DISEÑO, DEFINICIÓN DE POLÍTICAS DE GESTIÓN DE UNA RED LAN PARA LA EMPRESA APP MACHINES LTDA. EN LA CIUDAD DE BOGOTÁ.

DIEGO ARMANDO CASTRO MONTEALEGRE

JAIRO HERNANDO PUENTES FERNANDEZ

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2009

DISEÑO, DEFINICIÓN DE POLÍTICAS DE GESTIÓN DE UNA RED LAN PARA LA EMPRESA APP MACHINES LTDA. EN LA CIUDAD DE BOGOTÁ.

DIEGO ARMANDO CASTRO MONTEALEGRE

JAIRO HERNANDO PUENTES FERNANDEZ

Proyecto de Grado como requisito para optar por el título de Ingeniero de Sistemas

Asesor:

ING. LUIS GUILLERMO MARTINEZ B.

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2009

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C. (día, mes, año)

AGRADECIMIENTOS:

A Dios por darme la oportunidad de vivir día a día, a mis padres, Melvin Castro R., María Clemencia Montealegre M. y mi hermana Monika Castro Montealegre (Q.E.P.D), ellos son los que me empujaron y me dieron fuerza para seguir adelante cada vez que caí, realmente son quienes me impulsan para salir adelante. Al Ingeniero Aldo Forero, al Ingeniero Luis Guillermo Martínez mi tutor, por tener tanta paciencia con mi grupo de trabajo, a la Ingeniera Patricia Giraldo por ser la persona que me exigió y aconsejo cuando quise dejar a medias la carrera, al Ingeniero Álvaro Camilo Polo por abrirme las puertas de su empresa para desarrollar este proyecto, al Ingeniero Esteban Talavera por el apoyo y el acompañamiento durante el proyecto. A Ángela Marcela Flórez por ser mi brújula y mi norte durante estos años que he pasado en la Universidad, la gran mayoría de las cosas las hice por ella, finalmente a todos aquellos que me acompañaron durante este camino y que ahora ven cumplido este sueño, compañeros y amigos Rolando Sánchez, Felipe Orozco, Fabián Vargas, Daniel Ortiz, David Pardo, entre muchos otros a los cuales ofrezco disculpas por no nombrarlos, todos han aportado su granito de arena para mi crecimiento integral como persona…

Diego Armando Castro Montealegre.

AGRADECIMIENTOS:

A Dios fuente de sabiduría por iluminar mi razón mi voluntad y mi inteligencia para lograr esta gran meta. A mis padres Luis Ignacio Puentes, mi madre Soledad Fernández Fernández y hermanas Mónica Puentes y Diana Puentes y mi sobrino David López por el sí generoso y constante en mi proceso de formación. Al Rector de la Universidad de San Buenaventura Fray José Wilson Téllez Casas O.F.M., por la compañía en esta gran etapa de mi vida profesional. A Fray Fernando Garzón Ramírez provincial de la comunidad Franciscana quien ha sido el amigo compañero y confidente. Al grupo de Ingenieros que desde sus conocimientos orientaron el día a día de mi interés de conocer y aprender esta disciplina. En especial al Ingeniero Luis Guillermo Martínez el cual guió y orientó este trabajo. A Diego Armando Castro Montealegre compañero de esta etapa de nuestra vida el cual ha sido de gran ayuda para sacarla adelante. A Paola Ramírez que siempre me ha acompañado y apoyado, también ha sido fuente de inspiración para salir adelante en momentos difíciles A todos mis amigos y compañeros que intervinieron y participaron en mi proceso de formación…

Jairo Hernando Puentes Fernández

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

Carta de Marzo 24 de 2009, que certifica la visita en Marzo 12 de 2009, para el levantamiento de información relacionada con la planta física y la distribución de equipos.

Carta de Marzo 24 de 2009, que certifica la aprobación del presupuesto para ser utilizado en el proyecto de grado.

Carta de Abril 3 de 2009, que certifica la visita realizada el 2 de Abril de 2009, para el levantamiento de información relacionada con la conexión a internet y el rendimiento de la misma.

Carta de Abril 3 de 2009, que certifica la visita realizada el 2 de Abril de 2009, para el levantamiento de información relacionada con los nuevos requerimientos de red.

Anexo C: Informes y demás.

Informes EVEREST (Formato .txt)

Archivo configuración R1

Archivo configuración Sw1

Archivo configuración Sw2

Cotizaciones de las Empresas: Q&C Ingeniería Ltda; Tecknolink Ltda; Daga S.A.

Costo Final Proyecto

GLOSARIO

ADMINISTRACIÓN DE LA RED: Término genérico que se usa para describir sistemas o acciones que ayudan a mantener, describir o solucionar los problemas de una red.

AGENTE: 1. Por lo general, software que procesa consultas y envía respuestas en nombre de una aplicación.
2. En los NMS, un proceso que reside en todos los dispositivos administrados e informa sobre los valores de variables especificadas a las estaciones de administración.
3. En la arquitectura de hardware de Cisco, una tarjeta de procesador individual que proporciona una o más interfaces de medios.

AGUJERO NEGRO: término de enrutamiento para un área de la internetwork donde los paquetes entran, pero no emergen, debido a condiciones adversas o una mala configuración del sistema en una parte de la red.

ANALIZADOR DE RED: dispositivo de control de la red que mantiene información estadística con respecto al estado de la red y de cada dispositivo conectado a ella. Las versiones más sofisticadas que usan inteligencia artificial pueden detectar, definir y solucionar los problemas de la red.

ANCHO DE BANDA: diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. También se utiliza este término para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

ARMARIO PARA EL CABLEADO: habitación diseñada especialmente para realizar un tendido de cables en una red de datos o de voz. Los armarios para el cableado sirven como un punto de unión central para el cableado y para el equipo de cableado que se utiliza para interconectar dispositivos.

ARP (PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES): protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC.

ATENUACIÓN: pérdida de energía de la señal de comunicación.

BACKBONE: parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de, y se destina a, otras redes.

BANDA ANCHA: sistema de transmisión que multiplexa varias señales independientes en un cable. En la terminología de telecomunicaciones, cualquier

canal que tenga un ancho de banda mayor que un canal de grado de voz (4 kHz). En la terminología de las LAN, un cable coaxial en el que se usa señalización analógica.

BASH (**BOURNE-AGAIN SHELL)**. Intérprete de comandos interactivo de UNIX basado en el intérprete de comandos tradicional Bourne, pero con mayor funcionalidad.

BROADCAST DE IP: técnica de enrutamiento que permite que el tráfico de IP se propague desde un origen hasta una serie de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, un paquete se envía a un grupo de broadcast identificado a través de una sola dirección IP de grupo de destino.

CABLE: medio de transmisión de alambre de cobre o fibra óptica que se envuelve en una cubierta protectora.

CABLE BLINDADO: cable que tiene una capa de material aislante para disminuir la EMI.

CABLE COAXIAL: cable compuesto por un conductor cilíndrico externo hueco, que reviste un conductor con un solo cable interno. Actualmente se usan dos tipos de cable coaxial en las LAN: el cable de 50 ohmios, utilizado para la señalización digital y el cable de 75 ohmios, utilizado para señales analógicas y para la señalización digital de alta velocidad.

CABLE DE FIBRA ÓPTICA: medio físico que puede conducir la transmisión modulada de luz. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otro lado no es susceptible a la interferencia electromagnética y permite mayores velocidades de transmisión de datos. A veces se le denomina *fibra óptica*.

