con los adaptadores RJ-45, implementando las respectivas normativas EIA/TIA 568A y la EIA/TIA-568B.**
- Switch a switch, para la cual utilizan el cable de red cruzado con las normas (T568A-T568B).

3.2.4 Uso de conexión digital con el exterior como Internet.

El uso de normas para la conexión o utilización del internet, correo electrónico no tienen establecidas en la Pasamanería.

Se trata de normas para el uso del internet para los usuarios que tienen acceso al mismo y de normas para el uso del correo electrónico interno, el cual todos los usuarios de la fábrica tiene acceso.

Estas normas pueden ser, los empleados no pueden acceder a internet con fines diferentes a los propios de las actividades laborales.

No dar a conocer códigos de seguridad tales como contraseñas a otras personas, divulgando información y contraseñas a personas que no tengan nada que ver con la Pasamanería que puede dañar la integridad de la misma.

En cambio en el uso del correo electrónico establecer normas como no enviar contenidos con fines publicitarios y comerciales de bienes y servicios en beneficio propio, de familiares o de terceros, salvo en los casos en los cuales el departamento de Sistemas o una instancia superior lo autorice expresamente.

Los empleados están de cierta forma autorizados o no es mal visto por sus superiores en la utilización del internet en la navegación de páginas como del gobierno por ejemplo el SRI, IEES y para realizar consultas sobres sus cuentas en los bancos, estas utilizaciones son permitidas.

3.2.5 Instalación de equipos de escucha como Sniffers (exploradores físicos).

La fábrica no cuenta con ningún equipo o software de escucha de sniffers, que ayude para la seguridad de la red.

Teniendo así un problema, mediante un programa de sniffers pueden robar información de la red como nombres de usuarios, contraseñas, mail, básicamente estos programas permiten registrar la información que envían los periféricos (unidades o dispositivos), así como la actividad realizada en un determinado ordenador.

A los sniffers se le pueden dar dos tipos de utilidades:

3.2.5.1 Para robar información.

En este punto se utilizó el programa ettercap el cual es un sniffer, con el se pudo escanear a toda la red, la misma que nos presentó cada una de las Ips que se encuentran utilizadas, con las cual se puede ver detalles de cada dirección ip, la Mac Address de la maquina que pertenece la ip y el sistema operativo que utilizaba esa máquina, en este caso se pude ver el detalle de la dirección Ip 192.168.1.32 la cual nos presentó la mac address de esa máquina y el sistema operativo que utilizaba esa máquina el cual era el Windows 2000 Profesional SP4. La cual se puede observar en la figura 3.20

Con estos detalles se puede realizar muchas cosas para dañar o robar información, ya que tenemos la mac address de la máquina la cual se la puede clonar.

Figura 3.20. ***Detalle de la maquina con IP 192.168.1.32***

A mas de ver los detalles de cada computadora conectada a la red, se puede ver los paquetes que se están transfiriendo de una máquina a otra, en este caso como se puede observar en la figura 3.21, aquí se puede ver claramente la información que se está transfiriendo , pero esta información no se la puede interpretar la cual se deberá tener un decodificador de información para poder entender de que se trata esa información, de esta forma se puede robar información confidencial que se este enviado por la red.

Figura 3.21. ***Paquetes que se transmiten de una maquina a otra.***

3.2.5.2 Utilidades que el Administrador puede dar a la Red.

- Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?
- Detección de intrusos, con el fin de descubrir hackers.
- Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.
- Analizar el tráfico de la red, detectando los cuellos de botella.

Siendo esta una forma adecuada para ayudar al administrador de la red para detectar estos problemas y así poder dar una solución al problema encontrado en la red.

3.3 Estrategias de comunicación a largo plazo.

La fábrica, al momento cuenta con un planeamiento estratégico, el mismo que corresponde a propuestas con respecto a las comunicaciones para el futuro.

- Instalación de equipos linksys Wireless en toda la fábrica.

Al momento está instalado en el departamento de sistemas y contabilidad un router para la comunicación inalámbrica mediante wireless de marca linksys.

Además actualmente está con el siguiente rango de direcciones IP privada.

Red privada

192.168.1.6

Y con el rango de direcciones de:

192.168.1.160-192.168.1.177

Dirección de IP publica, para la conexión a internet:

200.110.77.251

Ahora la estrategia de comunicación, es que se implemente varios router para la conexión inalámbrica de más alcance de la señal que funcionen como amplificadores de la señal, de esta manera se tenga internet en toda la fábrica.

Además asignar mayor capacidad de rango de direcciones IP, ya que en la actualidad el router instalado no abastece las necesidades del personal de la fábrica, porque es un rango aproximado de 10 usuarios.

- Implementación de un equipo de seguridad Firewall.

Este equipo de seguridad Firewall servirá para la protección de la red de la fábrica, el mismo que estaría conectado entre la conexión a internet del proveedor telconet y el Router Cisco, como se muestra en la figura 3.22.

Figura 3.22. ***Diagrama de los servidores de la red con muro de fuego.***

Este dispositivo estaría configurado para permitir, limitar, cifrar, descifrar el tráfico.

Especialmente para evitar que los usuarios de Internet no autorizados tengan acceso a la red privada de la fábrica, la misma que está conectada a internet, ya que todos los mensajes que entren o salgan de la red interna de la fábrica pasan a través del dispositivo o también llamado cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados por el administrador de la red.

3.4 Planes de comunicación a alta velocidad.

La tendencia actual en el mundo de las telecomunicaciones apunta hacia una red universal que soporte diferentes tipos de servicios, generalmente, con requerimientos distintos.

Esta red es conocida como B-ISDN (Broadband Integrated Services Digital Network) y algunos de los servicios que se espera proporcionar a través de ella son: teleconferencia, videoconferencia, televisión de alta definición (HDTV), transferencia de datos a altas velocidades, transporte de voz, videotelefonía y servicios mucho más diversificados y sofisticados que surjan por sí mismos cuando la capacidad de la red digital de banda ancha, demuestre su verdadero potencial y capacidad.

La fábrica al momento no tiene ningún plan de implementar redes como B-ISDN con sus respectivos servicios.

Entre las tecnologías de alta velocidad encontramos las siguientes:

3.4.1 FDDI (Interfaz de Datos Distribuida por Fibra Óptica)

Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex. Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

También existe una implementación de FDDI en cables de hilo de cobre conocida como CDDI. La tecnología de Ethernet a 100 Mbps (100BASE-FX y 100BASE-TX) está basada en FDDI.

Entre sus características más importantes tenemos:

- Distancia de 100m (UTP), 500m−2km (fibra multimodo) y 60km (SONET).
- Transmisión asíncrona o síncrona usando tokens.
- Doble anillo a 100Mbps.
- Inmune y no genera ruido electromagnético.

A continuación en la tabla 3.3 se muestra una comparación de las distintas tecnologías FDDI.

	FDDI asine	FDDI sine	FDDI−II
Arquitectura	Timed token passing	Timed token passing	Circuit Switching
Compatible con FDDI	SI	SI	NO
Retraso prom. Nodo a nodo	0.01−0.2 seg	0.008−0.016 seg	0.000125 seg.
Multimedia	No bien soportado	Trafico sensible con prioridad	Bien soportado

Tabla 3.3. ***Tecnologías FDDI.***

3.4.2 100 BASE−T (FAST ETHERNET)

Fast Ethernet o Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps.

Tradicionalmente Ethernet trabajaba a 10 Mbps. A estas velocidades, dado que las compañías producen grandes ficheros, pueden tener grandes demoras cuando envían los ficheros a través de la red. Estos retrasos producen la necesidad de mayor velocidad en las redes.

Características:

- Más de 2/3 de las redes actuales son ethernet.
- Plataforma dominante: 10 Base−T.
- En 100 Base−T (IEEE 802.3) se mantiene CSMA/CD.
- Topología de estrella.
- Nuevos esquemas de señalización.

3.4.3 GIGABIT ETHERNET

Es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet.

Características:

- Creado por la alianza Gigabit−Ethernet(11 compañias) en 1996.
- Draft standard IEEE 802.3z en julio de 1997.
- Compatible con ethernet existente: CSMA/CD, full and half duplex.
- Slot time −> 512 bytes (8 veces mas).
- 1000 Base−X basado en la capa fisica de Fibre Channel(FC0 and FC1), sobre fibra(3000m) o STP(25m).

3.4.4 ATM

Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales.

El ATM puede ser considerado como una tecnología de conmutación de paquetes en alta velocidad con las siguientes características:

- Los paquetes son de pequeño y constante tamaño (53 bytes).
- Es una tecnología de naturaleza conmutada y orientada a la conexión.
- Los nodos que componen la red no tienen mecanismos para el control de errores o control de flujo.
- El header de las células tiene una funcionalidad limitada.

3.5 Planificación de la recuperación de las comunicaciones en caso de desastre.

Una planificación de la recuperación de las comunicaciones se basa en un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que la fabrica pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos o también ante la pérdida repentina de personal clave.

Por lo que podemos decir de la fábrica:

3.5.1 Recuperación de los datos:

Cada uno de los empleados de la fábrica tiene acceso a determinados directorios, según las necesidades de cada empleado para desempeñar su trabajo, los mismos que están únicamente en el servidor de aplicaciones.

Entonces todos los datos generados durante el día por los empleados se guardan directamente en el servidor de aplicaciones, ya que todas las máquinas están en red y trabajan directamente en los directorios que se les ha otorgado el permiso de acceso.

Si falla la conexión a internet, por ejemplo las sucursales ya no pueden trabajar con el sistema que funciona con internet, por lo que en estos casos entra a funcionar el otro sistema, el mismo que es una aplicación instalada en cada máquina y que los datos de facturación se guardan en archivos localmente y posteriormente se envían al servidor de aplicaciones para realizar los respectivos respaldos diarios.

La manera de respaldar la información del servidor de aplicaciones es la siguiente:

El departamento de sistemas está compuesto de 7 personas, las mismas que tienen un horario para quedarse luego de las horas laborables normales un día a la semana, haciendo el respectivo respaldo de la información y guardando en 4 DVD, a fin de mes es entregada esta información al Dueño de la fábrica el cual traslada estos discos a un lugar fuera de la misma.

3.5.2 Recuperación del hardware:

La Pasamanería cuenta con un servidor adicional de correo externo, que en caso de que deje de funcionar el servidor de correo externo que actualmente está funcionando este entre a remplazarlo sin ninguna complicación.

Cabe recalcar que en caso de que haya algún tipo de desastre y el servidor de aplicaciones, correo interno, telefonía Ip quede inhabilitado, no existen servidores que puedan reemplazarse y continúe en funcionamiento normal la fábrica.

De igual manera en caso de que quede fuera de funcionamiento una PC no existen máquinas que remplacen y se continúe con el trabajo normal.

En caso de que un switch quede fuera de funcionamiento por cualquier tipo de desastre, en la fábrica no cuenta con switch para reponer el dañado.

Es importante mencionar que todos los equipos de la fábrica están asegurados, por lo que en caso de daño de los mismos el proveedor responde con un equipo nuevo, pero realizando el respectivo trámite y esto a su vez conlleva tiempo para volver al funcionamiento normal de la fábrica.

3.5.3 Recuperación del Software:

La fábrica cuenta con la licencia de todo el software instalado en cada equipo y servidor.

Por lo que en caso de que exista algún tipo de falla en el software instalado, proceden a instalarlo de nuevo sin ningún tipo de problema.

3.5.4 Recuperación del internet:

Como se había dicho el proveedor de internet es Telconet y en caso de que falle la conexión a internet con este proveedor, la fábrica no cuenta con otro proveedor que facilite la conexión a internet si ocurre algún tipo de desastre con Telconet.

3.5.5 Recuperación de energía eléctrica.

En el caso que en la fábrica se quede sin energía eléctrica, tienen un generador de energía propio, para continuar con el normal funcionamiento.

3.6 Documentación sobre el diagramado de la red.

Tener documentado el diagrama de red de la fábrica es importante, ya que es una representación gráfica de todos los puntos de red que están conectados, de manera que resulta más fácil para el administrador de la red llegar al punto de red que está fallando o hacer cambios en la misma.

Sin embargo, la documentación sobre el diagramado de la red en la Pasamanería esta desactualizado ya que no cuenta con las nuevas incorporaciones de maquinas y

switch que se han implementado en los diferentes departamentos, como se muestra en el Anexo2.

Este diagrama está conformado de la siguiente manera:

Servidores:

- Servidor de aplicaciones.
- Servidor de correo que se llama Correo Pasa.

Maquinas:

- Constan de 72 maquinas de escritorio.

Switch:

- Un switch el cual es el principal para las conexiones con los demás equipos.

Hub:

- El diagrama muestra siete hubs.

En el switch principal se conectan los dos servidores que tenían en ese momento la Pasamanería, a mas de ello también se conectan 11 maquinas, y a su vez 6 hubs, los mismos que tienes conectados diferentes maquinas para diferentes funciones.

Conexiones de los hub.

- El primer hub tiene conectado 14 maquinas de escritorio.
- El segundo hub tiene conectado 14 maquinas de escritorio.
- El tercer hub tiene conectado 9 maquinas de escritorio.
- El cuarto hub tiene conectado 4 maquinas de escritorio.
- El quinto hub tiene conectado 7 maquinas de escritorio.
- El sexto hub tiene conectado 6 maquina de escritorio, a más de las maquinas, se conectan los hubs siete y ocho, siendo el sexto hub como un puente con los dos hubs.

- El séptimo hub que viene conectado con el sexto hub, se conecta con 4 maquinas.
- El octavo hub que viene conectado con el sexto hub, se conecta solo con tres maquinas.

Para trabajar con el diagrama real de la fábrica, se ha realizado las respectivas actualizaciones de la misma con la ayuda del administrador de la red, el diagrama se lo elaboro en la herramienta de Microsoft Office Visio 2007, como se muestra en el Anexo3.

Los cambios que se han hecho en la fábrica son los siguientes:

- Nuevas máquinas de escritorio.
- Dos servidores, un servidor Correo Pasa Interno y el servidor de Telefonía Ip.
- Remplazar Switch por hub.
- Implementación de Router Cisco para la conexión a internet.
- Implementación de Router Linksys para la conexión inalámbrica dentro de la fábrica.

De igual forma se realizo los diagramas de red de las sucursales de la ciudad de Cuenca. A continuación se describen los componentes del diagrama de la red de las sucursales.

Sucursal Las Américas.

- Router Cisco
- Router Linksys
- Switch LB-Link
- Tres Cámaras.
- Una maquina de escritorio.
- Un teléfono IP.

Este diagrama se le puede ver en la figura 3.23, la conexión de esta red de la sucursal de las Américas es de la siguiente manera:

- Router Cisco, se conecta con el servidor de internet Telconet, y a su vez se conecta con el equipo Router de marca Linksys.
- Router Linksys, se conecta con el Router Cisco y con el switch de marca LB-Link, también con la máquina de escritorio y al teléfono IP.
- Switch LB-Link, se conecta a las tres cámaras de vigilancia.

Figura 3.23. ***Diagrama de red de la sucursal las Américas en la ciudad de Cuenca.***

Sucursal El Vergel.

- Router Cisco System 800 Series.
- Router Linksys.
- 2 Switchs D-Link
- Dos Cámaras.
- Una maquina de escritorio.
- Un teléfono IP.

Este diagrama se le puede ver en la figura 3.24, la conexión de esta red de la sucursal de El Vergel es de la siguiente manera:

- Router Cisco, se conecta con el servidor de internet Telconet, y a sus ves se conecta con el equipo Router de marca Linksys.

- Router Linksys, se conecta con el Router Cisco y a los switchs de marca D-Link, también con la máquina de escritorio y al teléfono IP.
- Switchs D-Link, se conecta a las dos cámaras de vigilancia y la máquina de escritorio.

Figura 3.24. ***Diagrama de red de la sucursal del Vergel en la ciudad de cuenca.***

3.7 Vigilancia constante sobre toda actividad on-line.

El administrador de red vigila constantemente las actividades de cualquier punto de red mediante software que permite el acceso remoto a cualquier maquina conectada a la red de la fabrica.

3.7.1 Software utilizado para la fábrica.

3.7.1.1 NetOp.

NetOp consta de dos módulos:

El módulo Administrador, que está instalado en el equipo del administrador de la red, y el módulo Cliente, que está instalado en todos los equipos que forman parte de la red.

A continuación se describen las acciones con el NetOp.

- **NetOp permite interactuar con los módulos clientes de forma individual o colectiva.** Se puede interactuar, mediante la difusión de la pantalla del administrador al resto de los empleados conectados a la red.
- **Demostrar el escritorio de un módulo cliente a otros módulos clientes.**
- **Demostrar un archivo multimedia a los módulos Cliente.**
- **Bloquear los equipos Cliente, en caso de que los empelados estén haciendo otras actividades fuera del trabajo.** Da la posibilidad de bloquear la pantalla, el teclado y el ratón de los equipos de los empleados.
- **Supervisar las pantallas de los módulos Cliente.** El administrador puede supervisar el progreso de los empleados mientras trabajan, ya sean individualmente o a todos los empleados a la vez.
- **Distribuir archivos a los módulos cliente.** El administrador puede distribuir o recopilar archivos de los equipos de todos los empleados, dependiendo de las necesidades.
- **Iniciar aplicaciones en los equipos Cliente.** Se puede iniciar documentos remotamente en los equipos seleccionados de los empleados.
- **Evitar que los módulos empleados ejecuten determinadas aplicaciones.** La herramienta da la posibilidad de que los empleados no puedan acceder a sitios Web no adecuados o se dedican a jugar en vez de a trabajar. Se puede crear medidas de seguridad específicas para aplicaciones o Internet con las que se prohíba el acceso a determinados programas y direcciones de Internet. Las medidas de seguridad pueden aplicarse y modificarse según se desee.
- **Grabación de las pantallas del módulo administrador o los módulos Cliente.** El administrador puede grabar paso a paso lo que hace y luego reproducir a la maquina del empleado que desee, si desea mostrarle cierta

actividad, incluso con una narración y además puede grabar y reproducir las pantallas de los empleados.

3.7.1.2 Team Viewer 5

A continuación se describen las acciones con el Team Viewer.

- **Servicio del sistema de Windows**. Puede acceder a ordenadores remotos directamente después de arrancar el sistema operativo y antes de iniciar sesión en Windows.
- **Reinicio remoto.** Reiniciar ordenadores remotamente de modo seguro.
- **Pantalla en negro.** Desactivar la visualización y control del monitor del ordenador remoto durante la sesión de TeamViewer.
- **Autenticación de Windows**. Utilizar el inicio de sesión de Windows como alternativa para acceder al ordenador remoto.
- **Llamada de conferencia.** El administrador puede presentar sus ideas a varias personas situadas en diferentes lugares y hablar por teléfono con ellas al mismo tiempo.
- **Lista de asociados.** En la lista de asociados de TeamViewer, se puede ver en todo momento cuáles de los empleados están accesibles, y conectarse con ellos con un clic de ratón. Ya que ofrece mensajería instantánea a nivel de la empresa.
- **Voz sobre IP.** Da la posibilidad de usar voz sobre IP para comunicarse.
- **QuickConnect.** Se puede iniciar rápidamente una conexión de TeamViewer directamente desde el software con el que esté trabajando, para mostrarlo visualmente.

Con respecto a la seguridad, TeamViewer como trabaja atreves de internet, para garantizar la seguridad de los datos, ofrece seguridad atreves de el intercambio de claves públicas/privadas RSA y el cifrado de sesión AES-256, los cuales garantizan que absolutamente nadie pueda ver los datos de su sesión. A cada inicio de TeamViewer, se genera una nueva contraseña de sesión dinámica que evita la posibilidad de acceso permanente para las aplicaciones.

3.7.2 La Vigilancia-online para las sucursales

La Vigilancia-online en las sucursales, es decir los almacenes de venta El vergel y Las Américas, son realizadas de manera profesional y con una alta tecnología de video-cámaras, las cuales proporcionan seguridad, control y supervisión de los almacenes de venta, además de asistir en el robo, fidelidad de empleados, etc.

Estas cámaras de red IP, son utilizadas para el control de las actividades diarias en los almacenes, las mismas que son de marca Panasonic de la serie BL-C. Una imagen de esta cámara se representa en la figura 3.25. Las cuales incluye una amplia variedad de funciones como: zoom digital de 10x, detección de movimiento, capacidad multi-cámara, modo de visión nocturna a color y sensor de imagen CMOS (falta decir q es cmos).

Las cámaras son alimentadas con 12v, las cual tiene una resolución máxima de 640x480, el formato de video es JPEG (movimiento JPEG para visualización de imágenes en movimiento), la cual está instalada en el sistema operativo Windows Xp.

Utiliza el software de grabación BB-HNP11 que permite almacenar imágenes y audio en el ordenador.

Figura 3.25.*Cámara de seguridad instalada en las sucursales.*[105]

Estas cámaras están configuradas para detectar la mayor cantidad de movimiento.

[105] http://listado.mercadolibre.com.ec/CAMARA-IP-PANASONIC-MODELO-BL%C3%98C111_DisplayType_G

Las imágenes de video son almacenadas en el equipo que está conectada la cámara, se puede tener acceso a las cámaras por medio de internet con la respectiva clave de acceso, por lo que de esta manera el administrador de la red de la Pasamanería puede controlar las actividades en los almacenes de venta.

CAPITULO 4

AUDITORIA DE LA RED FÍSICA

4.1Áreas de equipo de comunicación con control de acceso.

La fábrica tiene el control de acceso para el cuarto de telecomunicaciones de la siguiente manera:

4.1.1 Cuarto de telecomunicaciones.

El cuarto de telecomunicaciones esta en un lugar cerrado donde se encuentran servidores, tales como el servidor de aplicaciones, correo interno, correo externo y el de telefonía IP, los mismos que podemos visualizar en la figura 4.1.

Figura 4.1.*Cuarto de telecomunicación.*

Las personas que tienen acceso a este cuarto de telecomunicaciones son el gerente de sistemas, el administrador de la red y todo el personal del departamento de sistemas.

Estas personas no llevan ningún registro, indicando el motivo de ingreso, horario de entrada y salida al cuarto de telecomunicaciones.

Cabe mencionar que el cuarto de telecomunicaciones se encuentra dentro del departamento de sistemas y contabilidad. Como se puede ver en la Figura 4.2.

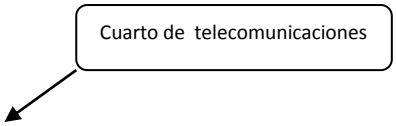


Figura 4.2. ***Departamento de Sistemas y Contabilidad.***

4.1.2 Cerradura de seguridad del cuarto de telecomunicaciones.

Para el ingreso no utilizan ninguna tecnología de autenticación como sistema de control con tarjetas inteligentes, el control de este cuarto de telecomunicaciones es mediante una cerradura con llave, la misma que podemos observar en la figura 4.3.

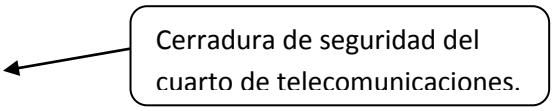


Figura 4.3.*Cerradura de seguridad del cuarto de telecomunicaciones*.

Las personas que tienen acceso a este cuarto de telecomunicaciones no llevan ninguna identificación personal.

4.1.3 Mensajes de alerta.

Este cuarto no tiene ningún mensaje de alerta indicando que únicamente puede acceder personal autorizado, como se puede observar en la figura 4.4.

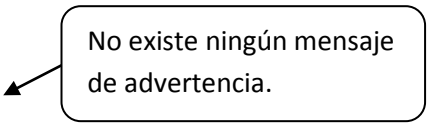


Figura 4.4. ***Sin mensaje de Alerta.***

4.1.4 Nivel de acceso a los Switch.

Todos los Switch que se encuentran instalados no tienen ningún nivel de seguridad, ya que están en los diferentes departamentos o secciones de la fábrica a la vista de todos sin la protección de un cuarto de telecomunicaciones, por lo que no tiene ningún control de acceso a los mismos como se puede ver en la figura 4.5.

Figura 4.5. ***Nivel de acceso a los Switch.***

4.2 Estándares y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.

4.2.1 Análisis de los elementos principales de un cableado estructurado.

Indicamos a continuación los puntos que definen el concepto de cableado estructurado de una red.

El cableado se encuentra instalado para que los usuarios de la red tengan acceso únicamente a lo que les corresponde y el resto del cable se encuentra con la debida protección.

El cableado estructurado es igual de funcional como por ejemplo el cableado eléctrico en dentro de la empresa.

Un cableado estructurado puede dar servicio por un periodo de hasta 20 años, independientemente de los avances tecnológicos en las computadoras.

Además tiene la capacidad de integrar varias tecnologías sobre el mismo cableado como voz, datos, video.

Contando con cableado estructurado se facilita la administración de la red, ya que se divide en partes manejables que permiten hacerlo confiable y perfectamente administrable, pudiendo así detectar fallas y repararlas sin complicaciones

4.2.1.1 Cableado Horizontal

El sistema de cableado horizontal, consiste en el cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones.

El cableado horizontal incluye:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo.
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles de empate (patch) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Para la realización de la auditoria a la red física de la fabrica nos hemos basado en la norma EIA/TIA 568 – A, por lo que se ha revisado lo siguiente.

4.2.1.1.1 La topología.

El Cableado Horizontal en la fábrica Pasamanería S.A siguen una topología estrella, ya que cada departamento tiene un switch central, al cual van conectadas las

computadoras que le corresponde y este a su vez va conectado al switch principal. Como se puede ver en la figura 4.6.

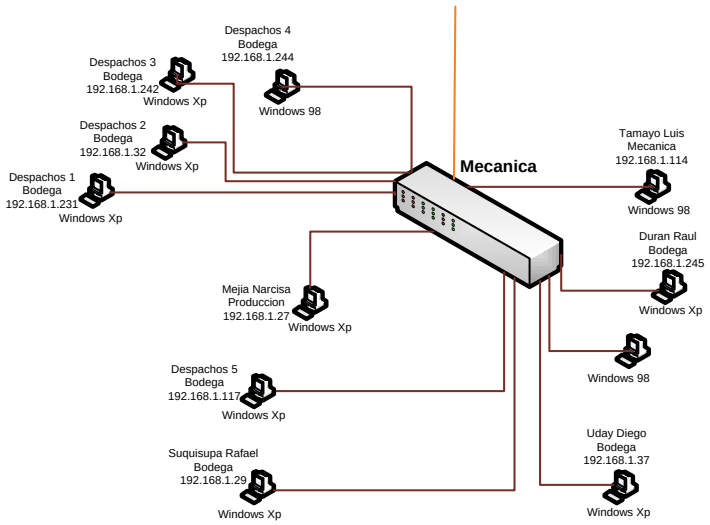


Figura 4.6.*Topologia estrella del cableado Horizontal*.

Cada toma/conector de telecomunicaciones de todas las áreas de trabajo está conectado directamente hacia el switch central, sin ningún tipo de interconexión como patch panels. Como se puede ver en la figura 4.7.

Figura 4.7. *Conexion Toma/Conector hacia switch.*

El cableado Horizontal termina en el mismo piso del área servida, es decir de cada departamento y además no tienen ningún tipo de empalme.

4.2.1.1.2 La distancia máxima de los cables.

- Las distancias del cableado Horizontal, es decir la medida del cable desde los respectivos switch de cada departamento a las diferentes toma/conector en las áreas de trabajo es de menos de 90 metros de longitud. Figura 4.8.

Figura 4.8. ***Distancia del cable desde el switch hasta la respectiva toma conector.***

- En todas las áreas de trabajo, se maneja una distancia máxima de 3 metros desde el equipo hasta la toma /conector de telecomunicaciones. Como se pude ver en la Figura 4.9.

Figura 4.9. ***Distancia del cable desde el equipo hasta la toma/conector.***

- Se separan los cables del área de trabajo y el switch en algunos casos menos de 10 metros, como es el caso del departamento Ventas. Como se puede ver en la figura 4.10.

Figura 4.10. ***Separación de los cables del área de trabajo al switch.***

4.2.1.1.3 Protección del cableado.

En la fábrica en algunos casos para proteger los cables de red hacen uso de, tuberías metálicas, canaletas de plástico, canaletas de madera y en otros casos los cables no se encuentran protegidos por ningún tipo de canaleta.

4.2.1.1.3.1 Tuberías metálicas

En la fábrica para algunos casos utilizan tubería metálica de ½ pulgada y 1 pulgada para proteger los cables de red ya sea para el cableado horizontal y el cableado Backbone, no tienen por separado estos dos tipos de cableado ya que se transportan por las mismas tuberías, esto se lo puede observar en la figura 4.11.

Figura 4.11. ***Tuberías Metálicas.***

4.2.1.1.3.2 Canaletas de plástico

Las canaletas de plástico son usados en algunos departamentos como secretaria. Como se puede observar en la figura 4.12.

Figura 4.12. ***Canaletas de Plástico.***

4.2.1.1.3.3 Canaletas de Madera.

Existen canaletas de madera para proteger los cables, las mismas que se encuentran instaldas en la piso, como es en el caso del departamento de contabilidad y sistemas. Como se puede observar en la figura 4.13.

Figura 4.13. ***Canaletas de Plástico***

4.2.1.1.3.4 Cables sin ningún tipo de protección.

En lo que corresponde a espacios de la fábrica como es producción ejemplo mecánica, corte, etc., los cables de red se encuentran sin ningún tipo de protección. Como se puede ver en la figura 4.14.

Figura 4.14. ***Cables de red sin ninguna protección.***

4.2.1.1.4 Rendimiento de los componentes.

La fábrica para el cableado horizontal trabaja con los siguientes medios:

- Cables de par Trenzado sin blindar (UTP) de 100 ohm categoría 5 y cuatro pares. Este tipo de cables puede transmitir datos a velocidades de hasta 100 Mbps. Las áreas que trabajan con cable UTP categoría 5 son las siguientes:
  - Secretaria General.
  - Supervisión General.
  - Almacén.
  - Diseño.
  - Corte.
  - Mecánica.

- Cables de par Trenzado sin blindar (UTP) de 1000 ohm categoría 6 y cuatro pares. Este tipo de cables puede transmitir datos a velocidades de hasta 1000 Mbps. Las áreas que trabajan con cable UTP categoría 6 son las siguientes:
  - Ventas.
  - Sistemas-Contabilidad.

4.2.1.1.5 Las tomas/conectores de telecomunicaciones.

En la fábrica se provee en algunas áreas de trabajo dos tomas/conectores y en otras únicamente una toma/conector, por lo que en estos casos en un futuro podría traer complicaciones cuando se requiera implementar servicio de voz. Figura 4.15.

Figura 4.15.*Toma/conectores.*

4.2.1.2 Cableado del Backbone

El cableado de backbone o también llamado vertical proporciona interconexión entre los cuartos de telecomunicaciones, los cuartos de equipo, cableado entre edificios.

El cableado backbone incluye:

- Cables vertebral.
- Interconexiones principales.
- Las terminaciones mecánicas y los cordones de parcheo o jumpers empleados en la interconexión de vertebral.

Basándonos en la norma EIA/TIA 568 –A, se ha revisado lo siguiente.

4.2.1.2.1 Topología.

La fábrica Pasamanería S.A, tiene una topología estrella para el cableado de backbone, ya que cuentan con un switch principal al mismo que se conectan 5 switch secundarios, como se puede ver en la figura 4.16.

Figura 4.16. ***Topología estrella del cableado Backbone.***

Todos los switch de los diferentes departamentos están conectados al switch principal de una manera directa, es decir sin ningún tipo de interconexión intermedia por ejemplo patch panels, como se puede ver en la figura (4.16).

En la fábrica, existe un nivel de conexión en cascada ya que el switch del departamento de Almacén y Diseño están conectados al switch de corte y este es el que se conecta con el switch principal, como se puede ver en la figura (4.17).

Figura 4.17.*Conexion en cascada de los switch Almacén y Bodega*.

En la fábrica no existe ningún tipo de empalme en el cableado de backbone, ya que los cables están directamente conectados hacia los switch.

4.2.1.2.2 Cable utilizado para bockbone de la fábrica.

- Cables de par Trenzado sin blindar (UTP) de 1000 ohm categoría 6 y cuatro pares. Estos cables transmiten datos a velocidades de hasta 1000 Mbps.

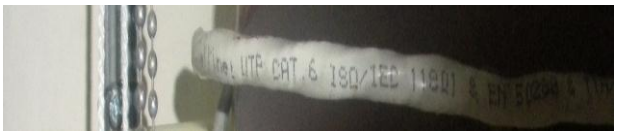


Figura 4.18. ***Cable Categoría 6.***

4.2.1.3 Área de Trabajo

El área de trabajo comprende desde la toma/conector de telecomunicaciones hasta el equipo de trabajo, puede incluir teléfonos, computadoras etc.

El cableado de las áreas de trabajo dentro de la fábrica no es permanente ya que fácilmente se puede cambiar.

Tienen en todas las áreas de trabajo cordones de cable con conectores idénticos a los dos lados Rj45.

Figura 4.19. ***Conectores RJ45 en área de trabajo.***

4.2.1.4 Especificaciones del cuarto de telecomunicaciones.

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones.

El mismo no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones.

Los cuartos de telecomunicaciones tienen estándares a seguir para su correcto funcionamiento, para revisar el cuarto de telecomunicaciones en la fabrica nos hemos basado en los entandares ANSI/TIA/EIA 568-A y ANSI/TIA/EIA 569-A.

El cuarto de telecomunicaciones de la pasamanería está diseñado de la siguiente manera:

4.2.1.4.1 Diseño:

La fábrica tiene solo un cuarto de telecomunicaciones que se encuentra en el departamento de Sistemas y contabilidad, el cual contiene 4 servidores, el router cisco, switch de 8 puertos, UPS y un cargador de baterías, como se puede ver la siguiente figura 4.20.

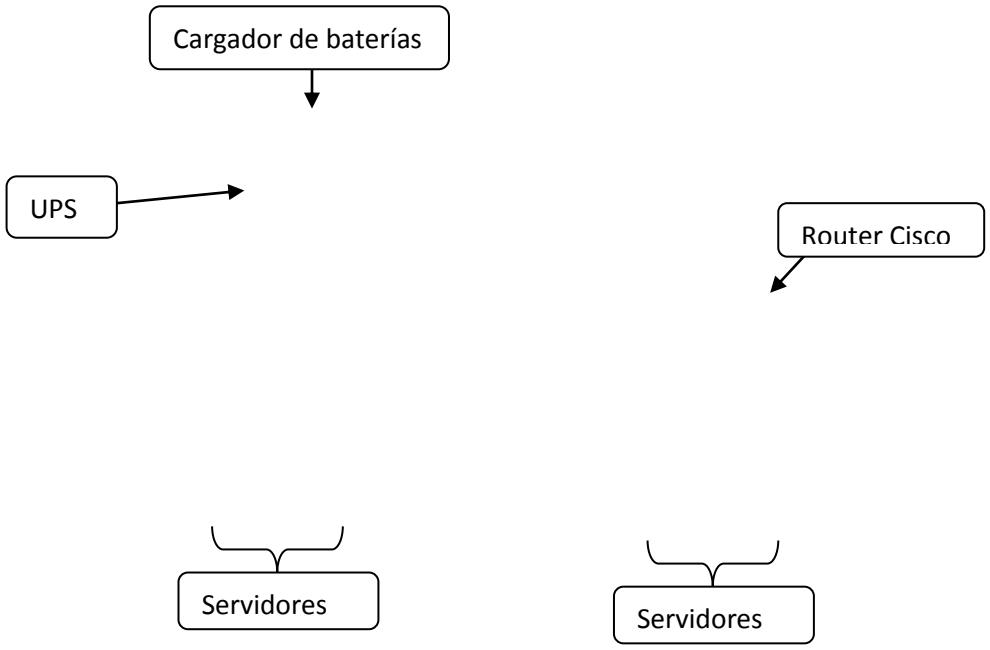


Figura 4.20. ***Cuarto de Telecomunicaciones.***

Este cuarto solo tiene incorporado sistemas de voz y de datos, no tienen ningún sistema de televisión por cable, alarmas, seguridad, etc.

4.2.1.4.2 Medidas.

El cuarto de telecomunicaciones, como se puede observar en la figura 4.18, tiene las siguientes medidas:

Alto: 2.97 m

Ancho: 1.50 m

Fondo: 97 cm

Figura 4.21. ***Medidas del cuarto de telecomunicaciones.***

4.2.1.4.3 Puertas.

Tiene dos puertas, estas se abren hacia afuera, son hechas de una estructura metálica con vidrio, y cuenta con las siguientes medidas.

Alto: 2.20 m

Ancho: 1.50 m

Estas puertas se abren al ras del piso, como se puede ver en ala figura 5.22.

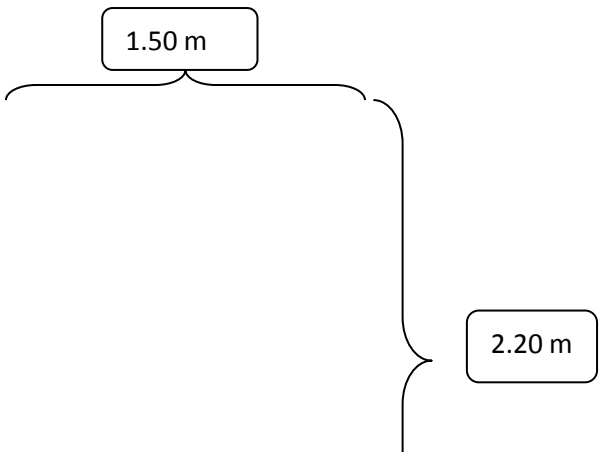


Figura 4.22. ***Medidas de las puertas del cuarto de telecomunicaciones.***

4.2.1.4.4 Patch Panels.

En la Pasamanería no utilizan los Patch Panels, el cual permite que el administrador de una red puede dividir o seccionar la distribución de cable que vaya para cada departamento que funcione en la fábrica, este sirve y cumple con la función de recibir la señal y enviarla por el puerto especifico del cual la recibe, por ejemplo si recibe señal del puerto 20 de entrada envía la señal hacia el puerto 20 de salida, en los puertos de salida se conectan los cables de red para poder enviar la señal a un router o un switch y de esa manera enviar la señal a las computadoras, el Patch Panels podemos ver en la siguiente figura 4.23.

Figura 4.23. ***Patch Panels.***

En la fábrica realizan las conexiones directas del switch a las rosetas, las mismas que se conectan a los equipos de trabajo.

En la fábrica Pasamanería S.A no tienen otros cuartos de telecomunicaciones para albergar los diferentes equipos q están distribuidos por la pasamanería como son los switch para cada departamento, por lo que estos equipos se encuentran a la vista de

todo mundo, de igual manera no utilizan los Patch Panels para realizar una conexión correcta y ordenada, esto se le puede observar en la figura 4.24.

Figura 4.24.Swtch sin ningún tipo de protección.

4.2.1.4.5 Ductos.

4.2.1.4.6 Polvo y electricidad estática.

En la fábrica para evitar el polvo y la electricidad estática en el cuarto de telecomunicaciones los servidores están en un mueble de madera y aparte utilizan un extractor de polvo el cual utiliza un tubo PVC (poli cloruro de vinilo) que se conecta con el extractor el cual está fuera del cuarto de telecomunicaciones, como se puede observar en la figura 4.25.

Figura 4.25. ***Extractor de polvo en el cuarto de telecomunicaciones.***

4.2.1.4.7 Control ambiental.

En el cuarto de telecomunicaciones la fábrica utiliza un aire acondicionador SMC para mantener una temperatura adecuada en el cuarto la misma que se encuentra en los 22 grados centígrados todos los días. Figura 4.26.

Figura 4.26. ***Acondicionar de temperatura SMC.***

4.2.1.4.8 Cielos falsos.

En el cuarto de telecomunicaciones se encontró la existencia de cielos falsos que es de un material de plástico, este cielo falso se la puede ver en la siguiente figura (4.27).

Figura 4.27. ***Cielo Falso dentro del cuarto de telecomunicaciones.***

4.2.1.4.9 Prevención de inundaciones.

En la parte posterior del cuarto de telecomunicaciones se encuentra los baños para el departamento de sistemas y contabilidad. Como se puede observar en la figura 4.28.

Figura 4.28. ***Parte posterior del cuarto de telecomunicaciones.***

En caso de haber una inundación por problemas de tuberías o de llaves que se queden abiertas no perjudicara en nada a los equipos que se encuentran en el cuarto de telecomunicación porque los mismos se encuentran en un mueble de madera con una altura de 83 cm. Como se puede ver en la siguiente figura 4.29.

Figura 4.29. ***Mueble del cuarto de telecomunicaciones.***

4.2.1.4.10 Iluminación.

No existe iluminación dentro del cuarto de telecomunicaciones, ya que no cuenta con ningún foco o lámpara, la única iluminación que tienen son las lámparas que existen

en el departamento de sistemas-contabilidad, las mismas que se encuentran en la parte de afuera al cuarto de telecomunicaciones, la cual se puede observar en la figura 4.30.

Figura 4.30. ***Iluminación en el departamento de sistemas-contabilidad.***

De igual forma se observo que las paredes del cuarto de telecomunicación utilizan un color claro el cual es un color blanco hueso ayudando así a tener más claridad en el cuarto.

4.2.1.4.11 Potencia.

Para la verificación de este punto nos hemos basado en el estándar ANSI.TIA/ EIA 568_A.

4.2.1.4.11.1 Tomacorriente.

En el cuarto de telecomunicaciones de la fábrica, se puede observar que cuentan con los suficientes tomacorrientes dobles para alimentar a los dispositivos de telecomunicaciones, sin embargo no cumplen con los estándares de instalación ANSI.TIA/ EIA 568_A, ya que estos tomacorrientes no están entre sí a una distancia como mínimo de 1.8m.

Además se verifico que los tomacorrientes si se encuentran a una distancia mayor de 15 cm como indica el estándar. Como se puede observar en la figura 4.31.

Figura 4.31. ***Tomacorrientes en el cuarto de telecomunicaciones.***

4.2.1.4.11.2 UPS

La alimentación de corriente para los respectivos equipos dentro del cuarto de telecomunicaciones en la fabrica la hacen mediante el dispositivo UPS, el mismo que protege de casi todos los problemas eléctricos conocidos como:

- Los cortes repentinos de luz.
- Caídas de energía.
- Subida de tensión.
- Caídas de tensión.
- Picos de alta tensión.
- Variación de frecuencia.

Se puede observar el equipo UPS que utilizan en la fábrica en la figura 4.32.

Figura 4.32. ***Equipo UPS.***

Especificaciones técnicas del UPS.

FÍSICA

- UPS de peso con la batería estándar 14,9 kg / 33 libras.

- Dimensiones UPS 9,9 "x 5,6 h" w x 15,8 "d

BATERÍA

- Tipo de batería sellada, lead-acid/maintenance libre
- Tiempo de carga completa de Apoyo 6 minutos
- Tiempo de recarga 4 horas a 80% de su capacidad

GENERAL

- Verdadera arquitectura en línea, doble conversión, líneas de alta tensión aisladas
- Interfaz de usuario 5 segmento de la exhibición de LED con medidores y alarmas
- Operación totalmente automática, panel de control táctil
- Diagnóstico del Sistema completo de auto prueba al encender el aparato
- UPS bypass automático de sobrecarga o fallo de la UPS

AMBIENTALES Y DE SEGURIDAD

- Audible el ruido 45 dBA a 1 metro
- Temperatura ambiente de funcionamiento 10 C a +40 C
- Ambiente Temperatura de almacenamiento-20C hasta +60 C
- Humedad relativa 5-95%, sin condensación

4.2.1.4.11.3 Cargador de Baterías.

Este cargador de baterías es usado para alimentar al dispositivo UPS, esto permite que el UPS este siempre cargado y a su vez listo para actuar en caso de que se fuera la luz, este cargador se puede ver en la siguiente figura 4.33.

Figura 4.33. ***Cargador de Baterías UPS***

4.2.1.5 Etiquetación y administración del cableado horizontal y backbone.

Para analizar este punto del etiquetado del cableado en la fábrica, nos hemos basado en el estándar TIA/EIA 606 (Etiquetación y administración).

4.2.1.5.1 Toma-conectores.

Ningún punto de terminación de cable en la fábrica tiene una etiqueta de identificación al igual que ningún punto intermedio. De igual manera en las toma/conectores no se encontró ninguna etiqueta que pueda ayudar a identificar de donde viene el cable de red, como se puede ver en la siguiente figura 4.34.

Figura 4.34. ***Toma-conector sin etiquetado.***

4.2.1.5.2 Cable del área de trabajo.

De igual manera no se encontró etiquetado ningún extremo de los cables de red que llega a las áreas de trabajo y de los equipos como se puede ver en la siguiente figura 4.35.

Figura 4.35. ***Cable del área de trabajo sin etiquetado.***

4.2.1.5.3 Colores de las terminales.

En la fábrica no han seguido ningún estándar para realizar el cableado de la red, por lo cual no manejan de una forma ordenada los colores de las terminales como son, para voz el color azul, datos el color blanco, y para datos/voz el color negro.

Basándonos en el estándar TIA/EIA 606 cada color tiene su respectiva utilidad, pero en la fábrica se encontró el uso de dos colores el blanco y el azul en cada terminal para el equipo de trabajo.

Los cuales son utilizados para datos y voz simultáneamente, siguiendo el estándar TIA/EIA 606 el color blanco es para las terminales de datos en el área de trabajo y el color azul para las terminales de voz.

La fábrica utiliza cualquier color de terminal ya sea de color azul o blanco en el departamento de sistemas, ya que en este caso esta implementado cable UTP de categoría 6, el cual da la posibilidad de utilizar la misma terminal para transmitir datos o voz.

Además cabe mencionar que en el resto de la Fábrica no se toma en cuenta el estándar de los colores de las terminales y se da uso una terminal de color azul para trasmitir datos y de igual manera se da uso una terminal de color blanco para trasmitir voz.

En la figura 4.36, podemos observar las terminales que utilizan en la fábrica

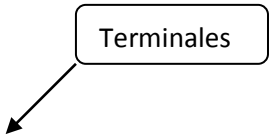


Figura 4.36. ***Colores de terminales utilizadas en la fábrica.***

4.2.1.5.4. Etiquetado de canaletas.

Las vías por dónde van los respectivos cables de red en la fabrica no están etiquetados, por ejemplo conductos, canaletas, etc. Como se puede ver en la figura 4.37.

Figura.4.37. ***Canaletas sin ser etiquetadas.***

4.2.1.5.5 Colores para el cableado de red.

De igual manera los colores de los cables de red también tienen diferentes funciones, por lo que en base al estándar TIA/EIA 606 nos hemos basado para revisar los respectivos usos que le dan en la fábrica.

- La fábrica maneja cualquier color de cable en las aéreas de trabajo, color blanco, azul y negro. Como se puede ver en la figura 4.38.

Figura 4.38. ***Colores de los cables para el área de trabajo.***

- La fábrica utiliza diferentes colores de cables para la interconexión de los equipos de datos dentro del cuarto de telecomunicaciones y no utiliza únicamente el color azul como dice el estándar. Como se puede observar en la figura 4.39.

Figura 4.39. ***Uso del color de cable azul dentro del cuarto de telecomunicaciones.***

- Además la longitud de los cables dentro del cuarto de telecomunicaciones es mayor a 1.5 metros como recomienda el estándar 606.Como se puede observar en la figura 4.40.

Figura 4.40. ***Longitud de los cables dentro del cuarto de telecomunicaciones.***

- El estándar indica que el cable de color amarillo se utiliza únicamente para la conexión de los equipos de telefonía, se observo que en la fabrica el cable de color amarillo se está utilizando para la conexión de equipos de datos, para esta conexión de equipos de telefonía se utiliza cualquier color, como podemos observar en la figura 4.41.

Figura 4.41. ***Uso del cable de color amarillo.***

4.3 Seguridad física de líneas telefónicas.

En la fábrica se pudo verificar que el correspondiente cableado de la telefonía se encuentra en varios lugares sin la debida protección de canaletas. Como se puede ver en la figura 4.42.

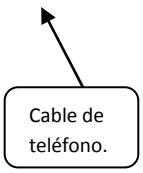


Figura. 4.42. ***Cableado de telefonía sin protección de canaletas.***

Para algunos puestos de trabajo, el cableado de telefonía se encuentra en las mismas canaletas en las que está el cableado de red y cableado eléctrico, dando la posibilidad de generar campo electromagnético, es decir que se pueda distorsionar la señal y dar lugar a problemas en la interferencia de los datos. Como se pude ver en la figura 4.43.

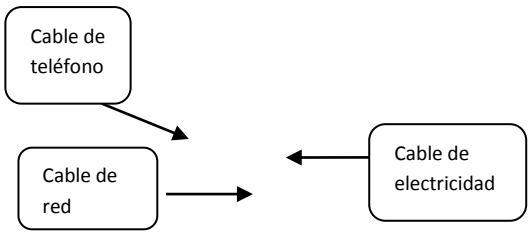


Figura 4.43. ***Cableado de red, telefonía y electricidad en una misma canaleta.***

En varios puestos de trabajo, los cables de teléfono se encuentran arrollados en el piso, ocasionando inconvenientes al personal que labora en los mismos. Como se puede ver en la figura 4.44.

Figura 4.44. ***Cable de teléfono enrollado en el piso.***

El Jack (puntos de red) está muy cerca de los tomacorrientes, esto puede ocasionar posibles inconvenientes generando campo electro magnético. Como se puede ver en la figura 4.45.

Figura 4.45. ***Puntos de red***.

En varios puestos de trabajo el tubo que protege el cable de teléfono se encuentra en deterioro y de igual manera los cajetines. Como se puede observar en la figura 4.46.

Figura 4.46. ***Cajetines en deterioro.***

4.4 Pinchazos a la Red.

Se entiende como pinchazo a la red, conectarse sin autorización a la misma, ya sea accediendo a un punto de red clandestinamente o realizando una conexión de cables mediante uniones.

En la fábrica Pasamanería S.A hasta el momento no han tenido pinchazos a la red.

Pero tiene el riesgo de que exista, ya que algunos de los cables de la red están sin protección de canaletas o ductos, se encuentran a la vista de cualquier persona. Como se puede ver en la figura 4.47.

Figura 4.47. ***Cables de red sin protección de canaletas.***

4.5 Análisis de la red Sucursal Las Américas.

4.5.1 Control de acceso para los equipos de comunicación en la sucursal de las Americes.

En la sucursal de Las Américas se pudo verificar que no cuentan con un cuarto de telecomunicaciones para la respectiva protección de los equipos de telecomunicación, ya que los mismos están colocados en un mueble de madera.

Cabe mencionar que este mueble que contiene los equipos de telecomunicaciones es también usado como puesto de cobro en el almacén. Como se puede observar en la figura 4.48.

Figura 4.48. ***Mueble que contiene los equipos en la sucursal de las Américas.***

Este mueble de madera contiene los siguientes equipos de comunicación:

- Router Cisco.
- Router LinkSys.
- Swich LB-link.
- Fast fiber Converter.

No hay ningún tipo de control de acceso a los equipos anteriormente mencionados, ya que están al alcance de los empleados que trabajan en el almacén.

Las personas que tienen acceso a los equipos son el administrador de la red y el personal que trabaja en el almacén, los mismos que no llevan ningún registro, indicando el motivo de ingreso y manipulación a los equipos.

Además el mueble únicamente tiene puertas corredizas y otras que se abren a los lados sin ningún tipo de seguridad con llave. Como se puede observar en la figura 4.49.

Figura 4.49. ***Mueble que contiene los quipos de comunicación sin protección de una cerradura.***

Este mueble de madera que contiene los equipos, no tiene ningún mensaje de alerta indicando que solo puede acceder a los equipos únicamente personal autorizado, como se puede observar en la siguiente figura 4.50.

Figura 4.50. ***Mueble de madera sin alarmas***

El Router LinkSys que se encuentran instalado en el almacén no tiene ningún nivel de seguridad, ya que está instalado a la vista de todos. Como se puede ver en la figura 4.51.

Figura 4.51. ***Nivel de acceso al Router LinkSys del Almacén Las Américas.***

4.5.2 Estándares y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos en la sucursal las Américas.

45.2.1 Cableado Horizontal en la sucursal las Américas

4.5.2.1.1 La topología en la sucursal las Américas.

El Cableado Horizontal en la sucursal Las Américas, siguen una topología estrella, ya que tiene un switch LB-link al cual van conectadas 3 cámaras de seguridad instaladas en el almacén y además un router Cisco al cual está conectado de una manera directa una PC y un teléfono IP. Como se puede ver en la figura 4.52.

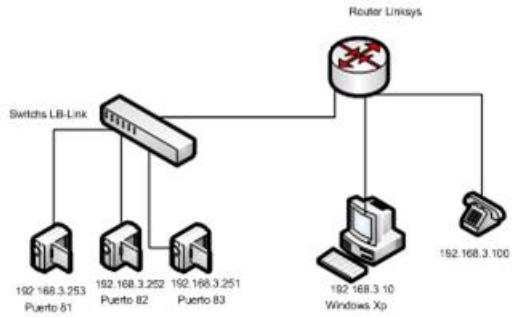


Figura 4.52. ***Topología estrella del cableado Horizontal de la sucursal las Américas.***

El cableado Horizontal termina en el mismo piso del área servida y además no tienen ningún tipo de empalme.

4.5.2.1.2 La distancia máxima de los cables en la sucursal las Américas.

Las distancias del cableado Horizontal en la sucursal las Américas corresponden a lo siguiente:

- Medida del cable desde el Router LinkSys hasta el switch LB-Link es de 1.50m.
- Medida del cable desde el Router LinkSys hasta la toma/conector es de menos de 10m y corresponde a una medida aproximada de 1m.
- Medida del cable el router hasta la PC es de 3m.

4.5.2.1.3 Rendimiento de los componentes en la sucursal las Américas.

En la sucursal de las Américas se encuentran instalados cables de par Trenzado sin blindar (UTP) de 100 ohm categoría 5 y cuatro pares.

4.5.2.1.3 Las tomas/conectores de telecomunicaciones en la sucursal de las Américas.

En la sucursal las Américas no tienen instalados en el área de trabajo una toma/conector, ya que el cable de red que se conecta con la PC va directamente desde el router LinkSys. Como se puede ver en la figura 4.53.

Figura 4.53. ***Conexión de la PC al Router LinkSys en la sucursal las Américas.***

4.5.2.1.4 Área de Trabajo en la sucursal de las Américas.

El cableado de las áreas de trabajo dentro de la sucursal de las Américas es permanente ya que la computadora se encuentra conectada al router directamente, en lugar de tener instalado toma/conectores.

El área de trabajo tiene cordones de cable con conectores idénticos a los dos lados Rj45.

4.5.2.1.4.1 Salidas de Área de trabajo en la sucursal de las Américas.

En la sucursal de las Américas cuentan con canaletas de plástico para la protección de los respectivos cables. Como se pude ver en la figura 4.54.

Figura 4.54. ***Canaletas de plástico en la sucursal de las Américas.***

4.5.3 Etiquetación y administración del cableado horizontal en la sucursal de las Américas.

4.5.3.1 Etiquetación y administración del cableado horizontal.

La etiquetación y administración del cableado horizontal en la sucursal las Américas hemos supervisado basándonos en el estándar TIA/EIA 606 (Etiquetación y administración).

4.5.3.1.1 Etiquetación de cables.

Ningún punto de terminación de cable o punto intermedio en la sucursal las Américas tiene una etiqueta de identificación. Como se pude ver en la figura 4.55.

Figura 4.55. ***Cables sin etiquetado en la sucursal de las Américas.***

4.5.3.1.2 Etiquetación de canaletas en la sucursal de las Américas.

Las canaletas por dónde van los respectivos cables de red de la sucursal de las Américas no están etiquetados. Como se puede ver en la figura 4.56.

Figura.4.56. ***Canaletas sin ser etiquetadas en la sucursal de las Américas.***

4.5.3.1.3 Colores para el cableado de red en la sucursal de las Américas.

De igual manera los colores de los cables de red también tienen diferentes funciones, por lo que en base al estándar TIA/EIA 606 nos hemos basado para revisar los respectivos usos que le dan en la Fábrica.

4.5.3.1.4 Color de cable en el área de trabajo.

La sucursal de las Américas maneja el cable de color negro para la conexión del router al área de trabajo. Como se puede ver en la figura 4.57.