CABLE DE PAR TRENZADO: medio de transmisión de velocidad relativamente baja, que consta de dos cables aislados colocados según un patrón de espiral regular. Los cables pueden ser blindados o no blindados.

CABLEADO DE CATEGORÍA 5: uno de los cinco grados de cableado UTP descritos en el estándar EIA/TIA 568B. El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps

CACHÉ: almacenamiento local y temporal de un programa, de los mensajes de respuesta y el subsistema que controla el almacenamiento, la recuperación y eliminación de sus mensajes. Un caché, almacena respuestas para reducir el tiempo de respuesta y el consumo de ancho de banda de red en demandas equivalentes futuras.

CANALETA: canal montado en la pared que tiene una tapa móvil que se utiliza para colocar cableado horizontal.

CIFRADO: aplicación de un algoritmo específico a los datos a fin de alterar su apariencia y volverlos incomprensibles para quienes no estén autorizados a ver la información.

CISCO SYSTEM: empresa multinacional ubicada en San José (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones tales como:
Dispositivos de conexión para redes informáticas: routers (enrutadores, encaminadores o ruteadores), switches (conmutadores) y hubs (concentradores).

- Dispositivos de seguridad como Cortafuegos y Concentradores para VPN.
- Productos de Telefonía IP como teléfonos y el CallManager.
- Software de gestión de red como CiscoWorks.
- Equipos para Redes de Área de Almacenamiento.
- Actualmente, Cisco Systems, es Líder Mundial en soluciones de red e infraestructuras para Internet.

CLIENTE: nodo o programa de software (dispositivo front-end) que requiere servicios de un servidor.

CODEC (CODIFICADOR-DECODIFICADOR): dispositivo que normalmente usa PCM para transformar las señales analógicas en una corriente de bits digitales, y las señales digitales en analógicas.

CODIFICACIÓN: técnicas eléctricas utilizadas para transportar señales binarias. 2. Proceso a través del cual los bits son representados por voltajes.

CÓDIGO DE CORRECCIÓN DE ERRORES: código que tiene la inteligencia suficiente y que incorpora suficiente información de señalización como para permitir la detección y corrección de varios errores en el receptor.

CÓDIGO DE DETECCIÓN DE ERRORES: código que puede detectar los errores de transmisión a través del análisis de los datos recibidos sobre la base de la conformidad de los datos a las pautas estructurales apropiadas.

COLISIÓN: en Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de los dos dispositivos chocan y se dañan cuando se encuentran en los medios físicos

CONECTOR RJ CONECTOR DE JACK REGISTRADO: conectores estándar utilizados originalmente para conectar las líneas telefónicas. En la actualidad, los

conectores RJ se utilizan para conexiones telefónicas y para 10BaseT y otros tipos de conexiones de red. RJ-11, RJ-12 y RJ-45 son tipos de conectores RJ populares.

CONFIABILIDAD: relación entre la cantidad de señales de supervivencia (keepalives) esperada y la recibida de un enlace. Si el porcentaje es alto, la línea es confiable. Se utiliza como una métrica de enrutamiento.

CONGESTIÓN: tráfico que supera la capacidad de la red.

CONSOLA: DTE a través del cual se introducen las instrucciones a un host.

CONTROL DE ERRORES: técnica utilizada para detectar y corregir errores en las transmisiones de datos.

CONTROL DE FLUJO: técnica que permite asegurar que una entidad de transmisión, como por ej., un módem, no sobrecargue una entidad receptora con datos. Cuando los búferes de un dispositivo receptor están llenos, el mensaje se envía al dispositivo emisor para que suspenda la transmisión hasta que los datos del búfer se hayan procesado.

CSMA/CD ACCESO MÚLTIPLE CON DETECCIÓN DE PORTADORA Y DETECCIÓN DE COLISIONES: mecanismo de acceso a medios mediante el cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que coliden. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

DIAFONÍA: energía de interferencia que se transfiere de un circuito a otro.

DIRECCIÓN: estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular.

DIRECCIÓN DE BROADCAST: dirección especial reservada para enviar un mensaje a todas las estaciones. Por lo general, una dirección de broadcast es una dirección MAC de destino compuesta exclusivamente por todos los números uno.

DIRECCIÓN IP: 1. dirección de 32 bits asignada a los hosts que usan TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host... Los números de red y de subred se utilizan conjuntamente para

el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet.

2. Instrucción utilizada para establecer la dirección de red lógica de esta interfaz.

DNS SISTEMA DE DENOMINACIÓN DE DOMINIO: sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DOMINIO: 1. en la Internet, una parte del árbol jerárquico de denominación que se refiere a agrupamientos generales de redes basados en un tipo de organización o geografía.

2. En SNA, un SSCP y los recursos que controla.

3. En IS-IS, un conjunto lógico de redes.

DOMINIO DE BROADCAST: conjunto de todos los dispositivos que recibirán tramas de broadcast que se originan en cualquier dispositivo dentro del conjunto. Los dominios de broadcast se encuentran normalmente delimitados por routers, debido a que los routers no envían tramas de broadcast.

DOMINIO DE COLISIÓN: en Ethernet, el área de la red en la que se propagan las tramas que colisionan. Los repetidores y los hubs propagan las colisiones; los switches de LAN, puentes y routers no lo hacen.

ENRUTAMIENTO: proceso de descubrimiento de una ruta hacia el host de destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host de destino.

ESTÁNDAR: conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

ETHERNET: tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment, que se ha convertido en un estándar. Es compatible con distintos medios físicos (cable coaxial, par trenzado, fibra óptica) y con distintas topologías de red (bus, estrella). El ancho de banda ha evolucionado desde los 10 Mbps originales hasta 100 Mbps (Fast Ethernet) y 1000 Mbps (Gigabit Ethernet), incluyendo compatibilidad hacia atrás.

FAST ETHERNET: cualquiera de las especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un aumento de velocidad diez veces mayor que el de la especificación 10BaseT de Ethernet, preservando al mismo tiempo cualidades

tales como el formato de trama, los mecanismos MAC y MTU. Estas similitudes permiten el uso de aplicaciones 10BaseT existentes y herramientas de administración de red en las redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

FILTRADO DE TRÁFICO LOCAL: proceso a través del cual un puente filtra (descarta) tramas cuyas direcciones MAC de origen y de destino se encuentran ubicadas en la misma interfaz del puente, evitando de esta forma que se envíe tráfico innecesario a través del puente. Definido en el estándar IEEE 802.1.

FIREWALL: router o servidor de acceso o varios routers o servidores de acceso designados como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de acceso así como otros métodos para garantizar la seguridad de la red privada.

FIRMWARE: instrucciones de software que se establecen de forma permanente o semipermanente en la ROM.

FLUJO: corriente de datos que viaja entre dos puntos finales a través de una red (por ejemplo, de una estación LAN a otra). Varios flujos se pueden transmitir a través de un mismo circuito.

GATEWAY: en la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término *router* se utiliza para describir nodos que desempeñan esta función y *gateway* se refiere a un dispositivo especial que realiza una conversión de capa de aplicación de la información de una pila de protocolo a otro.

HDLC: control de enlace de datos de alto nivel. Protocolo de la capa de enlace de datos, orientado a bit y síncrono desarrollado por ISO.

HOST: sistema informático en una red. Similar al término *nodo*, salvo que *host* normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y routers.

HUB: dispositivo de hardware o software que contiene múltiples módulos independientes pero que están conectados a los equipos de red y de internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten las señales sino simplemente dividen las señales enviadas a través de ellos).

ICMP PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET: protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP.

INTERFAZ: 1. conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red.

INTERFERENCIA: ruido no deseado del canal de comunicación.

INTERNET: término utilizado para referirse a la internetwork más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real.

INTERNETWORK: agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (en general) como una sola red.

IP PROTOCOLO INTERNET: protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientada a la conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y re ensamblaje, y seguridad.

KB: Kilobyte.

Kb: Kilobit.

Kbps: Kilobits por segundo

LAN (**RED DE ÁREA LOCAL)**: red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada.

LATENCIA: retraso entre el tiempo que un dispositivo solicita acceso a una red y el tiempo en que se le otorga el permiso para transmitir.

LINUX: sistema operativo que posee un núcleo del mismo nombre. El código fuente es abierto, por lo tanto, está disponible para que cualquier persona pueda estudiarlo, usarlo, modificarlo y redistribuirlo.

MAC CONTROL DE ACCESO AL MEDIO: capa inferior de las dos subcapas de la capa de enlace de datos, según la define el IEEE. La subcapa MAC maneja el acceso a los medios compartidos.

MAPA DE CABLEADO: función que ofrecen la mayoría de los equipos que se utilizan para analizar cables. Cuando se utiliza para probar las instalaciones de cable de par trenzado, muestra qué pares se conectan a qué pines en los enchufes y los tomas.

MÓDEM MODULADOR/DEMODULADOR: equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica, mediante un proceso denominado de modulación (para transmitir información) y demodulación (para recibir información), de ahí su nombre.

NODO: punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo.

OSI INTERCONEXIÓN DE SISTEMAS ABIERTOS: programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.
PAQUETE: agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario.

PING: instrucción utilizada por el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red. Este es un mecanismo de prueba sumamente básico.

PROTOCOLO: descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información.

PROXY: entidad que, para aumentar la eficiencia, esencialmente reemplaza a otra entidad.

PUERTO: 1 interfaz en un dispositivo de internetworking (por ejemplo, un router). 2. En la terminología IP, un proceso de la capa superior que recibe información de las capas inferiores.

QOS CALIDAD DE SERVICIO: medida de desempeño para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

RED: agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de un medio de transmisión.

RENDIMIENTO: velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

REPETIDOR: dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

RETARDO: el tiempo transcurrido entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor.

ROUTER: dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red.

RUIDO: señales indeseables del canal de comunicación.

RUTA: recorrido a través de una internetwork.

SERVIDOR: nodo o programa de software que suministra servicios a los clientes.

SWITCH: dispositivo de red que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

TCP (**PROTOCOLO PARA EL CONTROL DE LA TRANSMISIÓN**): protocolo de la capa de transporte orientado a conexión que proporciona una transmisión confiable de datos de full dúplex. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP (**PROTOCOLO DE CONTROL DE TRANSPORTE/PROTOCOLO INTERNET):** nombre común para el conjunto de protocolos desarrollados por el DoD de los EE.UU. en los años '70 para soportar el desarrollo de internetwork a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

TELNET: instrucción utilizada para verificar el software de capa de aplicación entre estaciones de origen y de destino. Este es el mecanismo de prueba más completo disponible.

TERMINAL: dispositivo simple en el que se pueden introducir o recuperar datos de una red. En general, las terminales tienen un monitor y un teclado, pero no tienen procesador o unidad de disco local.

TOPOLOGÍA: disposición física de nodos de red y medios dentro de una estructura de redes empresarias.

TRAMA: agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión.

UDP (PROTOCOLO DE DATAGRAMA DE USUARIO): protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP.

VLAN (LAN VIRTUAL): grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, de hecho, están ubicados en una serie de segmentos de LAN distintos. Debido a que las VLAN están basadas en conexiones lógicas en lugar de físicas, son sumamente flexibles.

WAN RED DE ÁREA AMPLIA: red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por proveedores de servicio comunes.

10 Mbps: millones de bits por segundo. Una unidad de velocidad de transferencia de la información. Ethernet transporta 10 Mbps.

100BaseFX: especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una correcta temporización de la señal, un enlace 100BaseFX no puede superar los 400 metros de longitud. Se basa en el estándar IEEE 802.3.

100BaseT: especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la que se basa, 100BaseT envía impulsos de enlace a través del segmento de la red cuando no se detecta tráfico.

100BaseTX: especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos pares de cableado UTP o STP. El primer par de cables se utiliza para recibir datos y el segundo para transmitir.

10BaseT: especificación Ethernet de banda base de 10 Mbps que utiliza dos pares de cableado de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y el otro para recibirlos.

INTRODUCCIÓN

Durante la historia, el hombre siempre ha buscado millones de formas para comunicarse y para hacerse entender, debido a esto se ha preocupado por inventar y descubrir modelos o métodos como el lenguaje, el telegrama, el teléfono entre otros, como el mundo es un lugar que permanece en constante cambio el hombre debe preocuparse por desarrollar tecnologías de punta con el fin de satisfacer sus necesidades. La tecnología va de la mano con el cambio mundial y la globalización, este efecto hace que el hombre se preocupe por incluir las comunicaciones en el campo de las industrias y por eso es de gran importancia tener control sobre el manejo de los datos, los procesos y las comunicaciones bien solventadas para acortar distancias y fronteras.

De ahí que se incluyera el manejo de redes de comunicación (redes de datos), redes de microondas (transmisión), redes telefónicas (redes de planta externa) y redes de televisión en la industria, aunque sólo las empresas grandes pueden tener acceso a ellas debido a los altos costos de compra y mantenimiento. Actualmente las empresas medianas y pequeñas están empezando a incluir redes de datos que se acomodan a sus necesidades todo con el fin de posesionarse a un nivel óptimo para competir con las grandes empresas nacionales y multinacionales.

Las Redes de Área Local (LAN) tienen su nacimiento en los años ochenta, pues ya las empresas se encontraban con el paradigma de manejar grandes volúmenes de datos e información, hacer transacciones de tamaño monumental y sobretodo de llevar un orden y un control sobre los datos. Luego hace presencia la Internet, las redes PAN, MAN, y WAN, a ellas se unen otros conceptos como las bases de datos, los sistemas de información, las bodegas de datos la inteligencia de negocios y entre otros, ellos buscan dar rentabilidad y competencia en el mercado.

Ya en Colombia por ser un país en vía de desarrollo, este tipo de tecnologías han demorado su arribo debido a factores como el alto costo y la falta de conocimiento, como era de esperar hicieron su entrada por las empresas grandes pero ya ahora la mediana y pequeña empresa pueden hacer un uso de ellas acomodándolas a su presupuesto y necesidades, además el gobierno brinda un sinfín de posibilidades para apoyar las empresas del sector de las pymes como son alivios económicos, préstamos, e incentivos para crear y sostener este sector en el país.