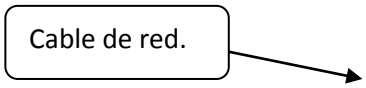


Figura 4.57. ***Colores de los cables para el área de trabajo en la sucursal de las Américas.***

4.5.3.1.5 Color de cable para la conexión de equipos de telecomunicación.

En la sucursal de las Américas para la conexión de los equipos de telecomunicación como lo son:

El router LinkSys con el router cisco y el router LinkSys con el switch LB-Link, hacen uso de cable color negro, blanco y amarillo en lugar de cable azul como indica el estándar. Como se puede ver en la figura 4.58.

Figura 4.58. ***Uso de varios colores de cable para la conexión de los equipos en la sucursal de las Américas.***

4.5.4 Seguridad física de líneas telefónicas en la sucursal de las Américas.

En la sucursal de las Américas se pudo observar que el cable de la a telefonía se encuentra mezclado con el cable de red que conecta los equipos de telecomunicación. Como se puede ver en la figura 4.59.

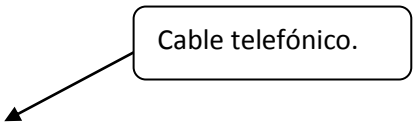


Figura. 4.59. ***Cableado de telefonía mezclado con cableado de red.***

Además se reviso que el cable de teléfono no se encuentra en la misma canaleta con el cable de red y el cable de electricidad. Como se puede ver en la figura 4.60.

Figura 4.60. ***Únicamente cable de red en canaletas.***

En el área de trabajo el cable del teléfono encuentra arrollados sin la debida protección, como se puede ver en la figura 4.61.

Figura 4.61. ***Cable de teléfono enrollado.***

4.5.5 Pinchazos a la red en la sucursal de las Américas.

En la sucursal de las Américas hasta el momento no han tenido pinchazos a la red.

Cabe mencionar que no hay el riesgo de que algo así como pinchazos a la red ocurra, ya que los cables de red están en un mueble de madera y bajo la vigilancia constante de dos personas que laboran en el almacén. Además los cables de red que se encuentran a la vista del público están bajo la protección de canaletas de plástico, como se puede observar en la figura 4.62.

Figura 4.62. ***Cables de red con protección.***

4.6 Análisis de la red Sucursal El vergel.

4.6.1 Control de acceso para los equipos de comunicación en la sucursal el Vergel.

El control de acceso al cuarto de telecomunicaciones en la sucursal el Vergel esta de la siguiente manera:

Esta sucursal no tiene implementado ningún cuarto de telecomunicaciones donde irían los equipos de telecomunicaciones.

Los equipos de telecomunicaciones están en un mueble de madrea el mismo está cerrado, en el cual están el Cisco Systems, 2 D-Link, Fast Fiber Converter, BLACKOUT BUSTER y el CPU de trabajo.

Este cuarto donde se encuentran los equipos de telecomunicaciones se puede ver en la siguiente figura 4.63.

Figura 4.63. ***Mueble donde se encuentran los equipos de telecomunicaciones.***

Las personas que tienen acceso a este mueble donde se encuentran los equipos de telecomunicaciones son el administrador de la red de la pasamanería y el personal que se encuentra trabajando en esta sucursal.

De igual forma como en la fabrica Pasamanería no llevan ningún registro, indicando el motivo de ingreso, horario de entrada y salida al mueble donde se encuentran los equipos de de telecomunicaciones.

Este mueble también es usado como caja donde se atiende a los clientes para su respectiva facturación de los productos comprados, como se puede ver en la siguiente figura 4.64.

Figura 4.64. ***Caja de la sucursal el Vergel.***

De igual manera como no tienen el cuarto de telecomunicaciones no utilizan ninguna tecnología de autenticación como sistema de control con tarjetas inteligentes, el control que se da a este cuarto es que está cerrado con puertas de madera las mismas se abren hacia afuera, pero el problema es que no tienen ninguna cerradura para poner llave, como se puede ver en la figura 4.65.

Figura 4.65. ***Puertas del mueble donde se encuentran los equipos de telecomunicaciones.***

Las personas que tienen acceso a los equipos de comunicación no llevan ninguna identificación personal.

Se puede observar el router que conecta a las dos cámaras y al equipo de trabajo que se encuentra a la vista de todo mundo sin ningún nivel se seguridad, de esta forma no se pude tener ningún control de acceso como se puede ver en la figura. 4.66.

Figura 4.66. ***Nivel de acceso a los Switch.***

4.7 Estándares y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.

4.7.1 Elementos principales de un cableado estructurado

4.7.1.1 Cableado Horizontal

4.7.1.1.1 La topología.

El Cableado Horizontal en la sucursal del Vergel siguen una topología estrella, como podemos observar en la figura 4.67.

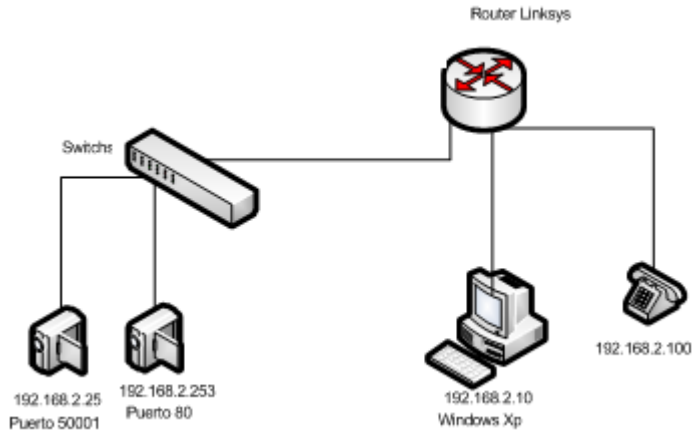


Figura 4.67. ***Topología estrella del cableado Horizontal de la sucursal del vergel.***

4.7.1.1.2 La distancia máxima de los cables.

Las distancias del cableado Horizontal, es decir la medida del cable del switch D-Link a las dos cámaras no pasa de los 10 metros, como se puede observar en la figura 4.68.

Figura 4.68. ***Distancia del Switch D-Link hacia las cámaras.***

También la medida de los cables Router Linksys a las tomas/conector no exceden los 4 metros. Como se puede ver en la siguiente figura 4.69.

Figura 4.69. ***Distancia del cable desde el router Linksys hasta la respectiva toma conector.***

En el área de trabajo se maneja una distancia máxima de 3 metros desde el equipo de trabajo hacia el toma/conector. Como se puede ver en la figura 4.70.

Figura 4.70. ***Distancia entre el equipo de trabajo y el conector de red.***

La longitud del cable para la conexión de los equipos de telecomunicaciones exceden a 1.5 metros, además estos cables están enrollados estando uno encima del otro, esto se la puede ver en la figura 4.71.

Figura 4.71. ***Longitud de los cables para la conexión de los equipos.***

4.7.1.1.3 Rendimiento de los componentes.

La sucursal del vergel trabaja con cables de par Trenzado sin blindar (UTP) de 100 ohm categoría 5e y cuatro pares. Este tipo de cables puede transmitir datos a velocidades de hasta 1000 Mbps

Este cable se lo utiliza para las diferentes conexiones ya sea para conectar a las cámaras, al equipo de trabajo, entre el router Linksys y el switch D-Link etc, este cable se puede ver en la figura 4.72.

Figura 4.72. ***Cable UTP de categoría 5e.***

4.7.2 Etiquetación y administración del cableado horizontal de la sucursal el Vergel.

De igual manera para analizar este punto del etiquetado en la sucursal el Vergel, nos hemos basado en el estándar TIA/EIA 606 (Etiquetación y administración).

4.7.2.1 Toma-conectores.

En el único toma/conector que se puede observar en la sucursal el Vergel no tenía ninguna etiqueta de identificación que pueda ayudar a identificar de donde viene cada cable de red, como se puede ver en la figura 4.73.

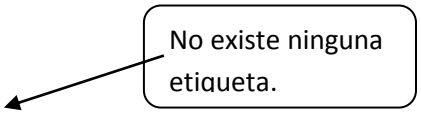


Figura 4.73. ***Toma-conector sin etiquetado.***

4.7.2.2 Etiquetado para cables para el área de trabajo.

También no se encontró etiquetado ningún extremo de los cables de red que salen del conector y que llegan al equipo de trabajo y al switch D-Link como se puede ver en la figura 4.74.

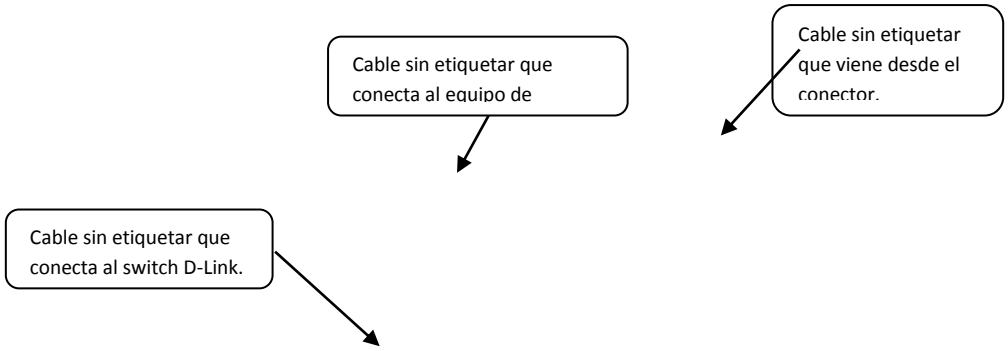


Figura 4.74. ***Cables para el área de trabajo y switch D-Link sin etiquetado.***

4.7.2.3 Canaletas.

Las canaletas por dónde van los respectivos cables de red no están etiquetados, como se puede ver en la figura 4.75.

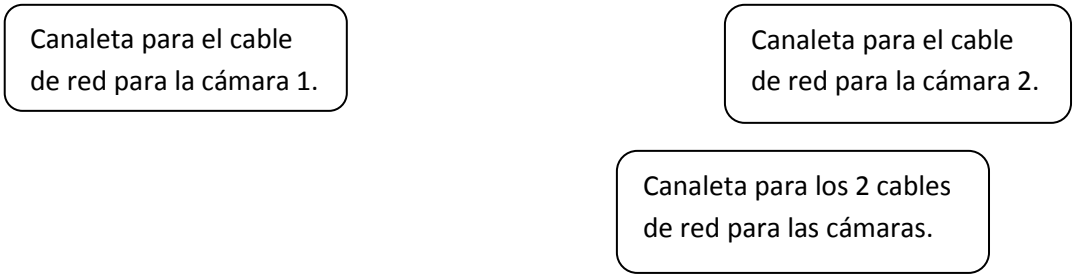


Figura 4.75. ***Canaletas sin ser etiquetadas.***

4.7.2.4 Colores de las terminales.

Para los colores de las terminales de igual forma nos hemos basado en el estándar TIA/EIA 606 para verificar en la sucursal el Vergel.

El color de las terminales que se pudo observar es de color rojo el cual indica que es para cable UPT de categoría 5e los que se utilizan para la conexión del equipo de trabajo y conectar al switch D-Link, estas terminales podemos observar en la figura 4.76.

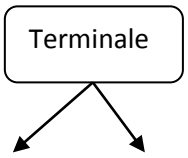


Figura 4.76. ***Terminales de color rojo.***

4.7.2.5 Colores para el cableado de red.

De igual manera como se reviso los colores de los cables de red en la fábrica basándonos en el estándar TIA/EIA 606 también se reviso los colores en la sucursal del Vergel.

En la sucursal el Vergel también se maneja cualquier color de cable para conectar al equipo de trabajo, en este caso se utiliza el cable de color negro, debiendo ser de color blanco, la cual se puede ver en la figura 4.77.

Figura 4.77. ***Color del cable para el área de trabajo.***

Según el estándar TIA/EIA/606 los colores de cable para la conexión de los equipos dentro del cuarto de telecomunicaciones debe ser de color azul pero en la sucursal se usa cualquier color ya sea azul, plomo, amarillo y negro, como se puede observar en la figura 4.78.

Figura 4.78. ***Uso del color de cable azul dentro del cuarto de telecomunicaciones.***

4.7.2.6 Uso de canaletas de plástico.

En la sucursal el Vergel en ciertas partes si utilizan canaletas de plástico y en otras partes no, se pudo observar que estas canaletas se utilizan para proteger los cables que van al Router Linksys, como se puede ver en la figura 4.79.

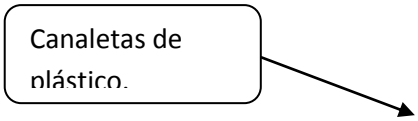


Figura 4.79. ***Canaletas utilizadas para la protección de cables de red.***

De igual manera también se utiliza estas canaletas para proteger los cables de red que van conectadas hacia las cámaras Ips, como se puede ver en la figura 4.80.

Figura 4.80. ***Canaleta que protege al cable de red para conexión de la cámara IP.***

4.7.2.7 Tendido de los cables.

Los cables de red para la conexión de los equipos de telecomunicación están en canaletas de plástico, pero la misma canaleta es utilizada para proteger un cable de electricidad, como se puede ver en la figura 4.81

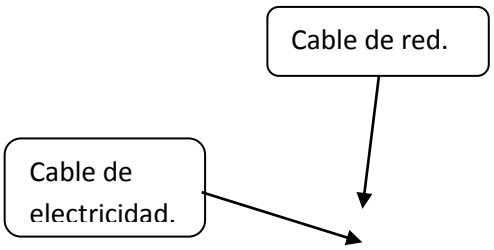


Figura 4.81. ***Cables de electricidad y de red en una misma canaleta.***

Se puede observar que las tomas corrientes están muy juntos a más que los cables de electricidad y los cables de red están mesclados, siendo esto un problema ya que se puede dar un campo electromagnético perjudicando a los cables de red en su correcto funcionamiento en la transmisión de datos, como se puede observar en la figura 4.82.

Figura 4.82. ***Cables mezclados de electricidad y de red.***

4.7.3 Control de las líneas telefónicas.

En el control de las líneas telefónicas se pudo observar que el cable de la línea telefónica no está protegido con ninguna canaleta ya que está mezclado con los demás cables de red y de electricidad, esto se puede observar en la siguiente figura 4.83.

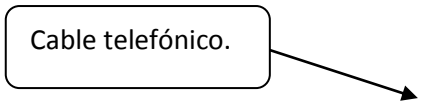


Figura 4.83. ***Cable telefónico.***

4.7.4 Pinchazos a la red

Se observo que en la sucursal el Vergel no se pueden dar pinchazos a la red ya que es un local comercial donde se vende los productos confeccionados en la fábrica Pasamanería a mas de que los cables que podrían estar a la vista de todo mundo están protegidos por canaletas, estos cables protegidos se puede observar en la siguiente figura 4.84.

Figura 4.84. ***Cables protegidos por canaletas.***

CAPITULO 5

AUDITORIA DE LA RED LÓGICA

5.1 Contraseñas de acceso.

5.1.1 Contraseñas de acceso a las PC.

Cada una de las máquinas que actualmente se encuentran en funcionamiento en la Pasamanería S.A, están configuradas para que accedan los usuarios al sistema operativo con privilegio de administrador, los mismos que pueden ser:

- Instalar y desinstalar software.
- Administrar la tarjeta de red.

Una de las razones por la cual las máquinas están instaladas como usuario administrador, es que trabajan como cliente-servidor, ya que en todas las maquinas cliente se encuentran instaladas los respectivos ejecutables del sistema que manejan en la Pasamanería y esto a la vez facilita dar soporte al usuario en caso de que lo solicite, accediendo remotamente en cada PC y realizando los cambios necesarios sin la necesidad de reiniciar las máquinas.

Todas las máquinas tienen su respectivo usuario y contraseña de acceso, la cual es generada por el software Lotus Symphony, el mismo que funciona creando las contraseñas con una función randómica.

El mismo que está compuesto por tres elementos:

- Procesador de texto.
- Hoja de cálculo.
- Programa de presentaciones.

Para el mismo se utilizó la hoja de cálculo para generar las contraseñas de 4 dígitos, dentro del programa se seleccionó la opción RANGE y luego FILL, ya dentro de esta

opción se llenó las siguientes opciones para generar las contraseñas, Fill range, start value, step value y stop value, de esa manera se generaron las contraseñas.

5.1.2 Contraseñas de acceso a Servidores y equipos de comunicación.

5.1.2.1 Contraseñas de acceso a Servidores.

La contraseña para acceder al servidor de aplicaciones está compuesta de 5 dígitos y fue generada con el software Lotus Symphony.

Para acceder a los servidores de correo interno y externo existe una misma clave, la cual está compuesta de 6 dígitos.

El servidor PasaWeb tiene una contraseña de acceso de 8 dígitos, la cual es creada por el administrador de la red sin la ayuda ningún software.

Únicamente el administrador de la red, tiene acceso a las contraseñas anteriormente mencionadas.

Los usuarios que utilizan el sistema para sus labores diarias tienen acceso al servidor de aplicaciones mediante los respectivos aplicativos, ya que graban las transacciones directamente en dicho servidor.

5.1.2.2 Contraseñas de acceso a los equipos de comunicación.

Los equipos de comunicación Routers, los cuales son utilizados para la red inalámbrica interna de la Pasamanería, cuentan para todos con la misma contraseña de 8 dígitos, la cual fue cambiada por la contraseña predeterminada Admin.

Esta contraseña es la misma que es utilizada para el servidor PasaWeb.

Mientras que la contraseña que utilizan los usuarios para acceder a la red inalámbrica de la Pasamanería está compuesta por 10 dígitos entre letras y números, la misma que fue creada por el Administrador de la red, dicha contraseña tienen acceso únicamente el administrador de la red y usuarios con la necesidad de conectarse a internet.

Los switch no cuentan con contraseñas de acceso, ya que a pesar de que son switch de capa 3, no son administrados y son utilizados únicamente como puente.

5.1.3 Contraseñas de acceso al sistema.

Las aplicaciones que se encuentran implementadas en la Pasamanería S.A son las siguientes:

- SPP = Sistema Producción Pasamanería.
- SCP=Sistema Comercialización Pasamanería.
- CRM= Customer Relationship Management.

Cada usuario tiene una única contraseña para acceder a las aplicaciones, las cuales son generadas con una función randómica en el programa llamado Lotus Symphony, esta clave es de 4 dígitos.

5.1.4 Contraseñas de acceso al correo Interno.

Para el acceso al correo Interno, todos los usuarios tiene en sus respectivas máquinas un icono de acceso directo al correo Outlook express, no tienen la necesidad de ingresar ninguna contraseña para acceder al correo, porque ya está configurado para acceder directamente.

Para la administración del correo interno, es decir eliminar, hacer respaldos de los mismos, existe una única clave para todos los usuarios de la Pasamanería, la misma que está compuesta de 4 dígitos.

En el caso de que un usuario quiera acceder al correo interno mediante internet desde de un lugar diferente de la fábrica, debe ingresar a la página web de la Pasamanería y buscar el acceso al correo, ingresar la dirección de correo personal la cual es común para todos los usuarios.

El correo interno funciona solo dentro de la red de la Pasamanería y sus sucursales es decir se puede enviar un correo a usuarios que tengan cuenta pasa.ec, mientras que el correo externo funciona con cualquier cuenta de correo, es decir se puede enviar un correo a otro tipo de cuenta ya sea de hotmail, gmail etc.

El correo externo es asignado a pocas personas como los gerentes generales, gerente de sistemas, administrador de la red, etc. Cada uno tiene su cuenta de correo. A diferencia del correo interno las claves de acceso son diferentes ya que cada dueño de su cuenta crea su propia contraseña para acceder.

5.1.5 Administración de cuentas de correo Interno o Externo

Para administrar las cuentas de correo interno y externo utilizan el software Webmin, el mismo que se encuentra instalado en el servidor PasaWeb, cabe recalcar que este

servidor es utilizado por el administrador de la red como una PC para las labores diarias.

La contraseña para acceder a Webmin es la misma que se utiliza para acceder a los servidores de correo Interno y Externo con el usuario root, el acceso al Webmin se lo puede ver en la figura 5.1.

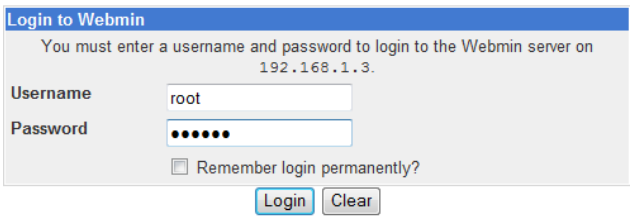


Figura 5.1. ***Acceso al Webmin.***

En el Webmin se puede realizar las siguientes tareas:

- Lectura de cuentas de correo de usuarios.

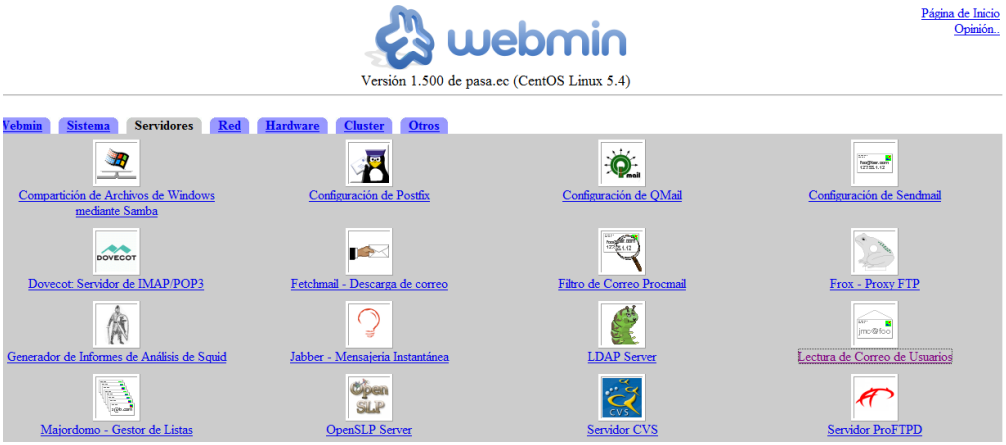


Figura 5.2. ***Menú de Webmin en la pestana se Servidores para acceder a la Lectura de correo de usuarios.***

- Lectura de correos electrónicos grabados en el servidor antes de ser entregados a su respectivo usuario.

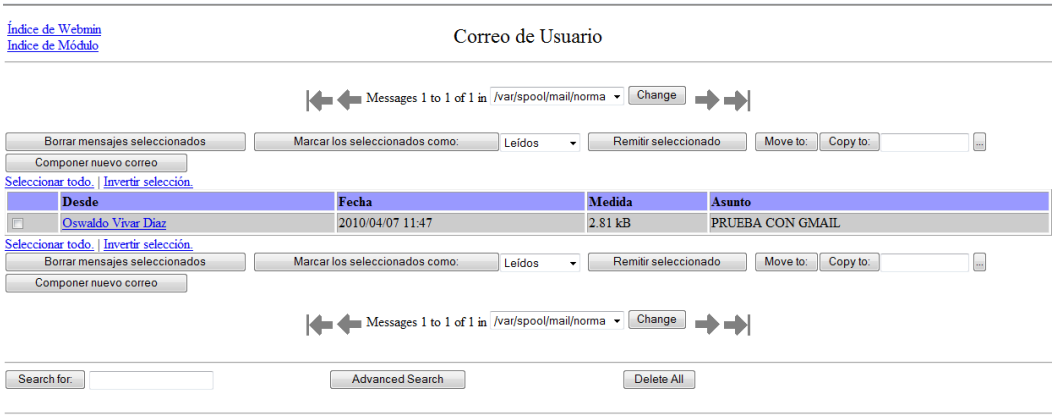


Figura 5.3. ***Lectura del correo personal antes de ser entregados.***

- Cambiar contraseñas de los correos.

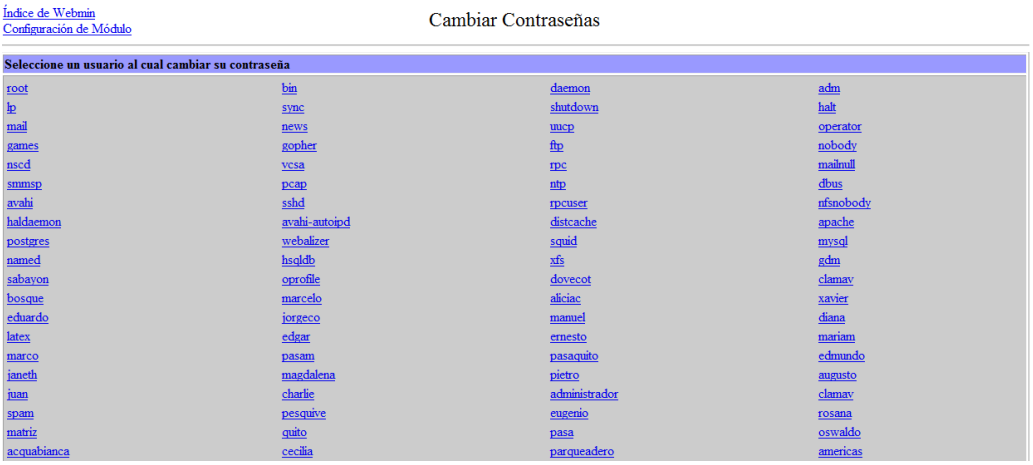


Figura 5.4. ***Lista de cuentas de usuarios.***

- Cambiar contraseña de una cuenta de correo específico.

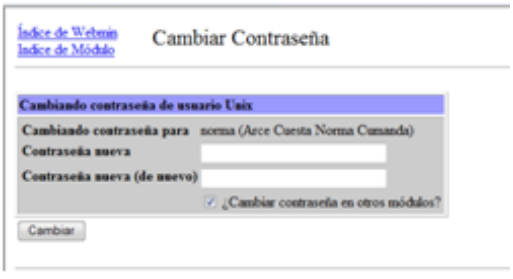


Figura 5.5. ***Ventana para cambiar la contraseña de una cuenta de correo.***

5.2 Control de errores.

5.2.1 Protocolos con detección de errores.

En la pasamanería no utilizan ningún protocolo, que ayude a detectar los errores automáticamente en la red, ejemplo cuando se cae un determinado enlace, es decir un punto de red.

La manera de que el administrador de la red tiene conocimientos de los problemas en toda la red, es mediante una llamada telefónica por parte de los usuarios, para posteriormente solucionar el problema.

5.3 Garantías seguridad de transmisión de datos.

5.3.1 Control de impresión de datos sensibles.

Se verificó que existen varias impresoras instaladas en toda la fábrica y estas a su vez están compartidas para que se pueda mandar a imprimir desde distintas máquinas, como es en el caso del departamento de sistemas y contabilidad.

En estos casos la impresión es únicamente de datos que no sean de mayor importancia.

Para el caso de usuarios que necesitan imprimir documentos de carácter confidencial como son los gerentes, ellos tienen sus propias impresoras y no esta compartida con ninguna otra máquina.

De esa forma se controla la impresión de datos sensibles en la Pasamanería.

5.4 Actividades de los usuarios en la red.

En la Pasamanería no utilizan ningún software o herramienta que ayude a ver las actividades de los usuarios en la red tales como:

- Ver el tráfico de la red.
- Paquetes enviados y recibidos por máquina.
- Carga de la red.
- Protocolos de distribución que están trabajando en la red como: TCP, UDP, ICMP, RARP, IGMP, STP.
- También el uso o consumo de los protocolos como: PROXY, HTTP, DNS, TELNET, etc.
- Puntos de vista históricos en la fecha que se desee, en forma gráfica ya sea:
- Fecha de inicio y fecha de fin. Por horas, la última hora, las 2 últimas horas, las 4 últimas horas, etc.

- Verificar la carga de la red ya sea:
    - Los últimos 10 minutos de rendimiento.
    - El rendimiento en la última hora.
    - El rendimiento día actual.
    - El rendimiento del mes pasado.
- Verificar el tráfico de todos los protocolos en un mismo instante en porcentajes.
- Información sobre los servidores o máquina que se encuentre en la red como:
    - La dirección IP de la máquina.
    - La fecha y hora desde que se analizó hasta la culminación.
    - La dirección MAC de la máquina que se analiza.
    - Nombre de la NetBios identificando a la maquina que se está analizando.
    - El total de datos enviados.
    - El número de Broadcast enviados o paquetes enviados.
    - El tráfico de multidifusión (multicast).
    - Los datos enviados en forma estadística.
    - El tipo de host.
    - Y entre otras especificaciones.
- Estadísticas de tráfico de servidores o máquinas que se desee monitorear.
- También en análisis del uso de memoria de servidores o máquinas.
- Porcentajes de carga promedio de servidores o máquinas.
- Porcentajes de los procesos de servidores o máquinas.
- Porcentajes de espacios de disco duros de servidores o máquinas.

Todos los puntos antes mencionados se podrían verificar de forma gráfica con sus respectivos porcentajes utilizando programas que nos ayuden a verificar estos puntos, estos programas pueden ser CACTI y NTOP los cuales serán utilizados y se mostrará su utilización en el Capitulo 6.

5.5 Encriptación de la información.

En la Pasamanería no utilizan ningún método o algoritmo para encriptar su información más crítica, los datos que van por internet no tienen ningún tipo de seguridad, a mas de que su página Web y el acceso al correo interno y externo no

utiliza ningún protocolo de seguridad como el SSL, cuando se conecta a un servidor seguro se muestra de esta manera (https://www…) , los navegadores avisan de esta circunstancia mediante un candado de color amarillo en la parte superior y además permiten comprobar la información contenida en el certificado digital que lo habilita como servidor seguro, esto se puede ver en la figura 5.6.

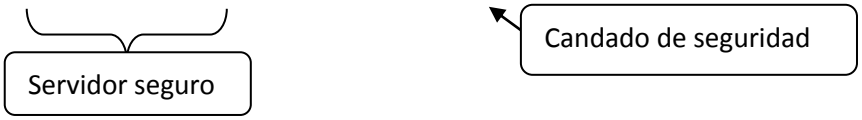


Figura 5.6. ***Pagina con seguridad SSL.***

Como se puede ver en la figura anterior vemos un claro ejemplo que el correo que utiliza google esta utilizando encriptación SSL ya que se puede ver con el candado amarillo y la forma de conexión https://mail.google.com.

Ahora veamos la pagina Web de la Pasamanería no utiliza ningún tipo de encriptación podemos darnos cuenta porque el tipo de conexión es http://www.pasa.ec y no https://www.pasa.ec y no se puede observar ningún candado amarillo indicando que es seguro ese servidor, esto se puede ver en la figura 5.7.

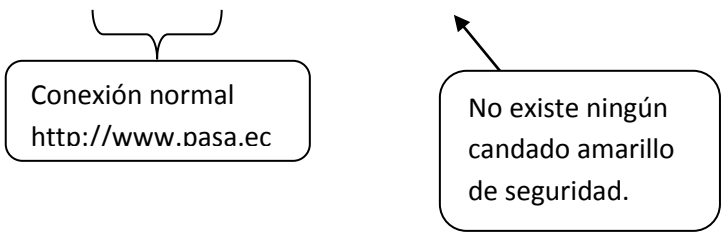


Figura 5.7. ***Pagina web de la Pasamanería sin seguridad SSL.***

De igual forma el correo interno y externo no utiliza ningún tipo de encriptación, como se puede ver en la figura 5.8.

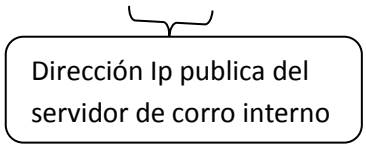


Figura 5.8. ***Ingreso al correo interno sin seguridad SSL.***

5.6 Inhabilitar el software con acceso libre.

En este punto se verificó que las contraseñas de los equipos de comunicación como son los routers son cambiados por los que vienen por defecto, para así controlar que ninguna persona extraña pudiera entrar a estos equipos y cambie la configuración o pueda saber cierta información que necesite para conectarse a la red de la fábrica.

Como se puede ver en la figura 5.9, vemos en la configuración del router Linksys utilizados para la red inalámbrica se cambio la contraseña por la que viene por defecto la misma que es Admin para ingresar al equipo.

Figura 5.9. ***Ventana de administración para cambiar la contraseña de ingreso al equipo.***

De esa forma se controla o se inhabilita el acceso al software de configuración de los equipos Routers Linksys.

5.7 Control de seguridad asociado para impedir el acceso de equipos foráneos a la red.

Para controlar la seguridad para el acceso de equipos foráneos a la red inalámbrica de la Pasamanería S.A, se verificó que se controla con un tipo de seguridad llamada WPA-Personal, la misma que permite la autenticación mediante clave compartida ([PSK], Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red, este tipo de seguridad es más que segura que la WEP.

En la cual se utiliza un tipo de encriptación TKIP que se trata de un protocolo de seguridad usado en WPA (Wi-Fi Protected Access) para mejorar el cifrado de datos en redes inalámbricas, la cual TKIP combina la clave temporal de 128 bits que comparte entre los clientes y puntos de accesos, es decir combina la clave temporal con la dirección MAC del cliente, esta configuración se la puede ver en la figura 5.10.

Figura 5.10. ***Ventana de configuración de seguridad para los equipos Routers.***

5.8 Políticas de prohibición de la instalación de programas o equipos personales en la red.

En la fábrica no existe ningún documento indicando políticas de prohibición de la instalación de programas en las maquinas que utilizan los empleados.

Tampoco utilizan algún tipo de software como el Inventory para controlar la instalación de software que no sea necesario para realizar las labores diarias de los empleados.

Pero el administrador de la red ha tomado precauciones para evitar este problema de cierta manera ya que ninguna máquina de escritorio tiene dispositivos como cd-rom o dvd.

Pero si podrían instalar programas mediante el dispositivo usb, ya que no se puede inhabilitar este dispositivo porque son utilizados para ratones, teclados, etc.

Además de que no puede controlar que instalen programas bajados por el internet de ciertos usuarios que tienen acceso a internet.

Cabe recalcar que no ha tenido problemas de este tipo el administrador ya que los usuarios no lo han hecho.

5.9 Seguridad de accesos a servidores remotos.

Se utiliza escritorio remoto para acceder a los servidores y a las respectivas sucursales para solucionar cualquier problema que se presente, mientras que a las demás máquinas que conforman la red de la Pasamanería no se accede mediante escritorio remoto para solucionar los problemas, si no que el administrador de la red lo soluciona directamente en lugar que se encuentre la maquina con problemas.

Los programas que se utilizan para hacer esta tarea son NetOp, el mismo que esta explicado todas sus funciones en el capitulo tres en el punto 3.7.1.1 y Team Viewer 5 que igual esta explicado en el capitulo tres en el punto 3.7.1.2.

La seguridad en el acceso a escritorio remoto mediante las herramientas explicadas anteriormente se limita a la configuración siguiente:

Esta abierto un puerto en el router que corresponde a escritorio remoto el cual es 3389, lo que ocasiona el peligro de que cualquier persona con conocimiento de la IP de la red podría acceder con facilidad a las respectivas computadoras.

CAPITULO 6

RECOMENDACIONES DEL ANÁLISIS DE LA RED FÍSICA Y LÓGICA DE LA FÁBRICA PASAMANERÍA S.A.

En este capítulo indicamos las respectivas recomendaciones al análisis realizado a la red física y lógica de la Pasamanería S.A.

6.1 Gestión de red: los equipos y su conectividad.

Para gestionar los equipos que se encuentran en funcionamiento tanto en la matriz como en las respectivas sucursales a nivel nacional, recomendamos la herramienta ULTRAVNC, ya que esta herramienta sería de gran ayuda para el administrador de la red, el mismo que da soporte a los usuarios de la red con problemas en las computadoras.

A continuación daremos una breve descripción del software mencionado.

UltraVNC es una sencilla herramienta con la cual es posible controlar cualquier equipo conectado a la Red.

Esta herramienta tiene una arquitectura cliente/servidor, de esta manera da la posibilidad de acceder remotamente a cualquier PC que tenga instalado el cliente (vncviewer).

Una de las razones por lo cual recomendamos Ultravnc es que este software es la versión mejorada de RealVNC o TightVNC , ya que incorpora las mejores funcionalidades de ambos programas y adicionalmente incorpora transferencia de archivos, Chat, nuevos algoritmos de compresión, etc.

Cabe recalcar que ultravnc funciona tanto en entornos Windows como Linux, por lo que sería de mucha ayuda para acceder remotamente a los servidores de la Pasamanería que se encuentran en Linux.

Sin embargo se recomienda utilizar ultravnc únicamente dentro de la red local, es decir instalar la herramienta solo en las máquinas que se encuentren en la misma red de la Pasamanería y no hacer una conexión de la herramienta mediante la conexión de Internet, ya que resultaría peligroso, porque cualquier persona únicamente con conocimiento de la contraseña se podría acceder a la máquina sin ningún inconveniente, a menos que se bloquee los puertos usados por el protocolo VNC en un firewall.

Indicaremos algunas ventajas de UltraVNC:

- Es rápido y estable.
- Tiene una interfaz muy sencilla.
- Permite encriptar los datos en las conexiones y además autenticarlas.
- Es posible descargar algunos *drivers, para optimizar el funcionamiento de la herramienta.*

6.1.1 Configuración.

El UltraVNC está dividido en dos:

- **UltraVNC Server**: Debe estar instalado en las máquinas que serán accedidas.
- **UltraVNC Viewer**: Debe estar instalado en la máquina cliente que se va a conectar a los servidores para lograr el acceso remoto.

Una vez terminado de instalar el programa, dando doble click al icono del vnc nos aparecerá la siguiente pantalla, para configurar lo más importante la contraseña de acceso en el caso de las PC que serán accedidas. En la figura 6.1 se indica la configuración de contraseña.

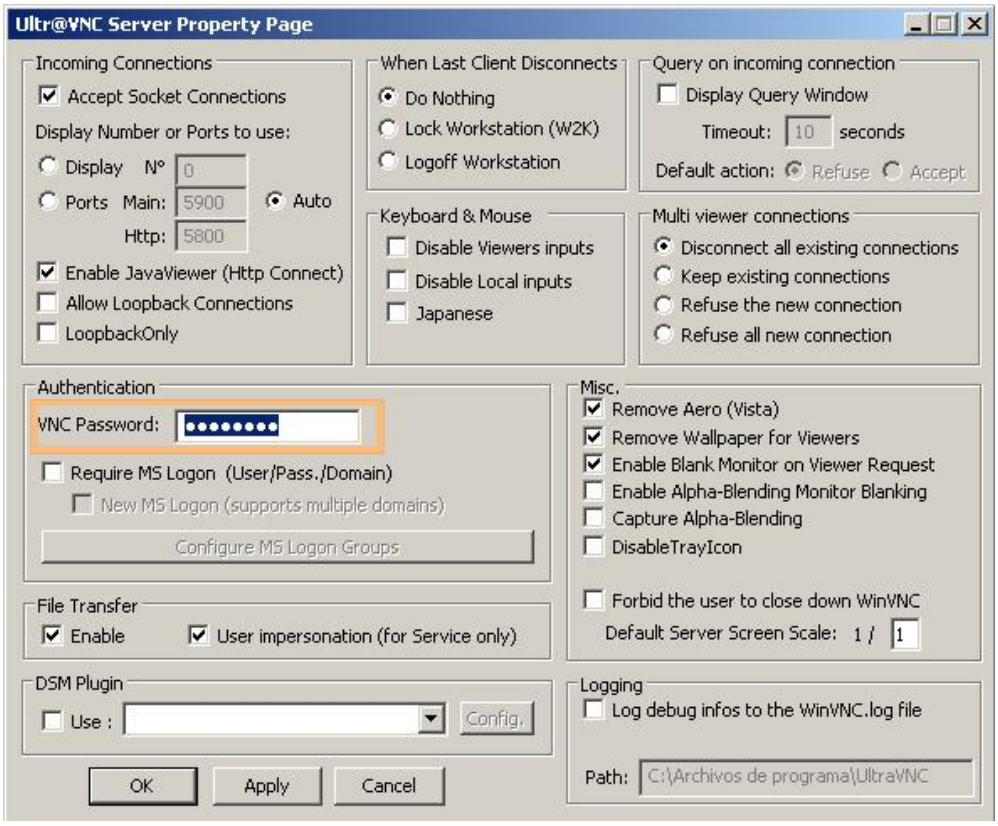


Figura 6.1. ***Configuración de contraseña.***

6.2 Monitorización de las comunicaciones y verificar las actividades de los usuarios en la red.

Para el buen funcionamiento de una red de una empresa es de vital importancia dar cabida a nuevas aplicaciones para que nos ayuden a mantener el funcionamiento de nuestra red. Todo esto ha generado la importancia de monitorear las redes.

Daremos una explicación de lo que se entiende por monitorear la red.

Monitoreo de red consiste en utilizar herramientas, para verificar y analizar el correcto funcionamiento de la red, por ejemplo buscar mediante un software específico componentes defectuosos o lentos y realizar las respectivas mejoras en la misma.

Por lo que nosotros damos la recomendación de monitorizar la red con las siguientes herramientas:

- CACTI.
- NTOP.

Estas herramientas permiten contar con un sistema experto que analiza y presenta resultados y además ayuda con la interpretación de los resultados obtenidos con las

mismas, cabe recalcar que esta información se queda únicamente con el administrador de la red todo el tiempo y pasa a ser parte del activo de la fábrica.

6.2.1 Herramienta Cacti.

Cacti es una herramienta que permite monitorizar y a su vez visualizar gráficas y estadísticas de dispositivos conectados a la red, siempre y cuando en los dispositivos a monitorizar, ya sean switch, router o cualquier servidor Linux tengan habilitado el protocolo SNMP.

SNMP es un protocolo que básicamente permite a los administradores de redes administrar los dispositivos de la red y diagnosticar los posibles problemas en las mismas.

Con Cacti es posible visualizar, ancho de banda consumido, detectar congestiones o picos de tráfico o monitorizar determinados puertos de un equipo de red, además es posible programar la colección de gráficas con las que queramos realizar el seguimiento. **Cacti** es una herramienta que funciona bajo entornos Apache + PHP + MySQL, por tanto, permite una visualización y gestión de la herramienta a través del navegador web.

La herramienta utiliza RRDtool, que captura los datos y los almacena en una base de datos circular.

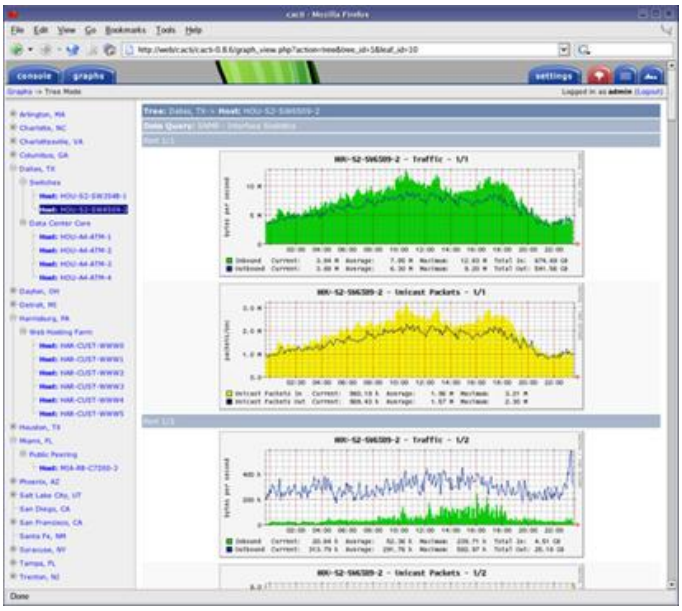


Figura 6.2. ***Herramienta Cacti.***

6.2.1.1 Instalación y configuración de CACTI sobre Ubuntu.

1. Corremos el siguiente paquete en una terminal de Linux y se descargará automáticamente los paquetes que son necesarios para la instalación del Cacti.
   sudo apt-get install php5 php5-gd php5-mysql
2. **Corremos el siguiente comandando para instalar el Cacti:**
   sudo apt-get install cacti-cactid
3. Seleccionar OK como se muestra eb la figura 6.3.

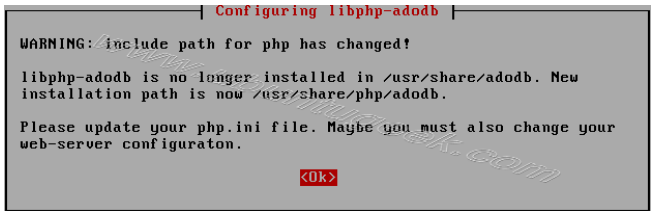


Figura 6.3. ***Configuración del libphp-adodb.***[106]

4. **Seleccionar el servidor web como se muestra en la figura 6.4.**

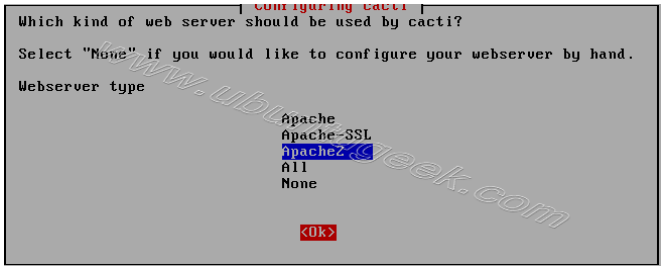


Figura 6.4. ***Selección del servidor Web.***[107]

5. Seleccione OK como se muestra en la figura 6.5.

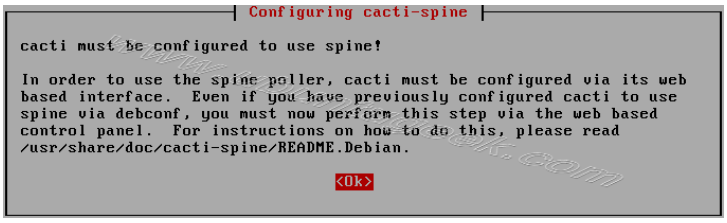


Figura 6.5. ***Configuración del Cacti.***[108]

6. En esta ventana configura la database, seleccione Yes, como se muestra en la figura 6.6.

[106] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html
[107] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html
[108] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html

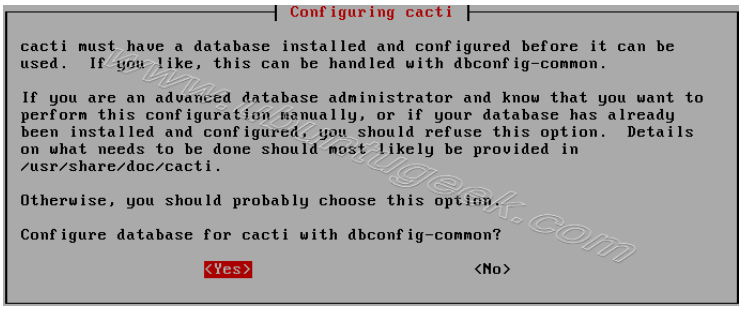


Figura 6.6. ***Configuración de la base de datos para el Cacti.***[109]

7. Ingresar un password para el usuario root del server de mysql. Seleccione enter y continuar como se muestra en la figura 6.7.

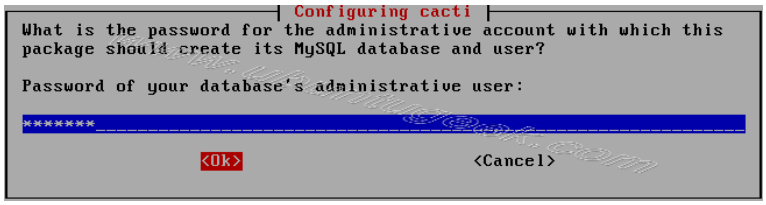


Figura 6.7. ***Ingreso de una contraseña para el administrador del Cacti.***[110]

8. Ingrese el password para la database del Cacti como se muestra en la figura 6.8.

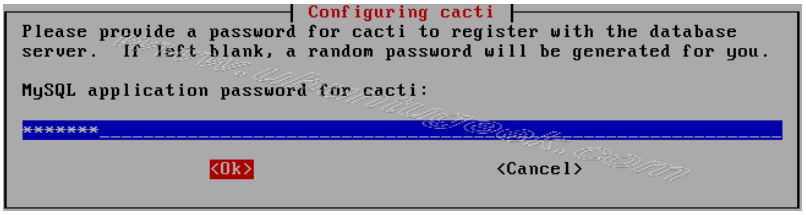


Figura 6.8. ***Ingreso de la contraseña del MySQL.***[111]

9. Vuelva a ingresar el password para la database del Cacti como se muestra en la figura 6.9.

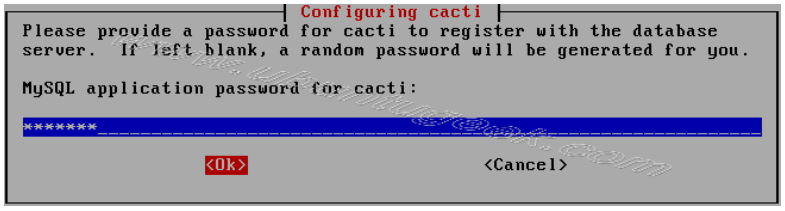


Figura 6.9. ***Confirmación de la contraseña del MySQL.***[112]

[109] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html
[110] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html
[111] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html

6.2.1.2 Configuración del Cacti.

Se ingresa al browser: http://serverip/cacti y aparecerá la siguiente pantalla como se puede observar en la figura 6.10.

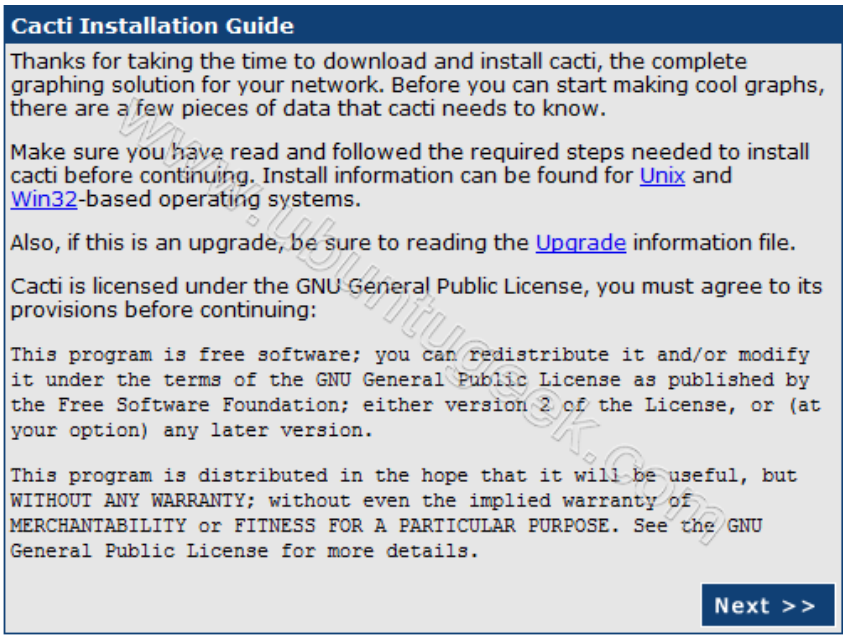


Figura 6.10. ***Configuración del Cacti.***[113]

A continuación indicaremos algunas actividades que se pueden realizar en la herramienta Cacti.

- Análisis del uso de menoría de servidores o máquinas.
- Porcentajes de carga promedio de servidores o máquinas.
- Porcentajes de los procesos de servidores o máquinas.
- Porcentajes de espacios de disco duros de servidores o máquinas.

6.2.1.3 Utilización de la herramienta Cacti.

Es posible monitorear el estado y rendimiento de cada máquina en funcionamiento dentro de la red.

Para poder monitorear cada máquina se debe crear en la herramienta cada componente ya sea una PC o un equipo de telecomunicación con su respectivo nombre y la dirección Ip. Para el ejemplo se crearon las siguientes maquinas:

---

[112] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html

[113] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html

El servidor Pasamanería (Servidor Pasa), el servidor PasaWEB y algunas máquinas adicionales, de la misma manera se debería crear todas las máquinas que se desee monitorear. Como se puede ver en la figura 6.11.

Figura 6.11. ***Menú de las máquinas creadas para analizarlas.***

Como ejemplo se analizo el servidor Pasamanería.

6.2.1.4 Uso de memoria.

El Servidor Pasamanería, es decir el servidor de aplicaciones tiene una memoria Ram de 4 GB, con el Cacti podemos monitorear el uso de esta memoria.

El análisis se realizo entre las 10 am y 4 pm, el gráfico nos indica que el uso de la memoria es un promedio de 1.69 GB y con un máximo de 2.02 GB de memoria libre, como se puede ver en la figura 6.12.

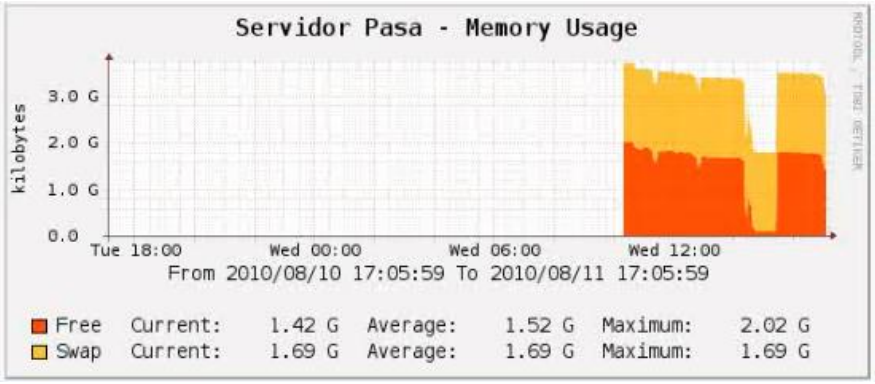


Figura 6.12. ***Uso de memoria.***

6.2.1.5 Carga promedio del Servidor Pasamanería.

El Load Average es la cantidad de procesos que están encolados para ser atendidos y calculados sobre un cierto periodo de tiempo.
En la figura 6.13 podemos ver los cálculos que se dieron en 1 minuto, 5 minutos y 15 minutos, estos porcentajes que se dieron son los procesos encolados, básicamente son procesos que se bloquearon esperando algo para continuar ejecutándose, lo típico es que pueden estar esperando a la CPU como el acceso de lectura/escritura de un disco, acceso a lectura/escritura de una red.

Entonces un proceso bloqueado sería por ejemplo, un proceso esperando que la CPU pueda procérsalo, u otro que está esperando a que el disco lo deje escribir, otra puede ser que se necesita leer algo de internet pero la red está ocupada.

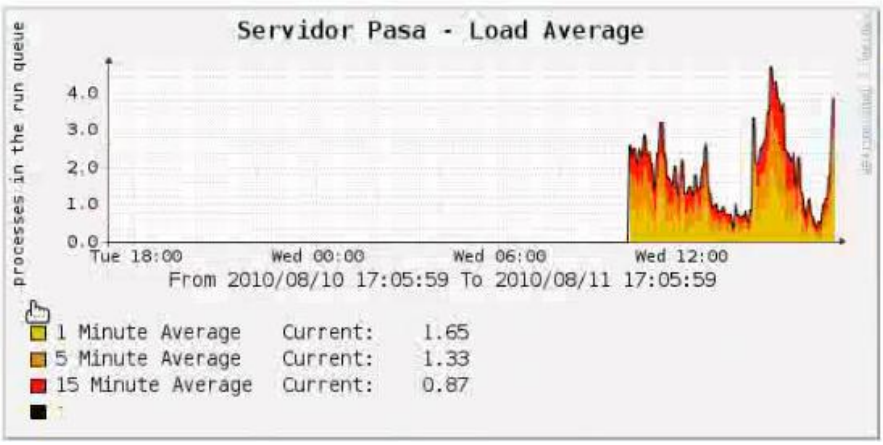


Figura 6.13. ***Carga promedio del servidor Pasamanería.***

6.2.1.6 Procesos del Servidor Pasamanería.

Un proceso es un programa en ejecución, los procesos son gestionados por el sistema operativo y están formados por:

- Las instrucciones de un programa destinadas a ser ejecutadas por el microprocesador.
- Su estado de ejecución en un momento dado, esto es los valores de los registros de la CPU para dicho programa.
- Su memoria de trabajo, es decir la memoria que ha reservado y sus contenidos.
- Otra información que permite al sistema operativo su planificación.

Como podemos ver en la figura 6.14 los procesos que se están corriendo en el servidor son de un promedio de 177 con un máximo de 180, este análisis se realizó en un horario que más se exige al Servidor Pasamanería como lo es entre las 10 am y 4 pm.