Con el efecto de la globalización mundial y el TLC las pymes deben prepararse para competir con el mercado extranjero y los poderosos monopolios nacionales, por eso directivos, empleados, e infraestructura deben estar acordes al cambio y preocuparse por adquirir tecnología y por capacitar el personal. Es así que este proyecto espera brindar una solución en telecomunicaciones a una empresa del sector de las pymes, cuya razón social es comercializar maquinaria, hacer mantenimientos preventivos, correctivos, asesorías consultorías y capacitación en la utilización de los equipos que comercializan. Entonces la tecnología que se va a poner a disposición de esta empresa servirá para captar más clientes, tener un orden en el manejo de los datos y la información, logrando así incrementar los ingresos de la empresa.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES

APP MACHINES soporta y acompaña a sus clientes en la búsqueda de soluciones para sus procesos, proyectos y desarrollos en las áreas de control de calidad, producción, análisis de producción e investigación. Para ello cuentan con un equipo humano integrado por ingenieros, científicos, técnicos y especialistas; capacitados todos en el exterior, en áreas tanto comerciales como técnicas. En esta empresa los clientes encuentran, asesoría, mantenimiento y ayuda siempre construida sobre una experiencia de años de las diferentes especialidades. AppMachines se encuentra ubicada en el sector de las pymes en Colombia. Su oficina está ubicada en la Calle 25C # 80C - 17 en Bogotá. Cuenta en el momento con 15 empleados. Afortunadamente la empresa ha crecido gradualmente tanto a nivel de clientes como a nivel administrativo. Por esta razón un mejor control de su información generaría una mayor productividad.

En la actualidad la empresa APP MACHINES cuenta con dos administradores, cuatro asesores comerciales, dos técnicos de soporte, un consultor interno, un contador y dos ingenieros, los cuales no se encuentran conectados entre sí, ya que la empresa en la actualidad no cuenta con una red.

Cada uno de los empleados ya mencionados cuenta con un computador para el manejo de su respectiva información, pero con el inconveniente de que la actualización de la información se hace sobre los equipos en los cuales trabajan cada funcionario y no en un punto centralizado como un servidor.

La empresa APP MACHINES en la actualidad cuenta con una página de internet la cual se encuentra en un servidor en la ciudad de México y por el cual pagan 1.200.000 anuales. El nombre del servidor donde se encuentra alojada la página es www.godaddy.com, además de esto la empresa paga por el derecho al nombre appmachines.com, appmachines.net, appmachines.org, appmachines.info.

1.2 DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA

APP MACHINES Ltda., es una empresa que se encuentra ubicada en la ciudad de Bogotá, es una nueva compañía en el mercado pero gracias a su crecimiento han surgido nuevas necesidades en sus campos de acción.

En la actualidad la empresa no cuenta con ningún tipo de conexión entre sus estaciones de trabajo lo cual lleva a un mal control a nivel de sus clientes, mercancía y empleados, ya que no hay una actualización de las modificaciones que pueda llegar a generar algún usuario o un control de quienes tienen privilegios

para realizar dichas modificaciones lo cual lleva a vulnerabilidad en la información y mal manejo de la misma.

Una de las preocupaciones de APP MACHINES es el control de la autenticación de usuarios registrados en el servidor, control de contenidos en páginas web, restricción del tiempo de navegación, control de ancho de banda, todo dependiendo de las necesidades y de los privilegios que se le den a los usuarios
Dadas estas dificultades se formula la siguiente pregunta:

¿Cómo integrar los diferentes componentes tanto a nivel de hardware como de software adoptando políticas de gestión de red para brindar una solución a la Empresa APP MACHINES Ltda.?

1.3 JUSTIFICACIÓN

Para la empresa APP MACHINES, es importante poseer una red LAN para mejorar la comunicación entre sus empleados y a la vez tener un canal para la transferencia de la información relacionada con la compañía; teniendo en cuenta que el mecanismo permite tener organizada la información y mantener al día a cada uno de los ingenieros; esto garantiza mayor efectividad y mejor servicio para el público

Es importante resaltar el número de clientes de la compañía que viene en aumento, A final del año 2007 se realizó el cierre con 15 clientes activos, y a 31 de Marzo de 2008 con 40 clientes activos lo que corresponde a un significativo incremento, hecho que obliga a tener un sistema de telecomunicaciones óptimo para la empresa.

Con el objetivo de brindar un mejor servicio al cliente en cuanto a ventas, soporte técnico y mantenimiento, conociendo de antemano que los clientes buscan una excelente calidad en el servicio, es importante sacar el mayor provecho de las herramientas de hardware y software que se vayan a implementar para no sobre utilizarlas o sub utilizarlas; lo anterior, con el fin de estar a la altura de la competencia de las grandes y pequeñas compañías que están en el sector.

1.4 OBJETIVOS

1.4.1 Objetivo general

Diseñar una red LAN bajo los diferentes estándares para la empresa APP MACHINES, definiendo las diferentes políticas de gestión para tener control y monitoreo de la red.

1.4.2 Objetivos Específicos

- Caracterizar la red actual de la empresa APP MACHINES Ltda.

- Diseñar la red LAN teniendo en cuenta las normas técnicas y legales que se requieren

- Determinar las políticas de gestión de la red en base a los requerimientos de la empresa.

- Validar el diseño propuesto mediante una simulación.

1.5 ALCANCES Y LIMITACIONES

- Este proyecto pretende diseñar una solución informática cuyo objetivo es el diseño físico y lógico de la red LAN, la definición de las políticas de gestión según las necesidades del cliente, anexo a esto según la disposición de la empresa se hará la implementación de un servidor en Linux para el manejo de la misma red, en este servidor estarán alojados los diferentes equipos informáticos como estaciones de trabajo, impresoras, así como que las aplicaciones que funcionan en red, con el fin de solucionar los problemas de comunicación entre los diversos usuarios de la organización.

- El diseño de esta solución garantiza los resultados esperados, pues en todos los procesos a desarrollar se tendrán en cuenta con una rigurosidad adecuada las normas técnicas y legales de instalación de cada elemento. Para todo esto las pruebas se realizarán con ayuda de simuladores con los cuales se espera encontrar la mejor alternativa, que posteriormente se aplicará a todo el montaje de la solución que se plantea en el proyecto.

- El diseño está supeditado a su implementación por la asignación de presupuesto de la empresa APP MACHINES Ltda.

2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO CONCEPTUAL

Entre los tipos de red que se encuentran, están las PAM o redes personales, las LAN o redes locales, las MAN o redes metropolitanas y las WAN y GAN que son redes globales. En lo que respecta al proyecto, interesa tocar el tema de redes LAN, de dónde nacieron y para dónde van. Una de las primeras soluciones a estos problemas fue la creación de redes de área local (LAN). Como eran capaces de conectar todas las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio, las LAN permitieron que las empresas utilizaran la tecnología informática para compartir de manera eficiente archivos e impresoras.

Las redes de área local (LAN) "son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo impresoras) e intercambiar información"[1].

Las LAN están diseñadas para realizar lo siguiente:

- Operar dentro de un área geográfica limitada
- Permitir que varios usuarios accedan a medios de ancho de banda alto
- Proporcionar conectividad continua con los servicios locales
- Conectar dispositivos físicamente adyacentes

A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. En un sistema LAN, cada departamento, o empresa, era una especie de isla electrónica. Lo que se necesitaba era una forma de transferir información de manera eficiente y rápida de una empresa a otra.

2.1.1 Hub[2]: "El propósito de un hub es regenerar y retemporizar las señales de red. Esto se realiza a nivel de los bits para un gran número de hosts (por ej., 4, 8 o incluso 24) utilizando un proceso denominado concentración". La confiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una

[1] TANEMBAUM, Andrew. Redes de computadoras. Amsterdan The Netherlands: Pearson, 2003. p. 16.
[2] Cisco Networking Academy CCNA Versión 2.1.2 Modulo 1 Capitulo 3.1.6

interrupción en toda la red. Esta es la diferencia con la topología de bus, en la que, si un cable falla, se interrumpe el funcionamiento de toda la red. Los hubs se consideran dispositivos de Capa 1 dado que sólo regeneran la señal y la envían por medio de un broadcast a todos los puertos (conexiones de red).