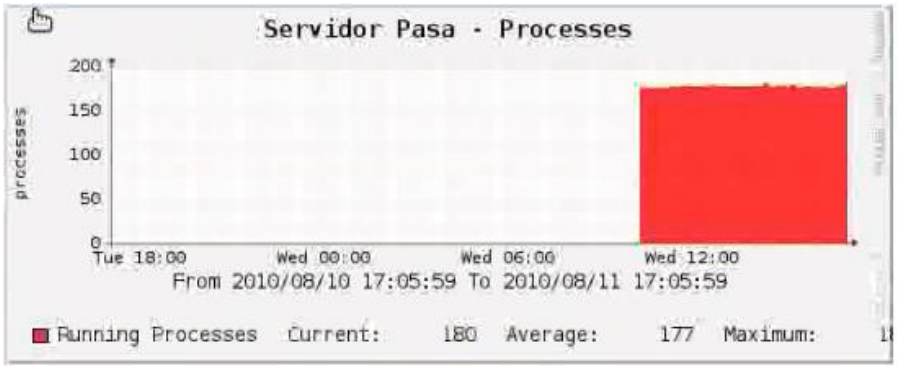


Figura 6.14. ***Procesos del Servidor Pasamanería.***

Además es posible graficar los usos de espacio en el disco duro de cada equipo y monitorear varias cosas más.

De esa forma con ayuda del Cacti podemos ver a detalle que es lo que está sucediendo con cada equipo que está en la red de la Pasamanería.

6.2.2 Herramienta ntop.

Recomendamos el software ntop, porque es una herramienta que permite monitorizar en tiempo real a los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y además es capaz de ayudar a la hora de detectar malas configuraciones de algún equipo.

Recalcamos las siguientes características de ntop:

- Es una herramienta de software libre.
- Es un software multiplataforma, pudiendo ser utilizado sobre: Windows, Linux, Solaris y MacOSX
- Su interfaz es web y muy fácil de usar.
- Dispone de gran variedad de informes: informes globales de carga de red, de tráfico entre elementos, de sesiones activas de cada elemento, etc.
- Permite exportar los datos a una base de datos relacional MySQL para su análisis.

- Detecta posibles paquetes que pueden causar daño a la red.

6.2.2.1 Utilización de ntop.

6.2.2.1.1 Tráfico en la red.

Ntop presenta estadísticas globales de tráfico en la red, por lo que en principio indicaremos el concepto de las tres clases de envíos de paquetes.

- **Unicast:** Hace referencia al envió de paquetes desde un único emisor a un único receptor. Por ejemplo aplicaciones unicast son los protocolos http, smtp, ftp o telnet. Ejemplo una llamada telefónica.
- **Multicast:** Hace referencia al envío de paquetes en una red a múltiples receptores de forma simultánea, un emisor envía un mensaje y son varios los receptores que reciben el mismo. Ejemplo una conferencia, en la que son varias las personas que se comunican entre sí.
- **Broadcast:** Es una transmisión de información donde un nodo emisor envía información a varios nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo. Un ejemplo de comunicación Broadcast es el de una emisora de radio, que emite señales sin saber quien la recibe.

6.2.2.1.2 Paquetes.

Una vez visto los conceptos de los términos relacionados con el envió de paquetes se pudo ver claramente en la parte de Paquetes los Unicast está en un 27.9%, Broadcast con un 55.8% y con Multicast el 16.3%, a mas de los porcentajes se pudo observar en la figura 6.15, también representada en un grafico de forma de pastel mostrando los porcentajes de forma estadística.
De igual manera también nos presenta un total de paquetes recibidos en este caso 111.003 paquetes y de igual forma el total de paquetes procesados siendo los mismos 111.003.

A más de eso también nos muestra el paquete recibido más corto de 42 bytes, de tamaño medio de 222 bytes y el más largo de 1514 bytes.

De igual forma nos muestra el tamaño de paquetes que se recibieron según el tamaño ya sea de 64 bytes, 128 bytes, 256 bytes 512 bytes, 1024 bytes y 1515 bytes

mostrando porcentajes o tamaños de paquetes recibidos según el tamaño de bytes. Como se puede ver en la figura 6.15.

Traffic Report for 'eth0' [switch]

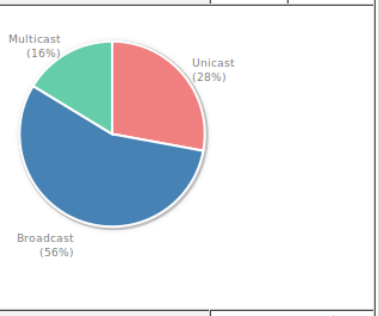
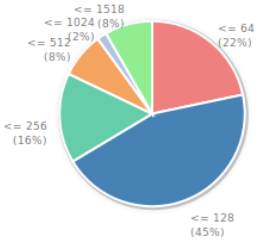
Packets	Dropped (libpcap)	0.0%	0
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		111,003
	Total Packets Processed		111,003
	Unicast	27.9%	30,915
	Broadcast	55.8%	61,947
	Multicast	16.3%	18,141
			
	Shortest		42 bytes
	Average Size		222 bytes
	Longest		1,514 bytes
	Size <= 64 bytes	21.6%	24,010
	64 < Size <= 128 bytes	44.7%	49,664
	128 < Size <= 256 bytes	15.7%	17,409
	256 < Size <= 512 bytes	7.9%	8,815
	512 < Size <= 1024 bytes	1.7%	1,832
	1024 < Size <= 1518 bytes	8.4%	9,273
	Size > 1518 bytes	0.0%	0
			
	Packets too long [> 1514]	0.0%	0
	Bad Packets (Checksum)	0.0%	0

Figura 6.15. ***Reporte de paquetes.***

6.2.2.1.3 Carga de la red.

De igual forma podemos ver la carga de la red en tiempo actual, la última hora, los 5 minutos antes, etc. Esto se lo puede ver en la figura 6.16 con sus respectivos tamaños y su equivalencia en paquetes.

Network Load	**Actual**	14.4 Kbit/s	9.3 Pkt/s
	Last Minute	12.3 Kbit/s	11.0 Pkt/s
	Last 5 Minutes	10.7 Kbit/s	9.4 Pkt/s
	Peak	539.1 Kbit/s	78.1 Pkt/s
	Average	23.6 Kbit/s	12.0 Pkt/s
Historical Data			[ ]

Figura 6.16. ***Carga de la Red.***

6.2.2.1.4 Protocolos mundiales de distribución.

Antes de entrar al análisis de los protocolos con los porcentajes estadísticos vamos a ver de qué se trata los protocolos que más porcentajes tienen.

- **TCP:** Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Básicamente sirve para crear conexiones entre computadoras y enviarse un flujo de datos. TCP da soporte a las aplicaciones más usadas en Internet, incluidas HTTP, SMTP, SSH y FTP.
- **UDP:** Protocolo de datagramas de usuario, con este protocolo aplicaciones informáticas pueden enviar mensajes, en este caso denominado datagramas, UDP no garantiza la entrega ni comprueba la secuencia de los datagramas, ya que proporciona una comunicación muy sencilla entre las aplicaciones de las máquinas, siendo no orientada a conexión ya que no establece una conexión previa con el otro extremo para transmitir un mensaje UDP y además utiliza el protocolo IP para transportar sus mensajes.

  Datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el receptor, de manera independiente a los fragmentos restantes.
- **ICMP:** Protocolo de mensajes de control de internet es el sub protocolo y notificación de errores del protocolo de internet IP, como tal se usa para enviar mensajes de error indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

- **RARP:** Es un protocolo de resolución de direcciones, es el responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP.

- **IGMP:** El protocolo IGMP funciona como una extensión del protocolo IP. Se utiliza para establecer los miembros de la red, pasar información de los miembros y establecer rutas. Otros muchos protocolos hacen uso de las funciones IGMP dentro de sus especificaciones.
- **STP:** El protocolo STP (Spanning Tree Protocol) automatiza la administración de la topología de la red con enlaces redundantes, su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. El protocolo permite a los dispositivos de interconexión habilitar o deshabilitar automáticamente los enlaces de conexión, de forma que se garantice que la topología esté libre de bucles.

6.2.2.1.5 Análisis de la gráfica.

En la figura 6.17 podemos darnos cuenta que los protocolos más utilizados para enviar o recibir paquetes son los protocolos TCP y el UDP estos datos son obtenidos gracias a la ayuda de ntop el cual nos brinda porcentajes y graficas para darnos cuenta que es lo que está pasando en la red.

Si nos damos cuenta el protocolo TCP trabaja con 15.1 MBytes con un porcentaje del 59.9% siendo el protocolo que más se utiliza para la transmitir los paquetes ya que este protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Global Protocol Distribution

Protocol	Data	Percentage			
IP	25.2 MBytes	95.9%	TCP	15.1 MBytes	59.9%
			UDP	9.8 MBytes	38.9%
			ICMP	7.2 KBytes	0%
			ICMPv6	0.3 KBytes	0%
			IGMP	308.6 KBytes	1.2%
			Other IP	0.2 KBytes	0%
(R)ARP	583.0 KBytes	2.3%			
IPX	38.0 KBytes	0%			
NetBios	22.7 KBytes	0%			
IPv6	0.5 KBytes	0%			
STP	272.8 KBytes	1.0%			
Other	21.7 KBytes	0%			

Figura 6.17. ***Protocolos mundiales de distribución.***

6.2.2.1.6 PROXY.

Hace referencia a un programa o dispositivo que realiza una tarea de acceso a internet de un lugar de otro ordenador. Un proxy es el punto intermedio entre un ordenador conectado a Internet y el servidor que esta accediendo. Cuando se navega a través de un proxy, en realidad no estamos accediendo directamente al servidor sino que realizamos una solicitud sobre el proxy y es este quien se conecta con el servidor que queramos acceder y nos devuelve el resultado de la solicitud.

Como podemos ver en la figura 6.18 dentro de los protocolos TCP/UDP soporta varias de las aplicaciones para conectarse a internet en este caso el Proxy como podemos ver en la parte de datos tenemos 298.5 KBytes que ha trabajado el proxy y de igual manera podemos ver en la parte gráfica el porcentaje acumulado y ver un historial del protocolo que se muestra de color verde en este caso de las 10 am.

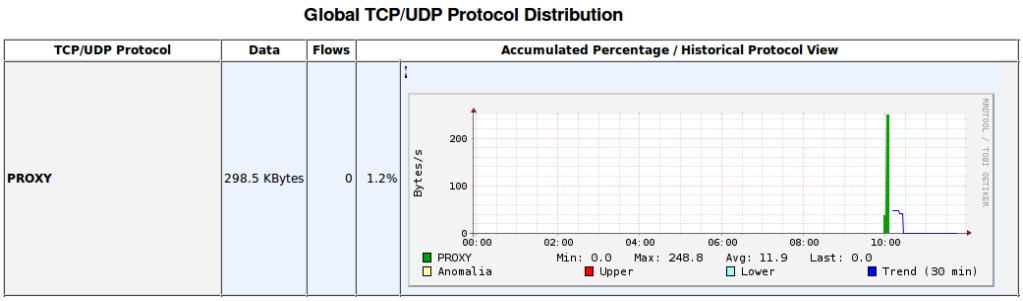


Figura 6.18. ***Análisis del Proxy.***

6.2.2.1.7 HTTP.

Protocolo de transferencia de hipertexto, usado para acceder a la Web. Se encarga de procesar y dar respuestas a las peticiones para visualizar una página web.

Este protocolo opera a través de solicitudes y respuestas, entre un "cliente" y un "servidor". El cliente para los usuarios es el navegador web, y el servidor es aquel en donde se almacenan las páginas de Internet. Donde este responde con un recurso ya sea texto, gráficos, etc.

Podemos observar en la figura 6.19, HTTP utiliza datos de 14.8MBytes siendo el que más se utiliza en la red de la fábrica, y de igual manera podemos ver en el gráfico el porcentaje acumulado y también ver el historial del protocolo de forma gráfica, este protocolo se muestra de color verde que va de un mínimo de 0.0 KBytes a un máximo de 13 KBytes en un horario de 10 am a 12 pm pudiendo utilizar hasta un superior de 100 KBytes como se ve en la grafica de color rojo.

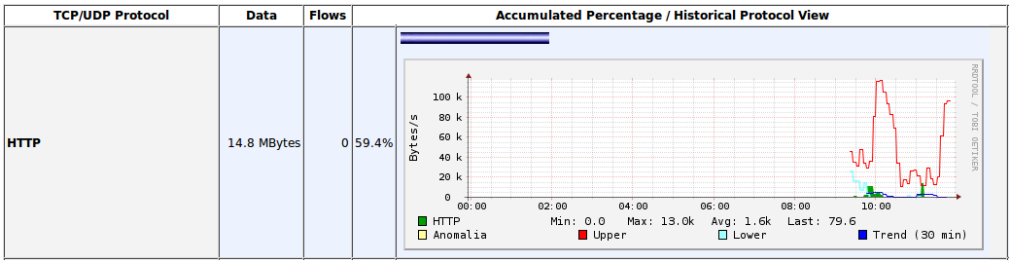


Figura 6.19. ***Análisis del HTTP.***

6.2.2.1.8 DNS.

Sistema de Nombres de Dominio que permite traducir nombres de dominio a direcciones IP y viceversa, el DNS permite que las personas usen nombres de dominio que son bastante más simples de recordar.

En la figura 6.20 podemos darnos cuenta que el sistema de nombres de dominio se ha usado un mínimo de 1.8 Bytes a un máximo de 276.6 Bytes como podemos ver en el historial del protocolo de color verde, estas cantidades de Bytes se han usado entre las 10 am a 12 pm.

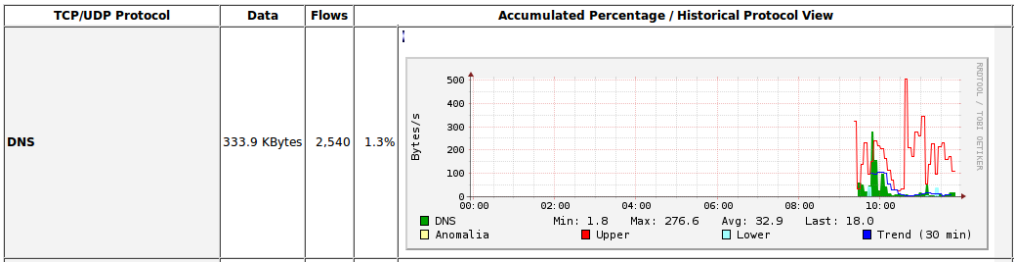


Figura 6.20. ***Análisis de DNS.***

6.2.2.1.9 TELNET.

Telnet es un protocolo de red, utilizado en internet para acceder remotamente a una máquina o servidor como si estuviéramos al frente de la máquina.

Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.

En la figura 6.21 podemos analizar este protocolo donde se puede ver porcentajes acumulados y gráficas que nos permite ver la utilización del mismo, de esta forma vemos que Telnet se utiliza hasta un máximo de 1.3 Bytes entre un horario de 10 am a 12 pm.

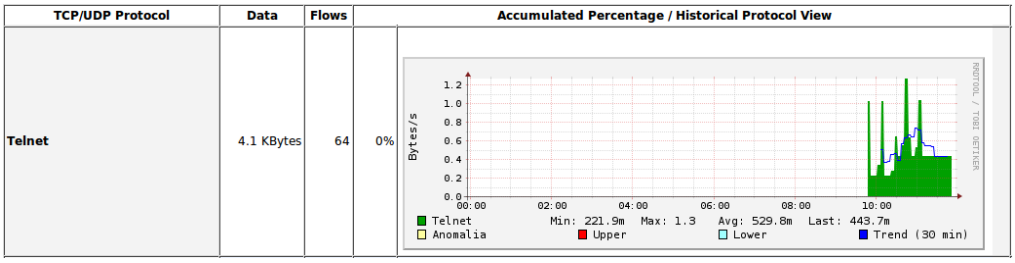


Figura 6.21. ***Análisis del TELNET.***

6.2.2.1.10 Punto de vista histórico.

En la figura 6.22 podemos ver también un historial de todos los protocolos utilizados de forma de gráfico y con sus respectivos porcentajes ya no de forma individual como las anteriores figuras, como podemos ver en el gráfico se ve que el protocolo HTTP es el que más se utiliza, el análisis se realizó desde las 7:57 am a 11:57 am

siendo un periodo de 4 horas de análisis, de esa forma se puede observar que las horas que más se utiliza es de 10 am y 11 am como se puede ver en el gráfico de color celeste.

También se pude ver un historial de la fecha que uno quiera, solo se debe de escoger la fecha de inicio y de fin, también se puede ver un historial según las horas ya sea las últimas 4 horas, 2 horas, la última hora, el último minuto, etc.

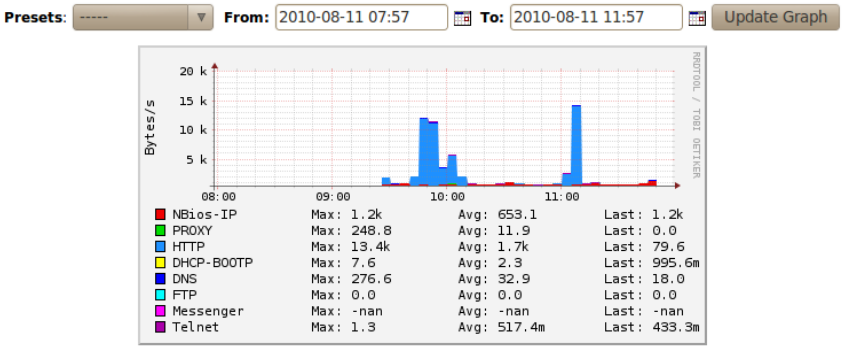


Figura 6.22. ***Análisis histórico.***

6.2.2.1.11 Carga de red.

Para ella utilizamos el programa ntop con este podemos ver un resumen de la carga de la red de una forma estadística tales como:

- Últimos 10 minutos de rendimiento.
- Rendimiento en la última hora.
- Rendimiento día actual.
- Rendimiento del mes pasado.

Para poder expresar el resumen de la carga de la red de forma estadística podemos observar en la figura 6.23, el rendimiento de la red en los últimos 10 minutos de rendimiento el mínimo es de 8.2.k y con un máximo de 82.1k no sobrepasando el máximo que esta de color rojo.

De igual manera se puede ver el rendimiento de la red de la ultima hora, como se puede observar en el gráfico nos da un mínimo de 3.1k y un máximo de 222.4k.

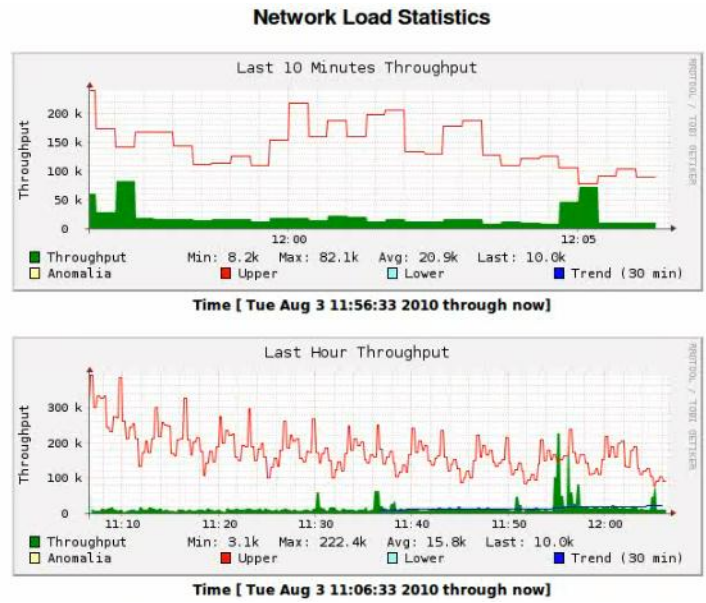


Figura 6.23. ***Análisis del rendimiento de la red en los últimos 10 minutos y la última hora.***

De igual forma podemos observar el rendimiento de la red del día actual y el rendimiento del mes pasado, esto se puede observar en la figura 6.24.

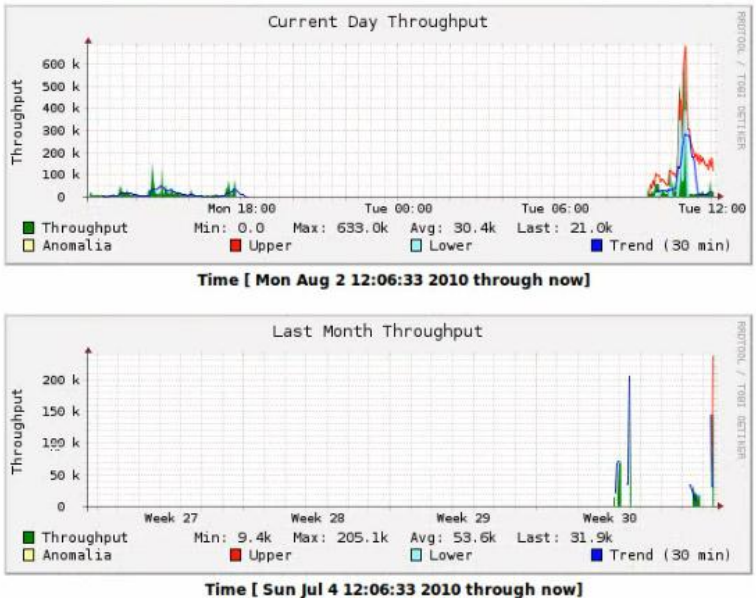


Figura 6.24. ***Rendimiento de la red del día actual y el último mes.***

6.2.2.1.12 Tráfico de todos los protocolos.

Ahora vamos a ver el tráfico de la red de todos los protocolos, de todas las máquinas que conforman la red de la Pasamanería, los datos que se enviaron y los recibidos,

para ver puntos estadísticos de este punto se puede realizar el análisis de cada una de las máquinas que conforma la red de la Pasamanería.

Como se puede observar en la figura 6.25 se listan los Host es decir la dirección IP de la máquina o el nombre que tiene la PC, por ejemplo se pudo observar el nombre del servidor de la Pasamanería el cual tiene la dirección IP 192.168.1.1 o simplemente una dirección IP que hace referencia a una máquina.

En este gráfico se puede observar los protocolos que se están utilizando por cada máquina y la cantidad de datos que se está utilizando según los protocolos ya sea TCP, UDP, ICMP, etc.

Network Traffic [All Protocols]: All Hosts - Data Sent+Received

Hosts: [**All**] [Local Only] [Remote Only] **Data:** [**All**] [Sent Only] [Received O

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios
andres		72.6 MBytes	82.3 %	71.7 MBytes	860.5 KBytes	97.1 KBytes	0	0	0	0	12.4 KBytes	0	0
host-200-110-77-254.cue.telconet.net		2.4 MBytes	2.8 %	0	2.4 MBytes	0	0	0	0	0	0	0	0
239.255.255.250		2.2 MBytes	2.5 %	0	2.2 MBytes	196	0	0	0	0	0	0	0
192.168.1.6		1.9 MBytes	2.1 %	696	1.9 MBytes	3.0 KBytes	0	0	0	0	7.6 KBytes	0	0
pasamaneria [NetBIOS]		1.0 MBytes	1.2 %	0	1.0 MBytes	3.5 KBytes	0	0	0	0	1.0 KBytes	0	0
dns1.cue.telconet.net		717.6 KBytes	0.8 %	0	716.7 KBytes	934	0	0	0	0	0	0	0
sn133w.snt133.mail.live.com		377.3 KBytes	0.4 %	377.3 KBytes	0	0	0	0	0	0	0	0	0
iMac de Alexandra Quezada		292.9 KBytes	0.3 %	0	292.7 KBytes	0	0	0	0	0	0	0	0
igmp.mcast.net		289.3 KBytes	0.3 %	0	0	0	0	0	0	0	0	0	0
gfx3.hotmail.com		282.9 KBytes	0.3 %	282.9 KBytes	0	0	0	0	0	0	0	0	0
iMac de Alexandra Quezada		278.8 KBytes	0.3 %	5.9 KBytes	271.7 KBytes	0	0	0	0	0	0	0	0
DISENO 3 [NetBIOS]		227.4 KBytes	0.3 %	0	226.7 KBytes	0	0	0	0	0	0	0	0
pasaweb [NetBIOS]		117.7 KBytes	0.1 %	7.0 KBytes	99.6 KBytes	10.4 KBytes	0	0	0	0	832	0	0
atcliente2 [NetBIOS]		107.9 KBytes	0.1 %	116	103.4 KBytes	0	0	0	0	0	28	0	0
analista5 [NetBIOS]		60.5 KBytes	0.1 %	0	60.5 KBytes	0	0	0	0	0	0	0	0
gecontrol [NetBIOS]		60.5 KBytes	0.1 %	0	60.5 KBytes	0	0	0	0	0	0	0	0
gesistemas [NetBIOS]		60.4 KBytes	0.1 %	0	60.4 KBytes	0	0	0	0	0	0	0	0
rhumanos4 [NetBIOS]		60.2 KBytes	0.1 %	0	60.2 KBytes	0	0	0	0	0	0	0	0
hilanderia [NetBIOS]		59.7 KBytes	0.1 %	0	59.7 KBytes	0	0	0	0	0	0	0	0
marketing [NetBIOS]		59.4 KBytes	0.1 %	0	59.4 KBytes	0	0	0	0	0	0	0	0
geproduccion [NetBIOS]		59.4 KBytes	0.1 %	0	59.4 KBytes	0	0	0	0	0	0	0	0
profile.ak.fbcdn.net		58.4 KBytes	0.1 %	58.4 KBytes	0	0	0	0	0	0	0	0	0
192.168.1.183		54.2 KBytes	0.1 %	5.9 KBytes	47.1 KBytes	0	0	0	0	0	0	0	0
bodespachos6 [NetBIOS]		49.7 KBytes	0.1 %	116	45.2 KBytes	0	0	0	0	0	28	0	0
gefinanzas [NetBIOS]		46.0 KBytes	0.1 %	0	46.0 KBytes	0	0	0	0	0	0	0	0
192.168.1.77		45.8 KBytes	0.1 %	464	40.9 KBytes	0	0	0	0	0	56	0	0
192.168.1.239		45.6 KBytes	0.1 %	464	40.8 KBytes	0	0	0	0	0	56	0	0
192.168.1.32		45.5 KBytes	0.1 %	116	41.1 KBytes	0	0	0	0	0	28	0	0
192.168.1.27		45.4 KBytes	0.1 %	464	40.6 KBytes	0	0	0	0	0	56	0	0
hiloscoser [NetBIOS]		45.3 KBytes	0.1 %	348	40.6 KBytes	0	0	0	0	0	28	0	0
bohilanderia [NetBIOS]		45.2 KBytes	0.1 %	348	40.5 KBytes	0	0	0	0	0	28	0	0
tintorerialab [NetBIOS]		45.2 KBytes	0.1 %	116	40.7 KBytes	0	0	0	0	0	28	0	0
boddespachos1 [NetBIOS]		45.0 KBytes	0.0 %	116	40.5 KBytes	0	0	0	0	0	28	0	0

Figura 6.25. ***Tráfico de todos los protocolos.***

6.2.2.1.13 Información sobre el servidor Pasamanería.

Una vez listado todos los host o máquinas que se encuentran en la red de la Pasamanería podemos ver la información de cada máquina de la red, en este caso analizamos la información del Servidor Pasamanería.
Donde podemos ver las siguientes especificaciones:

- La dirección IP de la máquina.
- La fecha y hora desde que se analizó hasta la culminación.
- La dirección MAC de la máquina que se analiza.

- Nombre de la NetBios identificando a la máquina que se está analizando.
- El total de datos enviados.
- El numero de Broadcast enviados o paquetes enviados.
- El tráfico de multidifusión (multicast).
- Los datos enviados en forma estadística.
- El tipo de host.

Y así entre otras especificaciones se puede ver en la figura 6.26.

Figura 6.26. ***Información del servidor Pasamanería.***

6.2.2.1.14 Estadísticas de tráfico del servidor Pasamanería.

En esta parte de análisis podemos observar el total del trafico enviado y recibido del servidor Pasamanería, en este caso se analizó desde las 9 am a 12 pm, el cual nos muestra un total en KBytes y un porcentaje del mismo, además nos muestra el gráfico que la mayor cantidad de tráfico enviado por el servidor se da a las 10 am con 425 KBytes y el total de tráfico recibido también se da a la misma hora con 1.5Kbytes.

Host Traffic Stats

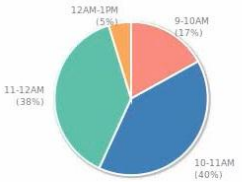
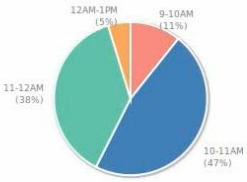
Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
12 PM	50.3 KBytes	4.7 %	158	4.7 %
11 AM	408.6 KBytes	38.4 %	1.2 KBytes	37.8 %
10 AM	425.0 KBytes	39.9 %	1.5 KBytes	46.7 %
9 AM	180.2 KBytes	16.9 %	358	10.7 %
8 AM	0	0.0 %	0	0.0 %
7 AM	0	0.0 %	0	0.0 %
6 AM	0	0.0 %	0	0.0 %
5 AM	0	0.0 %	0	0.0 %
4 AM	0	0.0 %	0	0.0 %
3 AM	0	0.0 %	0	0.0 %
2 AM	0	0.0 %	0	0.0 %
1 AM	0	0.0 %	0	0.0 %
Total				

Figura 6.27. ***Estadísticas de tráfico del servidor Pasamanería.***

6.2.2.1.15 Protocolo de distribución del servidor Pasamanería.

Podemos ver en la figura 6.28 que el protocolo de distribución más usado es el UDP ya que con este protocolo las aplicaciones informáticas pueden enviar mensajes, teniendo un porcentaje de 1 MBytes de datos enviados y 1.9 KBytes recibidos por el servidor.

Protocol Distribution

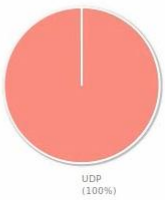
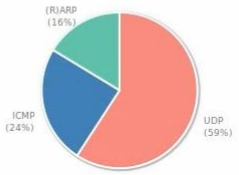
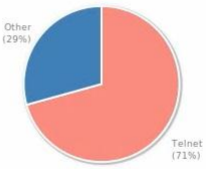
Protocol	Data Sent	Data Rcvd
UDP	1.0 MBytes	1.9 KBytes
ICMP	2.6 KBytes	0.8 KBytes
(R)ARP	0.5 KBytes	0.5 KBytes
IGMP	8.8 KBytes	0.0 KBytes
Protocol Distribution		
IP Distribution		

Figura 6.28. ***Protocolo de distribución del servidor Pasamanería.***

6.2.2.1.16 Información sobre el servidor PASAWEB.

Al igual que se analizó al servidor Pasamanería de aplicaciones podemos ver también información de cada máquina que se encuentre en red, para este caso hemos analizado al servidor PASAWEB, así podemos ver la IP asignada en este caso 192.168.1.4, el total de datos enviados 184.7 KBytes de 9am a 12pm siendo 657 paquetes y así se puede ver toda la información del servidor en la figura 6.29.

Figura 6.29. ***Información del servidor PASAWEB.***

6.2.2.1.17 Estadísticas del tráfico del servidor PASAWEB.

Como se puede observar el total de datos enviados por el servidor PASAWEB es de 184.7 KBytes visualizada en la figura 6.30 se puede ver el total distribuido en las 4 horas analizadas, de esa forma vemos que a las 11 am ha sido de mayor tráfico en el servidor, siendo 117.8 KBytes.

Host Traffic Stats

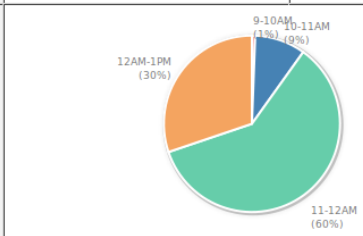
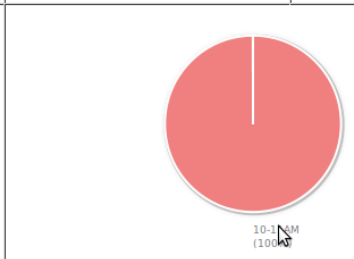
Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
12 PM	47.4 KBytes	25.7 %	0	0.0 %
11 AM	117.8 KBytes	63.8 %	0	0.0 %
10 AM	18.3 KBytes	9.9 %	559	100.0 %
9 AM	1.2 KBytes	0.6 %	0	0.0 %
8 AM	0	0.0 %	0	0.0 %
7 AM	0	0.0 %	0	0.0 %
6 AM	0	0.0 %	0	0.0 %
Total				

Figura 6.30. ***Estadísticas del tráfico del servidor PASAWEB.***

6.2.2.1.18 Protocolo de distribución del servidor PASAWEB.

Al igual que el análisis del servidor Pasamanería podemos observar en la figura 6.31 que el protocolo de distribución que mas utiliza el servidor PASAWEB es el UDP con 184.6 KBytes datos enviados y el ICMP es el más usado con los datos recibidos con 0.5 KBytes.

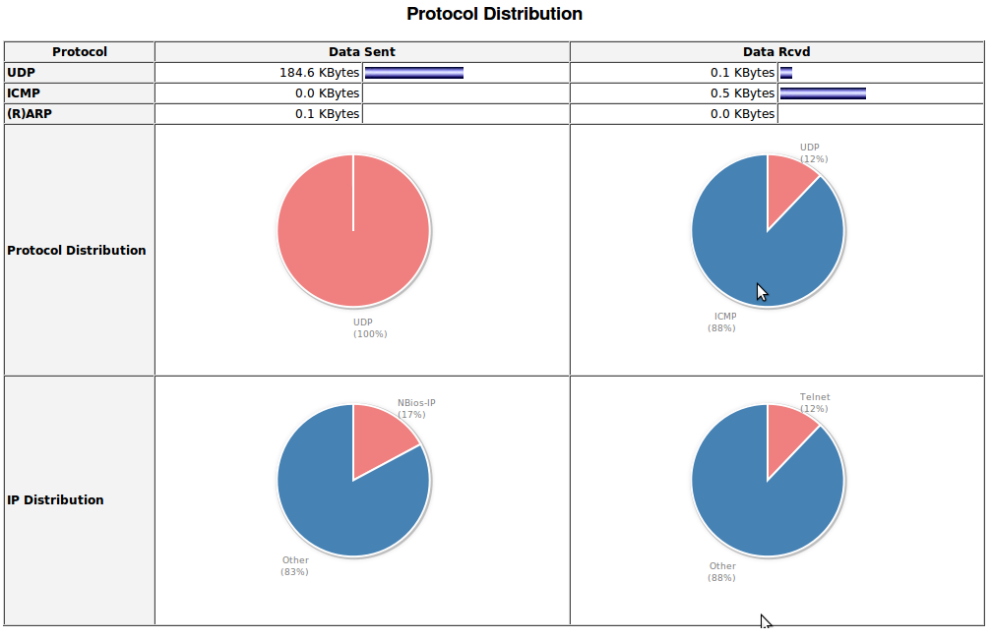


Figura 6.31. ***Protocolo de distribución del servidor PASAWEB.***

6.2.3 Herramienta PRTG.

Recomendamos PRTG la cual es una herramienta que se utiliza para supervisar la carga de tráfico en los enlaces de red. Para visualizar estos resultados genera páginas de HTML que contienen imágenes de los análisis en formato GIF.

Para recolectar la información del tráfico de los dispositivos, la herramienta utiliza el protocolo SNMP (Simple Network Management Protocol).

Con PRTG es posible monitorizar la carga de un sistema, las sesiones abiertas por los usuarios de un determinado equipo, disponibilidad de módems, etc.

A continuación mostraremos un ejemplo de la utilización de la herramienta en una empresa x.

La figura 6.32 muestra el tráfico de la red de la empresa x, ejemplo indica la señal verde la información que se está recibiendo para la empresa x y por otro lado la señal roja indica la información que se está enviando desde la empresa.

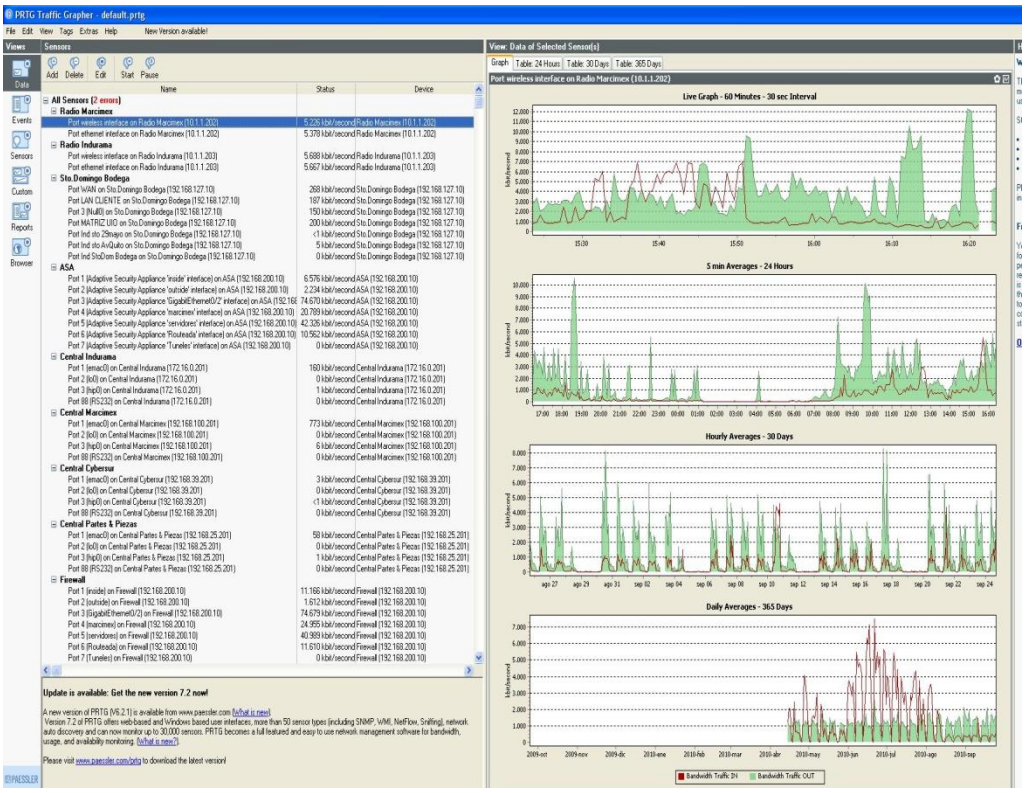


Figura 6.32. ***Herramienta PRTG.***

6.2.4 Protocolo SNMP y la herramienta MRTG.

Se recomienda la instalación de un servidor SNMP y la herramienta MRTG para interpretar la información obtenida por el protocolo, el cual es usado principalmente para monitorizar y controlar el estado de dispositivos en la red.

Es decir facilita el obtener información de intercambio entre los dispositivos de la red, además de supervisar el desempeño de la red.

6.2.4.1 Como se usa el SNMP.

El gestor envía una petición de información proporcionando el Id del objeto de interés (OID, Object ID), este ID consiste en una serie de números separados por puntos decimales por: (ejemplo, 1.3.6.1.4.1.2682.1) Estos identificadores forman parte de un árbol que se le puede ver en la figura 6.33 que sirve como diccionario para poder interpretar el código del mensaje.

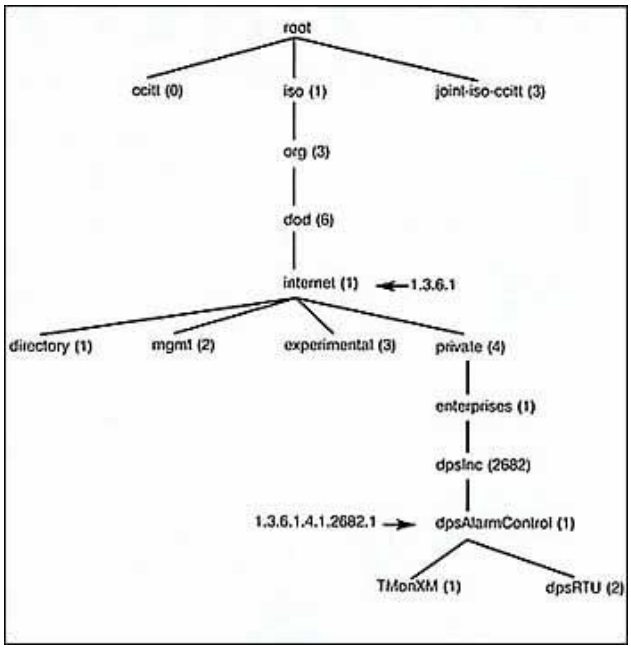


Figura 6.33. ***Árbol de identificación de los OID.***

Una vez explicado la funcionalidad del protocolo SNMP vamos a instalarle en una distribución Linux en este caso en Ubuntu.

6.2.4.2 Instalación del servidor SNMP.

Dentro del Ubuntu abrimos un terminal donde ingresaremos la siguiente línea:

root@andres1:~# apt-get install snmp snmpd

Instalado el SNMP, se debe de editar el archivo de configuración, para acceder a ese archivo debemos poner la siguiente línea:

root@andres1:~# nano /etc/snmp/snmpd.conf

Ya dentro del archivo se debe de poner la siguiente línea:

com2sec readonly 127.0.0.1 public

Esta línea lo que hace es consultar al servidor SNMP, para esta demostración se lo ha hecho solo a esta dirección, pero se puede ver información de cualquier dispositivo que este en la red. Esta configuración se la puede ver en la figura 6.34.

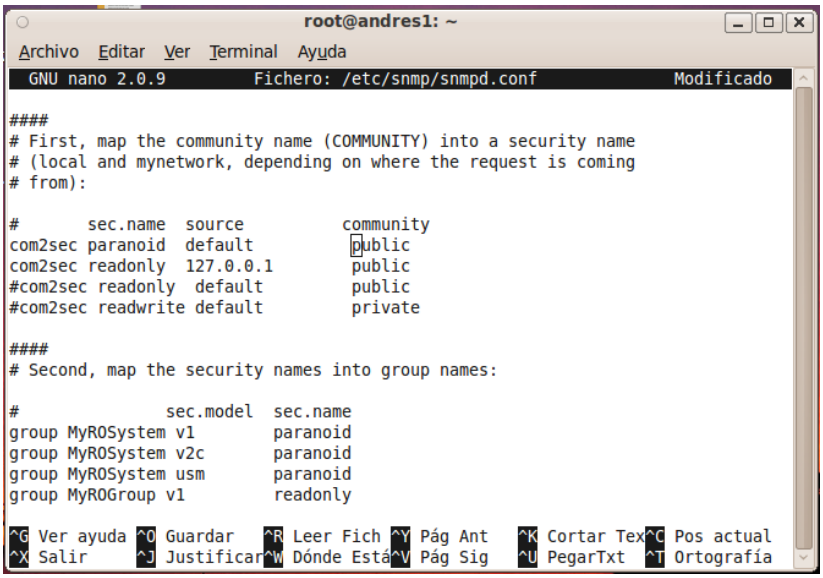


Figura 6.34. ***Archivo de configuración /etc/snmp/snmpd.conf***

Si se quiere ver la información de otros equipos que están en red se debe de crear la comunidad con su red asignada, la comunidad viene a ser en nuestro caso una subred es decir un departamento: La línea que se debe de poner es la siguiente:

com2sec readonly 192.168.1.0 SecretariaGeneral

Esta configuración se la puede ver en la figura 6.35.

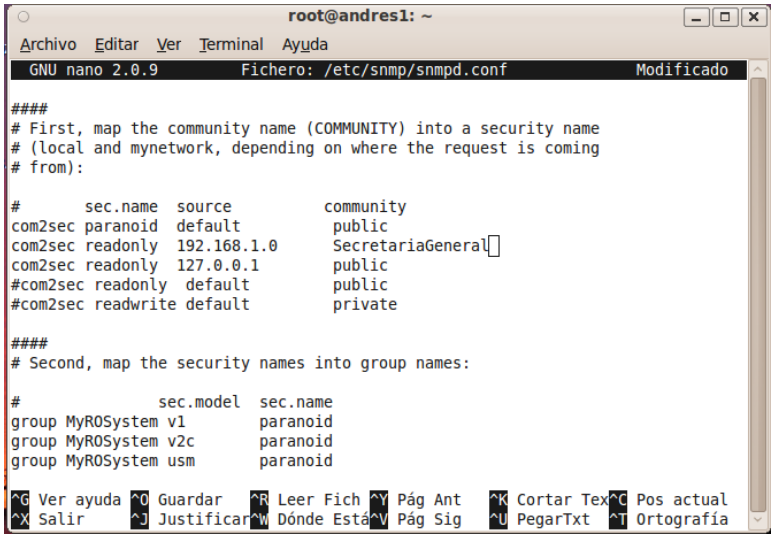


Figura 6.35. ***Creación de la comunidad SecretariaGeneral en el archivo de configuración /etc/snmp/snmpd.conf***

Una vez realizado la configuración del archivo se lo debe de guardar con Ctrl +O.

Luego debemos reiniciar el servicio para actualizar la configuración la cual es la siguiente línea:

root@andres1:~# /etc/init.d/snmpd restart

Ahora debemos comprobar que la configuración sea correcta donde debería aparecer varias líneas sobe el sistema. La línea para comprobar es la siguiente:

root@andres1:~# snmpwalk -v 1 -c public localhost system

Y la respuesta debería ser una parecida como se muestra en la figura 6.36.

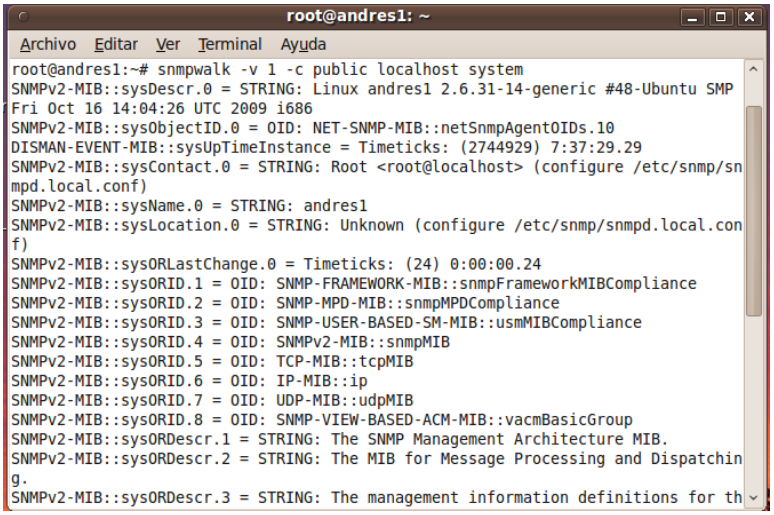


Figura 6.36. ***Comprobación de que sea correcta la configuración.***

El siguiente paso a realizar es instalar MRTG para poder interpretar la información adquirida por el protocolo SNMP para ello debemos poner la siguiente línea en un terminal:

root@andres1:~# apt-get install mrtg

En plena instalación debemos de configurar el MRTG el cual se puede leer en la figura 6.37.

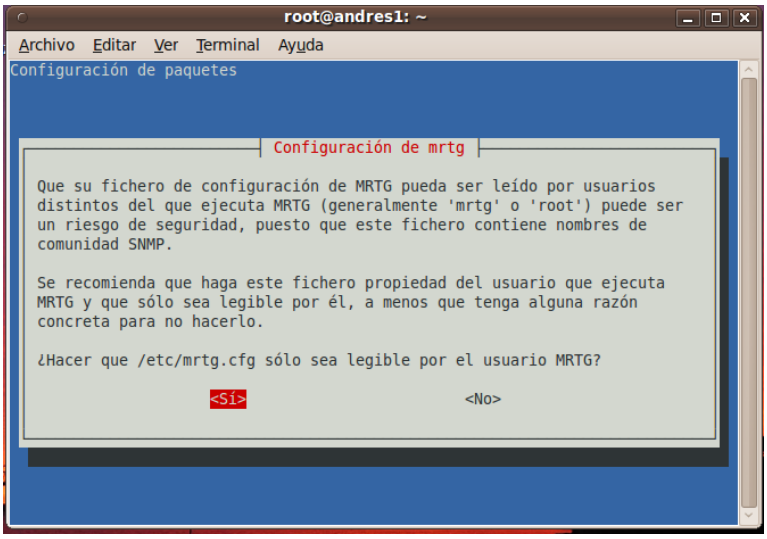


Figura 6.37. ***Configuración del MRTG***

Ahora para hacer una configuración inicial, en la cual nos mostrará la información automática de las interfaces de la red debemos ejecutar lo siguiente en un terminal:

root@andres1:~# cfgmaker --community public --output /etc/mrtg.cfg localhost

Una vez ejecutado la línea para ver la información de las interfaces nos debe de mostrar información parecida a la que se muestra en la figura 6.38.

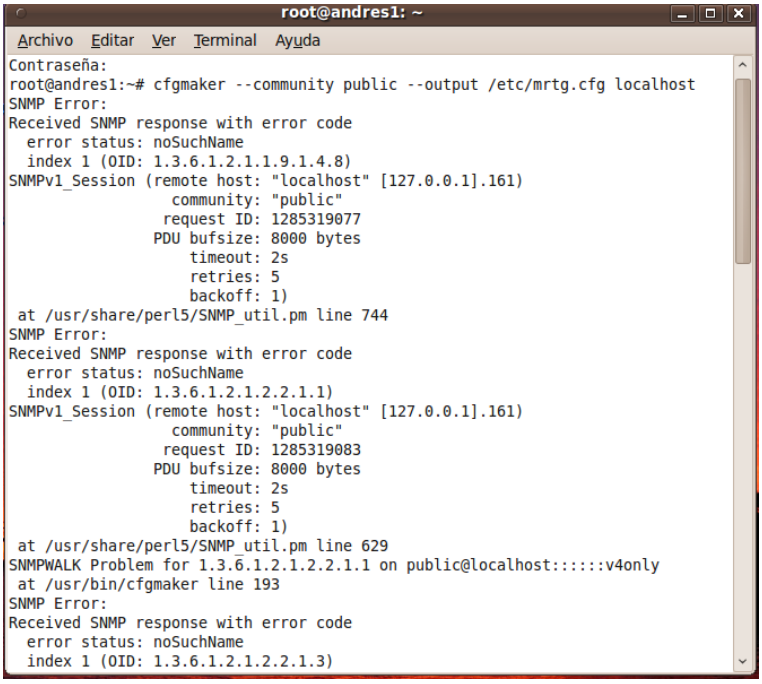


Figura 6.38. ***Información de las interfaces de la red.***

En la cual nos mostrará los OID los cuales serán interpretados por el MRTG para mostrar información que podamos entenderla en forma grafica.

Para ello debemos editar el archivo de configuración /etc/mrtg.cfg el cual fue creado por el cfgmaker para añadir gráficos para poder entender a los OID. Para ello debemos poner la siguiente línea en una terminal:

root@andres1:~# nano /etc/mrtg.cfg

Dentro del archivo de configuración debemos poner las siguientes líneas para poder ver la información sobre lo que nos interesa ver, un ejemplo pude ser lo siguiente:

#Consumo de CPU:
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[localhost.cpu]:ssCpuRawUser.0&ssCpuRawUser.0:public@localhost +
ssCpuRawSystem.0&
ssCpuRawSystem.0:public@localhost +
ssCpuRawNice.0&ssCpuRawNice.0:public@localhost
RouterUptime[localhost.cpu]: public@localhost
MaxBytes[localhost.cpu]: 100
Title[localhost.cpu]: CPU Load
PageTop[localhost.cpu]: Carga de CPU %
Unscaled[localhost.cpu]: ymwd
ShortLegend[localhost.cpu]: %
YLegend[localhost.cpu]: Uso de CPU
Legend1[localhost.cpu]: CPU Activa en % (Carga)
Legend2[localhost.cpu]:
Legend3[localhost.cpu]:
Legend4[localhost.cpu]:
LegendI[localhost.cpu]: Active
LegendO[localhost.cpu]:
Options[localhost.cpu]: growright,nopercent

#Memoria RAM:
LoadMIBs: /usr/share/snmp/mibs/HOST-RESOURCES-MIB.txt
Target[localhost.mem]: . 1.3.6.1.2.1.2.2.1.1 &.1.3.6.1.2.1.9.1.4.8
:public@localhost
PageTop[localhost.mem]: Memoria RAM
Options[localhost.mem]: nopercent,growright,gauge,noinfo
Title[localhost.mem]: Memoria Libre
MaxBytes[localhost.mem]: 1000000
kMG[localhost.mem]: k,M,G,T,P,X
YLegend[localhost.mem]: bytes
ShortLegend[localhost.mem]: bytes
LegendI[localhost.mem]: Free Memory:
LegendO[localhost.mem]:
Legend1[localhost.mem]: Free memory, not including swap, in bytes

#Memoria SWAP:
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[localhost.swap]: memAvailSwap.0&memAvailSwap.0:public@localhost
PageTop[localhost.swap]: Memoria Swap
Options[localhost.swap]: nopercent,growright,gauge,noinfo
Title[localhost.swap]: Memoria Libre
MaxBytes[localhost.swap]: 1000000
kMG[localhost.swap]: k,M,G,T,P,X
YLegend[localhost.swap]: bytes
ShortLegend[localhost.swap]: bytes
LegendI[localhost.swap]: Memoria Libre:
LegendO[localhost.swap]:
Legend1[localhost.swap]: Swap memory avail, in bytes

Una vez que tengamos todos los gráficos que nos interesa ver, debemos generar el directorio web de MRTG para ello debemos poner las siguientes líneas en un terminal:

root@andres1:~ # indexmaker --output /var/www/mrtg/index.html/etc/mrtg.cfg

Ahora tan sólo nos quedará añadir a nuestro crontab a MRTG para que actualice los gráficos:

Editamos el crontab para acceder a este archivo debemos poner lo siguiente en un terminal:

root@andres1:~ # nano crontab –e

Dentro del archivo debemos poner la siguiente línea para que actualice cada 5 minutos los gráficos:

***/5 * * * * mrtg /etc/mrtg.cfg**

Una vez realizada las configuraciones nos presentará gráficas con la que se puede ver en la figura 6.39.

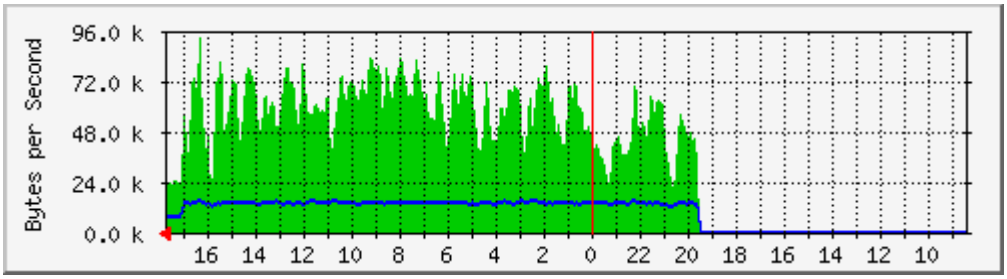


Figura 6.39. ***Grafica generada por la herramienta MRTG.***

6.2.4 Herramienta sniffer.

Nosotros recomendamos el software de sniffer *Wireshark,* ya que es una herramienta que permite analizar el tráfico de la red y la utilización de cada uno de los protocolos, esto se logra poniendo la red de la Pasamanería en modo promiscuo, lo que significa que una máquina acepte todos los paquetes sin importar lo que contenga la cabecera del mismo.

Wireshark monitorea y analizar el tráfico en la red detectando los cuellos de botellas y problemas que existan en la misma, ya que capta los datos que son transmitidos en la red y pueden leer los datos dentro del paquete así como la dirección de destino.

Soporta multitud de protocolos y se puede instalar en las siguientes plataformas:

Linux, Windows, MacOs, *BSD, además acaba de liberar nueva versión en la que se han aplicado revisiones de seguridad y añadido características de filtrado para comunicaciones por USB y para protocolos de VoIP.

El programa wiresharck es gratuito y además funciona con WinPcap.

WinPcap es una herramienta que permite a las aplicaciones capturar y transmitir paquetes de red sin pasar por la pila de protocolos y proporciona acceso de bajo nivel de la red y además una biblioteca que se utiliza para acceder fácilmente a las capas de red de bajo nivel.

6.2.5.1 Pantalla principal de Wiresharck.

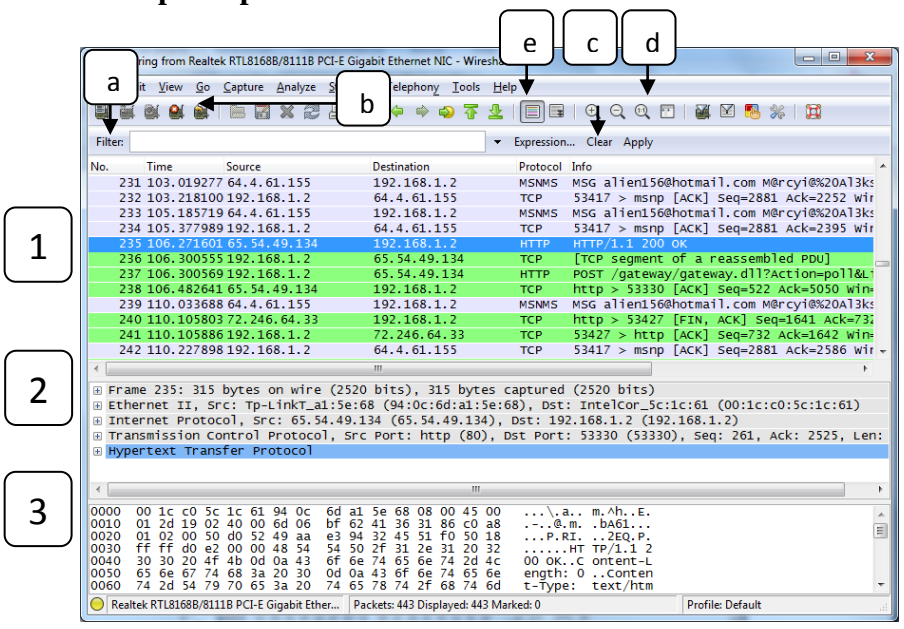


Figura 6.40. ***Pantalla principal de Wireshark.***

A continuación indicaremos como está distribuida la pantalla principal de la herramienta.

1. **Panel de lista de paquetes:** Muestra el respectivo resumen de cada paquete capturado y analizado.

2. **Panel de vista en árbol:** Muestra el paquete seleccionado en el panel superior (1) con más detalle

3. **Panel de detalle de los datos:** Muestra el contenido del paquete seleccionado en el panel superior (1) en formato hexadecimal y ASCII.

Además de los tres paneles principales, hay cinco elementos adicionales siguientes en la barra de herramientas de filtrado, que se encuentra debajo de la barra de herramientas principal de Wireshark:

a. **Botón de filtro:** Permite definir un filtro para la visualización de los paquetes, de forma que se pueda observar el análisis de un determinado protocolo o en el tráfico entrante o saliente de un ordenador determinado.

   Existen una serie de expresiones de filtro predeterminadas que se pueden emplear directamente, también existe la posibilidad de crear una nueva, asignándole un nombre para una utilización posterior más cómoda.

b. **Texto del filtro:** Aquí aparece el texto del filtro, es posible introducir el texto del filtro directamente en este campo o seleccionar alguno de los filtros que se hayan utilizado anteriormente.

c. **Botón para eliminar el filtro:** Pulsando este botón se elimina el filtro que estuviera activo.

d. **Botón para aplicar el filtro:** Pulsando este botón se aplica el filtro definido y en el panel principal (1) se muestran únicamente los paquetes que cumplan las condiciones indicadas en el filtro.

e. **Botón de expresión del filtro:** Al pulsar en este botón se accede a un cuadro de diálogo para la definición de la expresión del filtro.

6.2.5.2 Ejemplo de funcionamiento de la herramienta Wireshark.

En la figura 6.41 se puede observar los protocolos que se están ejecutando en la PC que tiene instalada la herramienta Wireshark, para el ejemplo tomaremos el protocolo MSNMS el cual es para utilizar el Messenger.

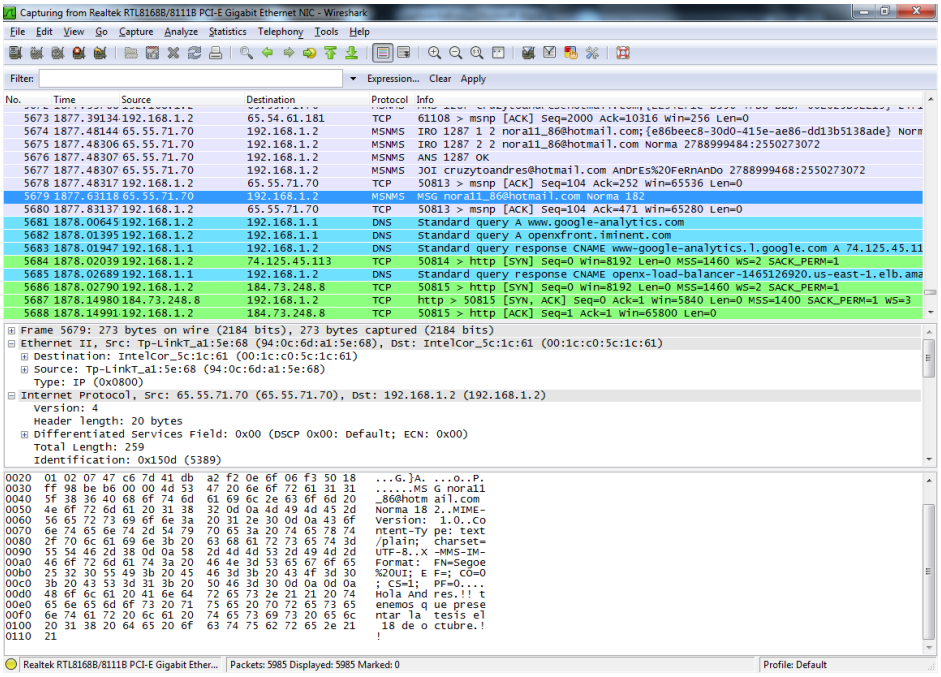


Figura 6.41. ***Protocolos que se están ejecutando.***

Dando doble click en el protocolo se abrirá una ventana indicando de forma detallada la conversación, como se puede ver en la figura 6.42.

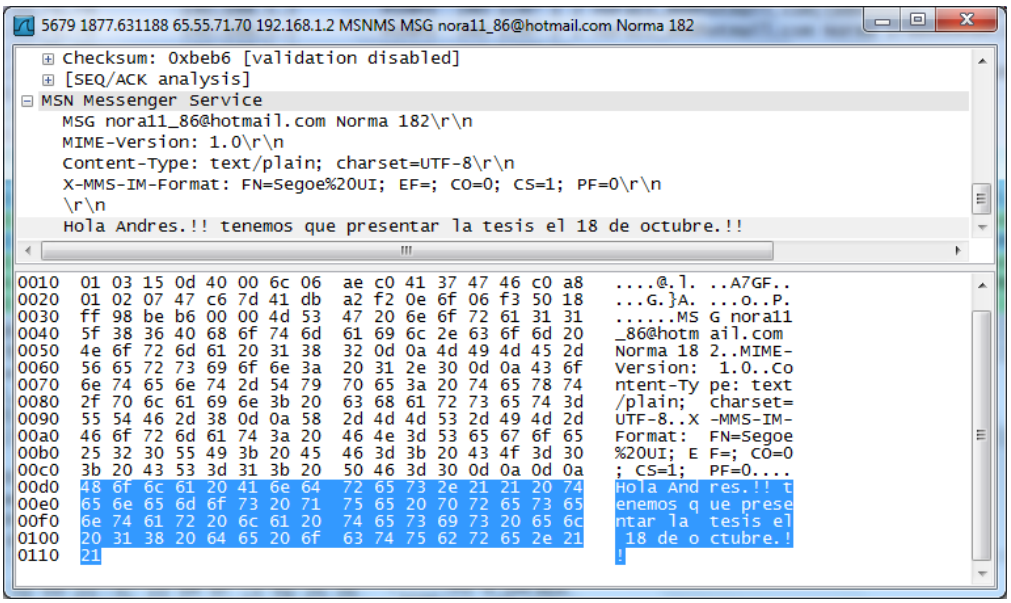


Figura 6.42. ***Captura de paquetes que se envía en la red.***

6.3 Planificación de la recuperación de las comunicaciones en caso de desastre.

Recomendamos para la fábrica tener elaborado un plan de contingencia, el mismo que contemple un conjunto de procedimientos alternativos a la operativa normal de la fabrica en lo que respecta las telecomunicaciones, esto sería de gran ayuda en caso de que se presente algún tipo de desastre ya sea natural o causado por personas, la que permitiría a la fábrica continuar son sus labores diarias sin tener complicaciones o detener el trabajo.

Cabe recalcar que el hecho de contemplar un plan de contingencia en la fábrica no quiere decir un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, ya que sería importante superar todas aquellas situaciones descritas con anterioridad y que pueden provocar grandes pérdidas económicas.

Este plan de contingencia podría contemplar lo siguiente:

6.3.1 Recuperación de los datos:

Es de mucha importancia tener respaldado y asegurado los datos de cada uno de los usuarios ya que esta información es de ayuda para realizar las labores diarias de los usuarios.

Recomendamos controlar los respaldos de las PC remotamente con la aplicación Amanda en un sistema operativo Linux ejemplo Centos.

Con Amanda se puede crear un servidor de respaldo para respaldar múltiples servidores de Linux, Windows, Solaris y MAC OS. Amanda también protege bases de datos como Oracle, MSSQL y aplicaciones de E-Mail.

Para instalarlo se lo puede realizar con yum de la siguiente manera.

```
# yum -y install amanda*
```

Este software funciona de la siguiente manera:

Se instalará Amanda en un servidor que será de respaldos de usuarios y se instala un cliente en cada máquina que se desee respaldar la información, en estos clientes se tendría creado un acceso directo de una carpeta en al cual el usuario deberá grabar toda la información que le sea útil y desee respaldar.

El software según la configuración que se le dé, respaldará la información de todos los usuarios cada cierto tiempo al día.

Incluso este software permite realizar filtros de la información de los usuarios que se desee respaldar, por ejemplo en el caso de que no interese hacer un backup de música.

Además recomendamos que una vez hecha la recopilación automática de la información en el servidor de backup, guardar esta información en discos DVD cada semana y guardar estas copias de seguridad en un lugar seguro fuera de la fábrica, previniendo de esta manera pérdida de información de suma importancia.

6.3.2 Recuperación del hardware:

En lo que respecta hardware recomendamos lo siguiente:

Virtualización de Servidores: Tener únicamente uno o dos servidores con buenas características para implementar la virtualización, lo que consiste en instalar varias máquinas virtuales en cada servidor, las mismas que serian administradas con el software VMWARE VCENTER SERVER, incluso con esta herramienta es posible migrar máquinas virtuales de un servidor a otro si fuera el caso, sin ningún tipo de complicación simplemente utilizando la interface que presenta este software.

Además esta herramienta permite crear un punto de restauración en el momento que el administrador de la red lo desee, por ejemplo uno cada noche, para que si se diera el caso y se llegara a dañarse por cualquier motivo uno de los servidores, se pueda sin ningún inconveniente volver al punto de restauración y continuar con el trabajo diario y en el peor de los casos no haya la necesidad de parar el trabajo en la fábrica.

En especial, esto resultaría de gran ayuda para proteger los datos que se graban en el servidor de aplicaciones.

Indicaremos algunas características del software VMWARE VCENTER SERVER:

- Detecta daños en los servidores y automáticamente migran las máquinas virtuales instaladas de un servidor a otro servidor.
- Esta herramienta se instala sobre cualquier hardware de servidor existente y particiona un servidor físico en múltiples máquinas virtuales reproduciendo los recursos de procesador, memoria, almacenamiento y redes para proporcionarle un mejor uso y mayor flexibilidad del hardware.

En lo que respecta a las PC, recomendamos tener un plan de alquiler de máquinas, de esta manera en caso que llegue a fallar alguna PC en la fabrica se proceda a reponer

por otra PC alquilada en cualquier institución que realice este trabajo y de esta manera no se tiene equipos que se estén depreciando todo el tiempo.

6.4 Recomendación de la nueva topología para la red de la Pasamanería S.A.

6.4.1 Topología de la red de la Pasamanería S.A.

6.4.1.1 DMZ.

Se recomienda implementar una DMZ es decir una zona desmilitarizada, la cual es una red local que se ubica entre la red interna de una organización y una red externa generalmente Internet.

El objetivo de esta recomendación es que por lo general la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está autorizado.
- El tráfico de la red externa a la red interna está prohibido.
- El tráfico de la red interna a la DMZ está autorizado.
- El tráfico de la red interna a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

Una DMZ se crea a menudo a través de las opciones de configuración de los cortafuegos, esta zona desmilitarizada se la puede ver en la figura 6.43, en la cual se puede ver que la DMZ está separada por un firewall con la red interna y la red externa es decir el internet.

Figura 6.43. ***Diagrama de la DMZ.***

Se recomienda realizar una nueva estructura de la red para un mejor funcionamiento de la red, en la cual se han utilizado los mismos equipos como Switchers, Routers y máquinas que actualmente tiene a su disposición la Pasamanería S.A.

6.4.2 Router Mikrotik BR 1100.

- Este equipo se implementó recientemente en la red, el cual tienes varios beneficios para el mejoramiento de la red en el cual se puede realizar varias configuraciones como:
- Backup y Restore de Configuración del Mikrotik 1100.
- Creación de un servidor de VPN para la comunicación con las sucursales de la Pasamanería S.A.
- Creación de un Servidor Web Proxy.
- Bloqueo de sitios no autorizados mediante en servidor Web Proxy.
- Modelado de colas es decir control de ancho de banda.
- Implementación del Firewall en el cual se realizarán varias políticas de restricciones para proteger a la red.
- Entre otras configuraciones.

Estas configuraciones se lo realizará desde el punto 6.8 que trata de recomendaciones de la configuración del Mikrotik 1100 con el sistema operativo RouterOS.

Este router y a su vez un firewall se conectara con los siguientes equipos:

- Se conectará con el Router Cisco de Telconet.
- También se conectara al Switch 3Com de 8 puertos.
- Y finalmente con el Switch 3Com administrable Baseline 2250 Plus de 48 puertos.

Esta conexión se la puede ver en la figura 6.44.

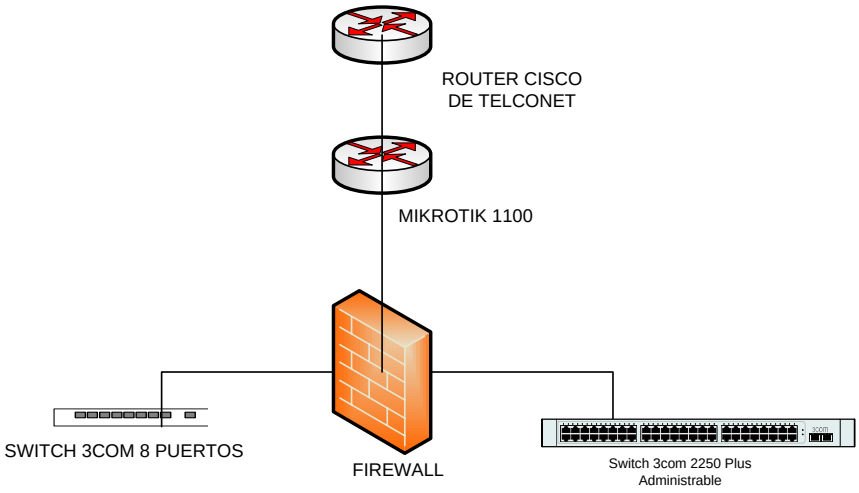


Figura 6.44. ***Diagrama de conexión del Mikrotik 1100.***

6.4.3 Conexión de la zona DMZ.

Esta zona desmilitarizada se encuentra conectada de la siguiente manera:

- El switch 3Com de 8 puertos se conecta con los diferentes servidores que existe en la red de la Pasamanería S.A los mismos que son:
    - Servidor Pasamanería.
    - Servidor CorreoPasa.
    - Servidor CorreoPasa Interno.
    - Servidor PALM.
    - Servidor PASAWEB.
- Y a su vez el switch 3Com de 8 puertos conectado con el Firewall el Mikrotik.

Esta conexión se la puede ver en la figura 6.45.

Figura 6.45. ***Diagrama de conexión de la zona DMZ.***

Una vez explicado la conexión del sector de la DMZ donde se encuentran los servidores de la Pasamanería S.A. se explicará las direcciones IPs que se les asignará a estos servidores estas direcciones IPs se la puede ver en la tabla 6.1.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Servidores	7	14	192.168.100.0	/28	255.255.255.240	192.168.100.1-192.168.100.14	192.168.100.15

Tabla 6.1. ***IPs asignadas para el área de Servidores.***

6.4.4 Switch 3Com Baseline 2250 Plus de 48 puertos.

Con esta nueva topología de red que se recomienda para la Pasamanería S.A el switch 3Com 2250 de 48 puertos se le ha tomado como el Switch principal el que se conectará con los demás switch 3Com 2226 de 24 puestos.

La conexión de este Switch esta de la siguiente manera:

- Se conecta con el Router Mikrotik que a su vez hace de Firewall.

- Luego este se conecta con los seis switch 3Com los cuales son repartidos para los diferentes departamentos que existen en la Pasamanería S.A los mismos que son:
    - Departamento de Ventas.
    - Departamento de Sistemas.
    - Departamento de Contabilidad.
    - Departamento de Secretaria General.
    - Área de Diseño.
    - Área de Corte.
    - Área de Almacén.
    - Área de Mecánica.
- Luego se conecta a los dos Router LinkSys que se utilizarán para la red inalámbrica de la Pasamanería S.A.

Esta conexión se la puede ver en la figura 6.46.

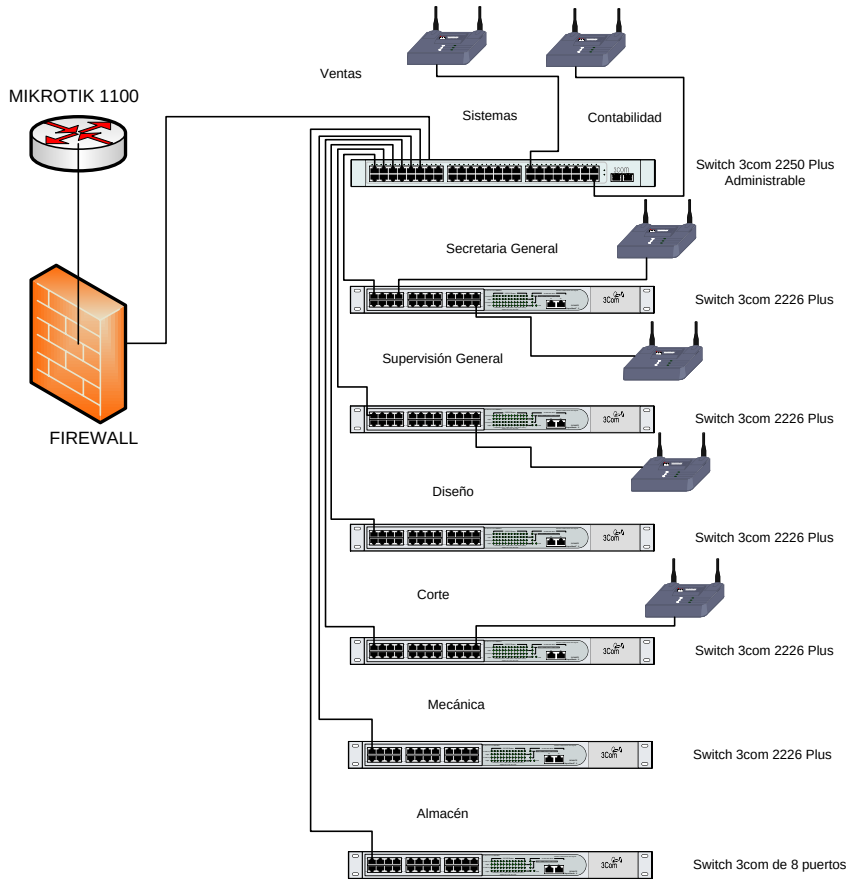


Figura 6.46. ***Diagrama de conexión del Switch 3Com Baseline 2250.***

Una vez explicado la conexión del Switch 3Com Baseline 2250 Plus de 48 puertos se explicará que departamentos no más se conectan a este switch.

Los departamentos que se conectan a dicho switch son los siguientes:

- Departamento de Ventas.
- Departamento de Sistemas.
- Departamento de Contabilidad.

6.4.4.1 Departamento de Ventas.

A este departamento se la tiene asignado el siguiente rango de direcciones IPs el cual se puede ver en la tabla 6.2.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Ventas	11	14	192.168.1.144	/28	255.255.255.240	192.168.1.145-192.168.1.158	192.168.1.159

Tabla 6.2. ***IPs aginadas al departamento de Ventas.***

6.4.4.2 Departamento de Sistemas.

A este departamento se la tiene asignado el siguiente rango de direcciones IPs el cual se puede ver en la tabla 6.3.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Sistemas	10	14	192.168.1.160	/28	255.255.255.240	192.168.1.161-192.168.1.174	192.168.1.175

Tabla 6.3. ***IPs asignadas al departamento de Sistemas.***

6.4.4.3 Departamento de Contabilidad.

A este departamento se la tiene asignado el siguiente rango de direcciones IPs el cual se puede ver en la tabla 6.4.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Contabilidad	7	14	192.168.1.176	/28	255.255.255.240	192.168.1.177-192.168.1.190	192.168.1.190

Tabla 6.4. ***IPs asignadas al departamento de Contabilidad.***

En la figura 6.47 se indica la conexión del Switch 3Com Baseline 2250 Plus de 48 puertos con las máquinas que corresponden a los respectivos departamentos.

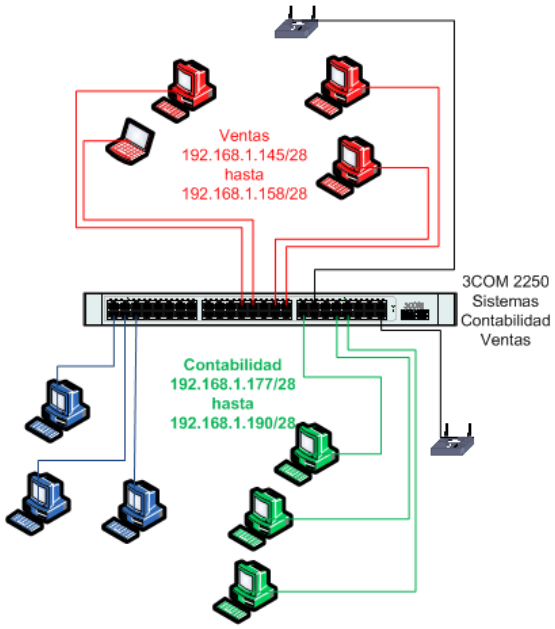


Figura 6.47. ***Diagrama de conexión de departamentos en el Switch Principal.***

6.4.5 Switch Baseline 2226 Plus de 24 puertos para el departamento de Secretaria General.

Con la nueva topología recomendada este switch no se le tocara, este se utilizará en este mismo departamento.

La conexión de este Switch esta de la siguiente manera:

- Este se conectará con el Switch 3Com Baseline 2250 Plus de 48 puertos el cual es el principal que se encuentra en el departamento de Ventas.
- Después este se conecta con el router Linksys que se utiliza para la red inalámbrica de la Pasamanería S.A.
- Y a su vez se conecta con los equipos de trabajo según el número que exista en este departamento.

La conexión física de este Switch Baseline 2226 Plus de 24 puertos se le puede ver en la figura 6.48.

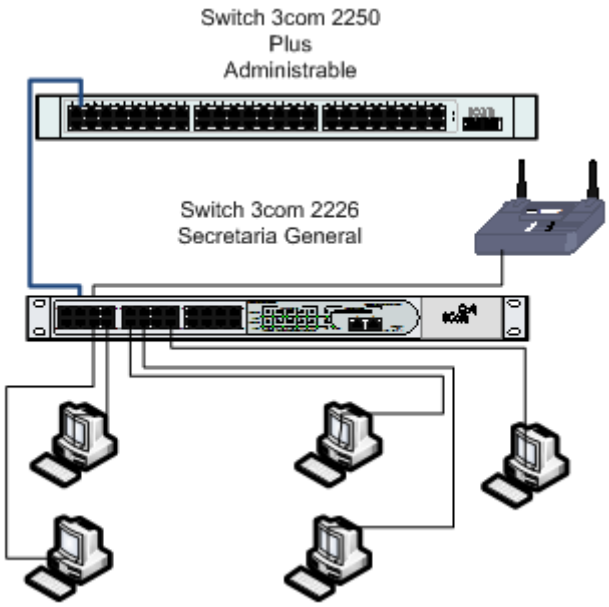


Figura 6.48. ***Conexión del Switch 3Com de 24 puertos con el departamento de Secretaria General.***

Una vez explicado la conexión del Switch Baseline 2226 Plus de 24 puertos para el departamento de Secretaria General se explicará las direcciones IPs que se les asignará a este de departamento. Las direcciones IPs se las pude ver en la tabla 6.5.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Secretaria General	19	30	192.168.1.0	/27	255.255.255.224	192.168.1.1-192.168.1.30	192.168.1.31

Tabla 6.5. ***IPs asignadas al departamento Secretaria General.***

6.4.6 Switch Baseline 2226 Plus de 24 puertos para el área de Corte.

Con la nueva topología recomendada, se utilizará el mismo switch que se está utilizando actualmente.

La conexión de este Switch esta de la siguiente manera:

- Este se conectará con el Switch 3Com Baseline 2250 Plus de 48 puertos el cual es el principal que se encuentra en el departamento de Ventas.
- Después este se conecta con el router Linksys que se utiliza para la red inalámbrica de la Pasamanería S.A.
- Y a su vez se conecta con los equipos de trabajo según el número que exista en esta Área de Corte.

La conexión física de este Switch Baseline 2226 Plus de 24 puertos se le puede ver en la figura 6.49.

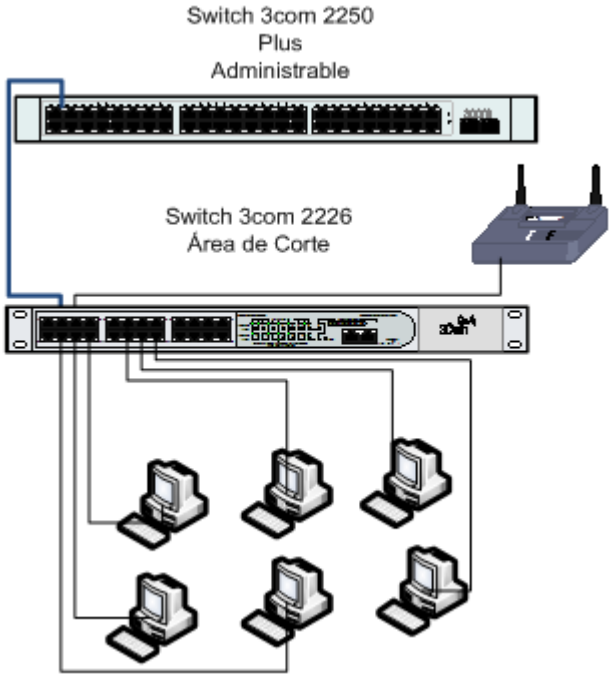


Figura 6.49. ***Conexión del Switch 3Com de 24 puertos con el área de Corte.***

Una vez explicado la conexión del Switch Baseline 2226 Plus de 24 puertos para el área de Corte se explicara las direcciones IPs que se les asignará a esta área. Las direcciones IPs se las pude ver en la tabla 6.6.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Corte	15	30	192.168.1.64	/27	255.255.255.224	192.168.1.65-192.168.1.94	192.168.1.95

Tabla 6.6. ***IPs asignadas para el área de Corte.***

6.4.7 Switch Baseline 2226 Plus de 24 puertos para el área de Supervisión General.

Con la nueva topología recomendada, se utilizará el mismo switch que se encuentra funcionando actualmente.

La conexión de este Switch esta de la siguiente manera:

- Este se conectará con el Switch 3Com Baseline 2250 Plus de 48 puertos el cual es el principal que se encuentra en el departamento de Ventas.
- Después este se conecta con el router Linksys que se utiliza para la red inalámbrica de la Pasamanería S.A.
- Y a su vez se conecta con los equipos de trabajo según el número que exista en esta área de Supervisión General.

La conexión física de este Switch Baseline 2226 Plus de 24 puertos se le puede ver en la figura 6.50.

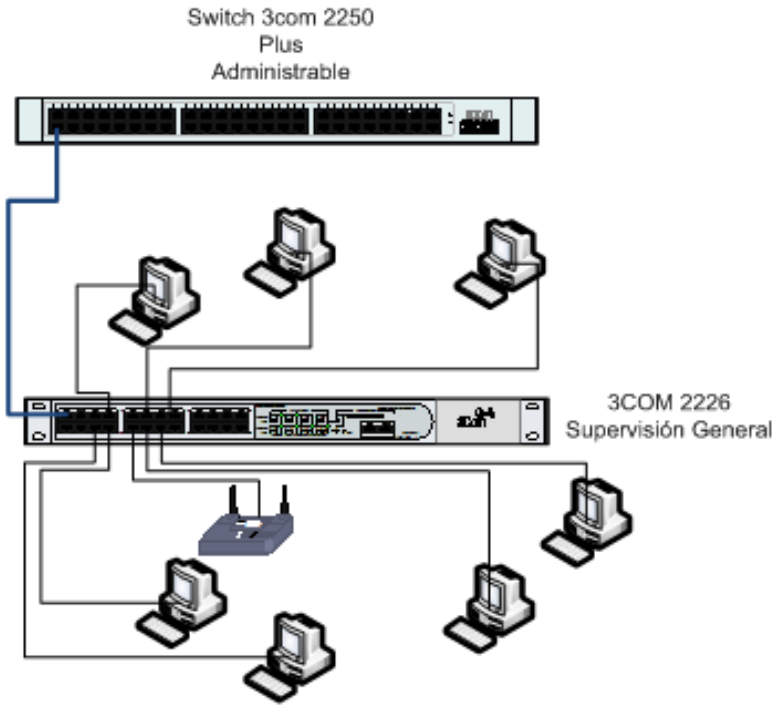


Figura 6.50. ***Conexión del Switch 3Com de 24 puertos con el área de Supervisión General.***

Una vez explicado la conexión del Switch Baseline 2226 Plus de 24 puertos para el área de Supervisión General se explicara las direcciones IPs que se les asignará a esta área. Las direcciones IPs se las pude ver en la tabla 6.7.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Supervisión General	15	30	192.168.1.96	/27	255.255.255.224	192.168.1.97-192.168.1.126	192.168.1.127

Tabla 6.7. ***IPs asignadas para el área de Supervisión General.***

6.4.8 Switch Baseline 2226 Plus de 24 puertos para el área de Mecánica.

Con la nueva topología recomendada, se utilizará el mismo switch que se encuentra funcionando actualmente.

La conexión de este Switch esta de la siguiente manera:

- Este se conectará con el Switch 3Com Baseline 2250 Plus de 48 puertos el cual es el principal que se encuentra en el departamento de Ventas.
- Y a su vez se conecta con los equipos de trabajo según el número que exista en esta área de Mecánica.

La conexión física de este Switch Baseline 2226 Plus de 24 puertos se le puede ver en la figura 6.51.

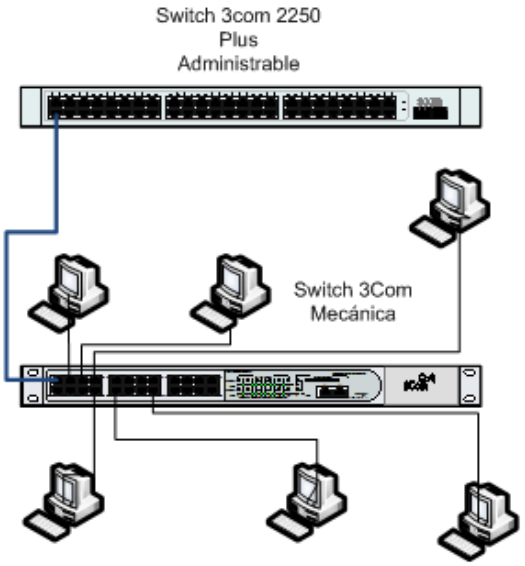


Figura 6.51. ***Conexión del Switch 3Com de 24 puertos con el área de Mecánica.***

Una vez explicado la conexión del Switch Baseline 2226 Plus de 24 puertos para el área de Mecánica se explicara las direcciones IPs que se les asignará a esta área. Las direcciones IPs se las pude ver en la tabla 6.8.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Mecánica	12	14	192.168.1.128	/28	255.255.255.240	192.168.1.129-192.168.1.142	192.168.1.143

Tabla 6.8. ***IPs asignadas para el área de Mecánica.***

6.4.9 Switch Baseline 2226 Plus de 24 puertos para el área de Diseño.

Con la nueva topología recomendada, se recomienda reubicar el switch que se encontraba en el departamento de Sistemas sea utilizado en esta área de Diseño.

La conexión de este Switch esta de la siguiente manera:

- Este se conectará con el Switch 3Com Baseline 2250 Plus de 48 puertos el cual es el principal que se encuentra en el departamento de Ventas.
- Después este se conecta con el router Linksys que se utiliza para la red inalámbrica de la Pasamanería S.A.
- Y a su vez se conecta con los equipos de trabajo según el número que exista en esta área de Diseño.

La conexión física de este Switch Baseline 2226 Plus de 24 puertos se le puede ver en la figura 6.52.

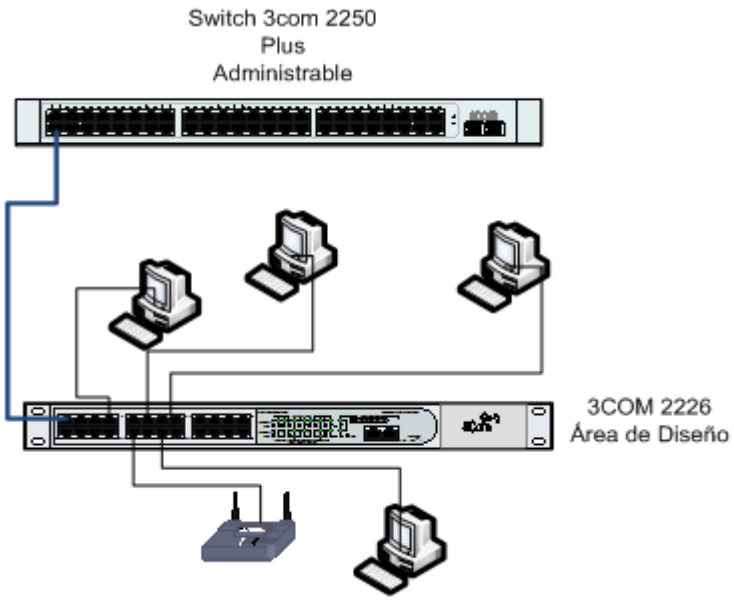


Figura 6.52. ***Conexión del Switch 3Com de 24 puertos con el área de Diseño.***

Una vez explicado la conexión del Switch Baseline 2226 Plus de 24 puertos para el área de Diseño se explicara las direcciones IPs que se les asignara a esta área. Las direcciones IPs se las pude ver en la tabla 6.9.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Diseño	7	14	192.168.1.192	/28	255.255.255.240	192.168.1.193-192.168.1.206	192.168.1.207

Tabla 6.9. ***IPs asignadas para el área Diseño.***

6.4.10. Área del Almacén.

La topología actual del almacén para tener conectividad o estar en red hace un puente con el Switch de Corte, ya que no se puede conectar directamente con el Switch Principal por la distancia considerable que existen entre estos dos puntos, según el estándar EIA/TIA 568A el cableado vertical utilizando cable UTP no debería de pasar los 100. Por esta razón se hace este puente para tener conectividad, la topología actual se la puede ver en la figura 6.53.

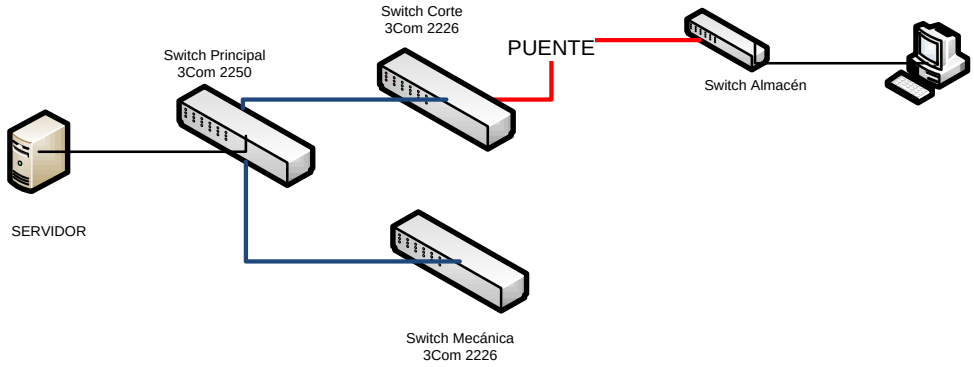


Figura 6.53. ***Conexión actual del área del Almacén.***

La topología que se recomienda para el área del Almacén es la que se muestra en la figura 6.54.

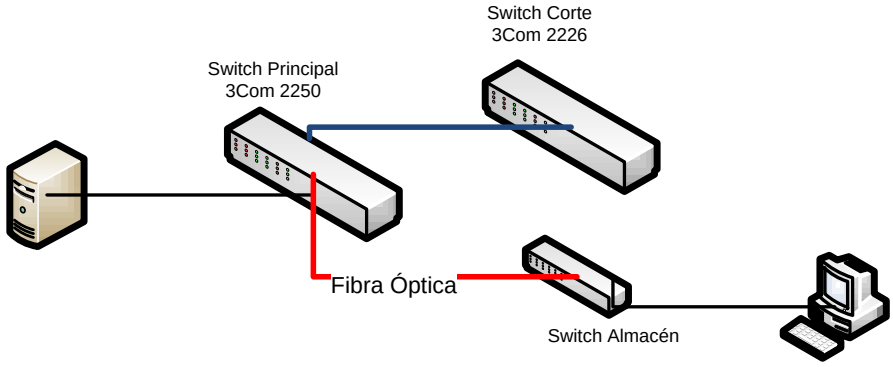


Figura 6.54. ***Topología recomendada.***

Ahora para evitar ese problema se recomienda eliminar ese puente considerando adquirir los siguientes componentes:

- Switch que tenga un puerto para conectar cable de fibra óptica.
- Cable de fibra óptica.
- Conectores SFP para los extremos del cable de fibra óptica.

6.4.10.1 Switch con puerto SFP.

Para la adquisición del switch con puerto SFP se recomienda el SWITCH 3COM OFFICECONNECT MANAGED de 8 puertos el cual tiene las siguientes características que se las puede ver en la tabla 6.10.

MARCA	3COM
MODELO	3COM OFFICECONNECT MANAGED SWITCH
NUMERO DE PARTE	3CDSG8
PUERTOS	8 AUTOSENSING
	1 SFP PARA CONECTIVIDAD POR FIBRA
ESTANDARES DE IEEE	IEEE 802.3, 802.3u, 802.3ab, 802.1p, 802.3x, 802.1ad, 802.1Q, 802.1d SPANNING TREE, 802.1X PORT SECURITY, 802.1w RAPID SPANNING TREE, 802.3ad LINK AGGREGATION, IEEE 802.3z GIGABIT ETHERNET
SOPORTE VLAN	SI
ESPECIFICACIONES ADICIONALES	8K MAC-ADDRESS TABLE
	WEB MANAGEMENT
	MULTICAST FILTERING
	FULL DUPLEX AND HALF DUPLEX FLOW CONTROL
CONTENIDO	SWITCH
	ADAPATADOR DC
	PATAS DE GOMA
	CABLE SERIE
	CD SOFTWARE Y GUIA
	GUIA DE INSTALACION RAPIDA
	MANUAL DE SEGURIDAD Y SOPORTE TECNICO
COMENTARIO	SISTEMA OPERATIVO: WINDOWS, MAC, LINUX.
	Conmutador Fast Ethernet de Nivel 2 administrado.
	Ocho puertos 10/100/1000 y un puerto SFP Gigabit, de propósito dual con 1 de los puertos 10/100/1000 RJ45; puerto de consola del panel frontal para la administración de CLI limitada.
	No es preciso configurar el conmutador si se aceptan los ajustes predeterminados.
	Las VLAN segmentan la red agrupando a los usuarios en función de sus requisitos de datos o tráfico, con el consiguiente mejor uso del ancho de banda disponible.
	El control de acceso de red IEEE 802.1X proporciona seguridad basada en estándares combinada con autenticación local.
	Compatibilidad con Jumbo Frame para una menor carga de red.
	IGMP snooping y el filtrado multicast optimiza el rendimiento de la red.

Tabla 6.10. ***Características del SWITCH 3COM OFFICECONNECT MANAGED***

Una vez establecida las características y beneficios del SWITCH 3COM OFFICECONNECT MANAGED se le puede ver en la figura 6.55.

Figura 6.55. ***SWITCH 3COM OFFICECONNECT MANAGED***

6.4.10.2 Cable de fibra óptica.

Debido a que existe una distancia considerable entre el Switch Principal y el Switch del Almacén se recomienda la utilización de fibra óptica multimodo la cual es la más barata, este cable se le puede ver en la figura 6.56.

Figura 6.56. ***Cable de fibra óptica.***

6.4.10.3 Conectores SFP.

Se recomienda adquirir conectores STP para el cable de fibra óptica para poder conectar el switch Principal con el del Almacén, este tipo de conector se le puede ver en la figura 6.57.

Figura 6.57. ***Conectores SFP***

Una vez echa las recomendaciones para el área del Almacén la topología quedaría de la siguiente manera:

- El switch recomendado se conectaría directamente con el Switch 3Com Baseline 2250 Plus de 48 puertos el cual es el principal que se encuentra en el departamento de Ventas mediante fibra óptica.
- Y a su vez se conecta con los equipos de trabajo según el número que exista en esta área.

La conexión física de este Switch 3COM OFFICECONNECT MANAGED de 8 puertos quedaría de la siguiente manera la cual se puede ver en la figura 6.58.

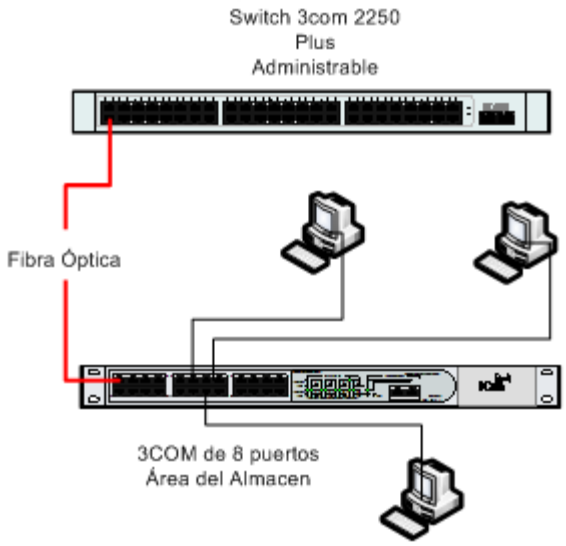


Figura 6.58. ***Conexión del 3COM OFFICECONNECT MANAGED con el área del Almacén.***

Una vez explicado la conexión del Switch 3COM OFFICECONNECT MANAGED de 8 puertos para el área del Almacén se explicará las direcciones IPs que se les asignará a esta área. Las direcciones IPs se las pude ver en la tabla 6.11.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Almacén	4	6	192.168.1.208	/29	255.255.255.248	192.168.1.209-192.168.1.214	192.168.1.215

Tabla 6.11. ***IPs asignadas para el área del Almacén.***

6.4.11 Red inalámbrica.

La red inalámbrica se conectará en los switch siguientes:

- En el 3Com 2250 de 48 puertos se conectarán 2 Router Linksys, uno para el departamento de Ventas y para los departamentos de Sistemas y Contabilidad.

- En el 3Com 2226 de 24 puertos se conectan Router Linksys para el departamento de Secretaria General uno en el primer piso y el otro en el segundo piso.
- En el 3Com 2226 de 24 puertos se conecta 1 Router Linksys para el área de Supervisión General.
- En el 3Com 2226 de 24 puertos que se encuentra en el área de Diseño se conecta 1 Router Linksys para el área donde se encuentra el edificio del Comisariato.

La conexión de la red inalámbrica se la puede ver en la figura 6.59.

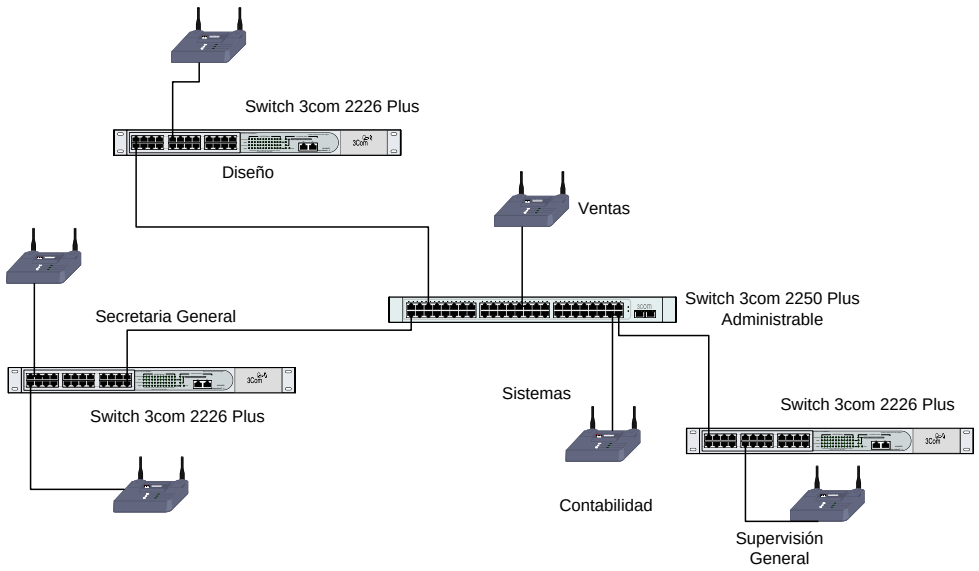


Figura 6.59. ***Conexión de la red inalámbrica.***

Para la red inalámbrica de la Pasamanería se recomienda las siguientes direcciones IPs que se las puede ver en la tabla 6.12.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Red Inalámbrica	16	30	192.168.1.32	/27	255.255.255.224	192.168.1.33-192.168.1.62	192.168.1.63

Tabla 6.12. ***IPs asignadas para la red inalámbrica.***

Entonces una vez explicada cada una de las conexiones de cada switch y sus diferentes equipos la topología de la red quedaría de la siguiente manera la cual se la puede ver en la figura 6.60.

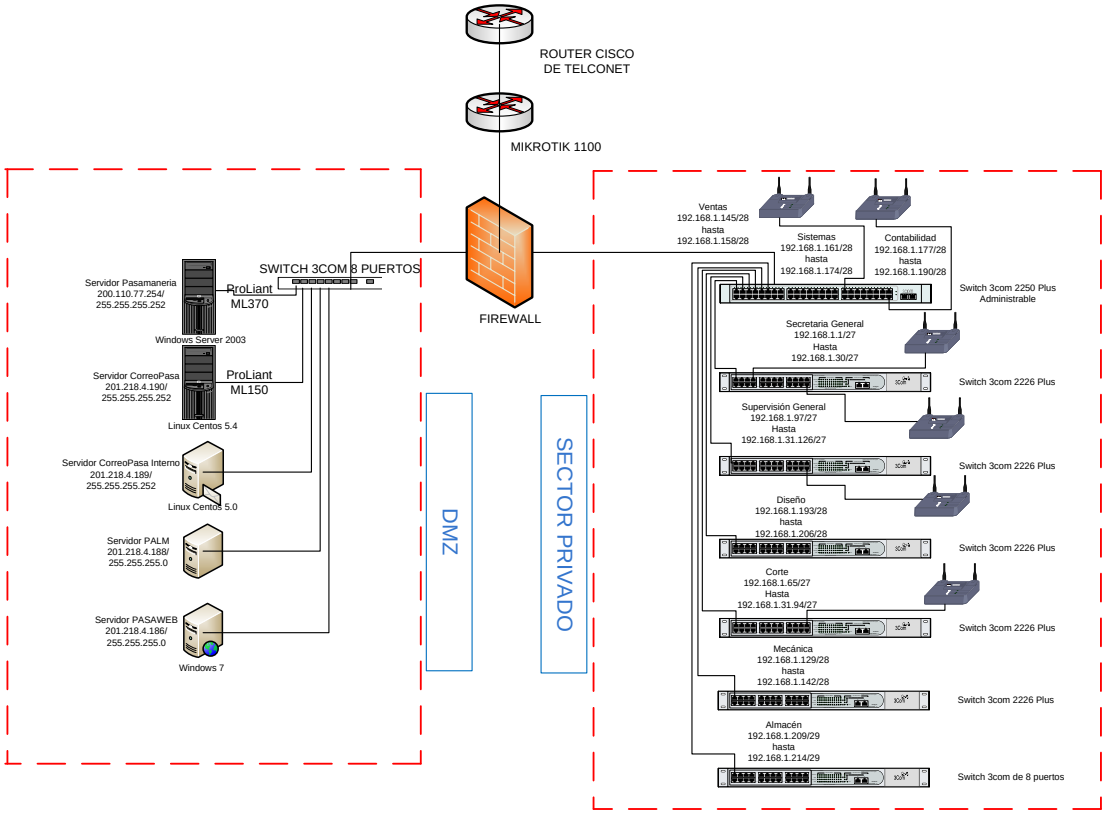


Figura 6.60. ***Topología de la red de la Pasamanería S.A***

Explicada cada una de las partes que compone a la red interna de la Pasamanaría S.A el diagrama final de la Red se la puede ver en la figura 6.61 o en el Anexo 4.

DIAGRAMA DE LA RED DE LA PASAMANERIA S.A

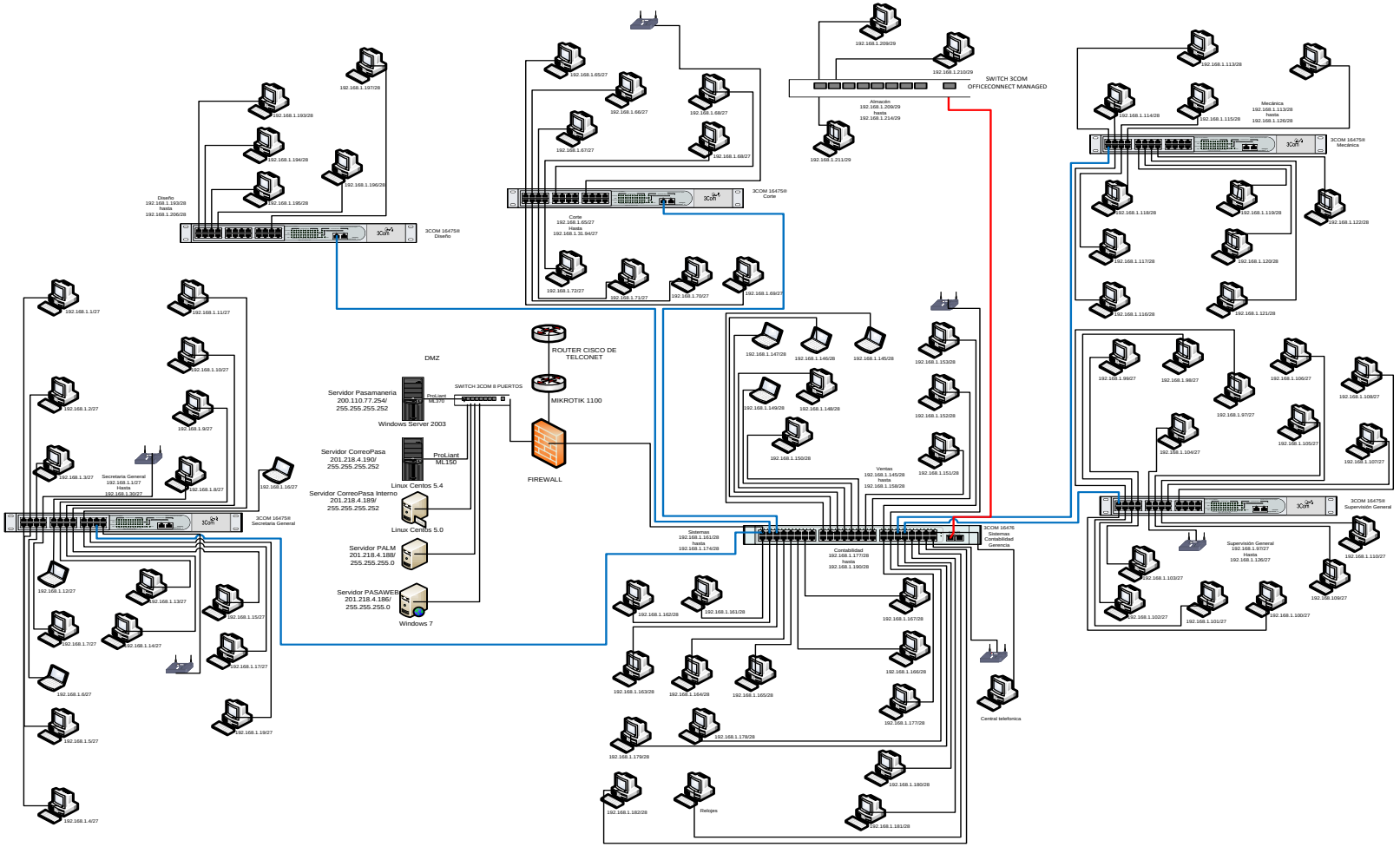


Figura 6.61. ***Diagrama final de la red de la Pasamanería S.A***

6.5 Topología de conexión con las sucursales.

La topología para la conexión con las sucursales se la ha diseñado para que sea una conexión directa es decir que el administrador de la red sea el que realice las respectivas configuraciones en cada uno de los Router de cada sucursal y el Router de la Pasamanería.

Para ello se recomienda la adquisición de Routers que sean administrables para cada sucursal en el cual se realizará cada una de las políticas para la conexión.

La topología que se indica para la conexión con las sucursales es para realizar la creación de un túnel o también conocida como encapsulación es un modo de utilizar una infraestructura de redes para transferir una carga, la carga está formada por tramas o paquetes. En lugar de enviarle tal y como la produce el host de origen, la trama se encapsula con un encabezado adicional. Este encabezado adicional proporciona información adicional de enrutamiento para que la carga encapsulada pueda atravesar un conjunto de redes públicas y privadas de transito. Luego los paquetes encapsulados se enrutan entre los extremos del túnel a través del conjunto de redes públicas y privadas de tránsito. Una vez que los paquetes de carga encapsulados llegan a su destino en el conjunto de redes públicas y privadas de tránsito, la trama se desencapsula y se reenvía a su destino final.

Todo el proceso de encapsulación, transmisión y desencapsulación de paquetes se denomina túnel. El túnel es la ruta de acceso lógica en el conjunto de redes públicas y privadas de tránsito a través de la cual viajan los paquetes encapsulados.

Esta recomendación es para garantizar, integridad y confiabilidad de toda la comunicación. Es decir que los paquetes enviados no sean alterados por personas que no tengan que ver con la empresa. Las direcciones IPs que se plantearon para esta conexión se las puede ver en la tabla 6.13.

Nombre Subred	Tamaño necesario	Tamaño máximo	Dirección de la Red	Mask	Dec Mask	Rango de asignación	Broadcast
Américas	2	2	200.0.0.0	/30	255.255.255.252	200.0.0.1-200.0.0.2	200.0.0.3
Vergel	2	2	200.0.0.8	/30	255.255.255.252	200.0.0.9-200.0.0.10	200.0.0.11

Tabla 6.13. ***IPs asignadas para las sucursales.***

Este esquema de encapsulamiento se le puede ver en la figura 6.62.

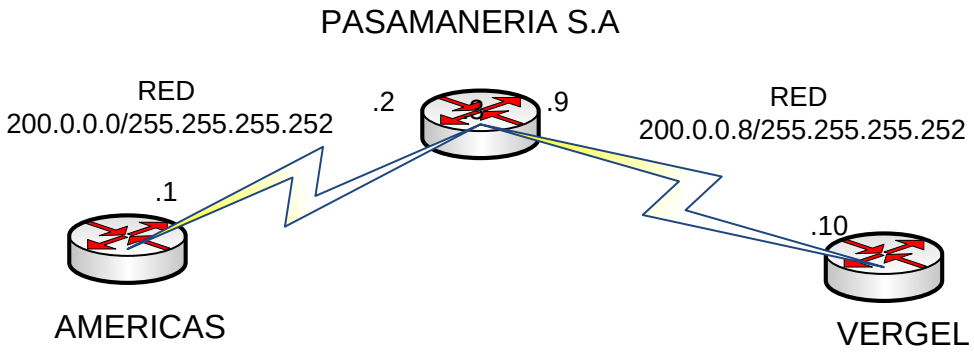


Figura 6.62. ***Esquema de conexión con las sucursales.***

Como se puede ver en la figura 6.62 se muestra como seria la conexión directa entre los Routers de las sucursales con el Router de la Pasamanería para la creación del encapsulamiento de los paquetes o los datos.