2.1.2 Puente[3]: "Un puente es un dispositivo de capa 2 diseñado para conectar dos segmentos LAN. El propósito de un puente es filtrar el tráfico de una LAN, para que el tráfico local siga siendo local, pero permitiendo la conectividad a otras partes (segmentos) de la LAN para enviar el tráfico dirigido a esas otras partes. Usted se preguntará, ¿cómo puede detectar el puente cuál es el tráfico local y cuál no lo es? La respuesta es la misma que podría dar el servicio postal cuando se le pregunta cómo sabe cuál es el correo local. Verifica la dirección local. Cada dispositivo de networking tiene una dirección MAC (Medium Access Control address o dirección de control de acceso al medio) exclusiva en la NIC (Tarjeta de Interfaz de Red), el puente rastrea cuáles son las direcciones MAC que están ubicadas a cada lado del puente y toma sus decisiones basándose en esta lista de direcciones MAC".

2.1.3 Switch[4]: "Un switch, al igual que un puente, es un dispositivo de capa 2. De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto conmutando los datos sólo hacia el puerto al que está conectado el host destino apropiado. Por el contrario, el hub envía datos desde todos los puertos, de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos".

2.1.4 Router[5]: "El propósito de un router es examinar los paquetes entrantes (datos de capa 3), elegir cuál es la mejor ruta para ellos a través de la red y luego conmutarlos hacia el puerto de salida adecuado. Los routers son los dispositivos de regulación de tráfico más importantes en las redes de gran envergadura. Permiten que prácticamente cualquier tipo de computador se pueda comunicar con otro computador en cualquier parte del mundo. Los routers también pueden ejecutar muchas otras tareas mientras ejecutan estas funciones básicas".

[3] Ibid., Capitulo 3.1.7.
[4] Ibid., Capitulo 3.1.8.
[5] Ibid., Capitulo 3.1.9.

2.2 MEDIOS DE CONEXIÓN:

2.2.1 Cable par trenzado STP (Par Trenzado Protegido)[6]: "El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico. Los 4 pares de hilos están envueltos a su vez en una trenza o papel metálico. Generalmente es un cable de 150 ohmios. Tal como se especifica en las instalaciones de redes Ethernet, el STP reduce el ruido eléctrico, tanto dentro del cable (acoplamiento par a par o diafonía) como fuera del cable (interferencia electromagnética [EMI] e interferencia de radiofrecuencia [RFI]). El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y es de instalación más difícil que el UTP".

2.2.2 Cable par trenzado UTP (Par trenzado no blindado)[7]: "El cable UTP es un medio compuesto por cuatro pares de hilos, que se usa en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislador. Además, cada par de hilos está trenzado. Este tipo de cable se basa sólo en el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuanto trenzado se permite por unidad de longitud del cable".

2.2.3 Cable Coaxial[8]: "El *cable coaxial* está compuesto por dos elementos conductores. Uno de estos elementos (ubicado en el centro del cable) es un conductor de cobre, el cual está rodeado por una capa de aislamiento flexible. Sobre este material aislador hay una malla de cobre tejida o una hoja metálica que actúa como segundo alambre del circuito, y como blindaje del conductor interno. Esta segunda capa, o blindaje, ayuda a reducir la cantidad de interferencia externa. Este blindaje está recubierto por la envoltura del cable.

Para las LAN, el cable coaxial ofrece varias ventajas. Se pueden realizar tendidos entre nodos de red a mayores distancias que con los cables STP o UTP, sin que sea necesario utilizar tantos repetidores".

2.2.4 Cable de Fibra Óptica[9]: "El *cable de fibra óptica* es un medio de networking que puede conducir transmisiones de luz moduladas. Si se compara con otros medios para networking, es más caro, sin embargo, no es susceptible a la

[6] Ibid., Capitulo 5.1.1.
[7] Ibid., Capitulo 5.1.2.
[8] Ibid., Capitulo 5.1.3.
[9] Ibid., Capitulo 5.1.4.

interferencia electromagnética y ofrece velocidades de datos más altas que cualquiera de los demás tipos de medios para networking descritos aquí. El cable de fibra óptica no transporta impulsos eléctricos, como lo hacen otros tipos de medios para networking que usan cables de cobre. Más bien, las señales que representan a los bits se convierten en haces de luz. Aunque la luz es una onda electromagnética, la luz en las fibras no se considera inalámbrica ya que las ondas electromagnéticas son guiadas por la fibra óptica".

2.2.5 El Modelo OSI[10]: "El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje".

[10] Ibid., Capitulo 2.2.1.

Las siete capas del modelo de referencia *OSI* son:

Capa 7: La capa de aplicación

Capa 6: La capa de presentación

Capa 5: La capa de sesión

Capa 4: La capa de transporte

Capa 3: La capa de red

Capa 2: La capa de enlace de datos

Capa 1: La capa física

2.3 Servidor: En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Este uso dual puede llevar a confusión. Por ejemplo, en el caso de un servidor Web, este término podría referirse a la máquina que almacena y maneja los sitios Web, y en este sentido es utilizada por las compañías que ofrecen hosting o hospedaje. Alternativamente, el servidor Web podría referirse al software, como el servidor de http de Apache, que funciona en la máquina y maneja la entrega de los componentes de los páginas Web como respuesta a peticiones de los navegadores de los clientes.

Los archivos para cada sitio de Internet se almacenan y se ejecutan en el servidor. Hay muchos servidores en Internet y muchos tipos de servidores, pero comparten la función común de proporcionar el acceso a los archivos y servicios.

Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

2.3.1Tipos de servidores: servidores hay muchos estilos para realizar cualquier cantidad de tareas pero enfocado al trabajo se puede señalar como uno de los más importantes el servidor de aplicaciones, pues en él se alojarán todos aquellos programas que requiera el cliente que se manejen centralizadamente, el servidor de correos que sirve para mover correos corporativos a través de la LAN o por internet, un servidor proxy que en este caso es un dispositivo que ofrece un servicio de red para permitirle al cliente realizar conexiones hacia otros servicios de red, trabajando en la capa tres del modelo de referencia OSI.

2.3.2 Servidores de Aplicaciones (Application Servers)[11]: Tipo de servidor que permite el procesamiento de datos de una aplicación de cliente.

Las principales ventajas de la tecnología de los servidores de aplicación es la centralización y la disminución de la complejidad del desarrollo de aplicaciones, dado que las aplicaciones no necesitan ser programadas; en su lugar, estas son ensambladas desde bloques provistos por el servidor de aplicación.

Es percibido como un modelo cliente/servidor que mejora la performance de grandes aplicaciones.Designados a veces como un tipo de *middleware* (software que conecta dos aplicaciones)**,** los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

Generalmente es un servidor en una red de computadores que ejecuta y gestiona la totalidad (o parcial) de las aplicaciones o funciones de lógica de negocio y acceso a los datos de la aplicación. Uno de sus beneficios es la centralización y la disminución de la complejidad en el desarrollo de aplicaciones. Actualmente una de las plataformas más conocidas es la J2EE[12] de Sun Microsystems.

Este tipo de servidor también incluye software de conectividad (middleware) el cual le permite intercomunicarse con variados servicios como confiabilidad y seguridad. También brinda a los desarrolladores una interfaz para programación de aplicaciones (API) en aplicaciones Web modernas.

2.3.3 Servidores de Correo (*Mail Servers*): Casi tan ubicuos y cruciales como los servidores Web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LANs y WANs) y a través de Internet.

2.3.4 Servidores Proxy (*Proxy Servers*): Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor Web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.