6.5.1 Sucursal de las Américas.

La conexión de la red de las Américas con la recomendación de la adquisición de un router administrable se puede ver en la figura 6.63.

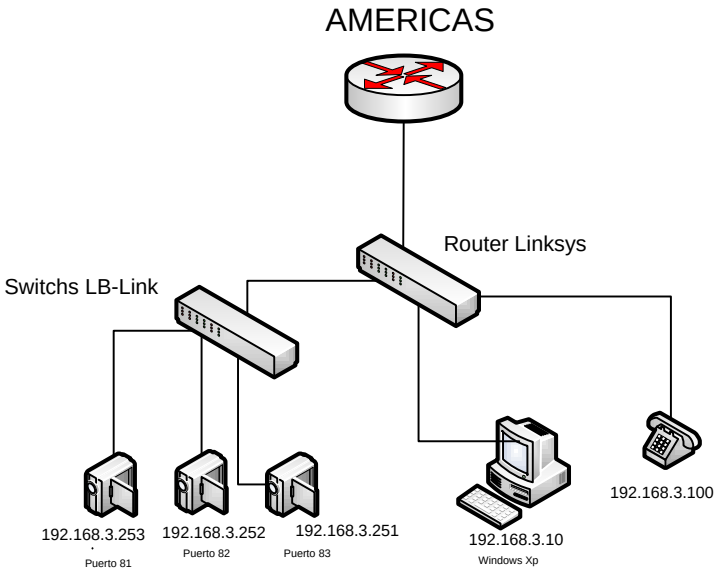


Figura 6.63. ***Diagrama de la sucursal de Las Américas.***

6.5.2 Sucursal El Vergel.

La conexión de la red EL Vergel con la recomendación de la adquisición de un router administrable se puede ver en la figura 6.64.

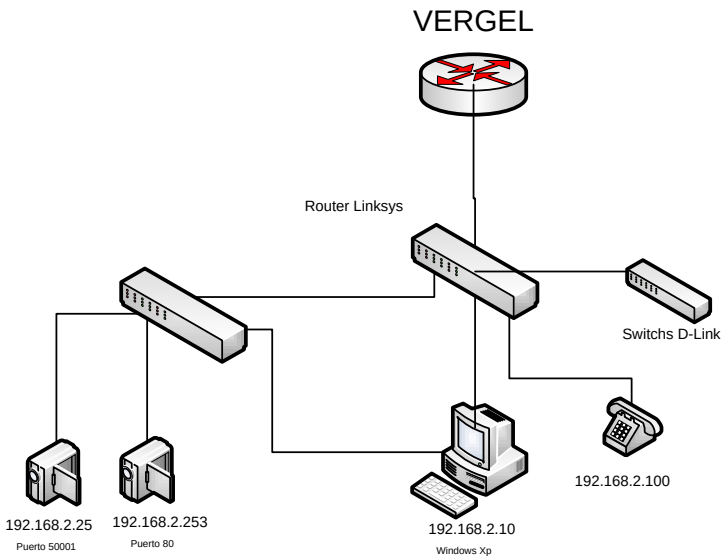


Figura 6.64. ***Diagrama de la sucursal El Vergel.***

Establecida cada una de las conexiones de las sucursales la topología general se la puede ver en la figura 6.65.

TOPOLOGÍA DE RED DE CONEXIÓN CON LAS SUCURSALES.

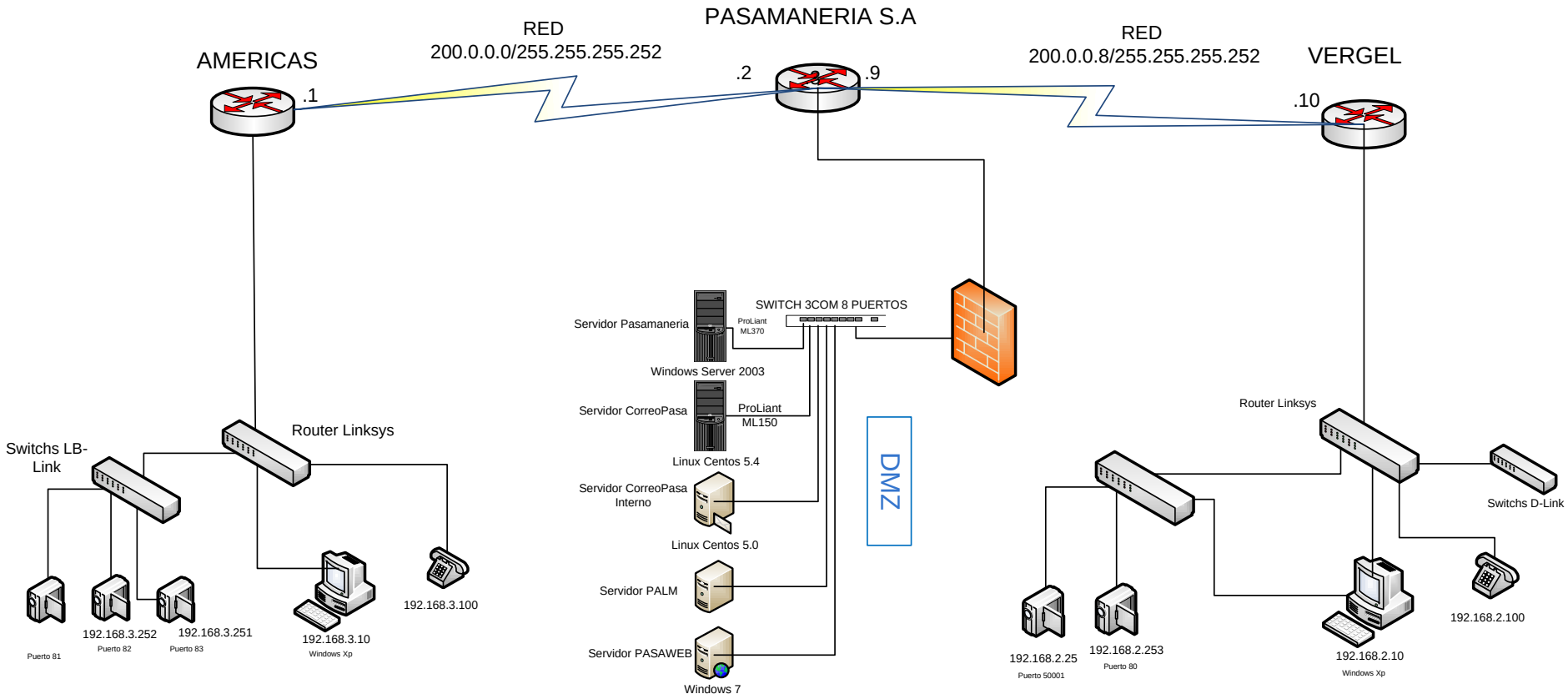


Figura 6.65. Topología de red de conexión con las sucursales.

Una vez explicado cada uno de las topologías de red y conexiones de cada departamento con sus respectivas direcciones IPs a continuación se explicará como quedaría la conexión de la red de la Pasamanería con las sucursales utilizando el programa Packet Tracer 5.0 donde se hará una simulación la red.

6.6 Simulación de la red de la Pasamanería S.A con las sucursales El Vergel y Las Américas en Packet Tracer 5.0.

Con la utilización de Packet Tracer se realizó la red de la Pasamanería donde se crearon Vlans para cada departamento incluyendo a los servidores a más de sus sucursales como son El Vergel y Las Américas.

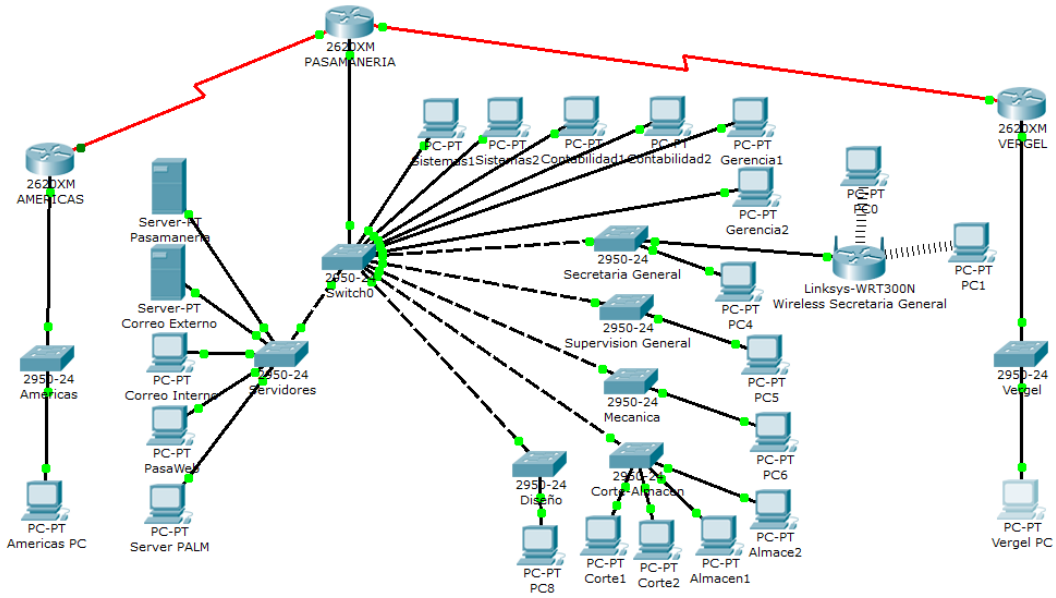


Figura 6.66. ***Conexión de la red en el Packet Tracer 5.0***

Realizada la conectividad de los diferentes equipos ya sean los Router, Switchs y Máquinas se realizó los siguientes puntos:

- Creación de VLAN en cada Switches a través de la base de datos de VLAN o de forma de comandos.
- Asignación de VLANS a cada una de las máquinas.
- Configuración de enlaces troncales entre los switches.
- Creación de un enlace troncal entre el switches y el routers.
- Asignación de subintefaces en el router para el enrutamiento entre VLAN y configuración de encapsulamiento adecuado.

6.6.1 Configuración de la red de la Pasamanería S.A.

6.6.1.1 Creación de las VLANS en el Switch principal a través de la base de datos de VLAN o de forma de comandos.

- **A través de la base de datos de VLAN:** Con la ayuda de la interfaz gráfica que nos presenta el Switch podemos crearnos fácilmente las Vlans como podemos en la figura 6.67 en la pestaña de Config y seleccionando VLAN Database podemos realizar la creación de la VLAN donde se le da un nombre y un número de identificación de la Vlan que se crea y así con cada VLAN de cada departamento.

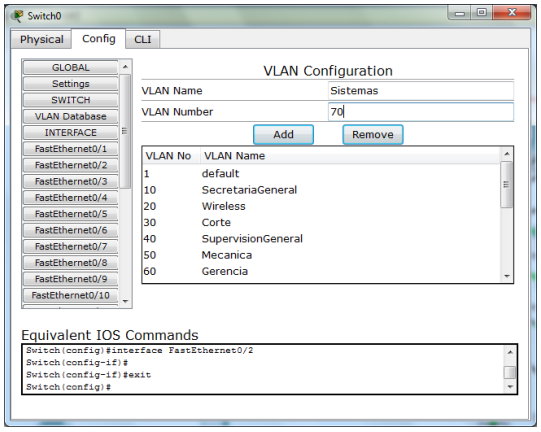


Figura 6.67. ***Creación de Vlans mediante el Database.***

- **Creación de las vlans en el switch principal en forma de comandos:** Con la misma interfaz grafica que no presenta el switch en la pestaña CLI podemos crearnos las VLAN en forma de comandos como se puede ver en la figura 6.68.

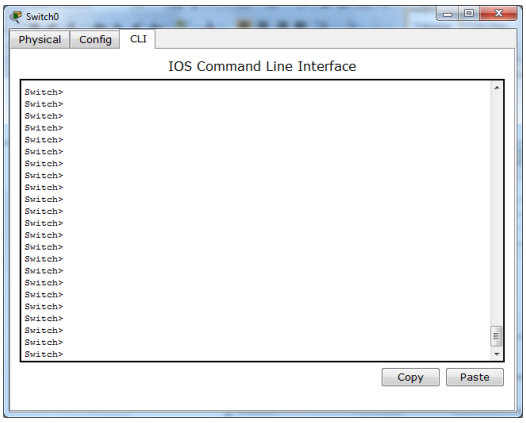


Figura 6.68. ***Creación de Vlans mediante comandos.***

Dentro de la pantalla se ingresa los siguientes comandos para la creación de cada una de las Vlans en el swicht principal.

```
Switch>enable
Switch#configure terminal
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name SecretariaGeneral
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Wireless
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Corte
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#name SupervisionGeneral
Switch(config-vlan)#exit
Switch(config)#vlan 50
Switch(config-vlan)#name Mecanica
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)#name Gerencia
Switch(config-vlan)#exit
Switch(config)#vlan 70
Switch(config-vlan)#name Sistemas
Switch(config-vlan)#exit
Switch(config)#vlan 80
Switch(config-vlan)#name Contabilidad
Switch(config-vlan)#exit
Switch(config)#vlan 90
Switch(config-vlan)#name Diseno
Switch(config-vlan)#exit
Switch(config)#vlan 100
Switch(config-vlan)#name Almacen
Switch(config-vlan)#exit
Switch(config)#vlan 110
Switch(config-vlan)#name Servidores
Switch(config-vlan)#exit
Switch(config)#
```

Para ver las vlans creadas en el switch se debe ejecutar el comando show vlan, como se puede ver en la figura 6.69.

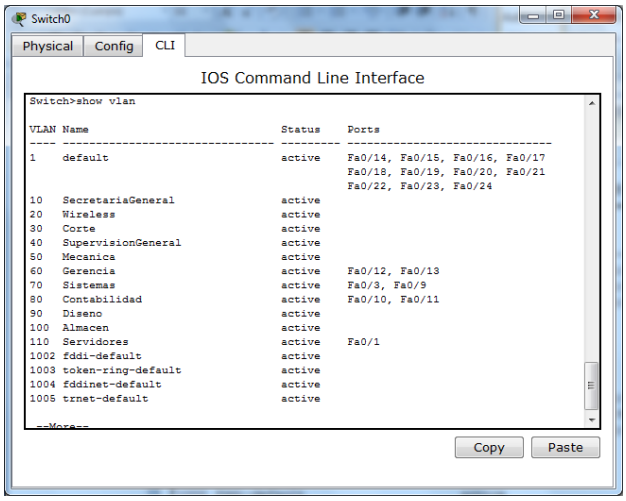


Figura 6.69. ***Vlans creadas.***

- **Creación de las Vlans en el switch de Sistemas-Contabilidad-Gerencia.**
  Switch>enable
  Switch#configure terminal
  Switch(config)#vlan 60
  Switch(config-vlan)#name Gerencia
  Switch(config-vlan)#exit
  Switch(config)#vlan 70
  Switch(config-vlan)#name Sistemas
  Switch(config-vlan)#exit
  Switch(config)#vlan 80
  Switch(config-vlan)#name Contabilidad
  Switch(config-vlan)#exit

- **Creación de la Vlan en el switch Secretaria General.**
  Switch>enable
  Switch#configure terminal
  Switch(config)#vlan 40
  Switch(config-vlan)#name SecretariaGeneral
  Switch(config-vlan)#exit
  Switch(config)#

- **Creación de la Vlan en el switch Supervisión General.**
  Switch>enable
  Switch#configure terminal
  Switch(config)#vlan 40
  Switch(config-vlan)#name SupervisionGeneral
  Switch(config-vlan)#exit
  Switch(config)#

- **Creación de la Vlan en el switch Mecánica**
  Switch>enable
  Switch#configure terminal
  Switch(config)#vlan 50
  Switch(config-vlan)#name Mecanica

```
Switch(config-vlan)#exit
Switch(config)#
```

- **Creación de la Vlan en el switch Corte-Almacén.**

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 30
Switch(config-vlan)#name Corte
Switch(config-vlan)#exit
Switch(config)#vlan 100
Switch(config-vlan)#name Almacen
Switch(config-vlan)#exit
Switch(config)#
```

- **Creación de la Vlan en el switch Diseño.**

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 90
Switch(config-vlan)#name Diseno
Switch(config-vlan)#exit
Switch(config)#
```

6.6.1.2 Asignación de VLANS a cada una de las máquinas.

Para que los hosts o máquinas puedan acceder a las VLANS, los switches deben tener asociados los puertos a cada red virtual.

En el modo de configuración de interfaz se debe digitar los siguientes comandos para asignar un puerto a una Vlan, a continuación se muestra los comandos para cada uno de los switches con sus respectivas interfaces.

- **Switch de Secretaria General con la Vlan 10.**

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#
```

- **Switch de Secretaria General con la Vlan 20 para el Wireless.**

```
Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
```

- **Switch de Corte con la Vlan 30 y Almacén con la Vlan 100.**

```
Switch(config)#
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 30
```

```
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 30
Switch(config-if)#

Switch(config)#
Switch(config)#interface FastEthernet0/4
Switch(config-if)#switchport access vlan 100
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
Switch(config-if)#switchport access vlan 100
Switch(config-if)#
```

- **Switch de Supervisión General con la Vlan 40.**

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 40
Switch(config-if)#
```

- **Switch de Mecánica con la Vlan 50.**

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 50
Switch(config-if)#
```

- **Switch Principal con la Vlan 60 de Gerencia, Vlan Sistemas con la Vlan 70 y Contabilidad con la Vlan 80.**

```
Switch(config)#
Switch(config)#interface FastEthernet0/12
Switch(config-if)#switchport access vlan 60
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/13
Switch(config-if)#switchport access vlan 60
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 70
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/9
Switch(config-if)#switchport access vlan 70
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/10
Switch(config-if)#switchport access vlan 80
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/11
Switch(config-if)#switchport access vlan 80
Switch(config-if)#
```

- **Switch de Diseño con la Vlan 90.**

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 90
Switch(config-if)#
```

- **Switch de Servidores con la Vlan 110.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport access vlan 110
  Switch(config-if)#

6.6.1.3 Configuración de enlaces troncales entre los switches.

- **Switch de Secretaria General.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#

- **Switch de Supervision General.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#

- **Switch de Mecánica.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#

- **Switch Corte y Almacén.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#

- **Switch de Diseño.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#

- **Switch de Supervision General.**
  Switch(config)#interface FastEthernet0/1
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#

- **Switch Principal.**
  Switch(config)#interface FastEthernet0/4
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#exit
  Switch(config)#interface FastEthernet0/5
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#exit
  Switch(config)#interface FastEthernet0/6
  Switch(config-if)#exit
  Switch(config)#interface FastEthernet0/7
  Switch(config-if)#switchport mode trunk
  Switch(config-if)#exit

```
Switch(config)#interface FastEthernet0/8
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

6.6.1.4 Creación de un enlace troncal entre el Switch Principal y el Router Pasamanería S.A.

```
Switch#configure terminal
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

6.6.1.5 Asignación de subintefaces en el router para el enrutamiento entre VLAN y configuración de encapsulamiento adecuado.

- **Asignación de subintefaces en el router para el enrutamiento.**

```
Router>enable
Router#configure terminal
Router(config)#interface Serial0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0
Router(config-if)#no shutdown
Router(config-if)#clock rate 64000
Router(config-if)#ip address 200.0.0.9 255.255.255.252
Router(config-if)#
```

```
Router>enable
Router#configure terminal
Router(config)#interface Serial0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1
Router(config-if)#no shutdown
Router(config-if)#clock rate 64000
Router(config-if)#ip address 200.0.0.2 255.255.255.252
Router(config-if)#
```

- **Configuración de encapsulamiento del router Pasamanería S.A.**

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config)# no shutdown
Router(config)#exit
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
```

```
Router(config-subif)#ip address 192.168.1.30 255.255.255.224
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.1.62 255.255.255.224
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.1.94 255.255.255.224
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.1.126 255.255.255.224
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.1.142 255.255.255.240
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.60
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.1.158 255.255.255.240
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.70
Router(config-subif)#encapsulation dot1Q 70
Router(config-subif)#ip address 192.168.1.174 255.255.255.240
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.80
Router(config-subif)#encapsulation dot1Q 80
Router(config-subif)#ip address 192.168.1.190 255.255.255.240
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.90
Router(config-subif)#encapsulation dot1Q 90
Router(config-subif)#ip address 192.168.1.206 255.255.255.240
Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.100
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip address 192.168.1.214 255.255.255.240
Router(config-subif)#exit

Router(config-subif)#interface fastEthernet 0/0.110
Router(config-subif)#encapsulation dot1Q 110
```

```
Router(config-subif)#ip address 192.168.100.14 255.255.255.240
Router(config-subif)#exit
Router(config)#
```

6.6.2 Configuración de la red de la sucursal Las Américas.

- **Creación de la Vlan 120 Américas.**

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 120
Switch(config-vlan)#name Americas
Switch(config-vlan)#exit
```

- **Asignación de la VLAN a la máquina de trabajo.**

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 120
Switch(config-if)#exit
```

6.6.2.1 Creación de un enlace troncal entre el Switch Américas y el Router Américas.

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

6.6.2.2 Asignación de subintefaces en el router para el enrutamiento entre VLAN y configuración de encapsulamiento adecuado.

- **Asignación de subintefaces en el router para el enrutamiento**

```
Router>enable
Router#configure terminal
Router(config)#interface Serial0/1
Router(config-if)#
Router(config-if)#clock rate 64000
Router(config-if)#
Router(config-if)#ip address 200.0.0.1 255.255.255.252
Router(config-if)#
```

- **Configuración de encapsulamiento del Router Las Américas.**

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.120
Router(config-subif)#encapsulation dot1Q 120
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

6.6.3 Configuración de la red de la sucursal El Vergel.

- **Creación de la Vlan 130 Vergel.**

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 130
Switch(config-vlan)#name Vergel
Switch(config-vlan)#exit
Switch(config)#
```

- **Asignación de la VLAN a la máquina de trabajo.**

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 130
Switch(config-if)#
```

6.6.3.1 Creación de un enlace troncal entre el Switch Vergel y el Router Vergel.

```
Switch(config)#
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
Switch(config-if)#exit
```

6.6.3.2 Asignación de subintefaces en el router para el enrutamiento entre VLAN y configuración de encapsulamiento adecuado.

- **Asignación de subintefaces en el router para el enrutamiento.**

```
Router>enable
Router#configure terminal
Router(config)#interface Serial0/1
Router(config-if)#
Router(config-if)#clock rate 64000
Router(config-if)#
Router(config-if)#ip address 200.0.0.10 255.255.255.252
Router(config-if)#
```

- **Configuración de encapsulamiento en el Router Vergel.**

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.130
Router(config-subif)#encapsulation dot1Q 130
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

6.6.4 Configuración de rutas estáticas en el Router Pasamanería.

```
Router(config)#ip route 192.168.2.0 255.255.255.252 200.0.0.10
Router(config)#ip route 192.168.3.0 255.255.255.252 200.0.0.1
Router(config)#
```

6.6.5 Configuración de rutas estáticas en el Router Américas.

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.100.0 255.255.255.240 200.0.0.2
Router(config)#
```

6.6.6 Configuración de rutas estáticas en el Router Vergel.

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.100.0 255.255.255.240 200.0.0.9
Router(config)#
```

6.7 Vulnerabilidad de la Red.

6.7.1 Mikrotik 1100.

Este es el equipo que se implementó recientemente para poder controlar la vulnerabilidad de la red de la Pasamanería S.A, el cual viene con un sistema operativo Mikrotik RouterOS ya que estos equipos brindan seguridad, flexibilidad y son muy económicos, lo cual es un gran beneficio para la Pasamanería S.A ya que la red es de un tamaño considerable. El equipo se le pude ver en la figura 6.70.

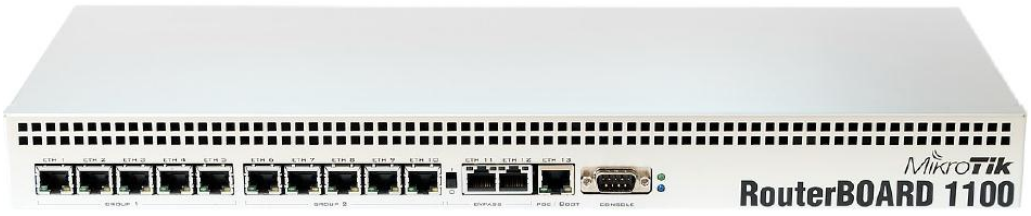


Figura 6.70. ***Mikrotik BR 1100.***

6.7.2 Mikrotik RouterOS.

El RouterOS es un sistema operativo y software del router, el cual convierte a una PC. Mikrotik RouterBOARD en un router dedicado, bridge, firewall, controlador de ancho de banda, punto de acceso inalámbrico, por lo tanto puede hacer casi cualquier

cosa que tenga que ver con las necesidades de red, además de ciertas funcionalidades como servidor.

El software RourterOS puede ejecutarse desde un disco IDE memoria tipoFLASH. Este dispositivo se conecta como un disco rígido común y permite acceder a las avanzadas características de este sistema operativo.

6.7.2.1 Características principales.

- El Sistema Operativo es basado en el Kernel de Linux y es muy estable.
- Puede ejecutarse desde discos IDE o módulos de memoria flash.
- Diseño modular
- Módulos actualizables
- Interfaz gráfica amigable.

6.7.2.2 Características de ruteo.

- Políticas de enrutamiento. Ruteo estático o dinámico.
- Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en El Bridge.
- Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
- Cache: web-proxy, DNS.
- Gateway de HotSpot.
- Lenguaje interno de scripts.

6.7.2.3 Interfaces del RouterOS.

- Ethernet 10/100/1000 Mbit.
- Inalámbrica (Atheros, Prism, CISCO/Airones)
- Punto de acceso o modo estación/cliente, WDS.
- Síncronas: V35, E1, Frame Relay.
- Asíncronas: Onboard serial, 8-port PCI.
- ISDN.
- xDSL.
- Virtual LAN (VLAN).

6.7.2.4 Herramientas de manejo de red.

- Ping, traceroute.
- Medidor de ancho de banda.
- Contabilización de tráfico.
- SNMP.
- Torch.
- Sniffer de paquetes.

Estas son las principales características del sistema operativo y software Mikrotik RouterOS el cual se utilizará en la fábrica y se recomienda el uso de diferentes beneficios que tiene este sistema operativo y software para el mejoramiento de la red en la Pasamanería S.A. en la figura 6.71 se muestra una interfaz del Mikrotik RouterOS.

Figura 6.71. ***Interfaz del Mikrotik RouterOS.***

Una vez explicado las principales características del Mikrotik RouterOS vamos a explicar los usos que se pueden dar de esta herramienta que se pueden aplicar en la red de la Pasamanería S.A.

6.7.3 Recomendación del uso del Mikrotik para la red de la Pasamanería S.A.

6.7.3.1 Backup y Restore de Configuración.

Debido a los problemas que pueden producirse en el equipo, siempre es recomendable tener back up de todas las configuraciones de los sistemas. Ahora se mostrará cómo se realiza un backup de la configuración y como se recupera.

6.7.3.1.1 Realización de un Backup.

Debemos dirigirnos al menú Files donde se nos abrirá una ventana y nos mostrará los archivos que se encuentran almacenados, debemos hacer clic en el botón de Backup para realizar nuestro backup. Esto se lo puede ver en la figura 6.72.

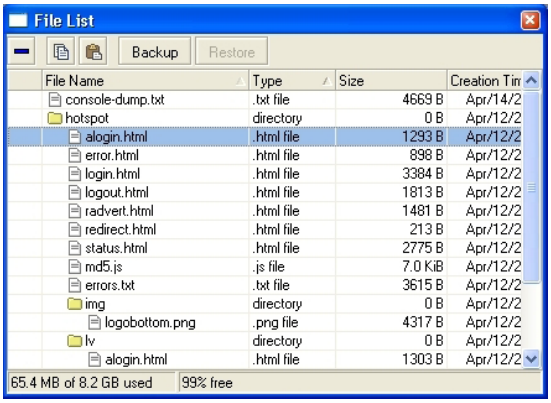


Figura 6.72. ***Backup realizado.***

Luego de haber hecho clic nos aparece un nuevo archivo en la lista, que sería el backup de toda la configuración del Mikrotik.

6.7.3.1.2 Restauración de la configuración.

Para realizar la restauración del backup guardado dentro del Mikrotik simplemente debemos ir al menú Files, en la ventana que se aparece debemos seleccionar la versión del backup que se desee recuperar y hacer clic sobre el botón Restore, como se puede ver en la figura 6.73.

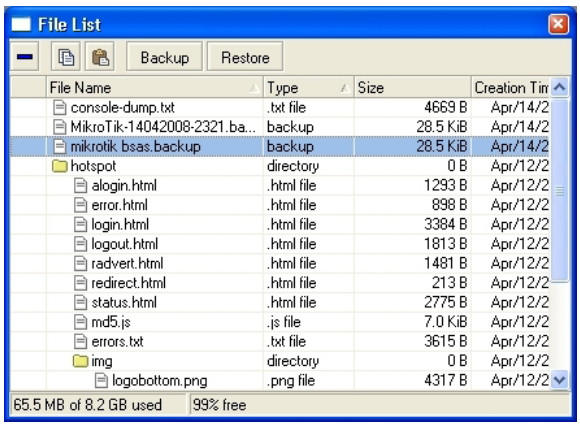


Figura 6.73. ***Restauración del Backup***

Una vez hecho clic sobre el botón Restore se nos abrirá una nueva ventana que nos aplicará la nueva configuración y nos hará reiniciar el Mikrotik. Como se puede ver en la figura 6.74.

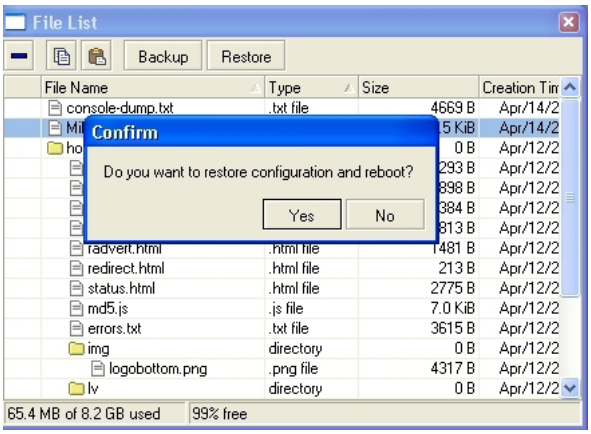


Figura 6.74. ***Reiniciar al Mikrotik.***

Debido a que el Mikrotik tiene varias alternativas que pueden ser configuradas para el mejoramiento de la red de la Pasamanería S.A, se recomienda los siguientes puntos:

- Configuración de Servidor – Cliente PPTP.
- Configuración de un Servidor Web Proxy.
- Bloqueo de pornografía.
- Bloqueo páginas que brinden el servicio de Web Messenger.
- Bloqueo del Live Messenger a través del Proxy.
- Bloqueo de páginas que brinden webmail.
- Bloqueo descarga directa de archivos MP3, MP4 y AVI.
- Bloqueo descarga directa de archivos RAR, ZIP, EXE.

Se recomienda la creación de un servidor PPTP que será utilizado para interconectarse con las sucursales que tiene la Pasamanería S.A.

6.7.3.2 Servidor – Cliente PPTP.

6.7.3.2.1 Configuración Servidor PPTP.

Debido a que la fábrica de la Pasamanería S.A tiene sucursales de puntos de venta se recomienda realizar una VPN entre las sucursales y la fábrica de la Pasamanería S.A.

Para ello se necesita configurar un servidor de PPTP en la Pasamanería S.A, los pasos para la configuración son:

Debemos ir al menú PPP, se nos abrirá la ventana de configuración de conexiones PPPx. Luego hacemos clic en la pestaña PROFILES. A continuación hacemos clic en

botón (+). Con la nueva ventana de profiles abierta la configuramos de la siguiente manera:

- Name: Profile_VPN
- Local Address: Sucursales
- Remote Address: Sucursales
- Use compresión: Default
- Use Vj Compression: Default
- User Encryption: Yes
- Change TCP MMS: Yes

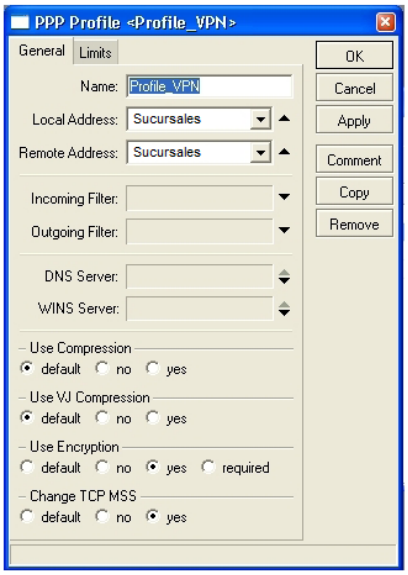


Figura 6.75. Configuración Servidor PPTP.

Con el profile ya generado para VPN debemos crear el usuario que utilizará dicho profile. Para ello vamos al menú PPP, hacemos clic en la pestaña SECRESTS.

Hacemos clic sobre el botón (+) y en la nueva ventana la configuramos de la siguiente manera:

- Name: vpn
- Password: vpn
- Service: pptp
- Profile: Profile_VPN

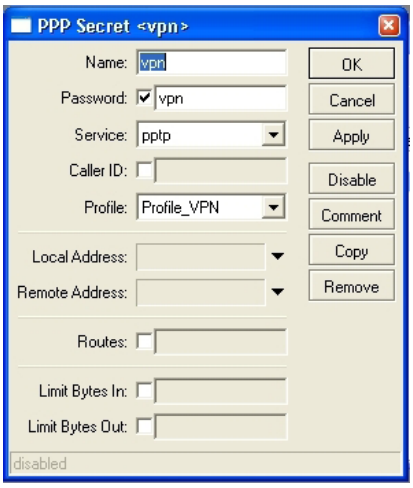


Figura 6.76. ***Ventana SECRESTS.***

Finalmente debemos dar de alta el servidor de PPTP. Para ello nos dirigimos al menú PPP, en la pestaña Interfaces hacemos clic sobre el botón PPTP Server. En la nueva ventana la configuramos de la manera siguiente:

- Enable (seleccionado)
- Max MTU: 1460
- Max MRU: 1460
- Keepalive Timeout:30
- Default Profile: Profile_VPN
- Mschap1 y mschap2 (seleccionados)

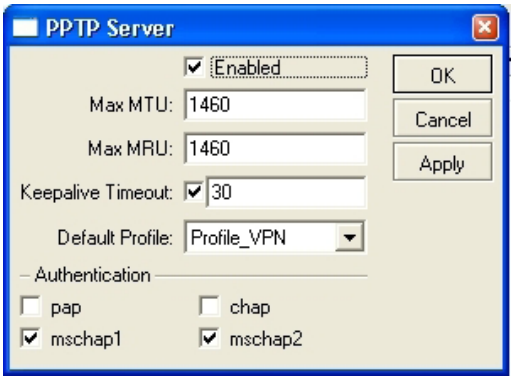


Figura 6.77. ***Ventana PPTP Server.***

6.7.3.2.2 Configuración Cliente PPTP o VPN.

Para que un cliente se conecte a su servidor VPN, es necesario configurar todos los parámetros de conexión (direcciones del servidor, protocolos a utilizar, etc.). El

nuevo asistente de conexión disponible en el icono Conexiones de red del panel de control permite esta configuración:

Hacemos clic en siguiente, como se muestran en las figuras.

Figura 6.78. ***Ventana asistente.***

De las cuatro opciones de la ventana, seleccionamos Configurar una conexión avanzada "Connect to the network at my place":

Figura 6.79. ***Seleccionar conexión avanzada***

En la siguiente pantalla, seleccionamos Conexión de red privada virtual "Virtual Private Network Connection".

Figura 6.80. ***Selección de conexión de red privada virtual.***

A continuación, escribimos el nombre que se designa a la red privada virtual a la que se desea conectarse:

Escribimos el nombre de la conexión: Pasamanería S.A.

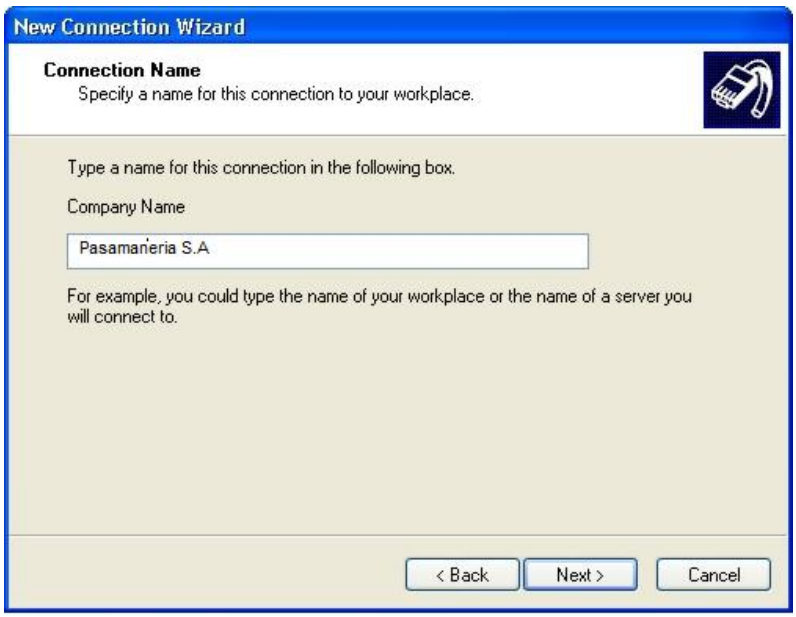


Figura 6.81. ***Escribir el nombre de la conexión.***

En la siguiente pantalla permite indicar si la conexión debe establecerse de forma anticipada a la conexión de la VPN. En la mayoría de los casos (si tiene una conexión permanente, DSL o cable), no será necesario este paso ya que el equipo estará conectado a Internet. De lo contrario, seleccione en la lista la conexión que desea establecer:

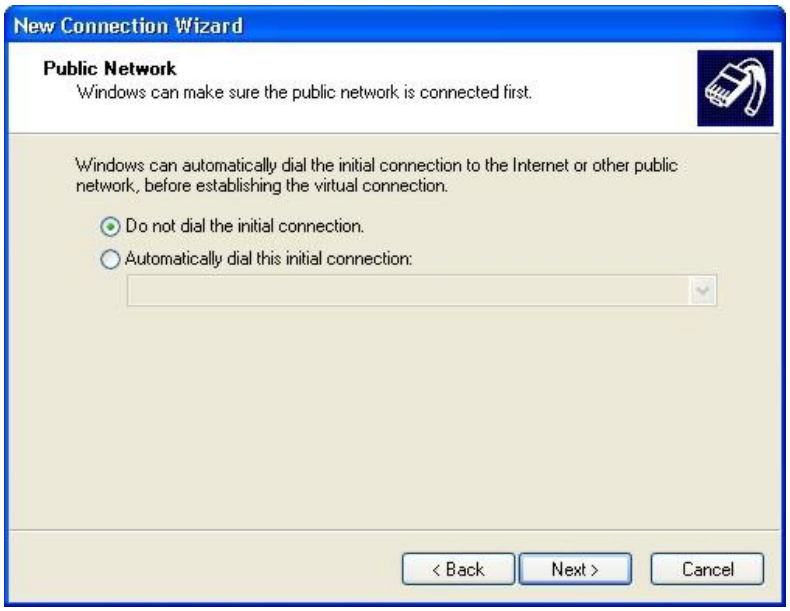


Figura 6.82.*Configurar conexión pública.*

Para tener acceso al servidor de acceso remoto (servidor VPN o host), se debe especificar su dirección (IP o nombre del host). Si no tiene una dirección IP, deberá implementar un sistema dinámico de asignación de nombres (DynDNS) que pueda generar un nombre de dominio, y especificarlo en el siguiente campo:

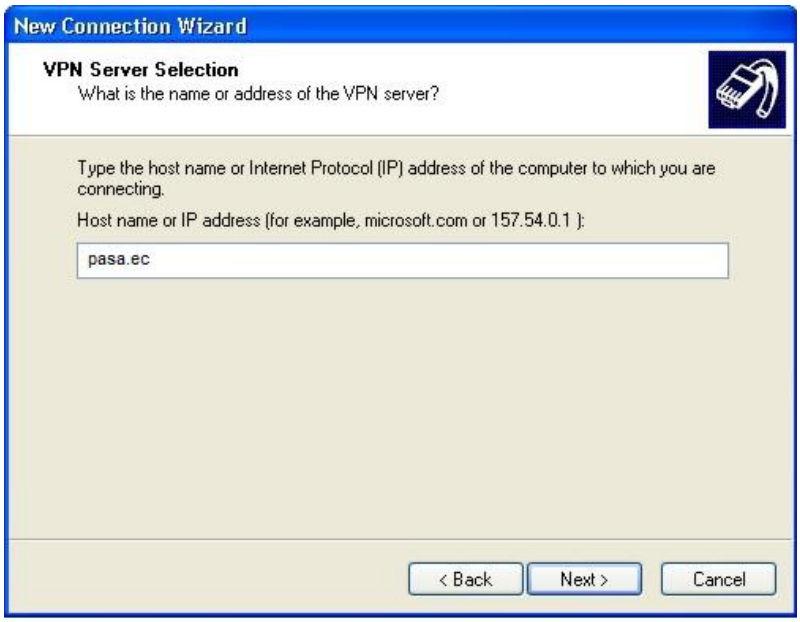


Figura 6.83. *Especificación de nombre del host de la fábrica.*

A continuación hay que configurar el tipo de autenticación que vamos a utilizar para ello debemos estar sobre la conexión Pasamanería, abrimos la ventana y la configuramos de la siguiente manera:

- Nombre de usuario: Vergel
- Contraseña: ****
- Guardar nombre de usuario y contraseña (seleccionado).

Figura 6.84. ***Conexión mediante VPN***

Antes de conectarse, se debe definir algunas opciones de configuración. Para hacerlo, hacemos clic en el botón Propiedades en la parte inferior de la ventana. Aparecerá una ventana con fichas que permiten un ajuste detallado de la conexión. En la ficha Networking, seleccionamos el protocolo PPTP en la lista desplegable, también seleccionamos Protocolo Internet (TCP/IP) y hacemos clic en Propiedades:

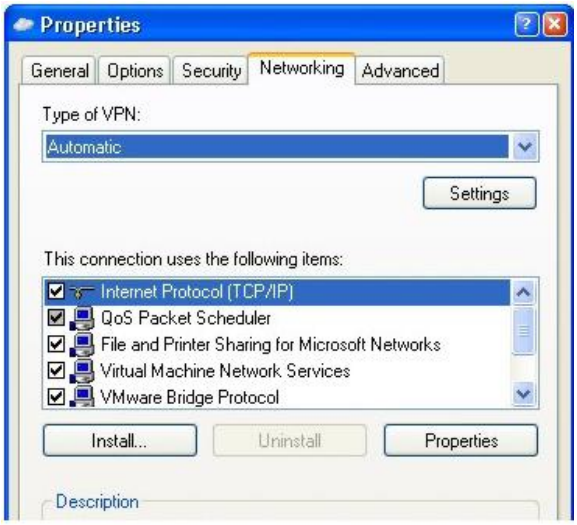


Figura 6.85. ***Configurar detalles de conexión con VPN.***

La ventana que aparecerá permite configurar la dirección IP que la máquina del cliente tendrá durante la conexión al servidor de acceso remoto. Esto permite que su direccionamiento sea coherente con el direccionamiento remoto. De esta forma, el servidor VPN puede actuar como un servidor DHPC, es decir, suministrar automáticamente una dirección válida al cliente VPN. Para esto, seleccione la opción "Obtener una dirección automáticamente":

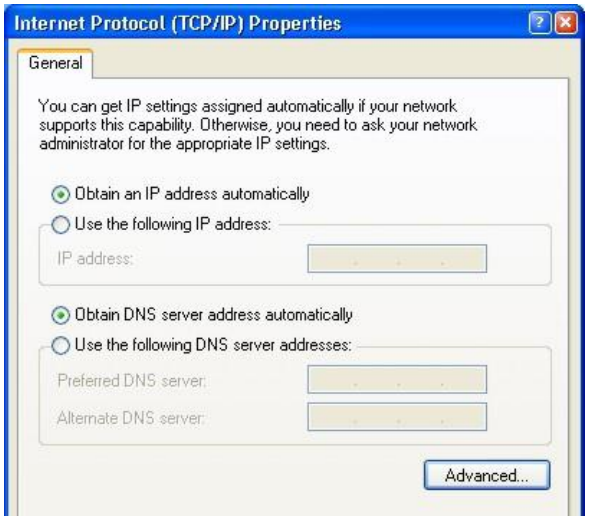


Figura 6.86. ***Configurar Ip para la conexión con VPN***

En la ventana de avanzado la configuramos así: User default Gateway on remote network (Deseleccionado).

Figura 6.87. ***Configuración de wateway para conexión con VPN***

De esa forma se podría configurar el servidor de Vpn y el cliente Vpn en las sucursales ya sea El Vergel y Las Américas.

Se recomienda la creación de un servidor Web Proxy que se utilizará para filtrar el contenido que los usuarios realicen al navegar a través de Internet. Para ello se aplicaran las siguientes políticas:

- Bloqueo de pornografía
- Bloqueo páginas que brinden el servicio de Web Messenger.
- Bloqueo del Live Messenger a través del Proxy.
- Bloqueo de páginas que brinden webmail.
- Bloqueo descarga directa de archivos MP3,MP4 y AVI.
- Bloqueo descarga directa de archivos RAR, ZIP, EXE.

6.7.3.3 Servidor Web Proxy.

Debido a las diferentes aplicaciones que tiene el Mikrotik RouterOS también se puede configurar un servidor Web Proxy para ahorrar ancho de banda utilizado por los usuarios en internet, para ellos nos dirigimos al menú IP / WEB-PROXY como se puede ver en la figura 6.88.

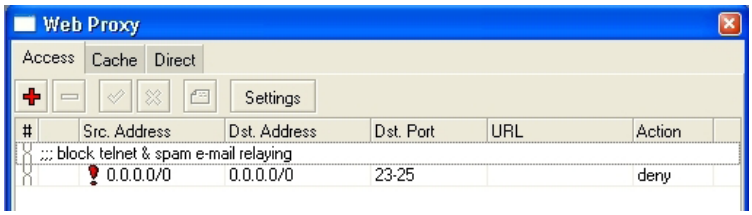


Figura 6.88. ***Ventana web proxy.***

En la ventana que se muestra anteriormente de configuración hacemos clic en SETTINGS. De esta manera entramos a la ventana de configuración del servidor Proxy. Dicha ventana se la configura de la siguiente manera.

- Src. Address: La dejamos en blanco
- Port: 3128
- Hostname: Proxy
- Transparent Proxy: Seleccionado.
- Parent Proxy: lo dejamos en blanco
- Parent Proxy Port: lo dejamos en blanco
- Cache Administrator: adminitrador@pasa.ec
- Maximum Object size: 4096
- Cache Drive: system
- Maximum cache Size : 2000000
- Maximum Ram Cache Size 128000

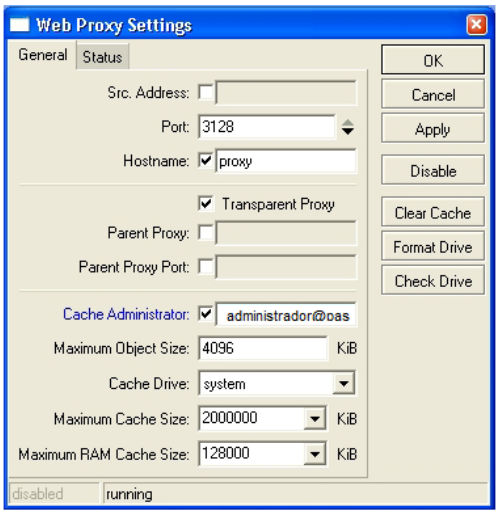


Figura 6.89.*Ventana de configuración servidor proxy.*

Ahora vamos a configurar un redireccionamiento al servidor Proxy según los departamentos que existen en la Pasamanería S.A en la cual vamos a utilizar como ejemplo al departamento de Sistemas.

A continuación hacemos clic en ENABLE. Se nos abre una ventana y hacemos clic en ok.

Como segundo paso debemos generar un una regla en el firewall para que haga un redireccionamiento al servidor Proxy. Para ello nos dirigimos al menú IP / FIREWALL en nuestra ventana de configuración hacemos clic en la pestaña NAT, luego clic en el botón (+). La ventana la configuramos de la siguiente manera.

Interfase : Sistemas

- Chain: dstnat
- Protocol: 6 (tcp)
- Interfase Sistemas

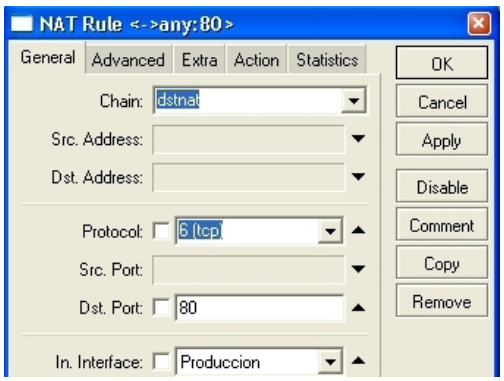


Figura 6.90. *Ventana2 de configuración servidor proxy.*

Luego hacemos clic sobre la pestaña ACTION y configuramos de la siguiente manera:

- Action: Redirect
- To ports: 3128

Figura 6.91. ***Ventana3 de configuración servidor proxy.***

Debemos realizar esta misma configuración para cada una de las interfaces o departamentos que existan en la Pasamanería S.A.

Una vez realizado la configuración con todos los departamentos, por último se configurará el NAT para el ruteo entre todas las subredes de la empresa. Para ello nos dirigimos al menú IP / FIREWALL en nuestra ventana de configuración hacemos clic en la pestaña NAT, luego clic en el botón (+). La ventana se la configura de la siguiente manera.

Pestaña General:

- Chain: srcnat

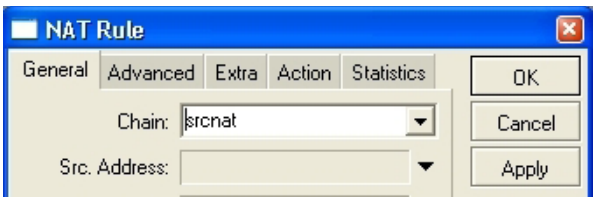


Figura 6.92. ***Configuración del NAT.***

Pestaña Action:

- Action: Masquerade

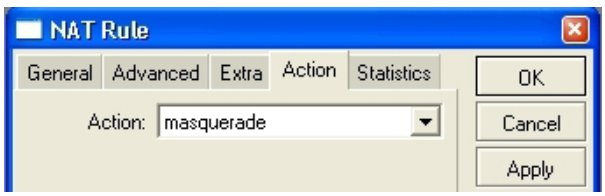


Figura 6.93. ***Configuración regla del NAT.***

Nuestra configuración de políticas de NAT se ven de la siguiente manera:

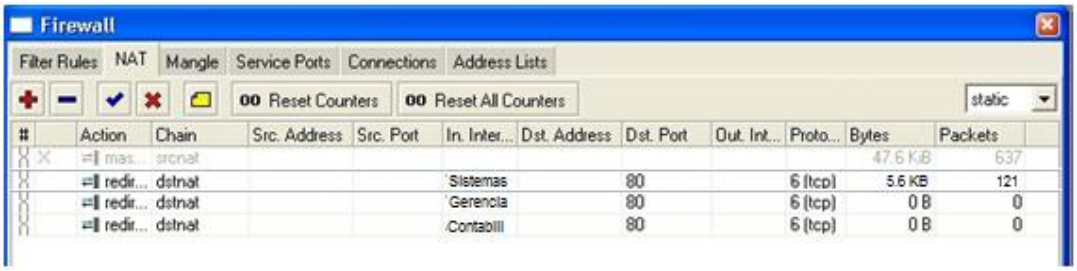


Figura 6.94. ***Políticas del NAT.***

A continuación debemos proteger nuestro servidor de cualquier utilización desde el exterior de la red. Para ello nos dirigimos al menú IP / FIREWALL. En la ventana nueva hacemos clic en la pestaña FILTER RULES, a continuación hacemos clic en el botón (+). Nuestra nueva política de filtrado de paquetes la configuramos de la siguiente manera:

Pestaña: General:

- Chain: input
- Protocol: 6 (tcp)
- Dst. Port.: 3128
- In. Interfase: Telconet

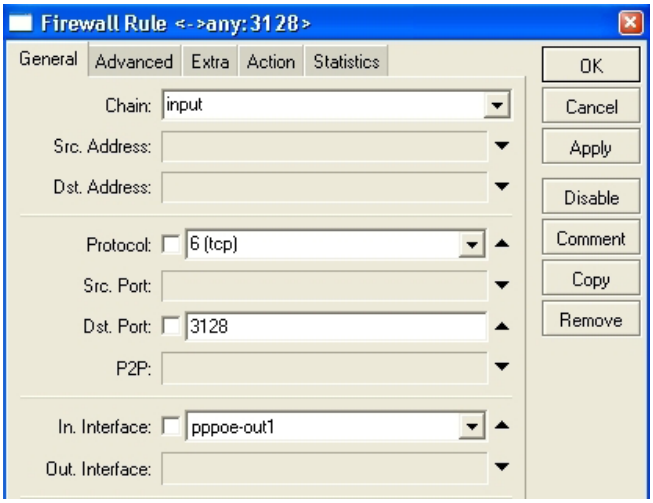


Figura 6.95. ***Ventana de configuración de políticas de filtrado de paquetes en la pestaña General.***

Pestaña Action:

- Action: Drop

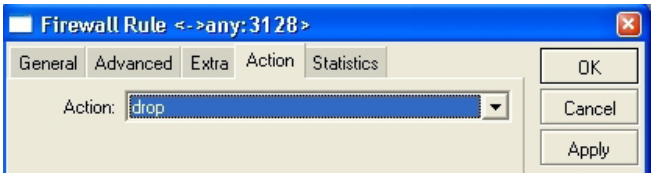


Figura 6.96. ***Ventana de configuración de políticas de filtrado de paquetes en la pestaña Action.***

Ahora veremos en la figura 6.97 la política establecida de filtrado es decir el bloqueo de utilización del proxy desde fuera de la red.

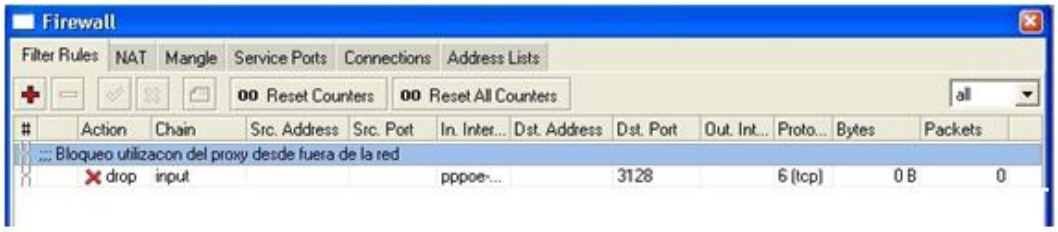


Figura 6.97. ***Política de bloqueo de utilización del proxy desde afuera de la red.***

De igual manera podemos bloquear páginas con la utilización del Web Proxy. Por ejemplo páginas pornográficas, páginas que tengan el servicio de Web Messenger al igual que Yahoo u otras páginas que se desee bloquear.

6.7.3.3.1 Bloqueo de páginas de pornografía.

Para ello nos dirigimos al menú IP / Web Proxy. En la nueva ventana dentro de la pestaña Access hacemos clic en el botón (+). Donde crearemos nuevas políticas que se configuran de la siguiente manera:

Política 1.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *porn*
- Method: any
- Action: deny

Figura 6.98. ***Configuración de bloqueo de páginas pornográficas.***

Política 2.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *sex*
- Method: any
- Action: deny

Figura 6.99. ***Configuración de bloqueo de páginas pornográficas.***

Política 3.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *xxx*

- Method: any
- Action: deny

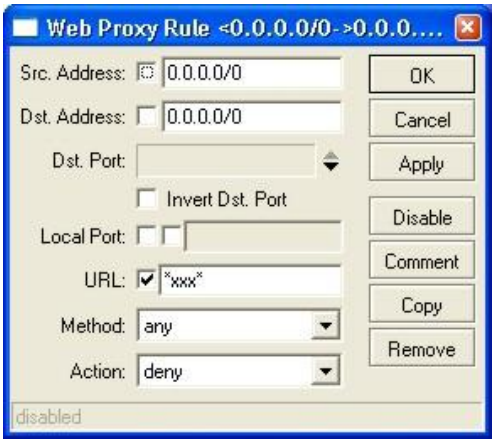


Figura 6.100. ***Configuración de bloqueo de páginas pornográficas.***

Estas tres políticas creadas o filtros nos bloquearan cualquier sitio que posea las palabras *porn*,*sex* y *xxx* en su nombre. También nos sirve debido a que si el usuario busca algo con cualquiera de estas palabras en Google o cualquier otro buscador también nos bloquee la búsqueda.

6.7.3.3.2 Bloqueo de páginas que brinden el servicio de Web Messenger.

De igual forma también se puede realizar el bloqueo de las páginas que brinden el servicio de Web Messenger. Para realizar esta configuración nos dirigimos al menú IP / Web Proxy. En la ventana que aparece dentro de la pestaña Access hacemos clic en el boton (+), para configurar las nuevas políticas de la siguiente manera:

Sitio: www.meebo.com.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *meebo.com*
- Method: any
- Action: deny

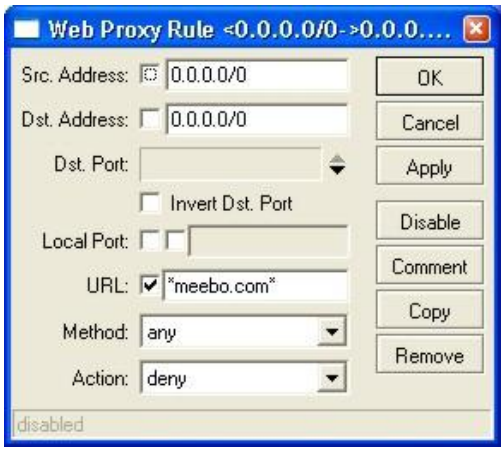


Figura 6.101. ***Bloqueo de la página web meebo.***

También la configuración para los demás sitios se repite de la misma forma:

Sitio: www.ebuddy.com.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: * ebuddy.com*
- Method: any
- Action: deny

Figura 6.102. ***Bloqueo de la página web ebuddy.***

Sitio: www.webmessenger.msn.com.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *webmessenger.msn.com*
- Method: any

- Action: deny

Figura 6.103. ***Bloqueo de la página webmessenger.msn.com***

Sitio: www.webmessenger.yahoo.com.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *webmessenger.yahoo.com*
- Method: any
- Action: deny

Figura 6.104. ***Bloqueo de la página www.webmessenger.yahoo.com.***

De esa forma se puede bloquear las páginas que brindan Web Messenger.

6.7.3.3.3 Bloqueo de páginas de redes sociales.

De igual forma como se puede bloquear páginas que brindan servicio de Web Messenger también se puede bloquear páginas de redes sociales como facebook, hi5, etc.

Sitio: www.facebook.com.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *facebook.com*
- Method: any
- Action: deny

Figura 6.105. ***Bloqueo de la página web facebook.com.***

Sitio: www.hi5.com.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *hi5.com*
- Method: any
- Action: deny

Figura 6.106. ***Bloqueo de la página web www.hi5.com.***

De esa forma podemos hacer con las diferentes redes sociales que se desee bloquear.

6.7.3.3.4 Bloqueo del Live Messenger.

Para realizar el bloqueo del Messenger utilizamos la siguiente política en el Web Proxy.

Para realizar esa política se sigue los siguientes pasos. Nos dirigimos al menú IP / Web Proxy. En la ventana que aparece dentro de la pestaña Access hacemos clic en el botón (+). La nueva política se configura de la siguiente manera:

Bloqueo Messenger.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *Gateway.messenger.*
- Method: any
- Action: deny

Figura 6.107. ***Bloqueo de la pagina web gateway.messenger.***

6.7.3.3.5 Bloqueo de páginas que brinden webmail.

También se puede realizar el bloqueo de páginas que brinden webmail como hotmail.com y mail.yahoo.com, etc. Para realizar este bloqueo de páginas debemos realizar la siguiente política en el Web Proxy. Para ello realizamos los siguientes pasos:

Nos dirigimos al menú IP / Web Proxy. En la ventana que aparece en la pestaña Access hacemos clic en el botón (+). La política que se debe de configurar es de la siguiente manera:

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *mail*
- Method: any
- Action: deny

Figura 6.108. ***Bloqueo de la página de web mail.***

6.7.3.3.6 Bloqueo para las descargas de archivos MP3 y AVI.

Para realizar el bloqueo de las descargas de archivos MP3, MP4, AVI, WMA entre otros debemos realizar la siguiente política en el Web Proxy. Para ello debemos realizar los siguientes pasos:

Nos dirigimos al menú IP / Web Proxy. En la ventana que se abre dentro de la pestaña.

Access hacemos clic en el botón (+). Las políticas que se deben de configurar son de la siguiente manera:

Bloqueo de archivos Mp3.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.mp3*
- Method: any

- Action: deny

Figura 6.109. ***Bloqueo de la página web para descargar archivos MP3.***

Bloqueo de archivos Mp4.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.avi*
- Method: any
- Action: deny

Figura 6.110. ***Bloqueo de páginas web para descargar archivos MP4.***

Bloqueo de archivos Avi.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.avi*
- Method: any

- Action: deny

Figura 6.111. ***Bloqueo de páginas web para descargar archivos AVI.***

6.7.3.3.7 Bloqueo descarga directa de archivos RAR, ZIP, EXE.

También si se quisiera bloquear archivos como RAR, ZIP, EXE debemos realizar las siguientes políticas en el Web Proxy. Para realizar esa configuración o políticas debemos realizar los siguientes pasos:

Nos dirigimos al menú IP / Web Proxy. En la ventana que se abre dentro de la pestaña Access hacemos clic en el botón (+). Las políticas que se deben de configurar son de la siguiente manera:

Bloqueo de archivos RAR.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.rar*
- Method: any
- Action: deny

Figura 6.112. ***Bloqueo de archivos RAR.***

Bloqueo de archivos ZIP.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.zip*
- Method: any
- Action: deny

Figura 6.113. ***Bloqueo de archivos ZIP.***

Bloqueo de archivos EXE.

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.exe*
- Method: any
- Action: deny

Figura 6.114. ***Bloqueo de archivos EXE.***

Una vez realizadas todas las políticas de cada sitio o página que se bloqueo las políticas del servidor Web Proxy se puede ver en la figura 6.115.

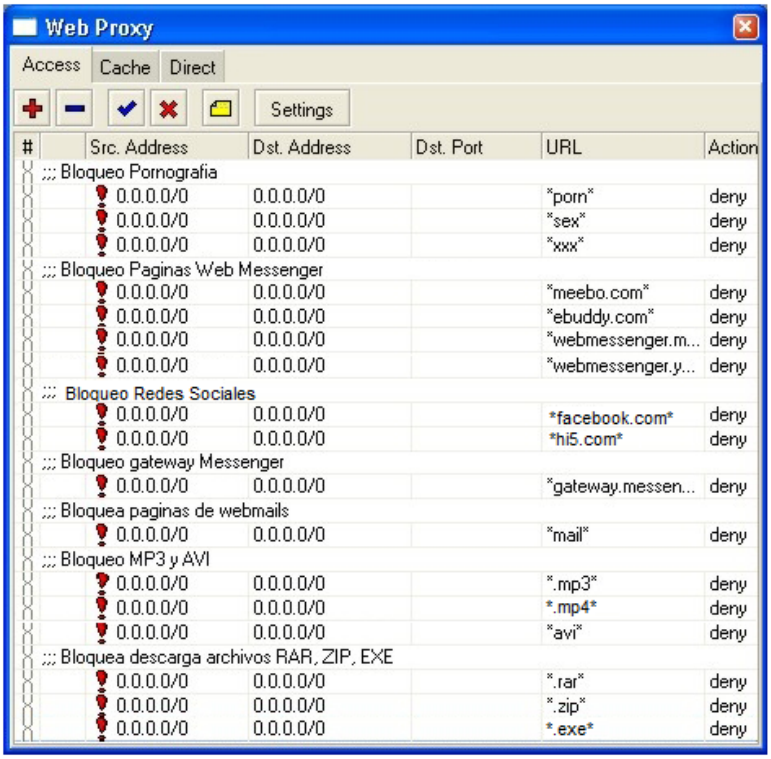


Figura 6.115. ***Vista de páginas bloqueadas.***

6.7.3.4 Modelado de colas.

Se recomienda el modelado de colas que se utilizará para asignarle un determinado ancho de banda a cada una de las sub redes. Al igual que se utilizará el modelado de colas para el control de ancho de banda para los clientes P2P.

6.7.3.4.1 Control de ancho de banda.

6.7.3.4.1.1 Asignación de ancho de banda por sub red o departamentos.

También con ayuda del Mikrotik RouterOS se puede asignar ancho de banda por departamentos debido a que existen usuarios que realizan el mal uso del ancho de banda, se podría implementar si lo fuera necesario, agregando políticas en el router para poder controlar este problema.

Donde para los distintos departamentos se lo podría asignar un distinto ancho de banda a continuación se pondrá ejemplos de cómo se debería asignar el ancho de banda a cada departamento cabe recalcar que el tamaño de ancho de banda que se ponga a continuación es como ejemplo ya que si se implementaría esta opción el Administrador de la Red pondrá los valores que sean acorde a cada departamento.

Sistemas:

- Subida 350 M/Bits
- Bajada 400 M/Bits

Contabilidad:

- Subida 300 M/bits
- Bajada 200 M/bits

Gerencia:

- Subida 300 M/bits
- Bajada 350 M/bits

Para realizar el control de ancho de banda debemos ir al menú QUEUES, donde se abrirá una ventana de configuración como se puede ver en la figura 6.116.

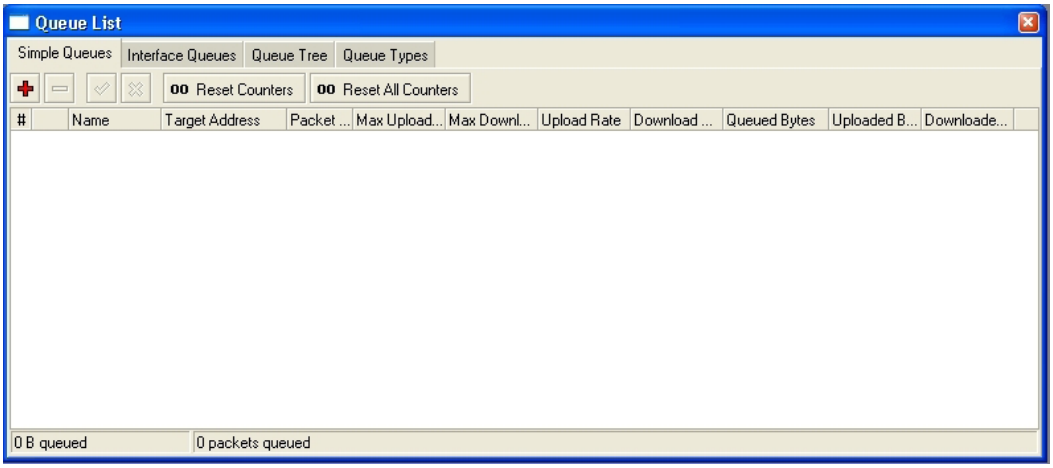


Figura 6.116. ***Ventana 1 de configuración de ancho de banda.***

Donde debemos hacer clic en el botón (+) de la pestaña Simple Queues. Una vez hecho clic en el botón (+) se abrirá una nueva ventana para configurar la nueva cola.

Departamento de Sistemas:

Pestaña General:

- Name: Queue_Sistemas
- Target Address: 192.168.1.160/28
- Max Limit: 350M (upload) , 400M (download)

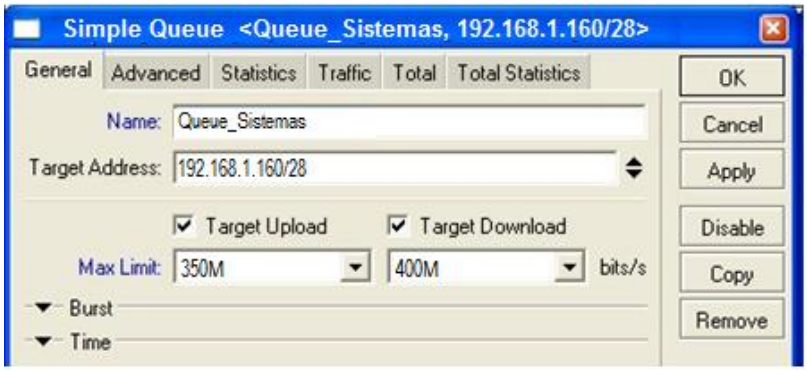


Figura 6.117. ***Ventana 2 de configuración de ancho de banda.***

Departamento de Contabilidad:

Pestaña General:

- Name: Queue_Contabilidad
- Target Address: 192.168.1.176/28
- Max Limit: 300M (upload) , 200M (download)

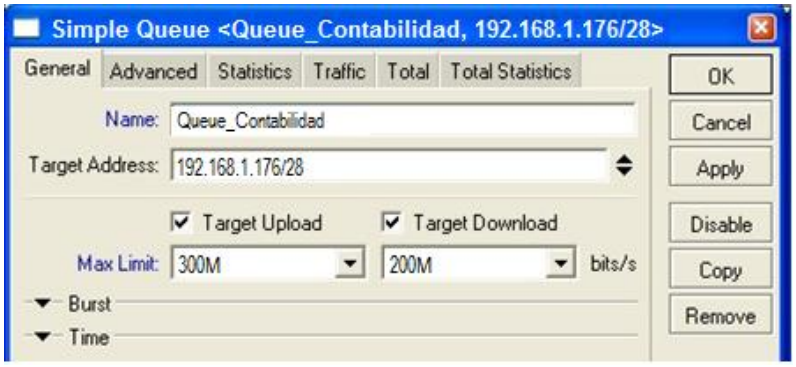


Figura 6.118. ***Ventana 3 de configuración de ancho de banda.***

Departamento de Gerencia:

Pestaña General:

- Name: Queue_Gerencia
- Target Address: 192.168.1.144/28
- Max Limit: 300M (upload) , 350M (download)

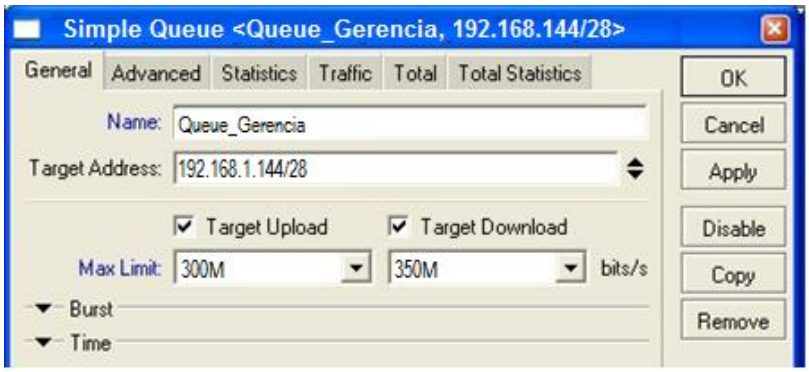


Figura 6.119. ***Ventana 4 de configuración de ancho de banda.***

Las colas configuradas para cada departamento se pueden ver en la figura 6.120.

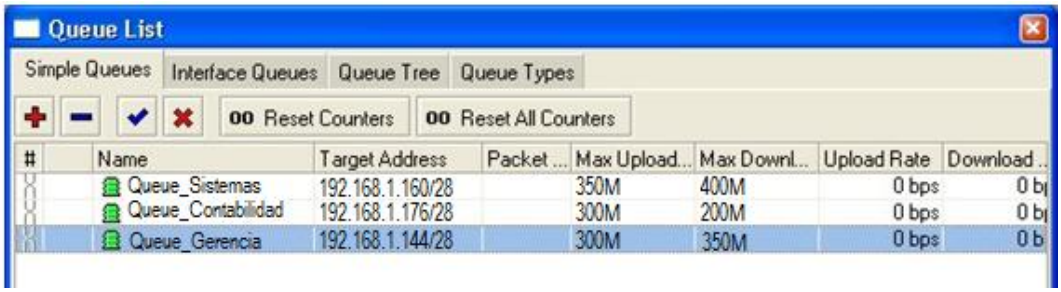


Figura 6.120. ***Ventana 5 de configuración de ancho de banda.***

6.7.3.5 Traffic Shaping de (P2P).

Esta política se la podría aplicar pero depende de las personas responsables de la Pasamanería en este caso de los Gerentes, esta política trata de que se pueda utilizar los P2P a cualquiera de los departamentos que se desee. Anteriormente se había recomendado asignar un ancho de banda para los departamentos de la Pasamanería ahora debemos modelar las colas del tráfico para que los P2P no consuman todo el tráfico dependiendo del departamento que se quiera aplicar esta política.

Para ello debemos ir al menú IP / FIREWALL. Donde se nos abrirá una ventana de configuración de políticas del firewall. Ahora debemos hacer clic sobre la pestaña Mangle, y a continuación debemos hacer clic sobre el botón (+).

Se abrirá una ventana que se la puede ver en la figura 6.121 donde se configurará lo siguiente:

- Chain: prerouting
- P2P: all-p2p

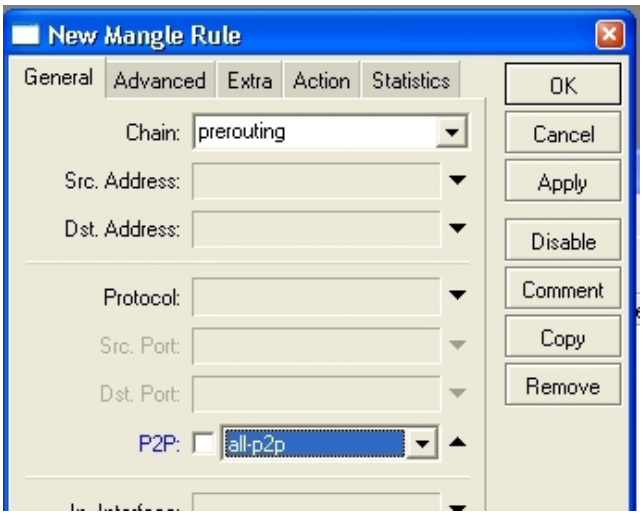


Figura 6.121. ***Ventana 1 de configuración de Traffic Shaping de (P2P).***

Luego debemos hacer clic en la pestaña Action, donde la configuración será la siguiente:

- Action: mark_connection
- New Connection Mark: (tipeamos) connexion_p2p
- Passthough (seleccionado).

Figura 6.122. ***Ventana 2 de configuración Traffic Shaping de (P2P).***

Luego de haber hecho esa configuración ahora vamos dentro de la pestaña Mangle para hacer nuevamente clic en el botón (+) para crear una nueva regla, la configuración es la siguiente:

- Chan: prerouting
- Connection Mark: conexión_p2p (la que habíamos creado anterior mente)

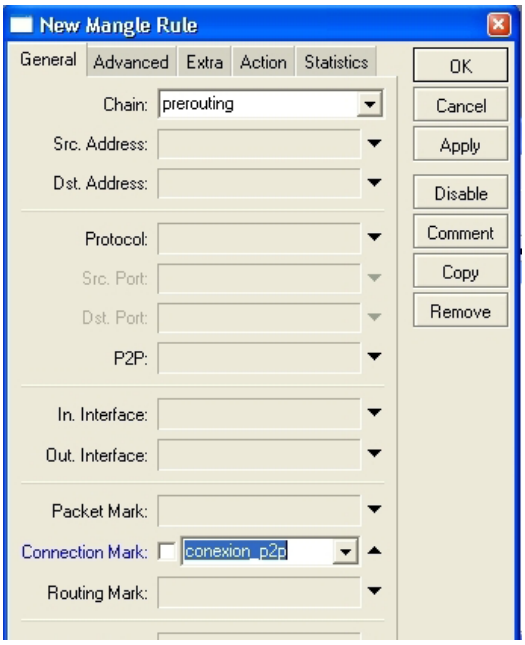


Figura 6.123. ***Ventana 3 de configuración Traffic Shaping de (P2P).***

Luego de haber hecho esa configuración nos dirigimos a la pestaña Action, en la cual la configuraremos de la siguiente manera:

- Action: Mark Packet
- New Packet Mark: p2p

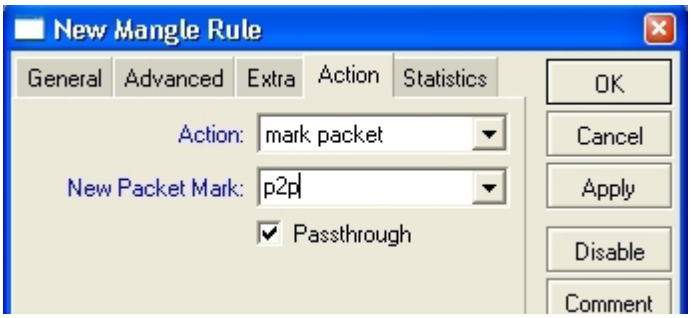


Figura 6.124. ***Ventana 4 de Configuración Traffic Shaping de (P2P).***

Una vez realizada dicha configuración ahora debemos configurar las políticas para que nos marque los paquetes p2p para poder bloquearlos en las otras redes.

Para realizar esta configuración debemos ir al menú IP /FIREWALL. Donde debemos hacer clic en la pestaña mangle y hacer clic en el botón (+), donde se abrirá una ventana la cual se la puede ver en la figura 6.125, ahora en la pestaña General configuraremos esta nueva política de la siguiente manera:

- Chain: prerouting

- Connection Mark: conexión_p2p

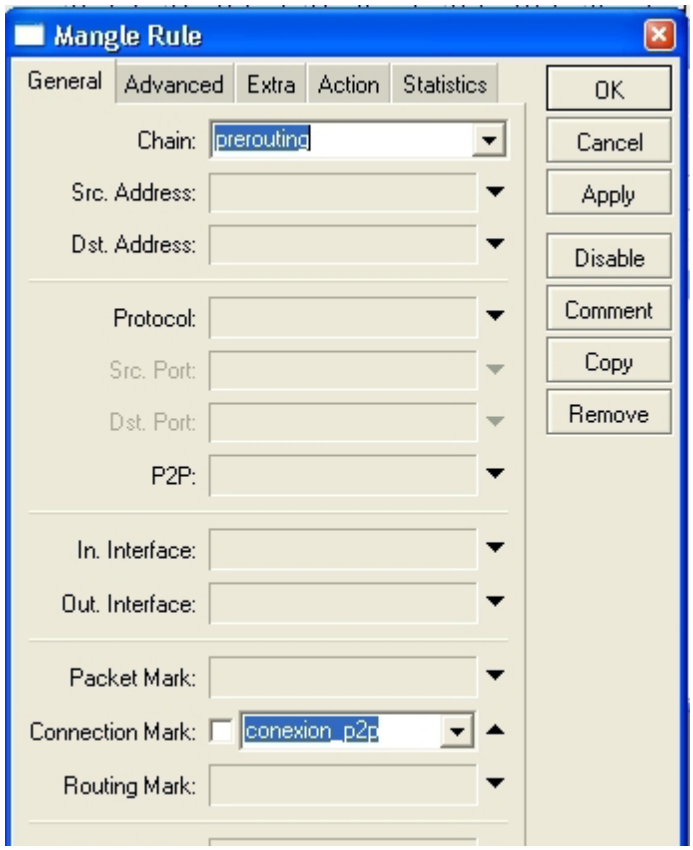


Figura 6.125. ***Ventana 5 de configuración Traffic Shaping de (P2P).***

Una vez realizada la configuración en la pantalla anterior, ahora nos dirigiremos a la pestaña Action para realizar la configuración siguiente la cual se puede ver en la figura 6.126:

- Action: mark packet
- Packet mark: p2p_bloqueado
- Pass though: (seleccionado)

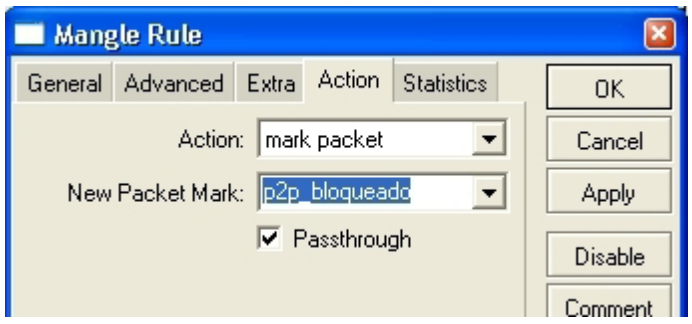


Figura 6.126. ***Ventana 6 de configuración Traffic Shaping de (P2P).***

Realizada la creación de las reglas anteriores se verán de la siguiente manera en la figura 6.127.

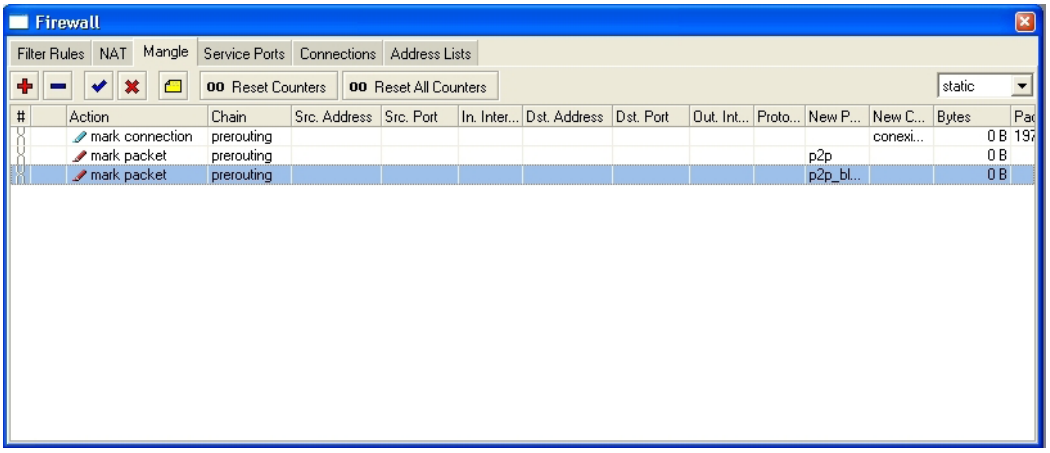


Figura 6.127. ***Ventana 7 de configuración Traffic Shaping de (P2P).***

Como anteriormente ya se configuró la asignación del ancho de banda para los departamentos y también la configuración de acceso a los P2P de determinado departamento que se le quisiera realizar esa configuración, para que los P2P no ocuparan todo el tráfico se debe de realizar las siguientes dos nuevas colas para las políticas de los P2P.

Para ello nos dirigimos al menú QUEUES. En la ventana que se nos aparecerá donde crearemos las dos políticas de los P2P, ahora debemos hacer clic sobre la pestaña Queue Tree. Y después hacemos clic sobre el botón (+).

La configuración de la cola de entrada será la siguiente la cual se puede ver en la figura 6.128:

- Name: Queue_p2p_in
- Parent: Global-in
- Packet Mark: p2p
- Queue Type: default
- Priority: 8
- Max Limit: 256k

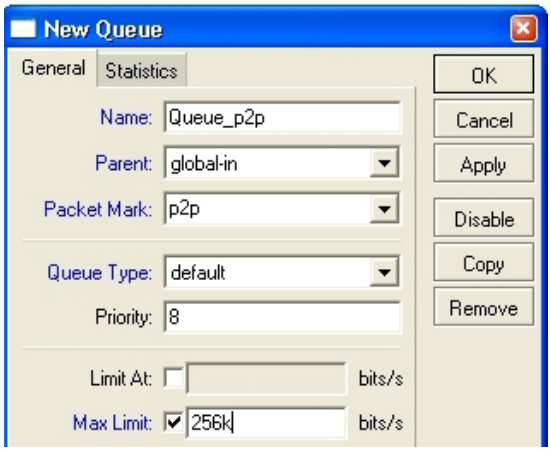


Figura 6.128. ***Ventana 7 de Configuración Traffic Shaping de (P2P).***

Ahora para la segunda cola hacemos clic en el botón (+) y generamos una nueva cola.

La configuración de la cola de salida es de la siguiente manera la misma que se puede ver en la figura 6.129:

- Name: Queue_p2p_out
- Parent: global-out
- Packet Mark: p2p
- Queue type: default
- Priority: 8
- Max Limit: 256k

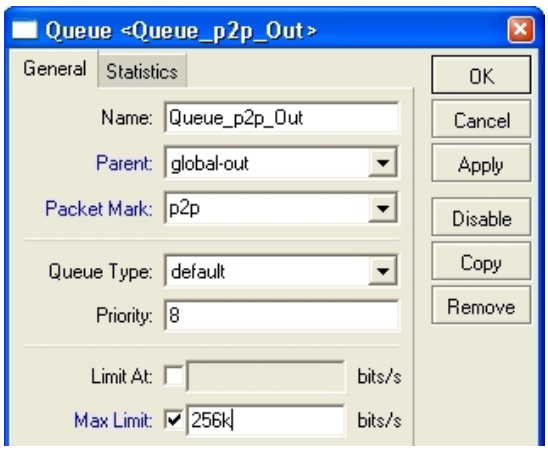


Figura 6.129. ***Ventana 7 de Configuración Traffic Shaping de (P2P).***

6.7.3.6 Firewall.

Se recomienda la utilización del Firewall para realizar las siguientes actividades:

- Bloqueo de los P2P para las subredes.

- Bloqueo del cliente MSN Live Messenger.
- Descartar conexiones inválidas.
- Aceptar conexiones establecidas.
- Acepta Trafico UDP.
- Descarta excesivos paquetes de icmp.
- Descarta el resto de las conexiones externas.

6.7.3.6.1 Bloqueo de los P2P para las subredes.

Los P2P son básicamente programas que utilizan una red común para comunicar entre si las computadoras de sus usuarios, los que comparten ciertos directorios donde se encuentran los archivos a intercambiar.

Uno de los peligros es el intercambio de archivos que no son lo que dicen ser, o que directamente se tratan de virus, gusanos o troyanos camuflados, esta es una de las más importantes fuentes de propagación e infección.

Pero también es más grave la instalación de otros programas no deseados como Spywares o Adwares que estas aplicaciones esconden.

Los programas espías o Spyware son usados por los patrocinadores de los productos P2P, para así obtener información sobre sitios que visita el usuario, cuáles son sus preferencias o que archivos prefiere descargar.

En muchas ocasiones, esto incluye información más comprometida, con datos más personales, siempre con la idea de enviar más publicidad basura.

También permite especificar que banners publicitarios que se muestran son los que se llaman como Adware, o sea los programas que se instalan para descargar y mostrar publicidad. Y de igual se empieza a recibir más spam a través del correo electrónico.

En las aplicaciones que se encuentran dicho problemas están los conocidos como el Ares, KaZaa programas para bajar música.

Una vez explicado de que se trata los P2P se recomienda configurar los P2P bloqueando para las subredes en este caso los departamentos que tiene la Pasamanería esta configuración dependerá de lo que se diga en Gerencia o el

Administrador de la red ya que también se puede dar acceso a los P2P como se configuró anteriormente si se lo desea.

Para realizar la configuración de bloqueo de dicho tráfico es de la siguiente manera:

Para ello nos dirigimos a IP / FIREWALL. En la ventana que se nos abre debemos hacer clic en el botón (+). Donde se nos abrirá una nueva ventana la cual se puede ver en la figura 6.130 donde se configurara de la siguiente manera:

Pestaña general:

- Chain: forward
- P2P: all-p2p
- Out. Interface: Contabilidad

Ponemos a contabilidad como ejemplo para realizar esta configuración, de igual manera se la puede permitir el tráfico de los P2P en este departamento.

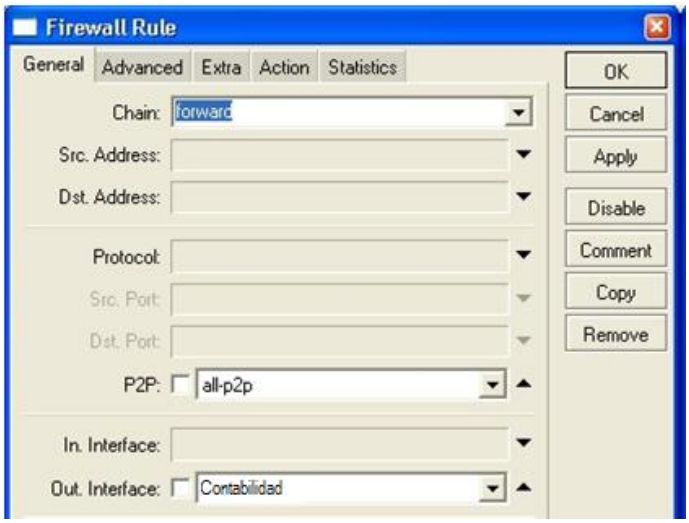


Figura 6.130. ***Ventana 1 bloqueo de los P2P para las subredes.***

Luego debemos ir a la pestaña Action para realizar la siguiente configuración la misma que se puede ver en la figura 6.131:

- Action: drop

Figura 6.131. ***Ventana 2 bloqueo de los P2P para las subredes.***

De esa manera podemos configurar el bloqueo del tráfico de los P2P en cada uno de los departamentos que se crea necesario implementar.

6.7.3.6.2 Bloqueo del cliente MSN Live Messenger.

Se recomienda esta configuración para evitar que los empleados no pudieran utilizar el MSN Live Messenger por el cual perderían demasiado tiempo en la utilización del mismo. Para ello se deben especificar las siguientes políticas de firewall.

Debemos ir al menú a IP/FIREWALL, en la ventana que se abrirá hacemos clic el botón (+). Donde se nos aparecerá una ventana la cual se puede ver en la figura 6.132 donde se configurará de la siguiente manera:

Primera política de firewall:

Pestaña General:

- Chain: Forward
- Protocol: Tcp (6)
- Dst. Port: 1863

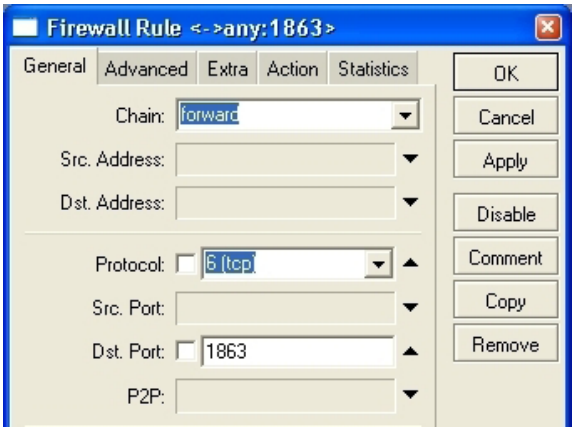


Figura 6.132. ***Ventana 1 bloqueo del cliente MSN Live Messenger.***

Luego de haber configurado en la pestaña General nos dirigimos a la pestaña Action que se la puede ver en la figura 6.133 donde se realiza la siguiente configuración:

- Action: Drop

Figura 6.133. ***Ventana 2 bloqueo del cliente MSN Live Messenger.***

Segunda política de Firewall, de la misma forma que se configuró la primera política realizamos la configuración de igual forma se la puede ver en la figura 6.134.

Pestaña General:

- Chain: Forward
- Protocol: Tcp (6)
- Dst. Port: 5190

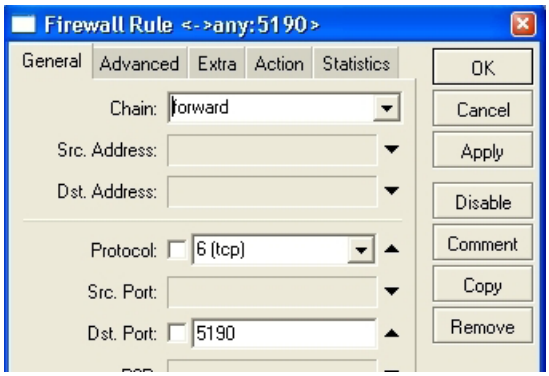


Figura 6.134. ***Ventana 3 bloqueo del cliente MSN Live Messenger.***

Ahora nos dirigimos a la pestaña Action para realizar la configuración como se puede ver en la figura 6.135.

- Action: Drop

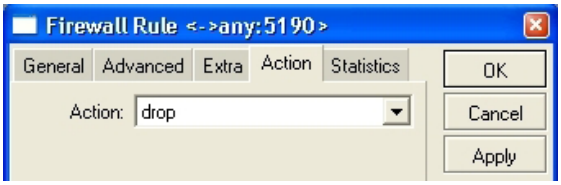


Figura 6.135. ***Ventana 4 bloqueo del cliente MSN Live Messenger.***

Tercera política de Firewall esta configuración se la puede ver en la figura 6.136:

Pestaña General:

- Chain: Forward
- Protocol: Tcp (6)
- Dst. Port: 6901

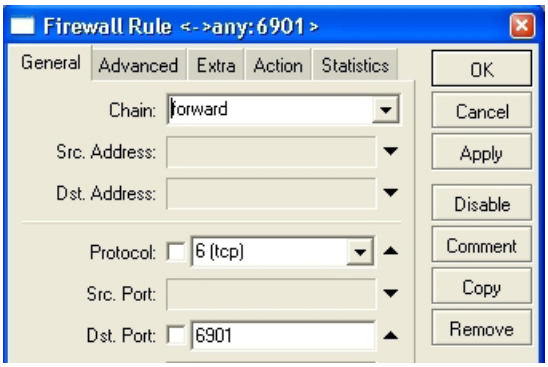


Figura 6.136. ***Ventana 5 bloqueo del cliente MSN Live Messenger.***

Pestaña Action: en esta pestaña se realiza la siguiente configuración que se la puede ver en la figura 6.137.

- Action: Drop

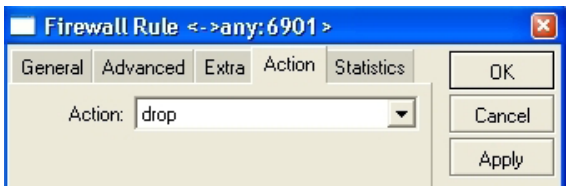


Figura 6.137. ***Ventana 6 bloqueo del cliente MSN Live Messenger.***

Cuarta política de Firewall: esta cuarta política se la puede ver en la figura 6.138.

- Pestaña General:
- Chain: Forward
- Protocol: Tcp (6)
- Dst. Port: 6891-6900

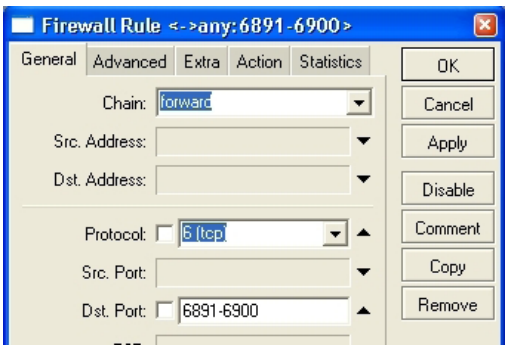


Figura 6.138. ***Ventana 7 bloqueo del cliente MSN Live Messenger.***

Pestaña Action: esta configuración se la puede ver en la figura 6.139.

- Action: Drop

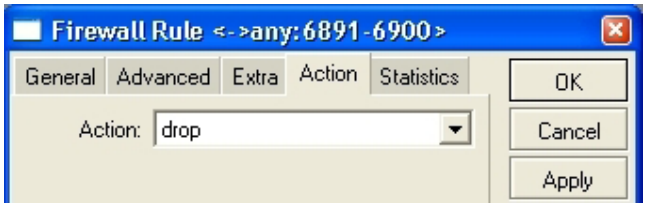


Figura 6.139. ***Ventana 8 bloqueo del cliente MSN Live Messenger.***

Los puertos que se han bloqueado tienen relación con el MSN Live Messenger los cuales se detalla cada uno a continuación:

- Puerto 1863, este puesto es del Windows Live Messenger.
- Puerto 5190, este puerto es un cliente de mensajería instantánea de América On Line.
- Puerto 6901, este puesto es para las comunicaciones de voz.
- Puertos 6891-6900, permite el envió de archivos.

Finalizada dichas configuraciones ningún usuario podrá conectarse al MSN Live Messenger.

6.7.3.6.3 Puerto 1723 PPTP que permite las redes privadas virtuales.

Para aceptar conexiones al puerto 1723 desde el exterior debemos realizar los siguientes pasos. Par ello debemos ir al menú IP / FIREWALL. Donde haremos clic en la pestaña FILTER RULES. Después debemos hacer clic en el botón (+). Donde se abrirá una venta la cual se puede ver en la figura 6.140 en la cual se realizará las siguientes configuraciones:

Primera política es para aceptar el tráfico al puerto 1723 tcp.

Pestaña General:

- Chain: input
- Protocol 6 (tcp)
- Dst. Port: 1723

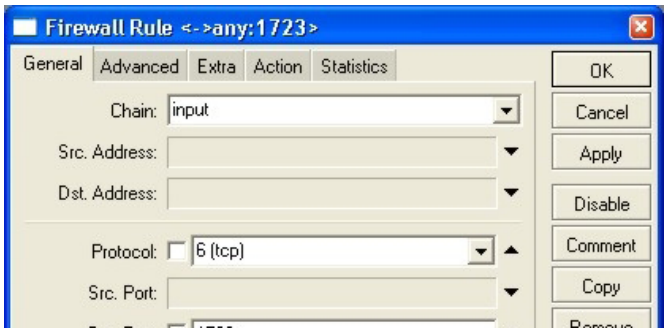


Figura 6.140. ***Ventana para aceptar el tráfico al puerto 1723.***

Luego nos situamos en la pestaña Action donde realizamos la siguiente configuración la misma que se la puede ver en la figura 6.141.