2.3.5 Servidores de páginas WEB (HTTP): Permite mantener un alojamiento de su página desde el propio servidor. Además puede crear varios sitios web, haciendo de este servidor algo ideal para difundir la información en cada área dentro y fuera de la empresa.

---

[11] Diccionario Informático "Definición Servidor de Aplicaciones" Disponible en: http://www.alegsa.com.ar/Dic/servidor%20de%20aplicaciones.php Consultado: [12 de Septiembre de 2008, 10:20 am].

[12] Wikipedia "Java Enterprise Edition" Disponible en: http://es.wikipedia.org/wiki**/J2EE** Consultado: **[**12 de Septiembre de 2008, 10:24 am]

2.4 POLÍTICAS DE GESTIÓN

La idea en general es dar una solución en cuanto a administración de red se refiere para tener el mayor control posible sobre lo que desarrollan los empleados en sus horas laborales, para eso es necesario tener un nombre de usuario y una contraseña para ingresar a los equipos de la empresa y para ingresar a la red, el servidor proxy en el proyecto tiene como fin ejercer control de contenido a páginas WEB indebidas dentro de las horas laborales pues en la parte del control del tiempo de navegación los empleados tendrán horas no laborales para ingresar sin restricción alguna a la red, con el fin de tener una red confiable el control de ancho de banda tendrá influencia en regular la velocidad de navegación de cada empleado dependiendo de su perfil de usuario y de los requerimientos del gerente de la empresa.

2.4.1 Autentificación de usuarios: Permite a las personas el ingreso a la red con los permisos necesarios, evitando que está sea vulnerada por extraños.

2.4.2 Control de contenido de páginas WEB: La idea es la de controlar el uso del servicio de internet a páginas WEB indebidas.

2.4.3 Restricción del tiempo de navegación: Permite programar el tiempo de uso de los usuarios para la utilización de la red de datos e internet.

2.4.4 Control de ancho de banda: Administra el uso eficiente del servicio de internet de la empresa, evitando congestión y lentitud en la red.

2.5 LINUX Y SOFTWARE LIBRE[13]

"Los Software Libres son programas o aplicaciones que funcionan igual que cualquier otro programa o aplicación comercial, pero que mantienen una diferencia más filosófica que económica en cuanto a la forma de desarrollarse. El software libre permite que los usuarios adapten los programas a sus necesidades y les permiten redistribuirlo sin necesidad de pagar por hacerlo. El software libre permite que los usuarios se beneficien económicamente de éste si así lo desean sin temor a ser llamados piratas.

GNU (Gnu is Not Unix) ó (GNU No es Unix), es el proyecto iniciado por el señor Richard Stallman en 1984, que busca desarrollar un Sistema Operativo totalmente libre. Su sigla hace referencia a los Sistemas Operativos Unix usados en aquellas

[13] Curso Básico de Linux "Linux: Sistema Operativo, Comandos y Utilidad" Disponible en: http://www.senavirtual.edu.co; http://www.gnu.org/software/grub/grub.html Consultado: [12 de Septiembre de 2008, 10:35 am]

épocas, que se consideraban los más estables y eficientes pero su origen era propietario. Las compañías y centros de investigación pagaban altas sumas de dinero para poder usarlos.

GPL es la GNU Public License (Licencia Pública GNU), es un tipo de licenciamiento que aclara que un software que ésta cobije, será Software Libre".

Libertades de la licencia GPL

- La libertad de usar el programa, con cualquier propósito.
- La libertad de estudiar cómo funciona el programa, y adaptarlo a sus necesidades. El acceso al código fuente es una condición previa para esto.
- La libertad de distribuir copias, con lo que puede ayudar a su vecino.
- La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.

Linux nace de las manos de un joven Finlandés llamado Linus Torvalds en el año 1991, estudiante de informática de la Universidad de Helsinki, quien como tesis de grado desarrolló lo que se llamó en ese momento un pequeño núcleo independiente que funcionaba en arquitecturas i386.

Todo el software desarrollado por el proyecto GNU desde 1984, que hasta la fecha no estaba siendo usado masivamente, y al ver que el proyecto GNU no desarrollaba aun su propio núcleo (con nombre código HURD), se unió con el núcleo de Linus Torvalds conformando el proyecto GNU/Linux, un sistema Operativo totalmente GPL. El Sistema Operativo GNU/Linux es mal llamado hoy en día "Linux".

Linux se ha convertido en un Sistema Operativo realmente importante dentro del mercado del software, a pesar de manejar un tipo diferente de comercialización, que más que por su costo real, es ganada por los servicios, productos y proyectos que se crean con base en éste. Linux es considerado como el mejor Sistema Operativo en el ámbito de redes, ya que desde su concepción estaba pensado como un Sistema Operativo capaz de interactuar con todo tipo arquitecturas y con la capacidad de soportar innumerables protocolos. Se puede decir entonces que Linux ha logrado posicionarse en el ámbito mundial y que el camino hasta la fecha ha sido y seguirá siendo ascendente.

2.6 MARCO LEGAL O NORMATIVO

2.6.1 Organismos

2.6.1.1 EIA: Electronics Industry Association. Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.

Organización de la industria americana de electrónica. Es una organización comercial de fabricantes de electrónica y alta tecnología en EE.UU. cuya misión es promover el desarrollo del mercado y competitividad. Su sede central es en Arlington, Virginia, y abarca a 1300 empresas[14].

2.6.1.2 TIA: Telecommunications Industry Association. Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas[15].

Las normas EIA/TIA fueron creadas como norma de industria en un país, pero se ha empleado como norma internacional por ser de las primeras en crearse. ISO/IEC 11801, es otra norma internacional. Las normas ofrecen muchas recomendaciones y evitan problemas en la instalación del mismo, pero básicamente protegen la inversión del cliente.

2.6.1.3 IEEE: Instituto de Ingenieros Eléctricos y de Electrónica. Asociación de profesionales con sede en EEUU que fue fundada en 1884, y que actualmente cuenta con miembros de más de 140 países. Investiga en campos como el aeroespacial, computacional, comunicaciones, etc. Es gran promotor de estándares. Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet[16].

[14] EIA Disponible en: http://www.eia.org/ Consultado: [12 de Septiembre de 2008, 10:45 am]
[15] TIA Disponible en: http://www.tiaonline.org/ Consultado: [12 de Septiembre de 2008, 10:50 am]
[16] IEEE Disponible en:http://www.ieee.org.co/ Consultado: [12 de Septiembre de 2008, 10:53 am]

2.6.2 NORMAS

2.6.2.1 EIA/TIA568-A[17]: "El propósito de esta norma es permitir la planeación e instalación de cableado de edificios con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad".

2.6.2.2 ANSI/TIA/EIA-569-A[18]: De Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. "Define la infraestructura del cableado de telecomunicaciones, a través de tubería, registros, pozos, trincheras, canal, entre otros, para su buen funcionamiento y desarrollo en el futuro"

2.6.2.3 EIA/TIA 570[19]: "Establece el cableado de uso residencial y de pequeños negocios".

2.6.2.4EIA/TIA 607[20]: "Define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y proteger los elementos del sistema estructurado".

2.6.2.5 IEEE 802.3[21]: Define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito más abajo, aunque no tenga CSMA/CD como método de acceso al medio.

2.6.2.6 ANSI/EIA/TIA[22]: Emiten una serie de normas que complementan la 568-A, que es la norma general de cableado: Las normas EIA/TIA fueron creadas como norma de industria en un país, pero se ha empleado como norma internacional por ser de las primeras en crearse. Las normas ofrecen muchas recomendaciones y evitan problemas en la instalación del mismo, pero básicamente protegen la inversión del cliente.