- Action: accept

Figura 6.141. ***Ventana Action para aceptar la regla..***

Segunda política es para aceptar todo el tráfico al puerto 1723 UDP la misma configuración se la puede ver en la figura 6.142.

Pestaña General:

- Chain: input
- Protocol17 (udp)
- Dst. Port: 1723

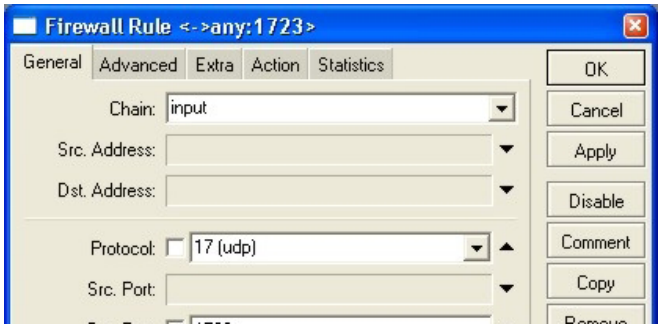


Figura 6.142. ***Ventana para aceptar el tráfico al puerto 1723 UDP.***

Por último realizaremos todas las configuraciones donde aceptaremos todas las comunicaciones que estén establecidas, esta configuración se la puede ver en ala figura 6.143.

Pestaña General:

- Chain: input
- Connection State: established

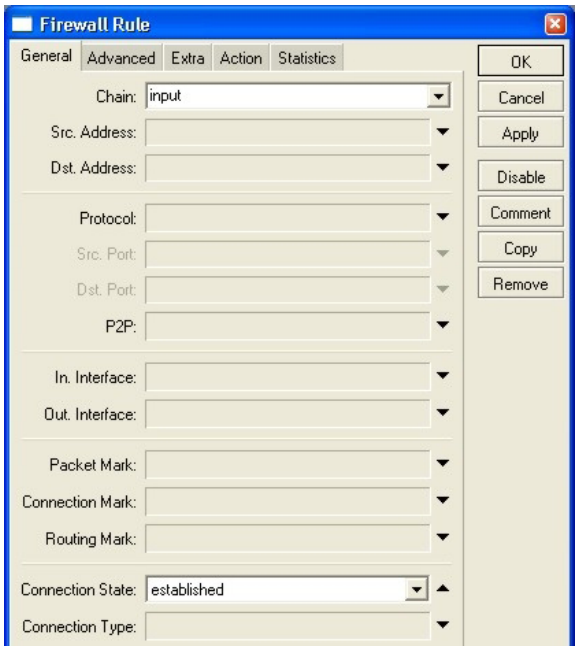


Figura 6.143. ***Ventana para configurar para aceptar todas las comunicaciones establecidas.***

Pestaña Action: en esta pestaña se configura lo siguiente la misma que se la puede ver en la figura 6.144.

- Action: accept

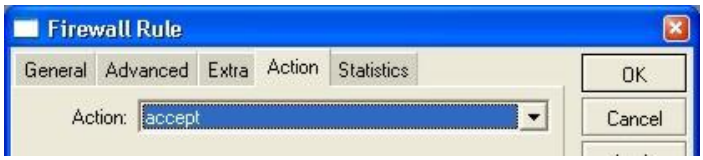


Figura 6.144. ***Ventana Action para aceptar todas las conexiones establecidas.***

6.7.3.6.4 Descartar conexiones inválidas.

Para descartar las conexiones inválidas desde el exterior debemos realizar los siguientes pasos. Ir al menú IP / FIREWALL. Hacer clic en la pestaña FILTER RULES.

Luego hacer clic en el botón (+). A la nueva ventana la configuramos de la siguiente manera, esta configuración se la puede ver en la figura 6.145:

Pestaña General:

- Chain: input
- Connection State: Invalid

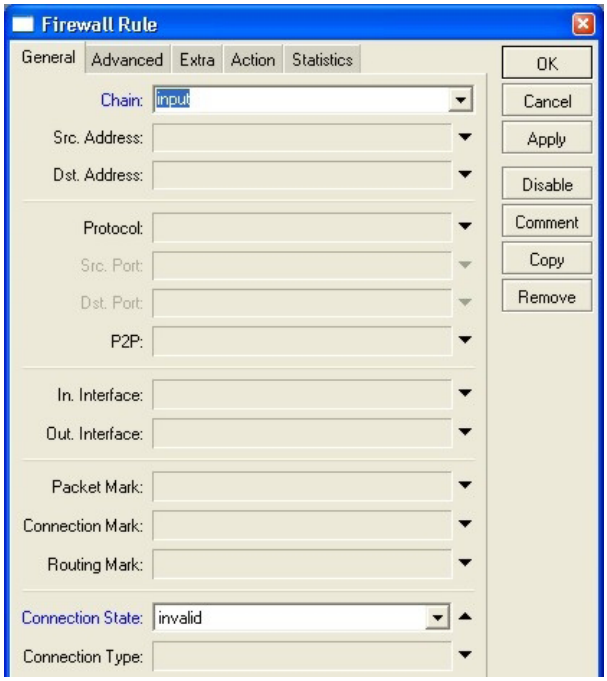


Figura 6.145. ***Ventana 1 descartar conexiones inválidas.***

Pestaña Action: en esta pestaña se configura lo siguiente la misma que se la puede ver en la figura 6.146.

- Action: drop

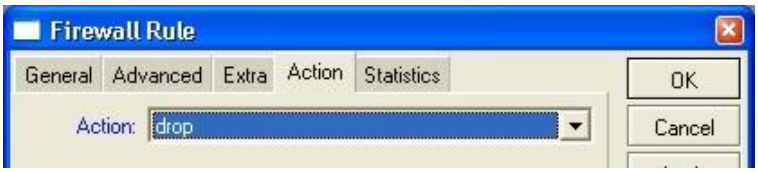


Figura 6.146. ***Ventana 2 descartar conexiones inválidas.***

6.7.3.6.5 Aceptar conexiones establecidas.

Para aceptar las conexiones establecidas desde el exterior debemos realizar los siguientes pasos. Donde debemos ir al menú IP / FIREWALL. En el cual haremos clic en la pestaña FILTER RULES.

Después haremos clic en el botón (+), donde se nos abrirá una ventana la cual podemos ver en la figura 6.147 en la cual se realizará la siguiente configuración:

Pestaña General:

- Chain: input
- Connection State: established

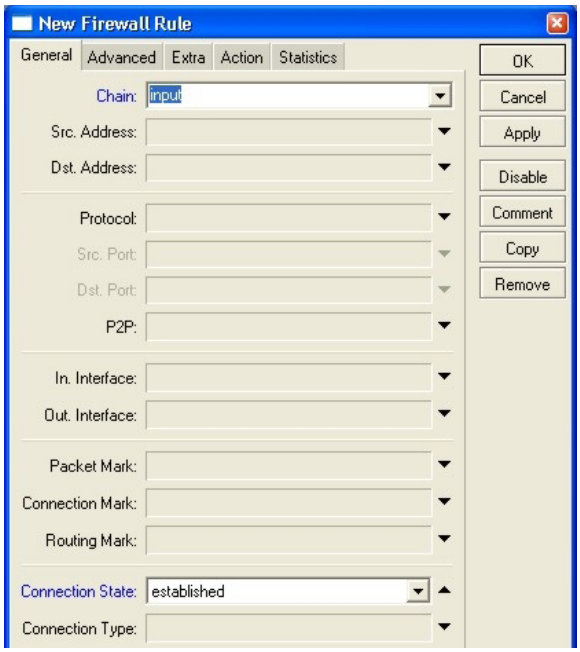


Figura 6.147. ***Ventana 3 descartar conexiones inválidas.***

Luego de haber realizado la configuración en la pestaña General debemos ir a la pestaña Action para realizar la siguiente configuración, la misma que se la puede ver en la figura 6.148:

Pestaña Action:

- Action: accept

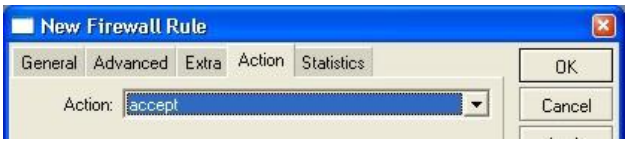


Figura 6.148. ***Ventana 4 descartar conexiones inválidas.***

6.7.3.6.6 Acepta el Trafico UDP.

Para aceptar las conexiones UDP establecidas desde el exterior debemos realizar los siguientes pasos. Donde debemos ir al menú IP / FIREWALL. Donde debemos hacer clic en la pestaña FILTER RULES. Luego hacemos en el botón (+). Se nos aparcera

una ventana la cual se puede ver en la figura 6.149 donde se configurará de la siguiente manera:

Pestaña General:

- Chain: input
- Protocol: 17 (udp)

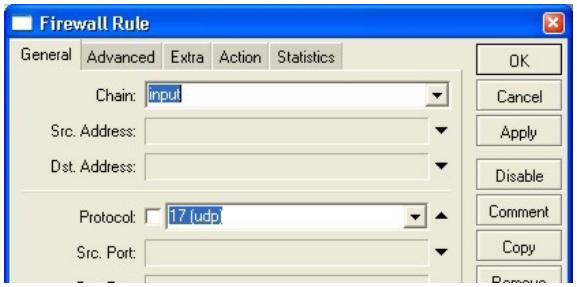


Figura 6.149. ***Ventana 5 Descartar conexiones inválidas.***

Luego nos dirigimos a la pestaña Action donde configuramos lo siguiente, de igual forma se la puede ver en la figura 6.150:

Pestaña Action:

- Action: accept

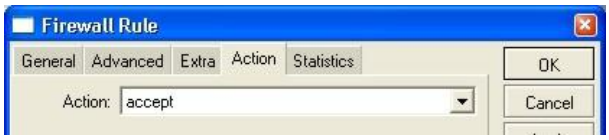


Figura 6.150. ***Ventana 6 descartar conexiones inválidas.***

6.7.3.6.7 Descartar excesivos icmp.

Para descartar excesivos icmp desde el exterior debemos realizar los siguientes pasos:

Donde debemos ir al menú IP / FIREWALL. Hacemos clic en la pestaña FILTER RULES. Luego hacemos clic en el botón (+). Se nos abrirá una ventana la cual se puede ver en la figura 6.151 donde se configurará de la siguiente manera:

Pestaña General:

- Chain: input
- Protocol: 1 (icmp)

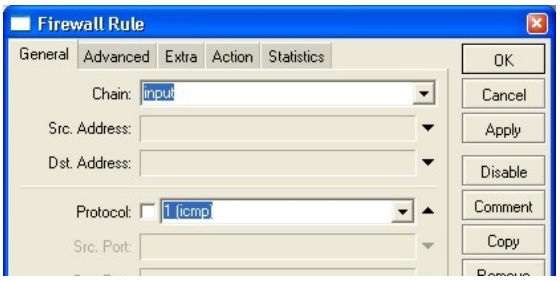


Figura 6.151. ***Ventana 1 descartar excesivos icmp.***

Luego de haber configurado en la pestaña General debemos ir a la pestaña Action para realizar la siguiente configuración, la misma que se la puede ver en la figura 6.152:

Pestaña Action:

- Action: Drop

Figura 6.152. ***Ventana 2 descartar excesivos icmp.***

Ahora se mostrará como quedaron las políticas configuradas en el Firewall la cual se puede ver en la figura 6.153.

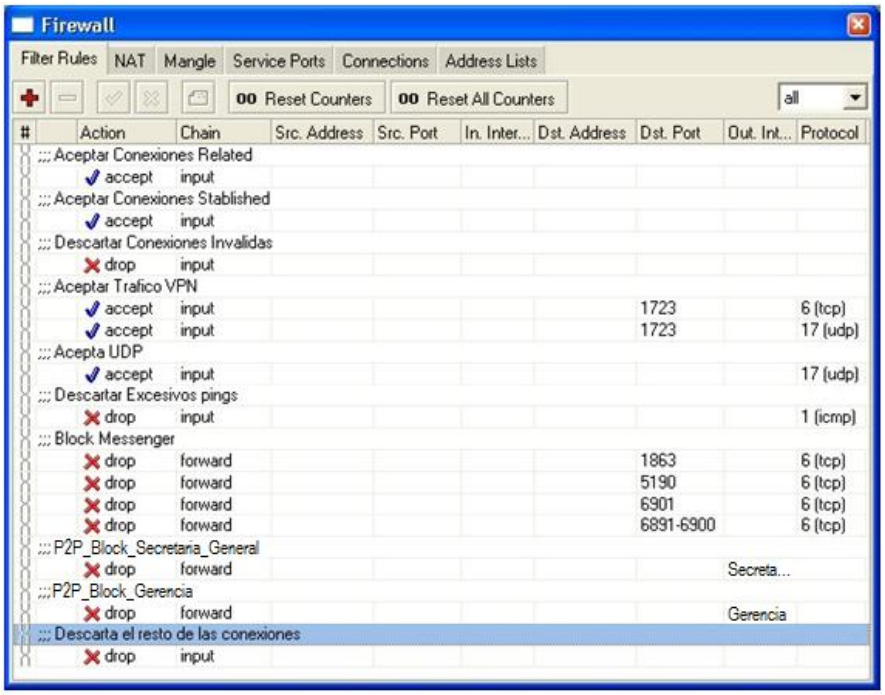


Figura 6.153. ***Políticas configuradas en el Firewall.***

6.8 Recomendación de configuración de los Switches 3Com.

Los switch que tienen en la Pasamanería S.A son los 3Com 2250 de 48 puertos y 3Com 2226 de 24 puertos, los mismos que son utilizados para cada uno de los departamentos que existen en la Pasamanería, son utilizados como punto de conexión entre las máquinas y los switch sin ninguna configuración en los mismos, se recomienda que se administren estos switch ya que tienen esta capacidad para ser administrados por ejemplo con la creación de Vlans para cada departamento que existe en la Pasamanería S.A para así evitar los congestionamientos en la red y un mejor desempeño de la misma.

6.8.1 Switch 3Com Baseline Switch 2250 Plus.

Ahora se indicará como se configura el switch 2250 para realizar la administración en el mismo para un mejor desempeño de la red.

6.8.1.1 Conexión a una interfaz Web.

El switch tiene incorporado una interfaz web que se puede utilizar para establecer la contraseña de administrador, cambiar la dirección IP que se asigna al switch y realizar una configuración avanzada.

6.8.1.2 Requisitos para acceder a la interfaz Web.

Para acceder a la interfaz web se necesita lo siguiente:

- La aplicación Discovery, que se incluye en el 3Com Baseline Switch 2250 Plus que viene en un CD que es suministrado con el Switch.
- Un equipo que se conecte al switch y que tenga un navegador Web.

6.8.1.3 Ejecución de la aplicación Discovery.

En el cd que viene con el Switch se encuentra la aplicación, para ejecutar esta aplicación se debe realizar lo siguiente:

- En el equipo que se encuentra conectado con el switch insertamos el Cd en la unidad de CD del equipo.

- La aplicación deberá iniciarse automáticamente, si no lo hace dentro del CD entramos en una carpeta llamada Discovery y a continuación hacemos doble clic en discovery.exe.

Una vez que corra el programa aparecerá una pantalla de bienvenida que se puede ver en la figura 6.154.

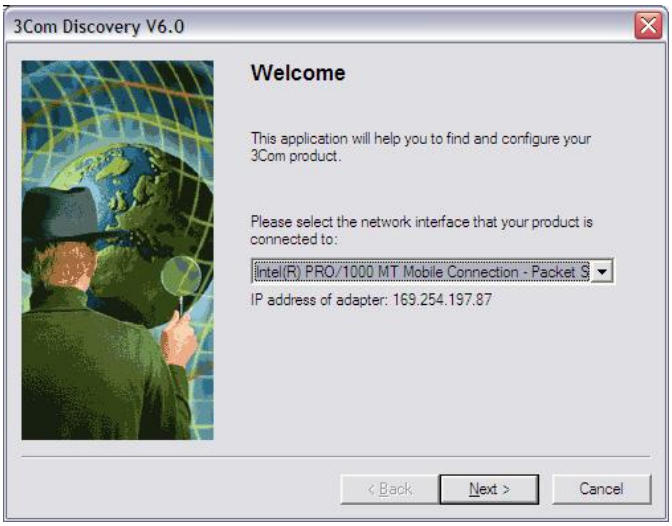


Figura 6.154. ***Ventana 1 ejecución de la aplicación discovery.***

Seleccionamos el adaptador de red que se conecte con el switch en caso de tener varios adaptadores de red en el equipo y a continuación hacemos clic en siguiente, donde aparecerá una pantalla donde se detecta los dispositivos de red como el switch al que se está conectando, esto se lo puede ver en la figura 6.155.

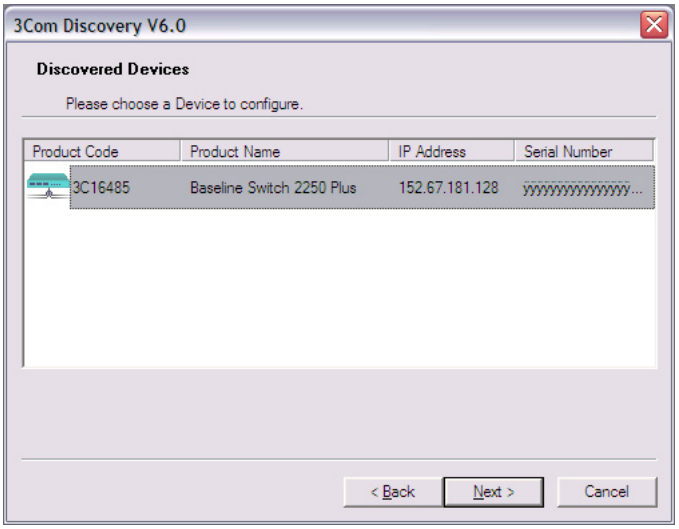


Figura 6.155. ***Ventana 2 ejecución de la aplicación discovery.***

Ahora debemos hacer clic sobre el Switch detectado y hacemos clic en siguiente donde se finalizará la aplicación Discovery 3Com. Aparecerá el cuadro de diálogo de inicio de sesión para la interfaz Web.

6.8.1.4 Inicio de sesión en la Interfaz Web.

Para conectarse a la interfaz Web se debe de hacer lo siguiente:

- User name: escribir admin
- Password: Dejar en blanco este campo de la contraseña.

Una vez introducido el usuario debemos hacer clic en Ok, la pantalla de conexión se puede ver en la figura 6.156.

Figura 6.156. ***Inicio de sesión en la Interfaz Web.***

6.8.1.5 Interfaz Web de 3Com Baseline Switch 2250 Plus.

Esta interfaz está diseñada para realizar fácilmente las tareas de configuración avanzada y ver la información sobre el Switch.

Donde se explicara el Menú de contenidos que se encuentra en el lado izquierdo de la interfaz web como se puede ver en la figura 6.157.

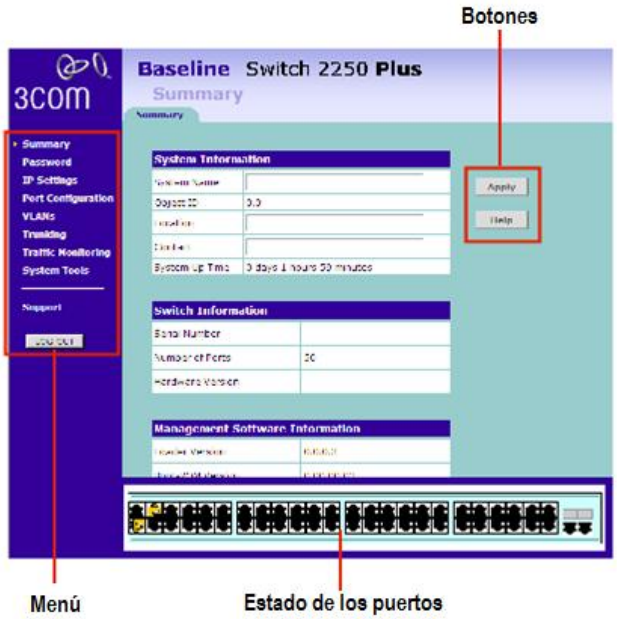


Figura 6.157. ***Interfaz Web de 3Com Baseline Switch 2250 Plus.***

6.8.1.5.1 Menú.

- **Resumen:** Esta opción proporciona un resumen de la configuración básica del Switch y las versiones de los actuales componentes.
- **Contraseña:** Esta opción permite cambiar la contraseña del administrador.
- **Configuración de IP:** Esta permite configurar la dirección Ip del Switch.
- **Configuración de Puertos:** Permite configurar el puerto del Switch.
- **VLAN:** Esta opción permite crear grupos de VLAN, agregar miembros al puerto, y especificar cómo se utiliza el etiquetado de la VLAN.
- **Trunking:** Permite crear y mantener tronco de grupos de miembros de puertos es decir es una función para conectar dos switch mediante dos cables en paralelo en modo Full-Duplex. Esto permite evitar los cuellos de botella.
- **Monitoreo de Tráfico:** Esta permite llevar a cabo el seguimiento del tráfico del puerto en el Switch, para supervisar un puerto.
- **Herramientas del sistema:** Contiene fichas que le permiten:
    - Reiniciar y establecer el Switch.
    - Copia de seguridad y restaurar la configuración.
    - Actualización de firmware.

    - Activar y desactivar la priorización 802.1p.
- **Apoyo:** Muestra la información de contacto de 3Com y describe cómo utilizar la línea de sistema de ayuda.
- **Cierre de sesión:** Esta opción permite desconectarse de forma segura fuera de la Interfaz web.

6.8.1.5.2 Botones.

Dependiendo de la pantalla que se muestra actualmente, los botones pueden ser los siguientes:

- Aplicar: Haga clic para guardar y aplicar los cambios que se hagan.
- Cancelar: Haga clic para descartar los cambios no guardados.
- Ayuda: Haga clic para mostrar la ayuda sobre punto que se esté realizando información para la pantalla que se muestre actualmente.

6.8.1.5.3 Estado del puerto.

Como se puede ver en la figura 6.157 en la parte inferior se indica los puertos que se usan actualmente.

Para configurar un puerto, se debe de hacer clic en el puerto en la imagen. Este le lleva a la pestaña de configuración del puerto de base, donde se puede:

- Asignar un nombre (o etiqueta) al puerto.
- Activar o desactivar el puerto.
- Activar o desactivar el control de flujo.
- Configurar la configuración de dúplex de velocidad.

6.8.1.6 Cambiar la contraseña del administrador.

Para evitar que usuarios no autorizados accedan a la interfaz web y modificar la configuración del Switch.

La configuración predeterminada de la cuenta del administrador es:

Nombre de usuario: admin
Contraseña: sin contraseña

Para garantizar que los usuarios no autorizados no tengan acceso a la interfaz web, se recomienda que se establezca una contraseña de administrador la primera vez que se configure el switch.

Este cambio de contraseña se la puede hacer de la siguiente manera:

- En Contraseña anterior, se escribe la contraseña actual, por defecto, el switch no tiene contraseña, se debe de dejar en blanco este campo.
- En una nueva contraseña, se escribe la contraseña que desea poner para el administrador.
- En Confirmar contraseña, se vuelve a escribir la contraseña que se escribió en nueva contraseña para confirmar.
- Hacer clic en Aplicar para guardar los cambios.

La ventana que se realiza este cambio de contraseña se puede ver en la figura 6.158.

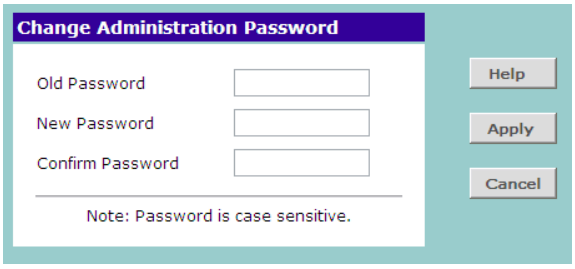


Figura 6.158. ***Pantalla para cambiar la contraseña.***

6.8.1.7 Configuración de la dirección IP.

Para realizar la configuración de la dirección IP del Switch se debe de hacer los siguientes pasos:

- Debemos hacer clic en Configuración de IP para el Switch, donde la pantalla de configuración aparece como se puede ver en la figura 6.159.
- Dentro de la ventana debemos escoger el tipo de configuración y llenar los campos necesarios.

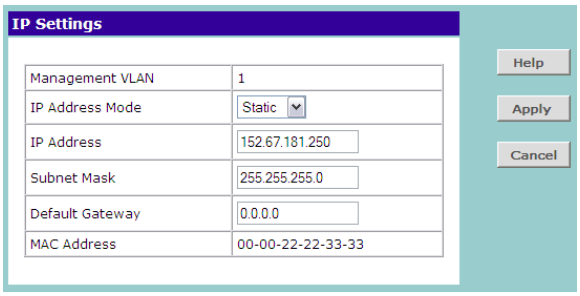


Figura 6.159. ***Pantalla de configuración de la dirección IP.***

6.8.1.7.1 Explicación de las opciones de la pantalla de configuración de la IP.

- **Modo de dirección IP:** Aquí se especifica como el interruptor tendrá su dirección IP, las opciones disponibles incluyen:
    - DHCP: se selecciona esta opción si se tiene un servidor DHCP en la red y si se desea que el Switch obtenga de forma automática una dirección IP.
    - Estática: se selecciona esta opción si se desea asignar manualmente una dirección IP al Switch.

- **Dirección IP:** Se especifica una dirección IP que se desea asignar al Switch, esta opción solo está disponible si la dirección IP está ajustada a modo estático. La dirección IP que se asigna al Switch se convierte también en la dirección IP para la VLAN1.
- **Mascara de subred:** Aquí se especifica una dirección de la máscara de la red que se desea asignar al Switch.
- **Puerta de enlace predeterminada:** Aquí se especifica la dirección IP del enrutador entre el Switch y la gestión de estaciones en otros segmentos de la red.
- **Dirección MAC:** Este campo es de solo lectura que muestra el Switch su MAC o dirección física. Luego de realizar la configuración del Switch de la dirección IP debemos hacer clic en Aplicar para guardar los cambios.

6.8.1.8 Configuración de las opciones de puerto.

Mediante la interfaz Web se puede configurar la velocidad/dúplex y configurar el control de flujo de cada puerto del Switch.

De igual manera se puede ver el estado actual de la conexión de cada puerto ya sea habilitado o deshabilitado.

Existen dos fichas en la configuración de puertos:

- Configuración básica del puerto.
- Configuración avanzada de puerto.

6.8.1.8.1 Configuración básica del puerto.

Esta opción se utiliza para apagar y desactivar el puerto y la configuración de control de flujo y ajustar la velocidad/dúplex del puerto.

Las opciones disponibles son las siguientes:

- Número: Número de puerto físico.
- Etiqueta: Nombre opcional para el puerto para ayudar a identificar los dispositivos conectados a ella.
- Estado: Activa y desactiva el puerto.
- Control de Flujo: Activa y desactiva el control de flujo en el puerto. Cuando el control de flujo está habilitado para el puerto, el switch regula el flujo de paquetes a fin de que un dispositivo emisor no transmita más paquetes de un dispositivo receptor para que pueda procesar. Si el control de flujo está desactivado, los paquetes pueden ser dejados en determinadas periodos de alto tráfico. El control de flujo está activado por defecto.
- Velocidad Dúplex: Establece la velocidad y modo dúplex del puerto. Las opciones disponibles incluyen automático, 10 half-duplex, 10 dúplex, dúplex de 100 y medio, y 100 full-duplex.

Si modifica cualquiera de estas configuraciones, de debe de hacer clic en Aplicar para guardar los cambios, esta pantalla se la puede ver en la figura 6.160.

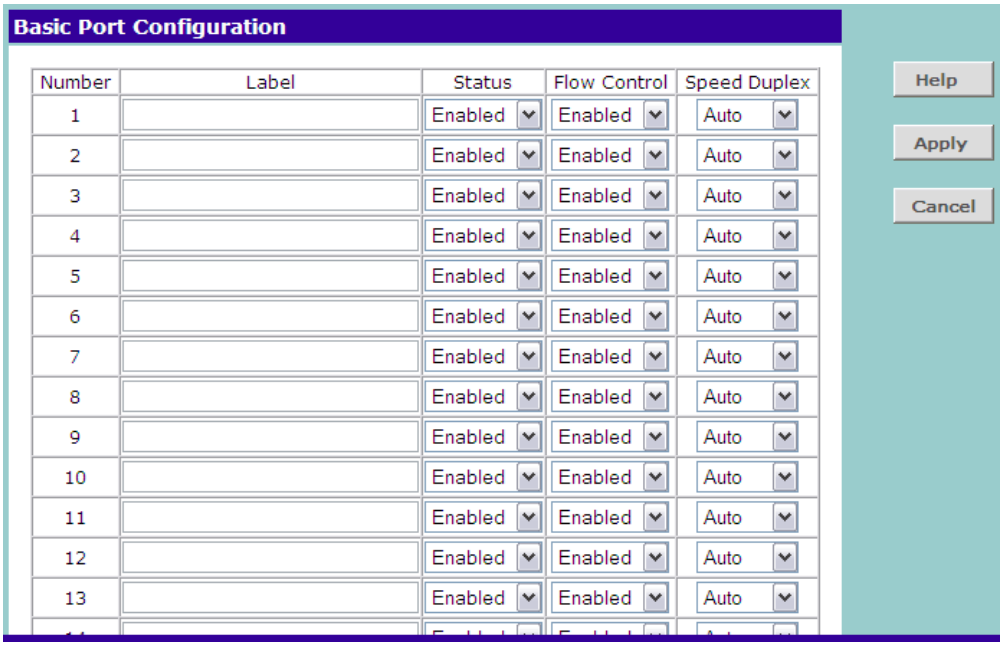


Figura 6.160. ***Pantalla de configuración básica del puerto.***

6.8.1.8.2 Configuración avanzada de puerto.

Esta opción se utiliza para la configuración de los puertos para establecer al Switch el control de tormentas de difusión y los límites del umbral.

Una tormenta de difusión es un paquete incorrecto enviado en una red.

Ajustes avanzados incluyen:

- Broadcast Storm Control: Activa y desactiva el control de tormentas de difusión.
- Paquete Precio Umbral: Establece la tormenta de difusión umbral (64-95232000 bytes por paquete) es decir número de paquetes por segundo.

Esta pantalla se la puede ver en la figura 6.161.

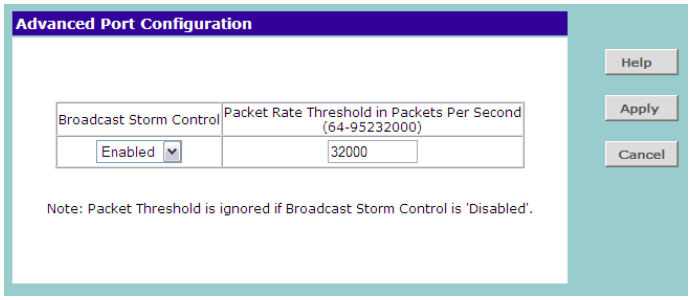


Figura 6.161. ***Pantalla de configuración avanzada del puerto.***

6.8.1.9 Configuración de VLAN.

Se recomienda utilizar el Switch para crear redes Vlan para organizar cualquier grupo o departamento con cada uno de los puertos que tiene el Switch, de esa forma para limitar el tráfico y ayudar a eliminar las tormentas de Broadcast en las grandes redes.

Esto también proporciona una red más segura. Pero si se quiere una comunicación entre diferentes Vlans solo se puede llevar a cabo si todas están conectadas a un router o a un switch de capa 3.

6.8.1.9.1 Creación de una VLAN.

Para crear una Vlan se debe de utilizar la pantalla Crear VLANs, donde se debe de especificar una ID a la Vlan para cada Vlan que se va a crear, la creación de una se la puede ver en la figura 6.162.

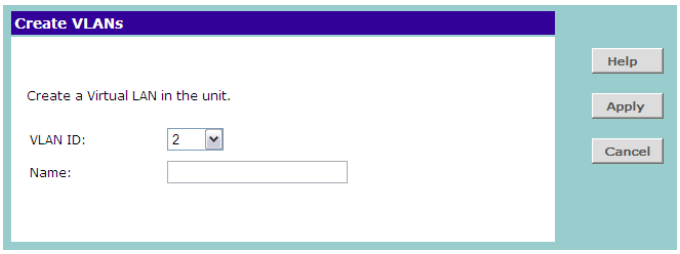


Figura 6.162. ***Pantalla Crear VLAN***

Las opciones disponibles en la pantalla Crear VLAN incluyen:

- VLAN ID: Aquí se pondrá un número de identificación de la Vlan, no se deberá de poner el ID 1 porque este ID viene por defecto y no se deberá poner ceros a la izquierda (035).
- Nombre: El nombre de la Vlan podría ser de 1 a 32 caracteres.

6.8.1.9.2 Eliminación de VLAN.

De igual manera como se crea un Vlan se puede eliminar una, para ello se debe de utilizar la pantalla Eliminar VLANs, esta pantalla se la puede ver en la figura 6.163.

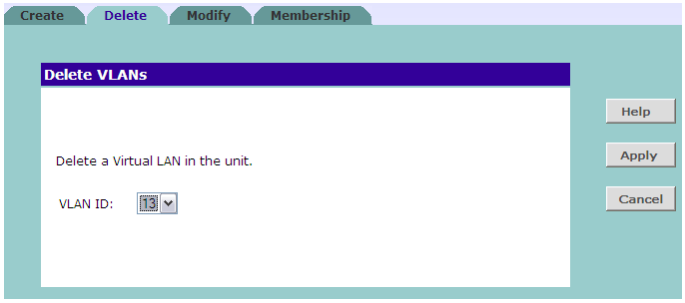


Figura 6.163. ***Pantalla de eliminación de una Vlan.***

La opción de la pantalla Eliminar VLANs incluye VLAN ID: Aquí se escoge el ID de la Vlan que se desea eliminar.

6.8.1.9.3 Modificación de las VLANs.

También se puede modificar una VLAN creada para ello se debe de utilizar la pantalla Modificar VLAN donde se puede cambiar la VLAN a la que pertenece un puerto y configurar el puerto para comunicarse con todas las otras VLNAs. Esta pantalla se la puede ver en la figura 6.164.

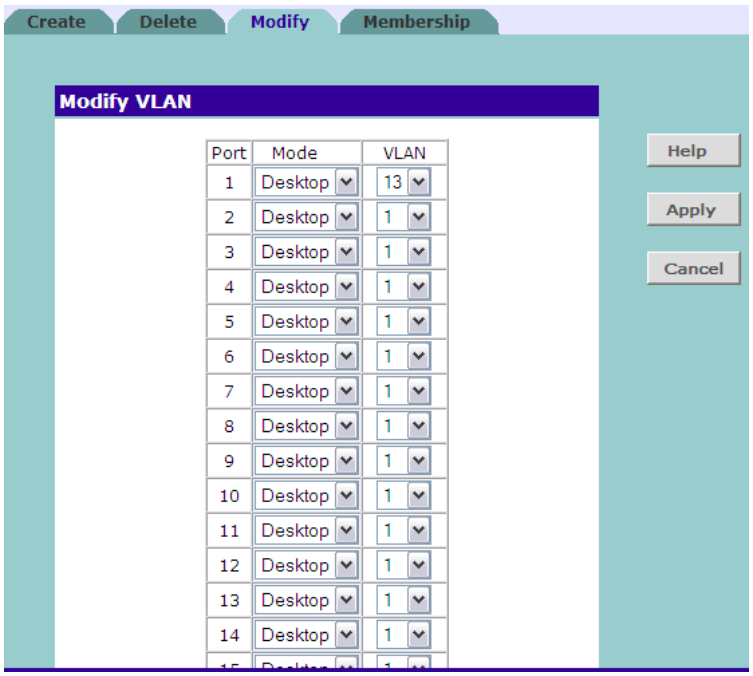


Figura 6.164. ***Pantalla de modificación de VLAN.***

Las opciones de la pantalla Modificar VLANs incluye:

- Puerto: Muestra el número de puerto del Switch.
- Modo: La opción del modo determina si el puerto puede comunicarse con todas las VLANs, o sólo con una Vlan seleccionada.
    - Uplink: Si se selecciona esta opción, el puerto es capaz de comunicarse
      con todas las VLAN en el Switch.
    - Escritorio: Si se selecciona esta opción, el puerto sólo se puede comunicar con otros puertos asignados a la VLAN.
- VLAN ID: Se introduce el ID de la Vlan configurada al puerto que se desea pertenecer.

6.8.1.9.4 La definición de pertenencia a la Vlan.

Esta opción se utiliza para configurar los miembros de puerto para la Vlan seleccionada, es decir asignarle el puerto del Switch a la Vlan creada, esta ventana se la puede ver en la figura 6.165.

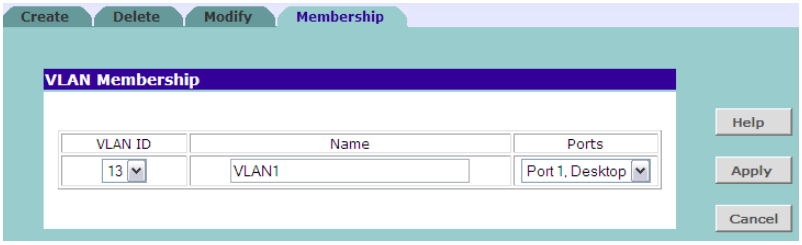


Figura 6.165. ***Pantalla de definición de pertenecía a la Vlan.***

Las opciones de la pantalla Membrecía incluye:

- VLAN ID: Se selecciona el ID de la Vlan creada.
- Nombre: Va el nombre de la Vlan creada.
- Puertos: Va el puerto que se le asigna a la Vlan.

Cada uno de los puntos expuestos anteriormente se recomienda su utilización para el mejoramiento de la red de la Pasamanería S.A, siendo este switch de 48 puertos el que se debe de considerar como el Switch principal para la conexión con los demás switch que se designaran para cada departamento donde se debe de crear todas las VLANs con su respectivo nombre en este caso con el nombre de cada departamento que existe en la Pasamanería S.A.

6.8.2 Switch 3Com Baseline 2226 Plus.

De igual forma se indicara como configurar el switch 3Com de 24 puertos el cual se recomienda que sea utilizada para cada una de sus departamentos con su respectivas VLANs creadas dependiendo de los departamentos que se asignen al cada switch.

6.8.2.1 Conexión a la interfaz web.

Para conectarse a la interfaz web se necesita el cd que viene con el switch en el cual está la aplicación Discovery, el cual se va a proceder de la misma manera que se ingreso a la interfaz web del switch 3com Baseline 2250 Plus.

6.8.2.2 Inicio de sesión en la Interfaz web.

Al cargar la interfaz web en el navegador de Internet, la primera página que aparece es la pantalla de inicio de sesión, donde se deberá introducir el nombre de usuario y la contraseña de administración para acceder a la configuración del equipo.

La pantalla de inicio también muestra la dirección IP que el switch está utilizando actualmente. Esta pantalla se la puede ver en la figura 6.166.

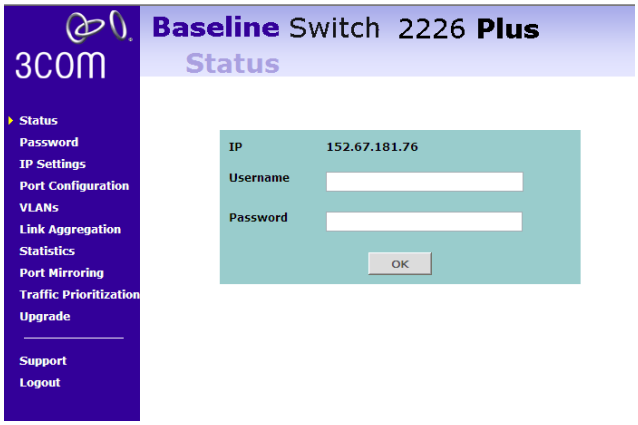


Figura 6.166. ***Pantalla de inicio de sesión.***

Para ingresar a la configuración del equipo se debe de realizar lo siguiente:

- Nombre de usuario: escribir admin.
- Contraseña: dejar en blanco.
- Hacer clic en OK.

6.8.2.3 Navegando por la interfaz web.

De igual forma esta interfaz ha sido diseñada para que se pueda realizar fácilmente las tareas de configuración avanzada y ver la información sobre el switch.

6.8.2.3.1 Menú.

El menú se encuentra en el lado izquierdo de la interfaz web, como se puede ver en la figura 6.167.

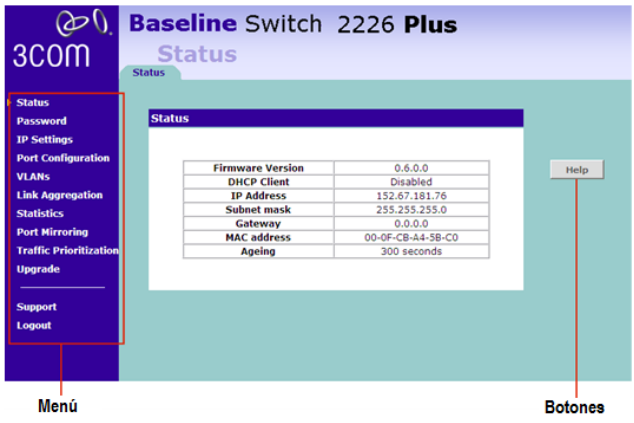


Figura 6.167. ***Pantalla de la interfaz web de switch 3Com Baseline 2226 Plus.***

- **Status:** Esta opción nos indica un resumen de la configuración básica del switch y las versiones de los componentes actuales.
- **Contraseña**: Esta opción permite cambiar la contraseña del administrador.
- **Configuración de IP:** Esta opción permite realizar la configuración de la dirección IP del switch.
- **Configuración de puertos:** Esta opción permite configurar los puertos del switch.
- **VLAN**: Esta opción permite crear grupos de VLAN, agregar miembros al puerto, y especificar cómo se utiliza el etiquetado de la VLAN.
- **Agregación de enlaces:** Permite crear y mantener la afiliación del tronco de grupos de puertos, es decir función para conectar dos switch mediante dos cables en paralelo en modo Full-Duplex.
- **Estadísticas**: Esta opción nos permite ver el número de paquetes recibidos y transmitidos desde cada puerto.
- **Monitoreo de tráfico:** Esta opción nos permite realizar el seguimiento del tráfico del puerto en el switch.
- **Priorización del tráfico**: Esta opción permite configurar la priorización de tráfico para los teléfonos IP que se conectan al switch.
- **Actualizar**: Esta opción permite actualizar el firmware en el Switch.
- **Apoyo:** Esta opción nos muestra información sobre el contracto 3Com y describe como utilizar el sistema de ayuda en línea.
- **Cierre de sesión**: Permite desconectarse de forma segura fuera de la interfaz web.

6.8.2.3.2 Botones.

Dependiendo de la pantalla que se muestra en cada una de las opciones del menú, los botones pueden ser los siguientes:

- Aplicar: Botón para guardar y aplicar los cambios realizados.
- Cancelar: Botón para descartar los cambios no guardados.
- Ayuda: Botón para mostrar la información de ayuda sobre la pantalla que se muestre actualmente.

Ahora que se explicó cada uno de las opciones del menú de la interfaz web del switch se recomienda realizar las siquientes configiraciones en el switch.

6.8.2.4 Cambiar la contraseña de administración del switch.

Es importante realizar esta configuración para evitar que usuarios no autorizados accedan a la interfaz web y modificar la configuración del switch.

La configuración predeterminada del administrador es la siguiente:

- Nombre de usuario: admin
- Contraseña: en blanco (sin contraseña).

Para establecer una contraseña de administrador se debe de realizar lo siguiente:

- En el menú, haga clic en Contraseña, donde aparece una pantalla de cambiar la contraseña de administrador, la cual se puede ver en la figura 6.168.
- En Contraseña anterior, se deja en blanco ese campo si no se tiene una contraseña establecida.
- En una nueva contraseña, se debe de escribir la contraseña que desea establecer.
- En confirmar contraseña, se vuelve a escribir la contraseña que escribió en el anterior paso para confirmar.
- Hacemos clic en aplicar para guardar los cambios.

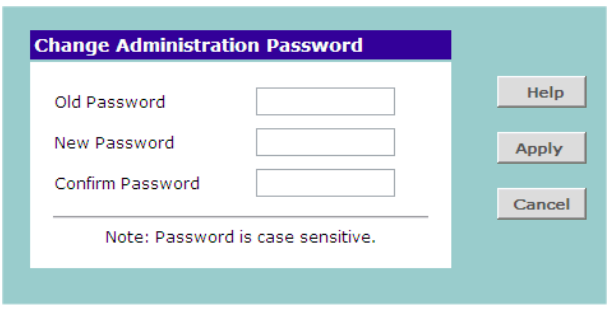


Figura 6.168. ***Pantalla para cambiar la contraseña de administración del switch.***

6.8.2.5 Configuración de la dirección IP.

Para realizar la configuración IP para el switch se debe de realizar los siguientes pasos:

En el menú damos clic en la opción Configuración de IP, la pantalla de configuración IP se la puede ver en la figura 6.169.

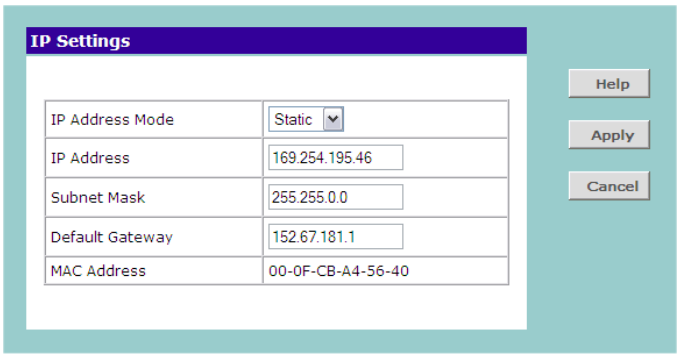


Figura 6.169. ***Pantalla de configuración de la dirección IP.***

Las opciones disponibles de la ventana de Configuración IP se detallan de la siguiente manera:

- **Modo de dirección IP:** Esta opción especifica como el switch obtendrá su dirección IP. Las opciones disponibles son:
    - DHCP: Se selecciona esta opción si se tiene un servidor DHCP en la red para que el switch obtenga una dirección IP automáticamente.
    - Estática: Se selecciona esta opción si se desea asignar manualmente una dirección IP al switch.
- **Dirección IP:** En esta opción se especifica una dirección IP que se desea asignar al switch, pero esta opción está disponible si la dirección IP esta de modo estática, esta misma dirección IP asignada al switch se convierte en la dirección IP para la VLAN1 creada por defecto.
- **Máscara de subred:** En esta opción se especifica una dirección de máscara de la subred que se desea asignar el Switch.

- **Puerta de enlace predeterminada:** Aquí se especifica la dirección IP del enrutador entre el switch y la gestión de estaciones en otros segmentos de la red.
- **Dirección MAC:** Este campo es de solo lectura que muestra el switch su MAC o dirección física.

Una vez realizado la configuración de las opciones de la dirección IP, debemos hacer clic en Aplicar para que se guarden los cambios realizados.

6.8.2.6 Configuración de los puertos.

Con esta opción se puede configurar la velocidad/dúplex y configurar el control de flujo de cada puerto. De la misma forma también se puede apagar o desactivar los puertos del Switch.

Para ver la configuración actual del puerto se debe ir al menú de la interfaz web y entrar en la opción Configuración de puertos, donde se abrirá una ventana con un resumen de la configuración actual, esta ventana se la puede ver en la figura 6.170.

Port Configuration

Port	Link Status	Speed Duplex	Flow Control	Port	Link Status	Speed Duplex	Flow Control
01	Up	100Mbps Full	Enable	16	Down	--	--
02	Down	--	--	17	Down	--	--
03	Down	--	--	18	Down	--	--
04	Down	--	--	19	Down	--	--
05	Down	--	--	20	Down	--	--
06	Down	--	--	21	Down	--	--
07	Down	--	--	22	Down	--	--
08	Down	--	--	23	Down	--	--
09	Down	--	--	24	Down	--	--
10	Down	--	--	25	Down	--	--
11	Down	--	--	26	Down	--	--
12	Down	--	--	AL1	Down	--	--
13	Up	100Mbps Full	Enable	AL2	Down	--	--
14	Down	--	--	AL3	Down	--	--
15	Down	--	--	AL4	Down	--	--

Figura 6.170. ***Pantalla de configuración del puerto.***

A continuación se describirá la información que aparece en la pantalla de configuración del puerto las mismas que son las siguientes:

- **Puerto:** Es el número físico del puerto que corresponde a la numeración de los puertos en la parte frontal del switch, debemos tener en cuenta que los puertos 25 y 26 son puertos con doble función es decir se puede conectar a un SFP es decir un cable de fibra óptica.

  De igual manera los puertos AL1 a AL4 estos sirven para grupos de troncales.

- **Estado del enlace:** Esta opción indica si el puerto esta activado o desactivado.

- **Velocidad/Duplex:** Si el enlace indica que esta activado el puerto, indica la configuración de velocidad del puerto.

- **Control de Flujo:** Si el enlace indica que esta activado el puerto, indica que el control de flujo esta activado en el puerto.

6.8.2.6.1 Cambiar la configuración de un puerto.

Para realizar esta configuración se debe de hacer clic en el número de puerto que se desea configurar en la pantalla de configuración de puertos, donde se mostrará una ventana de configuración del puerto, la misma que se puede ver en la figura 6.171.

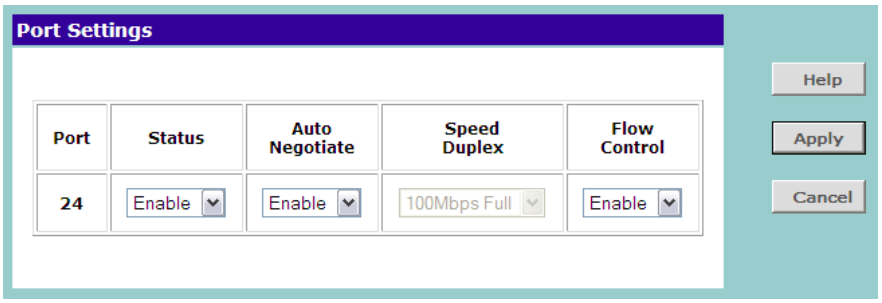


Figura 6.171. ***Pantalla de configuración de puertos.***

A continuación se explicará las opciones disponibles que se muestran en la pantalla de configuración del puerto las mismas que son las siguientes:

- **Condición del puerto.**
  - Activar: Activa el puerto.
  - Desactivar: Apaga o desactiva el puerto.

- **Auto negociación:** Esta opción está habilitada por defecto, pero las opciones disponibles para el auto negociación son:
    - Activar: Activa la negociación automática para el puerto. Si esta activada las opciones de velocidad dúplex no estarán activadas.
    - Desactivar: Desactiva la negociación automática para el puerto. Si esta desactivada, es necesario configurar el modo de velocidad dúplex.
- **Velocidad Dúplex:** Esta opción establece la velocidad y el modo dúplex en el puerto. Esta opción está disponible solo si la negociación automática esta desactivada, los modos de velocidad dúplex son los siguientes:
    - La mitad de 10Mbps.
    - 10 Mbps completo.
    - La mitad de 100Mbps.
    - 100Mbps completa.
    - Completo 1000Mbps (para los puertos 25 y 26 solamente).
- **Control de Flujo:** Cuando el control de flujo esta activado se controla el flujo de paquetes para que un dispositivo emisor no trasmita muchos paquetes a un dispositivo receptor para que pueda procesar.

Si se desactiva el control de flujo, los paquetes pueden ser dejados en ciertos períodos de cargas de alto tráfico.

6.8.2.7 Configuración de VLAN.

De igual manera que el anterior switch se recomienda utilizar el switch para crear redes Vlan para organizar cualquier grupo o departamento con cada uno de los puertos que tiene el switch, de esa forma para limitar el tráfico y ayudar a eliminar las tormentas de Broadcast en las grandes redes. Esto también proporciona una red más segura. En este switch se puede crear hasta 64 VLNAs.

6.8.2.7.1Creación de una VLAN.

Con la utilización de la interfaz web se puede crear las VLANs en el switch para ello debemos seguir los siguientes pasos:

- En el menú de la interfaz web debemos hacer clic en VLAN, donde aparece la pantalla.
- En VLAN ID, debemos hacer clic Crear nueva VLAN, donde aparece la pantalla Create VLANs la misma que se puede ver en la figura 6.172.
- En VLAN ID (1 a 4904), se debe escribir un número de identificación para la VLAN que se está creando, esta numero ira entre un rango de 1 a 4904.

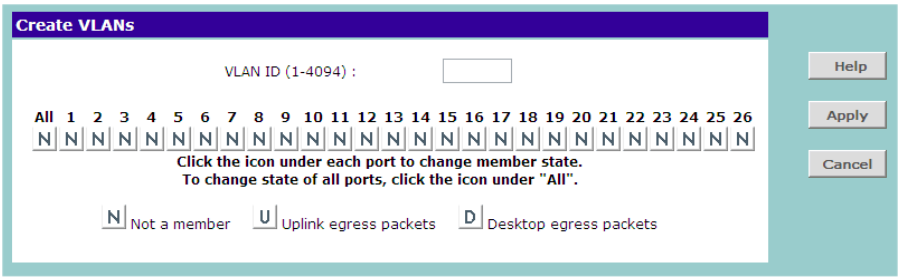


Figura 6.172. ***Pantalla para crear Vlan.***

- Ahora se define la pertenencia a la VLAN mediante el establecimiento de estado de cada puerto, donde se debe de hacer clic en el icono con el número de puerto varias veces para recorrer los diferentes estados, estos estados son los siguientes:
    - N: No es miembro.
    - U: Paquetes de enlace ascendente de salida.
    - D: Paquetes de escritorio de salida.
- Ahora debemos hacer clic en Aplicar para crear la VLAN.

6.9 Recomendaciones de estándares para aplicar cableado estructurado.

Realizada las recomendaciones anteriores ahora procedemos al siguiente punto el cual tratará de la parte física de la red de la Pasamanería S.A.

Recomendamos contar en la fábrica con un cableado estructurado, ya que de un buen cableado depende el buen desempeño de una red.

Es importante contar con un buen cableado estructurado por las siguientes características:

- Instalando cableado estructurado se garantizaría el desempeño de la red por aproximadamente 20 años.
- Se planea su instalación con miras a futuro y esto da la facilidad de un breve crecimiento.
- Al dividirlo en partes manejables, facilitaría la administración, se podrían detectar fácilmente fallas y corregirlas sin complicaciones.
- Se contaría con una de red segura, ya que al contar con cableado estructurado implica tener un área restringida o un gabinete cerrado que hacen las veces de un closet de comunicaciones y esto asegura que personal no autorizado no tenga acceso a alterar la estructura de la red o este en riesgo de un sabotaje.
- Incluso hablando estéticamente, se mejoraría mucho ya que existe una gran variedad de materiales que pueden lograr la perfecta combinación para adaptarse a las necesidades de la fábrica.

Los elementos principales de un cableado estructurado son los siguientes:

- Cableado horizontal.
- Cableado del backbone.
- Cuarto de telecomunicaciones.
- Cuarto de entrada de servicios.

Identificando los elementos principales de un cableado estructurado, recomendamos a la fábrica implementar el cableado estructurado basándose en los estándares que mencionamos a continuación.

6.9.1 Cableado Horizontal.

Para el cableado horizontal de la fábrica, recomendamos aplicar el estándar **TIA/EIA 568-A,** el mismo que básicamente considera y recomienda los siguientes puntos:

- La topología.
- La distancia máxima de los cables.
- El rendimiento de los componentes.

- La toma y los conectores de telecomunicaciones.

6.9.1.1 Topología.

La norma EIA/TIA 568A contempla las siguientes recomendaciones en cuanto a la topología del cableado Horizontal:

- Cada toma/conector de telecomunicaciones del área de trabajo debe conectarse a una interconexión en el cuarto de telecomunicaciones, que vendría a ser un patch panel.
- El cableado horizontal de cada oficina debe terminar en un cuarto de telecomunicaciones ubicado en el mismo piso.
- Los componentes eléctricos (como dispositivos acopladores de impedancia) no se instalarán como parte del cableado horizontal, cuando se necesiten estos componentes se deben poner fuera de la toma/conector de telecomunicaciones.
- No se debe tener empalmes de ningún tipo en el cableado horizontal, de igual manera no es necesario en este punto al recomendación ya que la fábrica no tiene empalmes.

6.9.1.2 La distancia máxima de los cables.

Independientemente del medio físico, la distancia horizontal máxima no debe exceder 90 m, esta distancia se mide desde el medio en la interconexión horizontal en el cuarto de telecomunicaciones hasta la toma/conector de telecomunicaciones en el área de trabajo.

Se recomiendan las siguientes distancias:

- Se separan 10 m para los cables del área de trabajo y los cables del cuarto de telecomunicaciones, los mismos que pueden ser cordones de parcheo, jumpers y cables de equipo.
- En el área de trabajo, se recomienda una distancia máxima de 3 m desde el equipo hasta la toma/conector de telecomunicaciones.

Estas medidas se pueden observar mejor en la figura 6.173.

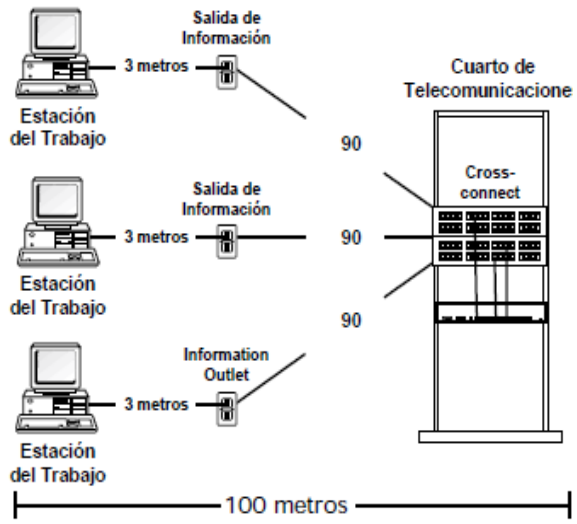


Figura 6.173. ***Esquema de distancias para cableado horizontal.***

6.9.1.3 El rendimiento de los componentes.

No se realizará en este punto ninguna recomendación, ya que la fábrica cuenta con los cables que reconoce el estándar anteriormente mencionado.

6.9.1.4 Las tomas y los conectores de telecomunicaciones.

Se recomienda proveer un mínimo de dos tomas/conectores de telecomunicaciones para cada área de trabajo en funcionamiento. Una toma/conector debería tener un servicio de voz y la otra con un servicio de datos.

Las dos tomas/conectores de telecomunicaciones se deben configurar de la siguiente forma:

- Una toma/conector de telecomunicaciones debe estar soportada por un cable UTP de 100 ohm y cuatro pares de categoría 3 o superior.
- La segunda toma/conector de telecomunicaciones debe estar soportada por uno de los siguientes medios como mínimo:
    - Cable UTP de 100 ohm y cuatro pares (se recomienda categoría 5).
    - Cable STP−A de 150 ohm y dos pares.
    - Cable de fibra óptica multimodo de 62.5/125 um y dos fibras.

6.9.1.4.1 Área de Trabajo.

El área de trabajo se extiende de la toma/conector de telecomunicaciones o el final del sistema de cableado horizontal, hasta el equipo de la estación y está fuera del alcance de la norma EIA/TIA 568A.

El equipo de la estación puede incluir, pero no se limita a, teléfonos, terminales de datos y computadoras.

Se deben hacer ciertas consideraciones cuando se diseña el cableado de las áreas de trabajo:

- El cableado de las áreas de trabajo generalmente no es permanente y debe ser fácil de cambiar.
- La longitud máxima del cable horizontal se ha especificado con el supuesto que el cable de parcheo empleado en el área de trabajo tiene una longitud máxima de 3 m.
- Comúnmente se emplean cordones con conectores idénticos en ambos extremos.
- Cuando se requieran adaptaciones específicas a una aplicación en el área de trabajo, éstas deben ser externas a la toma/conector de telecomunicaciones.

6.9.2 Cableado Vertebral o Backbone.

Para el cableado vertebral o también llamado Backbone, recomendamos al igual que el cableado horizontal aplicar el estándar **TIA/EIA 568-A.**

La norma EIA/TIA 568A define recomendaciones como:

Se recomienda que en la interconexión de cableado de backbone, es decir en la interconexión de switch a switch no debe haber más de dos niveles jerárquicos de interconexiones, precisamente para limitar la degradación de la señal.

Para un caso específico que tiene la fábrica, hay una interconexión de switch con tres niveles, ya que existe un nivel de conexión en cascada, porque el switch del

departamento de Almacén y Diseño están conectados al switch de Corte y este es el que se conecta con el switch principal.

Para este caso en específico recomendamos que se haga uso de cable de fibra óptica, para que de esta manera se conecte el switch de corte y switch del almacén de manera directa al switch principal y así se lograría que la señal no se distorsione con conexiones en cascada.

Sólo se debe pasar por una conexión cruzada para llegar a la conexión cruzada principal.

En ciertas instalaciones, la conexión cruzada del backbone (conexión cruzada principal) bastará para cubrir los requerimientos de conexiones cruzadas.

6.9.2.1 Cables reconocidos.

No tenemos recomendación al respecto ya que la fábrica utiliza cable categoría 6 para la conexión de backbone.

6.9.2.2 Distancias de cableado.

Para minimizar la distancia de cableado, la conexión cruzada principal debe estar localizada cerca del centro del área que se servirá los respectivos servicios.

6.9.2.3 Cableado y equipo de telecomunicaciones.

Los equipos de telecomunicaciones que se conectan directamente a las conexiones cruzadas o intermedias deben hacerlo a través de cables de 30 m o menos.

El cableado de backbone no debe exceder los 100 metros.

6.9.3 Recomendación para la red Sucursal Las Américas y la sucursal El Vergel.

6.9.3.1 Cableado horizontal.

6.9.3.1.1 Control de acceso.

Para controlar los accesos a los equipos de comunicación en la sucursal de Las Américas y El Vergel recomendamos tener instalado un armario o rack para guardar los equipos de telecomunicaciones, el mismo que protegerá todos equipo de

comunicación y pueda ser accedido únicamente por personal autorizado, además que se tendría instalado los equipos de comunicación de una manera más ordenada e independiente del mueble de puesto de cobro de cada sucursal.

Se recomienda instalar el armario o rack que se menciona en punto 6.9.4.1 de este capítulo.

6.9.3.1.2 Las tomas y los conectores de telecomunicaciones.

Recomendamos que se instale toma/conectores en cada sucursal y se evite tener conexiones directas como actualmente se encuentran instaladas, de esta manera se podría cambiar el área de trabajo sin ningún inconveniente.

Además recomendamos que se instalen toma/conectores para el futuro ya que podrían necesitarse más toma/conectores ya que se podrían implementar más áreas de trabajo.

6.9.4 Recomendación para el cuarto de equipos y cuarto de telecomunicaciones para la Pasamanería S.A.

Se recomienda tener el departamento de sistemas aislado de los demás departamentos en este caso del departamento de Contabilidad, la razón de esta recomendación es de tener un cuarto de equipos que este dentro del departamento de sistemas.

En este cuarto únicamente se debe de guardar equipos directamente relacionados con el sistema de telecomunicaciones tales como:

- Servidor Pasamanería.
- Servidor CorreoPasa.
- Servidor CorreoPasa Interno.
- Servidor PALM.
- Servidor PASAWEW.
- Central Telefónica.
- Servidor de Reloj.
- Router Cisco de Telconet.
- Mikrotik 1100.

De esa forma garantizando la seguridad de los mismos.

Para esta recomendación nos hemos basado en el estándar ANSI/TIA/EIA-569 la misma que se especificará a continuación:

- **Prevención de inundaciones:** El cuarto de equipos no debe estar localizado debajo de niveles de agua, debe ser colocado un drenaje en el cuarto en caso de que exista el ingreso de agua. Para ello se recomienda que este dentro del departamento de Sistemas.
- **Dimensiones del cuarto de equipos:** El cuarto de equipo debería tener medidas de al menos 3.0 m x 2.2 m. La altura mínima del cuarto de equipos debe ser de 2.44 metros (8 pies) sin obstrucciones.
- **Temperatura del cuarto de equipos:** Se recomienda que se le programe al acondicionar de temperatura SMC que tiene la Pasamanería a una temperatura entre un rango de 18 a 24 grados centígrados con una humedad del 30% al 55%.
- **Acabados Interiores**: Se recomienda que el piso, las paredes y el techo deban ser sellados para reducir el polvo. Las paredes deben ser pintadas con pintura resistente al fuego, lavable, de color claro para aumentar la iluminación del cuarto.
- **Iluminación**: Se recomienda que la iluminación deba colocarse en un lugar donde este libe de los equipos. La iluminación debe ser controlada por uno o más switches, localizados cerca de la puerta de entrada al cuarto.
- **Energía**: Se debe instalar un circuito separado para proveer energía al cuarto de equipos y debe terminar en su propio panel eléctrico. La energía eléctrica que llegue al cuarto no se especifica ya que depende de los equipos instalados.
- **Ductos:** Se recomienda utilizar canaletas de plástico para proteger los cables de interconexión de los equipos de telecomunicaciones. Los cables UTP no deben circular junto a cables de energía dentro de la misma canaleta por más corto que sea el trayecto.
- **Puerta:** Se recomienda que la puerta de acceso debe de ser de apertura completa, con llave y de al menos 91 centímetros de ancho y 2 metros de alto.

La puerta debe ser removible y abrir hacia afuera o que se habrá hacia los lados. La puerta debe abrirse al ras del piso y no debe tener postes centrales.

- **Extinguidores de fuego**: Se deben proveer extinguidores de fuego portátiles y hacerles mantenimiento periódicamente.
- **Seguridades de ingreso al cuarto de equipo:** El cuarto de equipo debe ser protegido de acceso no autorizado, utilizando tecnologías de autenticación como sistemas de control con tarjetas inteligentes, monitoreo y registro de entradas y salidas.

  La persona que ingrese al cuarto de equipos que no pertenezca a la Pasamanería deberá registrar el motivo del ingreso y estar acompañada permanentemente por la personal que está a cargo de este cuarto.
- **Cielos falsos:** Se debe evitar el uso de cielos falsos en los cuartos de equipos.
- **Potencia:** Se recomienda la instalación de tomacorrientes suficientes para alimentar los dispositivos. El estándar establece que debe haber un mínimo de dos tomacorrientes dobles de 110V C.A. dedicados de tres hilos.

  Estos dos tomacorrientes podrían estar dispuestos a 1.8 metros de distancia uno de otro.

  La alimentación específica de los dispositivos electrónicos se deberá hacer con UPS y regletas montadas en los andenes. Separado de estos tomas deben haber tomacorrientes dobles para herramientas, equipo de prueba etc.

  Estos tomacorrientes deben estar a 15 centímetros del nivel del piso y puestos en intervalos de 1.8 metros alrededor del perímetro de las paredes.

  El cuarto de equipos debe contar con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable mínimo 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA−607.
- **Disposición de equipos:** Se recomienda la instalación de un rack destinado a alojar equipamiento electrónico, informático y de comunicaciones.

En el cual se alojaría los servidores y los equipos de telecomunicaciones como los routers y switch.

Para la adquisición del Rack se debe de tomar las siguientes recomendaciones:

- Ancho de 60 cm.
- Fondo de 80 cm.
- Ancho interior de 19 "(48,2 cm estándar EIA/ NEMA para los rack).
- Que incluya sistema de filtración del aire.
- Puerta frontal con cerradura.
- Puerta posterior con cerraduras rápidas tipo universal.

Este rack para el cuarto de equipos recomendado se le puede ver en la figura 6.174.

Figura 6.174. ***Rack para el cuarto de equipos.***[71]

6.9.4.1 Cuarto de telecomunicaciones o armarios de seguridad.

Se recomienda adquirir 6 armarios de seguridad para los equipos que se encuentran en cada uno de los departamentos y áreas de trabajo los mismos que son:

- Departamento de Secretaria General.

[71] http://www.pergaminovirtual.com.ar/definicion/Rack.html

- Departamento de Ventas.
- Área de mecánica
- Área de Supervisión General
- Área de Corte.
- Área de Diseño.

Esta recomendación se la hace por que los equipos de telecomunicaciones están a la vista de todo mundo sin la debida protección, los mismos que son el Switch 3Com 2250 de 48 puertos que se encuentra en el departamento de Ventas y el router Links Sys que se utiliza para la red inalámbrica de la Pasamanería S.A y los 5 switch 3Com 2226 de 24 puertos que se encuentran distribuidos por las demás áreas de trabajo y el departamento de Secretaría General.

Para ello se recomienda adquirir estos armarios o rack con las siguientes características:

- **Características del interior:**
    - Altura 6U. "U" es equivalente a 4.45 cm.
    - Ancho: 19 "(48,2 cm estándar EIA/ NEMA para los rack).
    - Profundidad máxima de 61.2 cm.
    - Que incluya sistema de filtración del aire.
    - Dos ventiladores de ultra silencio.

- **Características del exterior:**
    - Uno o dos orificios para el ingreso del cable UTP a los equipos de telecomunicaciones.
    - Seguridad con llave en la puerta.

Este armario o rack que se recomienda puede ser como se muestra en la figura 6.175.

Figura 6.175. ***Rack recomendado.***[72]

A más del armario o rack que se recomienda, también es necesario adquirir 6 Patch Panel para cada uno de los armarios el cual permitirá seccionar la distribución de cable, es decir que cumpla la función de recibir la señal y enviarla por el puerto específico del cual la recibe, por ejemplo si recibe la señal de puerto 10 de entrada envía la señal hacia el puerto 10 de salida.

6.9.4.1.1 Patch panel de 24 puertos cat.5e.

Este patch panel deberá tener las siguientes características:

- Con montaje en rack de 19".
- Que sean ideales para redes Ethernet/ Fast Ethernet /Gigabit Ethernet (1000 Base-T).
- Que sea compatible con cableado de Categoría 3, 4, 5.
- Que cumpla con las norma EIA/TIA 568A.

Este patch panel recomendado se le puede ver en la figura 6.176.

Figura 6.176. ***Patch panel recomendado.***[73]

También se recomienda adquirir 6 regletas eléctricas para proveer de energía a los equipos de telecomunicaciones que van a estar en cada uno de los armarios o racks de seguridad en este caso paro los switch 3Com y el router Link Sys.

6.9.4.1.2 Regleta electica de 19".

Se recomienda adquirir las regletas con las siguientes características:

---

[72] http://www.pergaminovirtual.com.ar/definicion/Rack.html
[73] http://www.avanzada7.com/eshop/index.php?cPath=38

- Regleta de PVC preparada para usar en un rack de 19”.
- Altura de 1U.
- Que disponga de un interruptor para un apagado simultáneo de los equipos conectados.
- Que sea de 6 o 8 Schuckos.

Esta regleta eléctrica recomendada se la puede ver en la siguiente figura 6.177.

Figura 6.177. ***Regleta eléctrica recomendada.***[74]

6.9.4.1.3 Ductos.

Se recomienda la utilización de canaletas de plástico para la protección de los cables que van a acceder al armario de seguridad, el tamaño de la canaleta va depender de la cantidad de cables que salgan para el área de trabajo.

Esta canaleta para el acceso al armario se recomienda con las siguientes características:

- Canaleta de PVC de 1 compartimiento.
- Las medidas deben ser de 4 cm x 6 cm.
- De color blanco.
- Que sea auto extinguible.
- Que sea resistente a los impactos.

Esta canaleta se la puede ver en la figura 6.178.

Figura 6.178. ***Canaleta de plástico.***[75]

[74] http://listado.mercadolibre.com.ve/Regleta-Electrica-P%2FRack-10-tomas

Una vez realizada las recomendaciones para la protección de los equipos de telecomunicaciones, la arquitectura de cómo quedaría el armario de seguridad con los equipos instalados en este caso el Switch Principal 3Com 2250 de 48 puertos que se encuentra en el departamento de Ventas se la puede ver en la figura 6.179.

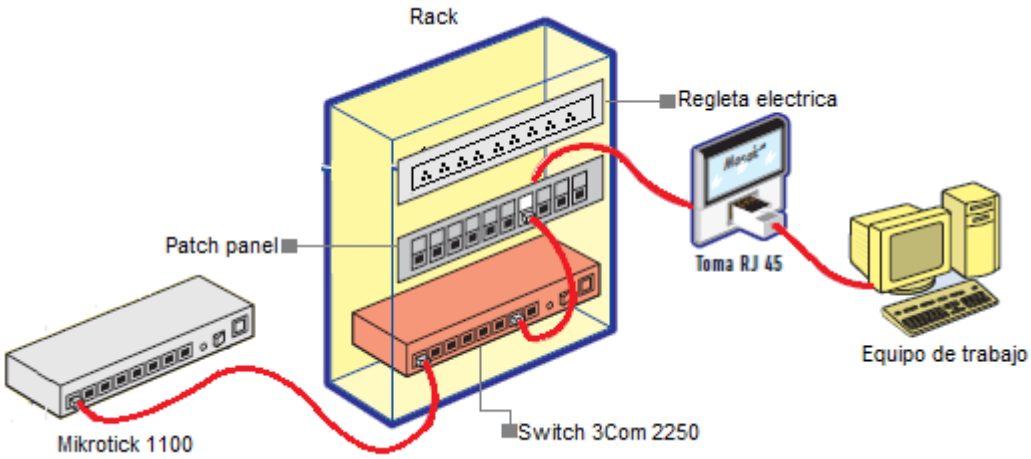


Figura 6.179. ***Arquitectura del armario de seguridad de quipos de telecomunicaciones principales.***

Y de igual manera la arquitectura de cómo quedarían conectados los equipos de telecomunicaciones en el armario de seguridad, en este caso para los demás switch 3Com 2226 de 24 puertos que se encuentra en los demás departamentos y áreas de trabajo, esta arquitectura se la puede ver en la figura 6.180.

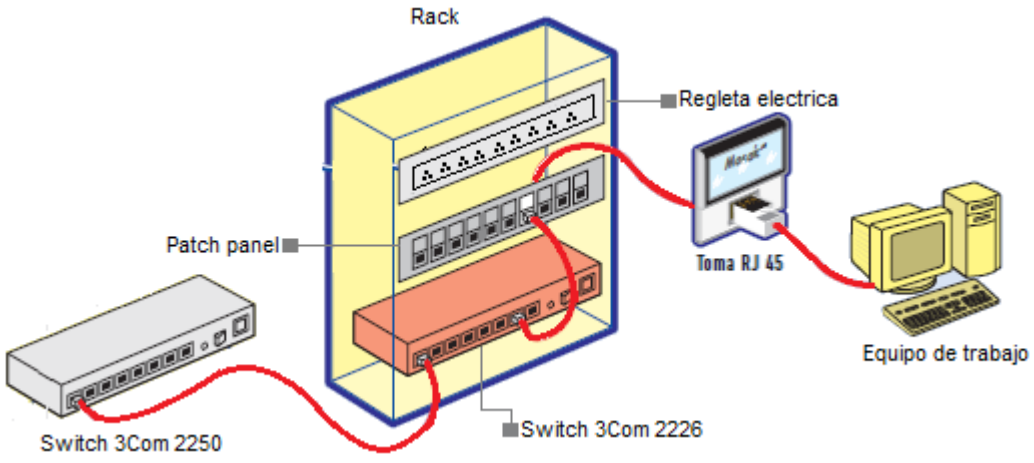


Figura 6.180. ***Arquitectura del armario de seguridad de quipos de telecomunicaciones secundarios.***

[75] http://www.tecnologialopez.com/residencial-comercial/

6.9.5 Recomendación de etiquetación y administración del cableado horizontal y backbone.

6.9.5.1 Etiquetación del cableado horizontal y backbone.

Para realizar las recomendaciones de este punto de la etiquetación nos hemos basado en el estándar ANSI/TIA/EIA 606 A (Etiquetación y administración).

6.9.5.2 Colores para el cableado de red.

6.9.5.2.1 Área de trabajo.

Basándonos en el estándar ANSI/TIA/EIA 606 A se recomienda lo siguiente:

La utilización de cables UTP de color blanco para el área de trabajo con una longitud de 3 metros mínimo. El color de cable se puede ver en la figura 6.181.

Figura 6.181. ***Colores para el cableado de red.***

6.9.5.2.2 Cuarto de equipos.

Basándonos en el estándar ANSI/TIA/EIA 606 A se recomienda la utilización de cables UTP de color azul para la interconexión de los equipos de datos.

Esta interconexión de los equipos se la puede ver en la figura 6.182 al igual que el color del cable.

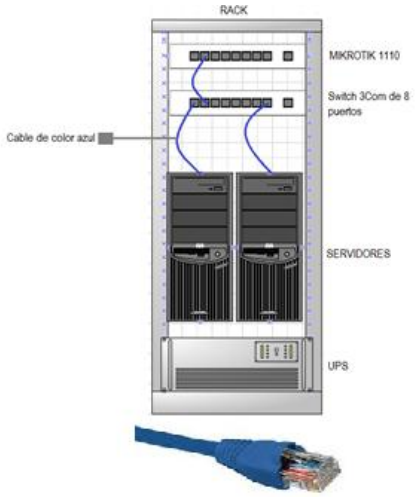


Figura 6.182. ***Colores para cables en el cuarto de telecomunicaciones.***

6.9.5.2.3 Armario de seguridad.

De igual manera se recomenda el cable de color azul para la conexión de los equipos de telecomunicaciónes en el armario de seguridad de cada uno de los departamentos y áreas de trabajos como mecánica etc. Esta conexión se la puede ver en la figura 6.183 al igual que el color de cable de red.

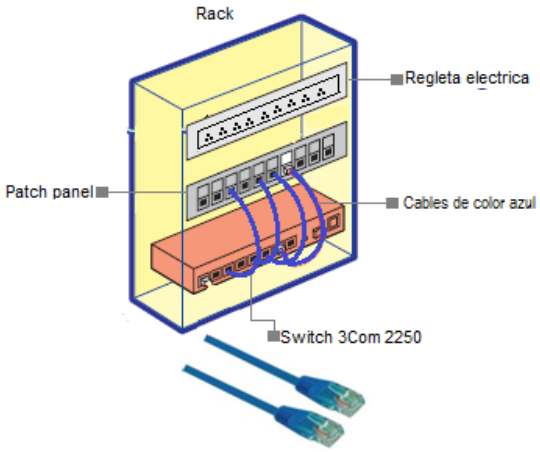


Figura 6.183. ***Colores de cables para el armario de seguridad.***

6.9.5.2.4 Conexión telefónica.

Basándonos en el estándar ANSI/TIA/EIA 606 A se recomienda la utilización de cables UTP de color amarillo para los equipos que se encuentre ubicados en el armario de telecomunicaciones o cuarto de equipo para la cross-conexión de los equipos de telefonía. Esta conexión se la puede ver en la figura 6.184 al igual que el color del cable de red.

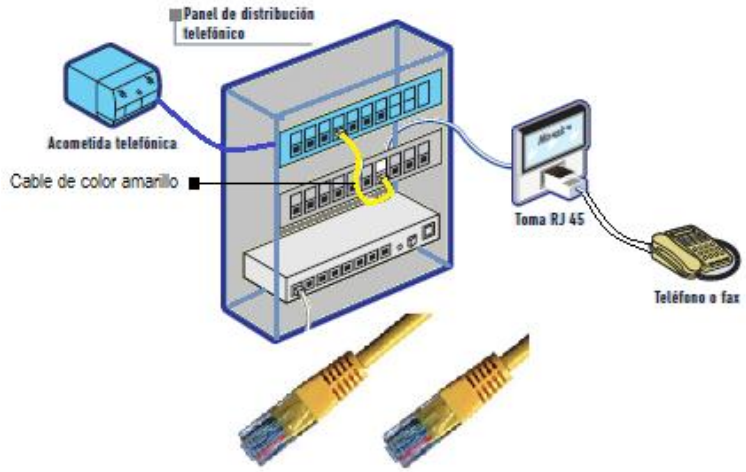


Figura 6.184. ***Colores para cables de telefonía.***

6.9.5.3 Colores de las terminales.

Debido a que la Pasamanería S.A no ha seguido ningún estándar para realizar el cableado de la red, tampoco se maneja de una forma ordenada los colores de las terminales para la salida al área de trabajo como lo es para voz, datos y para datos/voz.

Basándonos en el estándar ANSI/TIA/EIA 606 A se recomienda tener en consideración los colores para cada una de las terminales de salida para el área de trabajo.

6.9.5.3.1 Color azul.

Este color se maneja para la trasmisión de voz en el área de trabajo esta terminal se la puede ver en la figura 6.185.

Figura 6.185. ***Color de terminal azul.***[76]

[76] http://www.planetronic.es/sin-categorizar-c-1369.html?page=10&sort=3a

6.9.5.3.2 Color blanco.

Este color se maneja para la transmisión de datos en el área de trabajo, esta terminal se la puede ver en la figura 6.186.

Figura 6.186. Color de terminal blanco.[77]

6.9.5.3.3 Color negro.

Este color se maneja para la transmisión de datos y voz en el área de trabajo, esta terminal se la puede ver en la figura 6.187.

Figura 6.187. Color de terminal negro.[78]

6.9.5.4 Etiquetación.

Basándonos en el estándar ANSI/TIA/EIA 606 A se recomienda los siguientes puntos:

- Todos los cables deben estar etiquetados.
- Cada identificador debe ser único.
- Los componentes deben ser marcados donde sean administrados (etiqueta en todos los puntos de concentración: los paneles, los bloques, las salidas, etc.).
- Todas las vías deben ser etiquetadas (canaletas, etc.).

El etiquetado debe ser llevado a cabo de la siguiente forma: etiquetas individuales firmemente sujetas a los elementos con etiquetas adhesivas.

---

[77] http://www.planetronic.es/sin-categorizar-c-1369.html?page=10&sort=3a
[78] http://www.planetronic.es/sin-categorizar-c-1369.html?page=10&sort=3a

Las etiquetas deberán ser auto-laminadas, es decir las letras deben estar protegidas con una porción de la misma etiqueta.

Para cables utilizados en exteriores se utilizarán etiquetas especiales para exteriores.

6.9.6 Protección física de las líneas telefónicas.

6.9.6.1 Canaletas.

Se recomienda el uso de canaletas para la protección física de las líneas telefónicas esta recomendación se la hace por que se verifico una gran parte de las líneas telefónicas que no tenían su protección física, en su gran mayoría en el departamento de Secretearía General, la canaleta que se recomienda debe de tener las siguientes características:

- Canaleta de PVC de 1 compartimiento.
- De color blanco.
- Que sea auto extinguible.
- Que sea resistente a los impactos.

Esta canaleta se la puede ver en la figura 6.188.

Figura 6.188. ***Canaletas.***[79]

De esta forma para evitar que se tenga los cables de la línea telefónica en el piso, y que el cableado del teléfono, cableado de red y electricidad estén en una misma canaleta.

6.9.6.2 Cajetines.

Se recomienda cambiar los cajetines que se encuentran en su gran mayoría en el Departamento de Secretaria General. Este cajetín se le puede ver en la figura 6.189.

[79] http://desenchufados.net/protege-los-cables-electricos-ocultalos-o-empotralos/

Figura 6.189. Cajetines.[80]

6.9.7 Pinchazos a la Red.

Recomendamos que se tenga mayor cuidado con el cableado de red que se encuentra instalado actualmente en la fábrica, ya que algunas partes el cableado no tiene ningún tipo de protección y podrían ser cortados o manipulados con mala intensión por personal interno o externo de la fábrica, por lo que se recomienda no dejar cables sin la debida protección.

Recomendamos utilizar un software para detectar intrusos como son los sniffer a la red de la fábrica.

A continuación damos una breve explicación de una herramienta que sería de ayuda para detectar sniffer.

6.9.7.1 PromqryUI 1.0.

PromqryUI es una herramienta que detecta las interfaces de red que se estarían ejecutando en modo promiscuo, la misma que es un software que cuenta con una interfaz gráfica de usuario.

PromqryUI tienen la capacidad de:

- Consultar las interfaces del equipo local de la red.
- Consultar las interfaces de un único equipo remoto.
- Consultar una amplia gama de interfaces de equipos remotos.

Para la utilización de estas herramientas se requiere lo siguiente:

- Tener instalado .NET Framework en el ordenador desde el cual se va a ejecutar este programa. Los equipos remotos no necesitan tener instalado.

[80] http://articulo.mercadolibre.com.ve/MLV-19662724-cajetin-para-telefono-superficial-caj-03-2-tomas-paralelas-_JM

- Ejecutarse bajo el contexto de seguridad del administrador en el equipo que se está consultando.
- Utilizan Windows Management Instrumentation (WMI), el cual ya viene incorporado en las versiones de Windows.

6.9.7.1.1 Uso de PromqryUI 1.0.

La interfaz de PromqryUI tiene dos paneles. El panel de la izquierda muestra los sistemas a consultar, y el panel de la derecha muestra la salida que se genera cuando se hace clic en el botón START QUERY. Esta interfaz se la puede ver en la figura 6.190.

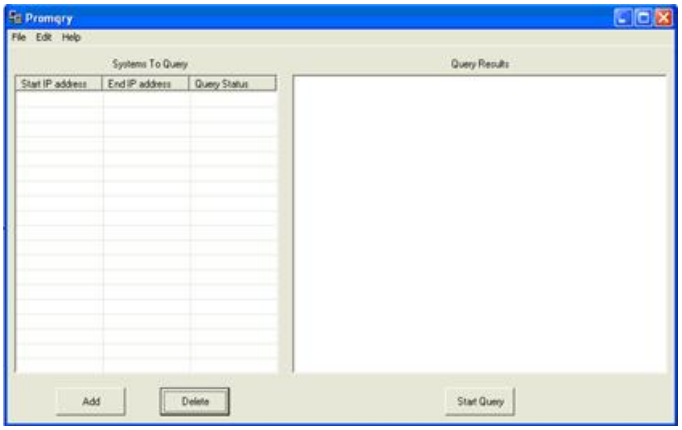


Figura 6.190. Ventana 1 descripción de la herramienta PromqryUI 1.0.[81]

Para agregar sistemas a la lista se hace clic en **Add.** A continuación se pedirá si desea agregar un único sistema o una gama de sistemas a la lista. Para agregar un sistema se puede ver en la figura 6.191.

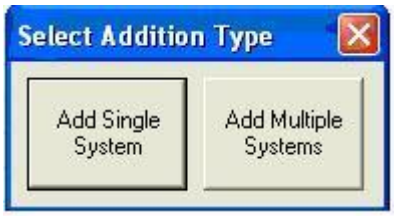


Figura 6.191. ***Ventana 2 descripción de la herramienta PromqryUI 1.0.***[82]

Sistemas simples pueden ser agregados con su dirección IP o con su nombre. Si un nombre se agrega, PromqryUI intenta resolver el nombre a una dirección IP al hacer

[81] http://support.microsoft.com/kb/892853/en-us
[82] http://support.microsoft.com/kb/892853/en-us

clic en el botón START QUERY. Si el nombre no se resuelve a una dirección IP, la consulta falla. En la figura 6.192 de puede ver como se agrega un dirección IP.

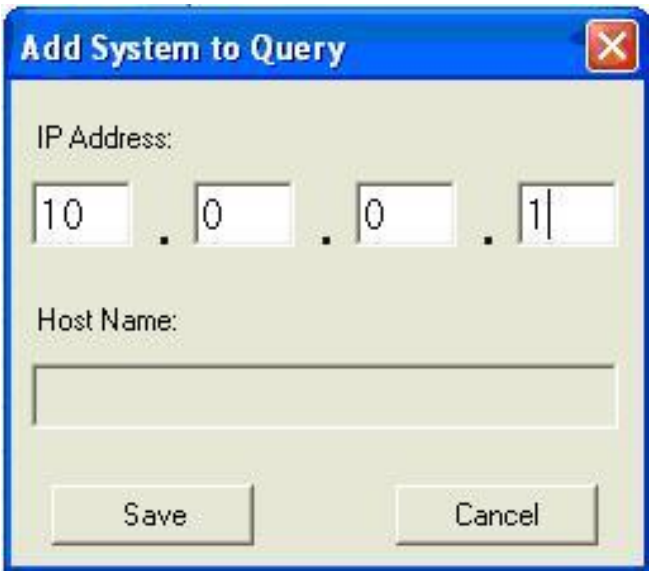


Figura 6.192. ***Ventana 3 descripción de la herramienta PromqryUI 1.0.***[83]

Cuando se agrega una gama de sistemas para la consulta, la dirección de IP de inicio debe ser inferior a la dirección IP de la final. Esta se la puede ver en la figura 6.193.

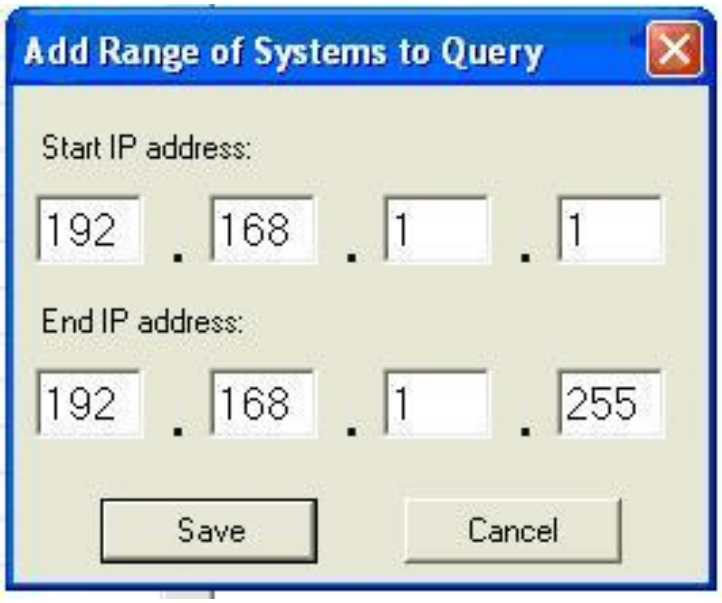


Figura 6.193. ***Ventana 4 descripción de la herramienta PromqryUI 1.0.***[84]

Después de agregar sistemas, se debe hacer clic para seleccionar la casilla junto a cada uno de ellos para seleccionar los sistemas que desea consultar. Esto se le puede ver en la figura 6.194.

[83] http://support.microsoft.com/kb/892853/en-us
[84] http://support.microsoft.com/kb/892853/en-us

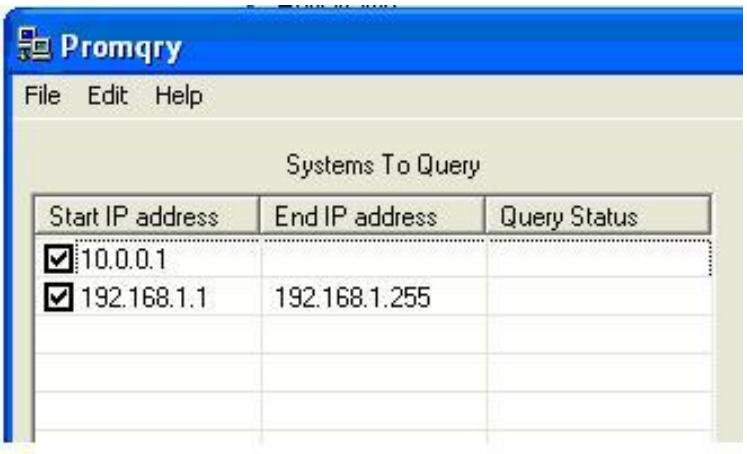


Figura 6.194. ***Ventana 5 descripción de la herramienta PromqryUI 1.0.***[85]

Todos los sistemas que han agregado a la lista se guardarán automáticamente cuando se salga del programa. La próxima vez que se inicie PromqryUI, la lista de **Sistemas para la consulta** se rellena automáticamente con los sistemas y los rangos que se guardaron.

Puede utilizar el menú **edición** para establecer la opción de ping. Esta se la puede ver en la figura 6.195.

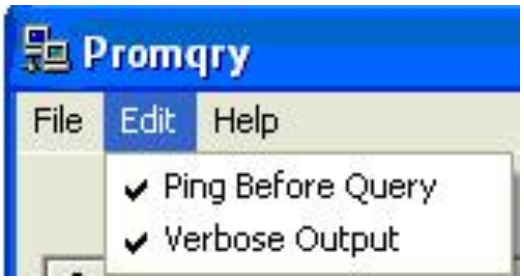


Figura 6.195. ***Ventana 6 descripción de la herramienta PromqryUI 1.0.***[86]

Pulse el botón de START QUERY para empezar a consultar los sistemas seleccionados. Si no hay interfaces que se esté ejecutando en modo promiscuo, recibirá un mensaje similar del mensaje que se muestra en la figura 6.196.

[85] http://support.microsoft.com/kb/892853/en-us
[86] http://support.microsoft.com/kb/892853/en-us

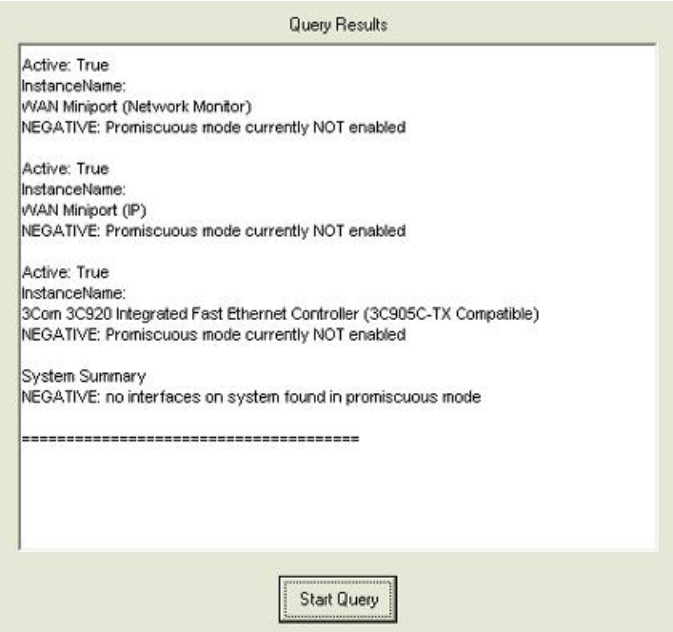


Figura 6.196. ***Ventana 7 descripción de la herramienta PromqryUI 1.0.***[87]

Si se encuentra una interfaz que se esté ejecutando en modo promiscuo, recibirá un mensaje similar a la que se muestra en la figura 6.197.

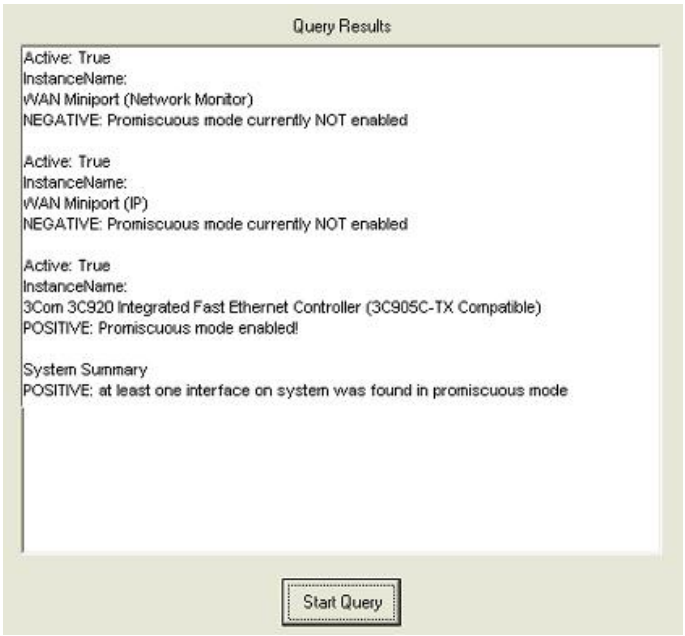


Figura 6.197. ***Ventana 8 descripción de la herramienta PromqryUI 1.0.***[88]

Cuando PromqryUI encuentra un host que tiene una interfaz que se ejecuta en modo promiscuo, PromqryUI utiliza WMI para consultar el host y obtener información

[87] http://support.microsoft.com/kb/892853/en-us
[88] http://support.microsoft.com/kb/892853/en-us

adicional para que sea más fácil de identificar ese host. El siguiente es un ejemplo de estos datos:

- Nombre del equipo: MiPC
- Dominio: contoso.com
- Fabricante de equipo: Dell Computer Corporation
- Modelo de ordenador: Precision WorkStation 340
- Dueño primario: John Smith
- Usuario actualmente conectado: contoso\user1
- Funcionamiento: Microsoft ® Windows ® Server 2003, Enterprise Edition Organización: Contoso Corp.

6.10 Recomendación de políticas de prohibición de la instalación de programas o equipos personales en la red.

Para controlar que los usuarios instalen software que la fábrica no lo autoriza ya que no se tiene la respectiva licencia o porque no son de apoyo para las labores diarias del usuario, se recomienda la utilización de la herramienta OCS Inventory, para la cual damos una breve descripción.

6.10.1 El Software Inventory (OCS).

Es un software que permite al encargado de la red administrar el inventario de las PC que se encuentran en funcionamiento en la fábrica, obteniendo un inventario completo de todo el software instalado y además del hardware.

Algunas características importantes de Inventory OCS, es que da la posibilidad de implementar aplicaciones en las PC de acuerdo a criterios de búsqueda, escanear la red por medio del IPDiscovery, o instalar aplicaciones remotamente.

IPDiscovery: Especifica el número de agente a pedir IP en funcionamiento. Si deja el valor por defecto 2, lo cual significa que el servidor de Comunicación solicitará a los 2 equipos más activos de cada sub red la IP para ejecutar descubrimiento de sus características. Si ajusta a 0, la IP para descubrimiento se desactivará.

Discovery_Latency: Devuelve el tiempo en segundos a esperar entre la exploración de cada dirección IP.

6.10.1.1 Funcionamiento de la herramienta.

Esta herramienta básicamente recopila información sobre el hardware y software de todos los equipos que hay en la red. Funciona instalando un servidor y en todas las PC como cliente, para la visualización de resultados se lo hace con una interfaz web.

La conexión entre los equipos clientes y el servidor se basan en el protocolo HTTP y el formato de los datos se realiza en XML.

En el servidor utiliza las siguientes herramientas:

- Apache.
- MySQL.
- Perl.

Con una interfaz web en PHP se puede tener servicios como:

- Consulta del inventario.
- Una interfaz de desglose servicio (o Helpdesk) para los técnicos.

La figura 6.198 muestra una pantalla de forma general como identifica las PC clientes.

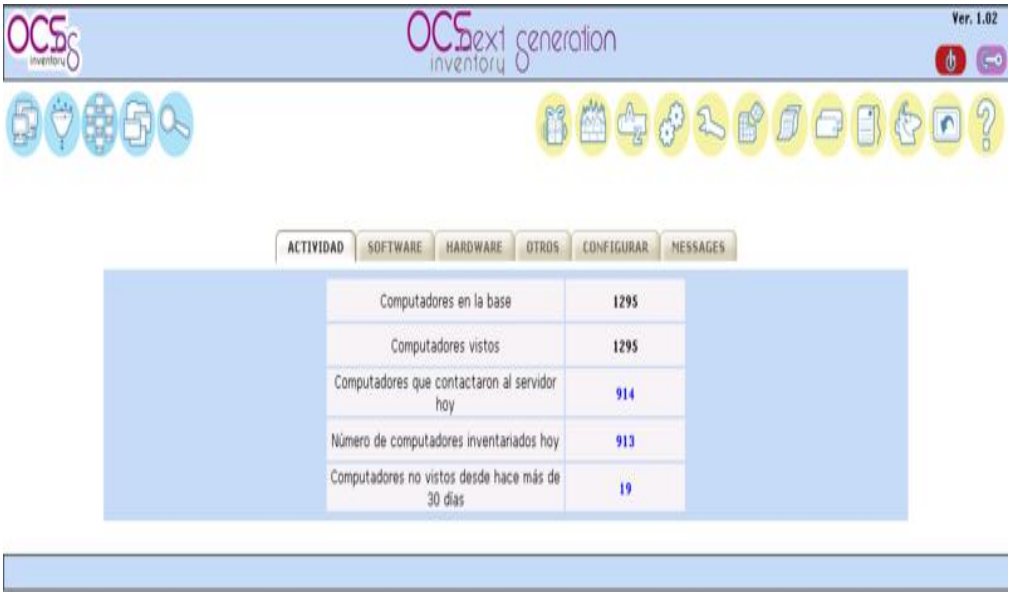


Figura 6.198. Ventana 1 descripción de la herramienta Inventory.[89]

Para realizar consultas predeterminadas se tiene en el menú. La cual se puede ver en la figura 6.198.

[89] http://www.scribd.com/doc/12882340/Manual-de-OCSInventory


Mirar todos los computadores.


Mirar distribución de computadores agrupados por TAG.


Buscar computadores utilizando varios criterios.

Para realizar búsquedas según criterios que se desee.

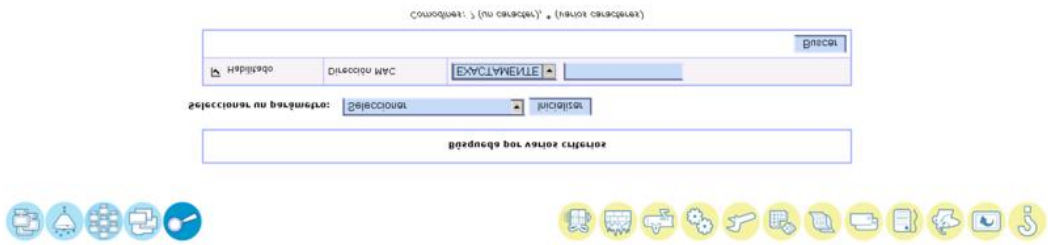


Figura 6.199. ***Menú de la herramienta Inventory.***[90]

Los parámetros predeterminados de búsqueda son:

- Versión del BIOS.
- Nombre del Computador.
- IpDiscover Personalizado.
- Distribución de Paquetes.
- Espacio Libre en Disco.
- Frecuencia de Inventarios.
- Punto de Salida (gateway).
- Dirección IP.
- Estado de IpDiscover.
- Inventario.
- Dirección MAC.
- Fabricante del Sistema.
- Memoria.
- Fabricante del Monitor.
- Número de Serie del Monitor.
- Número de Red.

[90] http://www.scribd.com/doc/12882340/Manual-de-OCSInventory

- Sistema Operativo.
- Velocidad del Procesador.
- Software.
- Valor de la Etiqueta.
- Usuario Conectado.

RESUMEN Y CONCLUSIONES

La auditoria informática que se realizo a las redes de comunicaciones de computadores de la Pasamanería S.A comprendió un análisis del estado de toda la red, es decir estructura existente, infraestructura lógica y física, problemas y rendimiento de la misma.

La auditoria de redes que se realizo se baso en el método de entrevistas en la que no se siguió un plan determinado, ni un método estricto de sometimiento a un cuestionario.

De esta manera se puso a prueba la red informática de la fábrica, evaluando su desempeño y seguridad.

Básicamente se identifico las áreas que necesitan tomar medidas para su mejor funcionamiento, esto se logro analizando el estado de la red.

A continuación se realizara un breve resumen de cada uno de los capítulos de la tesis.

En el capítulo I se presento una descripción general de la fábrica, en la cual se indica una reseña histórica y el estado en el que se encuentra actualmente, identificando las respectivas áreas en funcionamiento.

En el capítulo II, se presento los conceptos básicos de internetworking identificando de manera general como está conformada una red de computadores, es decir dispositivos que conforman una red, topologías de red etc., además de su funcionamiento basándose en la panorámica del modelo de referencia OSI.

En el capítulo III se presento la auditoria de las comunicaciones, en la misma que se analizo cual era la gestión de la red en la fabrica supervisando las herramientas de apoyo para realizar este trabajo, además se verifico los equipos y su respectiva conectividad.

En este capítulo se analizo la forma de monitorizar las comunicaciones y por supuesto la revisión de costes y asignación formal de proveedores, se realizó la respectiva supervisión de aplicabilidad de estándares.

En el capítulo IV básicamente se realizo la auditoria de la red física, en la cual se verifico el cuarto de telecomunicaciones que se encuentra implementado bajo los estándares que se han mencionado en el capitulo.

Además se verifico estándares y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos y el correcto funcionamiento de la red.

Inclusive se verifico la existencia de estándares de etiquetación y administración del cableado horizontal y backbone.

El Capitulo V, está más orientado a la red lógica ya que se analizo el uso de contraseñas de acceso tanto para las PC como para los respectivos servidores.

Además se analizo el control de errores, es decir el método para identificar un posible error en la red.

Lo fundamental que se presenta en este capítulo corresponde a las actividades de los usuarios en la red, encriptación de la información, seguridad de accesos a servidores remotos, entro otros.

Una vez analizada la red se procedió a la realización del capítulo final de la tesis.

El capítulo VI, el mismo que corresponde a las respectivas recomendaciones en cada caso que hemos considerado necesario para mejorar el funcionamiento de la red de la fábrica.

BIBLIOGRAFÍA

[1] http://download.netop.com/manuals/300/es_manual.pdf

[2] http://www.ubuntugeek.com/install-and-configure-cacti-monitoring-tool-in-ubuntu-810-intrepid-ibex-server.html

[3] http://www.cacti.net/downloads/docs/html/index.html

[4] http://www.guia-ubuntu.org/index.php?title=Ntop

[5] http://www.technoblog.com.ar/index.php/2010/02/como-instalar-ntop-en-ubuntu-9-10/

[6] http://www.solid-rock-it.com/web-solid-rock/blog/index.php/2008/03/11/35-monitorizacion-de-red-con-ntop

[7] http://jpangamarca.wordpress.com/2008/03/27/instalar-wireshark-y-packet-tracer-en-linux-ubuntu/

[8] http://www.scribd.com/doc/8770104/Manual-de-Monitoreo

[9] http://www.mcsebas.com.ar/apuntes/redes/diapositiva2.pdf

[10] http://seguridad.7espejos.com/auditoria

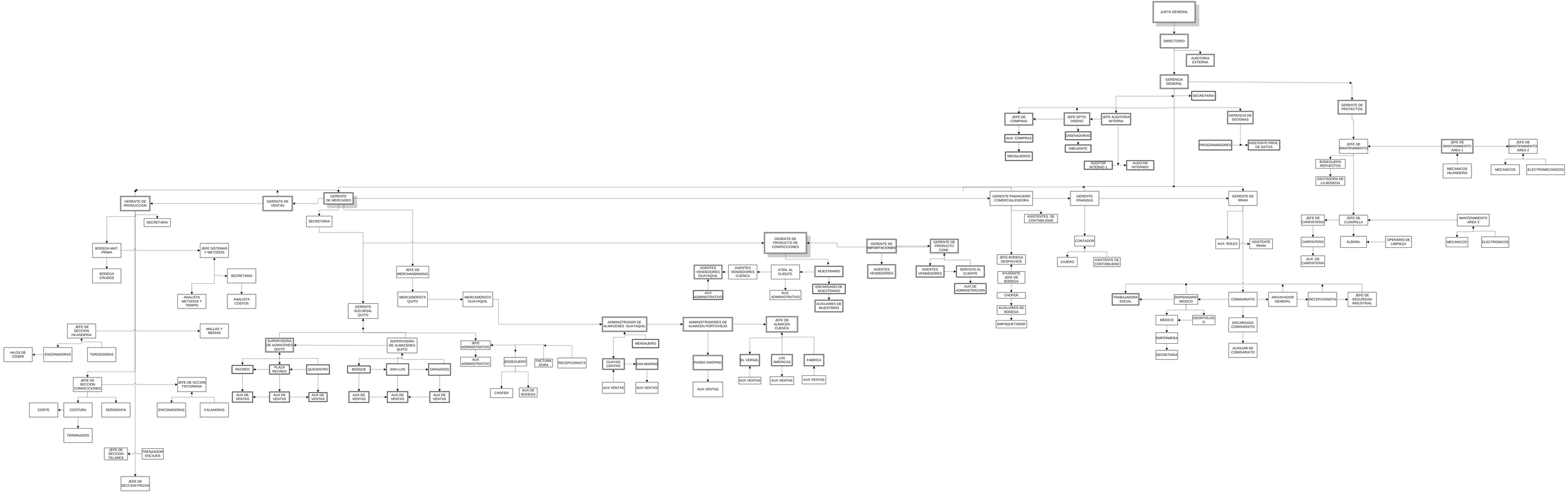
[11] http://comunicacionredes.wordpress.com/category/informatica/comunicacion-y-redes/

[12] http://topologiadered-kelvin.blogspot.com/2009/05/topologia-en-estrella.html

ANEXO 1

ESTRUCTURA ORGANIZACIONAL

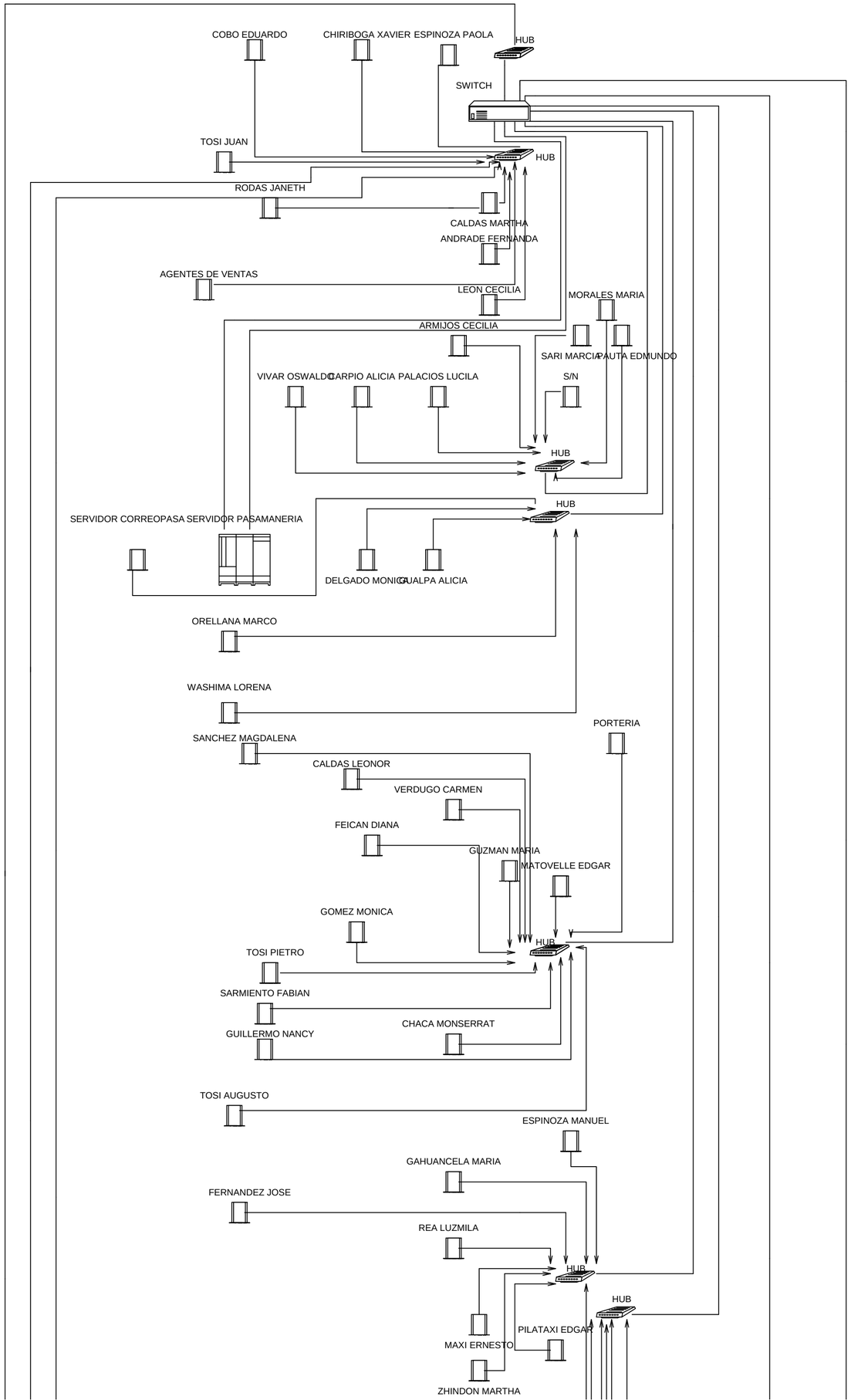
En este Anexo se muestra cual es la estructura organizacional de la fábrica Pasamanería S.A.

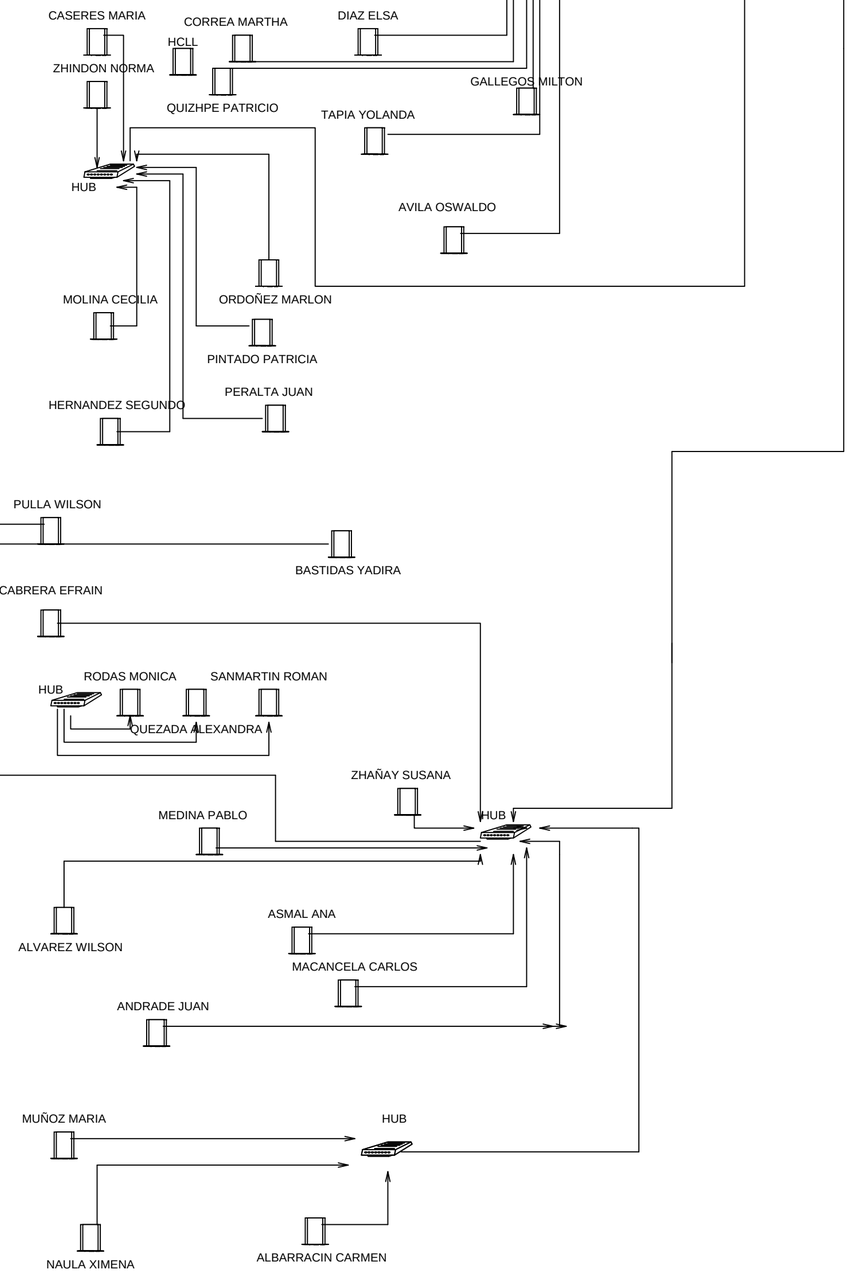

JUNTA GENERAL
DIRECTORIO
AUDITORIA EXTERNA
GERENCIA GENERAL
SECRETARIA
JEFE DE COMPRAS
AUX. COMPRAS
MENSAJEROS
JEFE DPTO. DISENO
DISENADORAS
DIBUJANTE
JEFE AUDITORIA INTERNA
AUDITOR INTERNO 1
AUDITOR INTERNO2
GERENCIA DE SISTEMAS
PROGRAMADORES
ASISTENTE PROC DE DATOS
GERENTE DE PROYECTOS
JEFE DE MANTENIMIENTO
BODEGUERO REPUESTOS
DIGITADORA DE LA BODEGA
JEFE DE MANTANIMIENTO AREA 3
MECANICOS HILANDERIA
JEFE DE MANTENIMIENTO AREA 7
MECANICOS
ELECTROMECANICOS
GERENTE DE PRODUCCION
SECRETARIA
BODEGA MAT. PRIMA
BODEGA CRUDOS
JEFE SISTEMAS Y METODOS
SECRETARIA
ANALISTA METODOS Y TIEMPO
ANALISTA COSTOS
JEFE DE SECCION HILANDERIA
HILOS DE COSER
ENCONADORAS
TORCEDORAS
MALLAS Y MEDIAS
JEFE DE SECCION CONFECCIONES
CORTE
COSTURA
SERIGRAFIA
TERMINADOS
REFE DE SECCION TINTORERIA
ENCONADORAS
CALANDRAS
JEFE DE SECCION TELARES
TRENZADOR ENCAJES
JEFE DE SECCION PIEZAS
GERENTE DE VENTAS
GERENTE DE MERCADEO
SECRETARIA
GERENTE SUCURSAL QUITO
SUPERVISORA DE ALMACENES QUITO
RECREO
PLAZA RECREO
QUICENTRO
AUX DE VENTAS
AUX DE VENTAS
AUX DE VENTAS
SUPERVISORA DE ALMACENES QUITO
BOSQUE
SAN LUIS
GRANADOS
AUX DE VENTAS
AUX DE VENTAS
AUX DE VENTAS
JEFE DE MERCHANDISING
MERCADERISTA QUITO
MERCADERISTA GUAYAQUIL
JEFE ADMINISTRATIVO
AUX ADMINISTRATIVO
BODEGUERO
FACTURADORA
RECEPCIONISTA
CHOFER
AUX DE BODEGA
ADMINISTRADOR DE ALMACENES GUAYAQUIL
MENSAJERO
GUAYAS CENTRO
SAN MARINO
AUX VENTAS
AUX VENTAS
GERENTE DE PRODUCTO DE CONFECCIONES
AGENTES VENDEDORES CUENCA
AGENTES VENDEDORES GUAYAQUIL
AUX ADMINISTRATIVO
ATEN. AL CLIENTE
AUX. ADMINISTRATIVO
MUESTRARIO
ENCARGADO DE MUESTRARIO
AUXILIARES DE MUESTRARIO
ADMINISTRADORES DE ALMACEN PORTOVIEJO
PASEO SHOPING
AUX VENTAS
JEFE DE ALMACEN CUENCA
EL VERGEL
LAS AMERICAS
FABRICA
AUX VENTAS
AUX VENTAS
AUX VENTAS
GERENTE DE IMPORTACIONES
AGENTES VENDEDORES
GERENTE DE PRODUCTO CONF.
AGENTES VENDEDORES
SERVICIO AL CLIENTE
AUX DE ADMINISTRACION
GERENTE FINANCIERO COMERCIALIZADORA
ASISTENTES DE CONTABILIDAD
JEFE BODEGA DESPACHOS
AYUDANTE JEFE DE BODEGA
CHOFER
AUXILIARES DE BODEGA
EMPAQUETADOR
GERENTE FINANZAS
CONTADOR
CAJERO
ASISTENTE DE CONTABILIDAD
GERENTE DE RRHH
AUX. ROLES
ASISTENTE RRHH
TRABAJADORA SOCIAL
DISPENSARIO MEDICO
MEDICO
ODONTOLOGO
ENFERMERA
SECRETARIA
COMISARIATO
ENCARGADA COMISARATO
AUXILIAR DE COMISARATO
ARCHIVADOR GENERAL
RECEPCIONISTA
JEFE DE SEGURIDAD INDUSTRIAL
JEFE DE CARPNTERIA
CARPINTERO
AUX. DE CARPINTERIA
JEFE DE CUADRILLA
ALBANIL
OPERARIO DE LIMPIEZA
MANTENIMIENTO AREA 3
MECANICOS
ELECTRONICOS

ANEXO 2

DIAGRAMA DE RED DESACTUALIZADA DE LA PASAMANERIA S.A

En este Anexo2 se muestra el diagrama de la red desactualizada en la fábrica.


COBO EDUARDO
CHIRIBOGA XAVIER
ESPINOZA PAOLA
HUB
SWITCH
TOSI JUAN
HUB
RODAS JANETH
CALDAS MARTHA
ANDRADE FERNANDA
AGENTES DE VENTAS
LEON CECILIA
MORALES MARIA
ARMIJOS CECILIA
SARI MARCIA
PAUTA EDMUNDO
VIVAR OSWALDO
CARPIO ALICIA
PALACIOS LUCILA
S/N
HUB
HUB
SERVIDOR CORREOPASA
SERVIDOR PASAMANERIA
DELGADO MONICA
GUALPA ALICIA
ORELLANA MARCO
WASHIMA LORENA
PORTERIA
SANCHEZ MAGDALENA
CALDAS LEONOR
VERDUGO CARMEN
FEICAN DIANA
GUZMAN MARIA
MATOVELLE EDGAR
GOMEZ MONICA
HUB
TOSI PIETRO
SARMIENTO FABIAN
CHACA MONSERRAT
GUILLERMO NANCY
TOSI AUGUSTO
ESPINOZA MANUEL
GAHUANCELA MARIA
FERNANDEZ JOSE
REA LUZMILA
HUB
HUB
PILATAXI EDGAR
MAXI ERNESTO
ZHINDON MARTHA


CASERES MARIA
CORREA MARTHA
DIAZ ELSA
HCLL
ZHINDON NORMA
GALLEGOS MILTON
QUIZHPE PATRICIO
TAPIA YOLANDA
HUB
AVILA OSWALDO
MOLINA CECILIA
ORDOÑEZ MARLON
PINTADO PATRICIA
PERALTA JUAN
HERNANDEZ SEGUNDO

PULLA WILSON
BASTIDAS YADIRA
CABRERA EFRAIN
RODAS MONICA
SANMARTIN ROMAN
HUB
QUEZADA ALEXANDRA
ZHAÑAY SUSANA
HUB
MEDINA PABLO
ASMAL ANA
ALVAREZ WILSON
MACANCELA CARLOS
ANDRADE JUAN

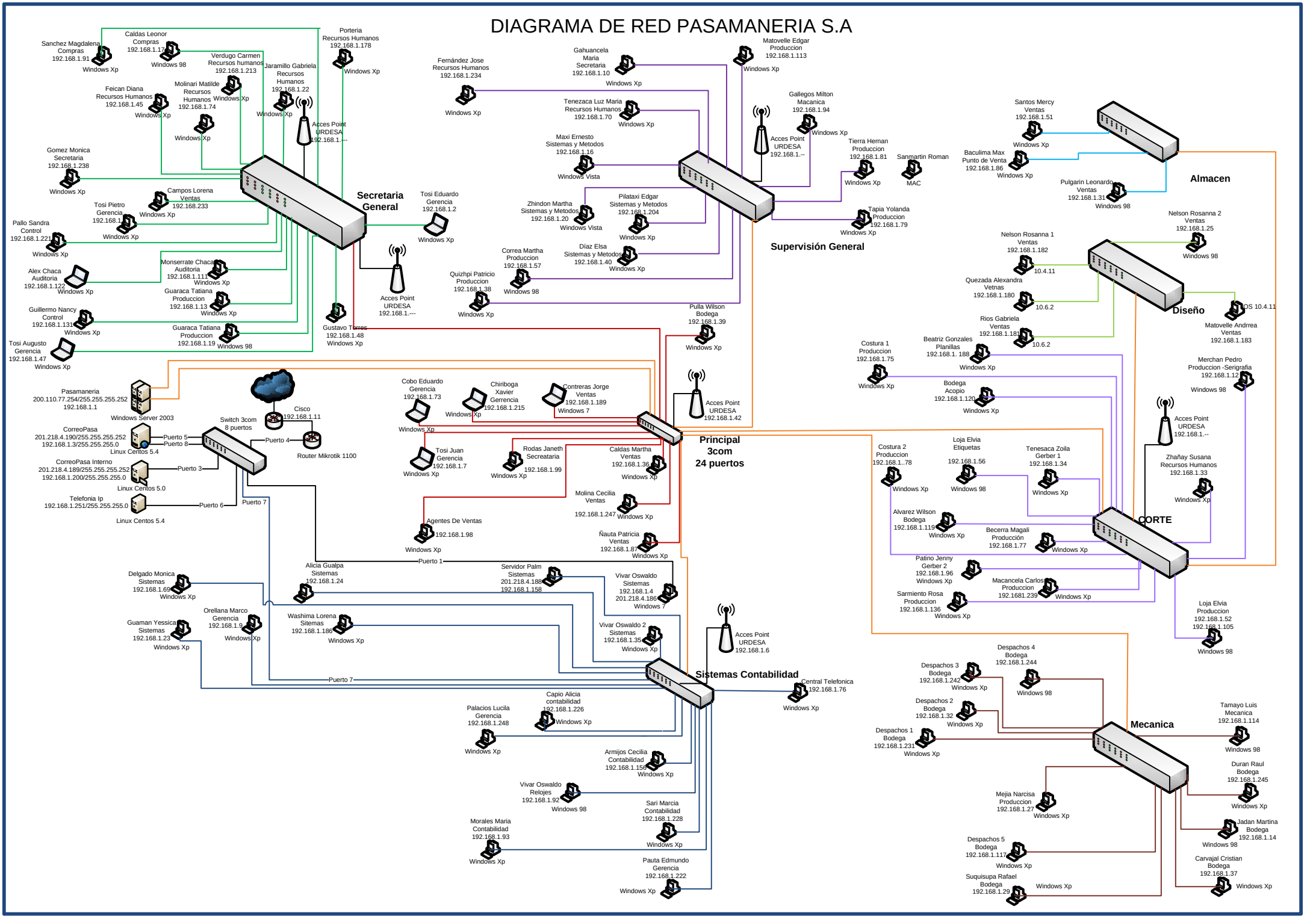
MUÑOZ MARIA
HUB
NAULA XIMENA
ALBARRACIN CARMEN

ANEXO 3

DIAGRAMA DE RED ACTUALIZADA DE LA PASAMANERIA S.A

En este Anexo3 se muestra el diagrama de la red actualizada de la fábrica.

DIAGRAMA DE RED PASAMANERIA S.A



ANEXO 4

DIAGRAMA DE RED RECOMENDADO

En este Anexo4 se muestra el diagrama de la red que se recomienda para la fábrica.

DIAGRAMA DE RED PASAMANERIA S.A