---

[17] Pdf. "Redes y Diseño de Cableado Estructurado" disponible en: http://investigacionfitec.googlepages.com/redesydiseodecableadoestructurado.pdf P. 40 Consultado: [12 de Septiembre 2008, 11:00 am]

[18] Ibid., P. 40.

[19] Ibid., P. 40.

[20] Ibid., P. 40.

[21] Ibid., P. 21.

[22] Ibid., P. 40.

3 METODOLOGÍA

3.1 ENFOQUE DE LA INVESTIGACIÓN

Empírico Analítico: Orientado a la interpretación y transformación del mundo material.

3.1.1 Línea de investigación

Tecnologías Actuales y Sociedad

- **Sublínea de investigación**
  Sistemas de Información y Comunicación

- **Campo temático del programa**
  Redes de Comunicación

3.2 TÉCNICAS DE RECOLECCIÓN

Encuesta del 100% de la población de la empresa APP MACHINES Ltda.

3.3 POBLACION Y MUESTRA

100% de la población de la empresa APP MACHINES Ltda.

4. DESARROLLO INGENIERÍL

4.1 CARACTERIZAR LA RED ACTUAL DE LA EMPRESA APP MACHINES LTDA.

4.1.1 Introducción

Como parte esencial del proyecto se tendrá en cuenta el libro Desingning Cisco Networks, Volumen 1. Versión 2.0, pues esta fuente cuenta con una explicación muy enfocada para caracterizar la red actual o existente en cualquier empresa o entorno de trabajo. Cisco propone para caracterizar una red 12 pasos:

- Caracterizar las aplicaciones del cliente.
- Caracterizar los protocolos del cliente.
- Documentar la red actual del cliente.
- Identificar los cuellos de botella potenciales.
- Identificar los negocios del cliente.
- Caracterizar la existencia de la red disponible.
- Caracterizar el rendimiento de la red.
- Caracterizar la confiabilidad de la red existente.
- Caracterizar la utilización de la red.
- Caracterizar el estado de los routers.
- Caracterizar el sistema de gestión y las herramientas de gestión en la red actual.
- Resumir la salud de la red existente.

Los pasos anteriormente señalados son recomendados por Cisco para realizar la caracterización dentro de compañías que poseen una red, ya sea para reestructurarlas o cambiarlas por una nueva, dependiendo de los requerimientos de la empresa. Para el proyecto es importante tener en cuenta las recomendaciones de Cisco debido a que es la empresa líder mundial en soluciones de red e infraestructura para Internet, por lo tanto se ha adoptado como guía parcial la propuesta de Cisco para diseño de redes. Sin embargo, en el proyecto no existe una red de datos, por lo que no se puede seguir paso a paso dichas recomendaciones, pues hay muchos datos que no se podrán obtener.

De acuerdo con lo anterior este proyecto adoptará los siguientes pasos:

- Caracterizar las aplicaciones del Cliente.
- Documentar los Protocolos.
- Documentar la red actual (hardware).
- Caracterizar los cuellos de botella.
- Identificar las limitaciones del negocio y las entradas para el diseño de red.
- Caracterizar la disponibilidad de la red actual.
- Caracterizar el uso de la red.
- Caracterizar el rendimiento de la red.
- Nuevos requerimientos del Cliente.

Enfocando el proyecto, se observa que APP MACHINES Ltda., no posee una red de datos, por lo tanto los análisis no se ceñirán punto por punto a todo lo que recomienda el libro y más bien se utilizarán solo los puntos que sean necesarios para el proyecto como se indicó anteriormente.

Buscando una solución en telecomunicaciones para la empresa APP MACHINES Ltda., se debe caracterizar la red actual del Cliente para poder tener un punto de partida en la búsqueda del nuevo diseño de la red. Es de vital importancia hacer una caracterización específica a todos y cada uno de los elementos que componen el hardware de la empresa, se debe hacer un análisis en el que se incluya los servidores, los grupos de trabajo, la conectividad, el ancho de banda, el tráfico, las aplicaciones que existen, documentar los protocolos, hacer un inventario de los equipos activos, pasivos y de los enlaces, observar y analizar limitaciones, confiabilidad, cuellos de botellas y perfiles de los usuarios, para desarrollar estos puntos se hará necesario el uso de aplicación de entrevistas, encuestas, herramientas como analizadores de protocolos, visitas a la empresa.

Se hace necesario decir que para este análisis la empresa APP MACHINES Ltda., cuenta con el hardware distribuido el cual se limita a la conexión que hay de un equipo PC al router o modem que brinda el ISP para poseer conexión a Internet, eso quiere decir que ellos no poseen ni grupos de trabajo, ni otra forma de compartición de archivos por medio de una red. La transferencia de archivos se hace por correo si no son muy pesados o sino por medio de memorias USB o discos duros extraíbles. A continuación se desglosarán por puntos los diferentes elementos que se encontraron al caracterizar la red actual de APP MACHINES Ltda., anexo a este documento existe una carta que soporta la aplicación de una encuesta de la cual se puede deducir lo dicho anteriormente. (Ver Anexo B. Correspondencia tramitada con la Empresa APP MACHINES).

4.1.2 Caracterizar las aplicaciones del cliente. Es ideal tener claro la misión, la visión y las metas de la empresa, para conocer la compañía objeto de este proyecto y verificar qué tanto influirá el posterior diseño. Anexo al documento se encuentra la misión y la visión de la empresa (Ver Anexo B. Correspondencia tramitada con la Empresa APP MACHINES).

Para efecto del proyecto se extrajo, primero el crecimiento como empresa, que se ve especificado en un 70% de ventas y un 30% en prestación de servicios como soporte, mantenimiento y asesorías, el apoyo del proyecto tendrá su énfasis en tener un diseño que soporte el crecimiento de la empresa basado en una red de datos escalable, esto se puede observar en los objetivos corporativos, APP MACHINES tiene proyectado crecer un 30% en 3 años de una forma global. Segundo, la red debe ser confiable y con un rendimiento óptimo pues deberá estar ligada a las ventas, ya que un gran porcentaje de los posibles clientes o clientes ya establecidos se concretan vía Web por el canal de Internet, además la mayoría de los productos que comercializa APP MACHINES Ltda., son marcas extranjeras por lo cual los proveedores se encuentran en otras partes del mundo y es importante tener el canal de internet y la red de datos siempre activos. Tercero, la red de datos deberá generar orden en el manejo de documentos, así mismo tendrá que mejorar el rendimiento de los empleados con la implementación de los perfiles de usuarios y las políticas de gestión que adopte la compañía, esto por supuesto supondrá un incremento en las ventas de la empresa, lo que permite observar un paralelo de lo que se tiene actualmente y a lo que se quiere llegar. Pues en este momento todos los empleados comparten el mismo canal de Internet, es decir están ocupando el mismo recurso, además no se tiene ningún control sobre el ancho de banda que usa cada persona, es decir, no hay una segmentación del ancho de banda según el perfil del usuario y las necesidades del mismo, tampoco se tiene control sobre el tipo de páginas Web que se visitan, no se tiene control sobre los archivos que se descargan y si alguna o algunas personas descargan archivos demasiado pesados, la red puede saturarse. Para corregir estos detalles el proyecto busca elaborar un diseño que permita implementar el uso de perfiles de usuarios, ejercer control sobre el ancho de banda y un control de páginas Web; que logre ver reflejados en estadísticas al interior de la empresa, el rendimiento de los empleados y en consecuencia genere un incremento en las ventas.

Después de revisar la misión, la visión y las metas de la empresa APP MACHINES Ltda., el paso siguiente es la caracterización de la red, para lo cual se empezó a evaluar las aplicaciones que existen dentro de la empresa, se diseñó y aplicó una encuesta, lo que se puede verificar en una oficio que se encuentra anexo a este documento (Ver Anexo B. Correspondencia tramitada con la Empresa APP MACHINES). Como resultado de este trabajo, se determinó que las aplicaciones que ellos utilizan normalmente se limitan a paquetes como Microsoft Word, Microsoft Excel, Microsoft Power Point, Adobe Acrobat para documentos pdf, MSN Messenger, Skype, Internet Explorer, Mozilla Firefox, Microsoft Outlook. Todos los

paquetes que se mencionan se utilizan por gran parte del personal, dependiendo la necesidad de sus cargos y las necesidades de la empresa, esto se refleja en un cuadro que aparece adelante. Es de advertir que no existe un mecanismo de control para monitorear el trabajo de los empleados, por tanto se busca evitar que los usuarios usen indebidamente su tiempo, lo que puede representar pérdidas financieras para APP MACHINES Ltda., la conclusión es que el rendimiento de los empleados no se puede ver afectado por realizar actividades no competentes con su trabajo.

Como ya se indicó anteriormente, la empresa no tiene una red constituida para transferencia de datos y aplicaciones. Para caracterizar las aplicaciones, se van a listar aquellas que se usan diariamente, tomando como modelo un cuadro que propone Cisco como estructura metodológica para caracterizar redes[23], con el fin de adaptarlo para el proyecto, buscando así una mejor comprensión de dicho cuadro. El significado de cada columna dentro de este se detalla a continuación:

Nombre de la Aplicación: es el nombre que lleva dicha aplicación.

Tipo de Aplicación: se refiere al uso que tiene el programa, como por ejemplo una hoja de cálculo de Excel.

Número de usuarios: Cantidad de usuarios que poseen la aplicación.

Número de usuarios activos: Cantidad de usuarios que poseen la aplicación y la utilizan.

Sistema Operativo: el tipo de sistema operativo o plataforma sobre el cual corre la aplicación.

[23] CISCO System. Desingning Cisco Networks. Cisco System, 1998, Volumen 1. Versión 2.0, pagina 2-8

Tabla 1. Caracterización de las aplicaciones del Cliente

Nº	Nombre de la aplicación	Tipo de aplicación	# de Usuarios	# de Usuarios Activos	Sistema Operativo	Comentarios
1	Microsoft Word	procesador de texto	12	12	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
2	Microsoft Excel	hoja de cálculo	12	12	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
3	Microsoft Power Point	presentación de diapositivas	12	4	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
4	Adobe Acrobat	visualizción de archivos PDF	12	10	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
5	MSN Messenger	mensajeria instantanea	12	12	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
6	Skype	llamadas sobre Internet	12	4	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
7	Internet Explorer	navegador WEB	12	12	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
8	Mozilla Fire fox	navegador WEB	7	2	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
9	Microsoft Outlook	Cliente e-mail Microsoft	12	12	Windows	Xp Home, Xp Professional, Longhorn Home (Vista)
10						

Para explicar más detalladamente el cuadro, se puede agregar que cada empleado trabaja por su cuenta en un Host, el acceso a Internet se usa cuando se necesita, el trabajo sobre las aplicaciones es por equipo, de manera que no se están compartiendo y mucho menos se tiene un servidor de aplicaciones para alojar dichos paquetes. Desde ese punto de vista actualmente no se encuentran perfiles de usuario por máquina y como se indicó anteriormente, cada quien trabaja en su equipo respectivo, por lo tanto, cada empleado cuenta con una máquina a su disposición con la mayoría de las aplicaciones instaladas sin que esto signifique que se usen. Exceptuando la aplicación Mozilla FireFox, que está instalada únicamente en 7 de los 12 Host PC, y que solo se utiliza por parte de dos usuarios.

Las pruebas para obtener dichos datos fueron tomadas en un día laboral y confrontadas con las encuestas aplicadas. Cabe resaltar que del momento en aplicar la encuesta al momento de obtener los datos de estas

aplicaciones, la aplicación que se utilizaba para carácter financiero se eliminó debido al costo y al poco soporte que brindaba.

Es importante conocer los requisitos de sistema de las aplicaciones que se usan normalmente en APP MACHINES Ltda., los cuales se basan en procesador, memoria y disco duro. Para desarrollar esta tarea se corrió un programa llamado Everest a todos los equipos, el cual genera un informe detallado acerca del sistema, hardware y los programas; este reporte permite verificar el estado actual de los equipos de cómputo contrastados con los requisitos mínimos de máquina para las aplicaciones señaladas anteriormente. Igualmente, será de gran utilidad para el posterior diseño de la red, consiguiendo así prevenir posibles cuellos de botella o que se colapse la misma. A continuación se hace un resumen de las aplicaciones encontradas y los requisitos que se necesitan para poder utilizarlas:

Microsoft Excel: Es una aplicación para manejar hojas de cálculo, normalmente se usa para tareas financieras y contables, en el caso especifico de APP MACHINES Ltda., la empresa usa este paquete para hacer pequeñas bases de datos, para asuntos financieros, para crear listados y para llevar la contabilidad.

Tabla 2. Requisitos mínimos de máquina Microsoft Office Excel 2007[24]

Para usar Microsoft Office Excel 2007, se necesitará:

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 500 Megahercios (Mhz) o superior
Memoria	256 Megabytes (MB) de RAM como mínimo
Disco Duro	1,5 Gigabytes (GB); una parte de este espacio se liberará después de la instalación si se elimina el paquete de descarga original del disco duro
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 1024 X 768 o superior
Sistema Operativo	Sistema Operativo Microsoft Windows XP con Service Pack (SP) 2, Windows Server 2003 con Service Pack 1 o posterior. Algunas características de entrada manuscrita requieren la ejecución de Microsoft Windows XP Tablet PC Edition o posterior. La funcionalidad de reconocimiento de voz requiere un micrófono para hablar de cerca y un dispositivo de salida de audio. Las funciones de Information Rights Management requieren acceso a un servidor Windows 2003 Server con SP 1 o posterior que ejecute los Servicios de Windows Rights Management.
Otros	Para algunas funciones de colaboración avanzada, se requiere conectividad a Microsoft Windows Server 2003 con SP1 o posterior ejecutando Windows SharePoint Service. Internet Explorer 6.0 o posterior, sólo exploradores de 32 bits. La funcionalidad de Internet requiere acceso a Internet (puede estar sujeto a cuotas).
Adicional	Los requisitos y funcionalidad reales del producto pueden variar en función del sistema operativo y la configuración del sistema.

Microsoft Power Point: Es un programa diseñado para hacer presentaciones con texto esquematizado, fácil de entender, animaciones de texto e imágenes, imágenes prediseñadas o importadas desde archivos de dibujos o figuras de la computadora. Se le pueden aplicar distintos diseños de fuente, plantilla y animación. Este tipo de presentaciones suele ser muy llamativo y mucho más práctico que los de Microsoft Word. En APP MACHINES Ltda., se usa para desarrollar presentaciones a Clientes, para observar presentaciones de diversos productos y para hacer socializaciones entre personal de la empresa.

[24] Microsoft Office Online "Requisitos de la versión Microsoft Office Excel 2007" Disponible en: http://office.microsoft.com/es-hn/word/HA101668653082.aspx Consultado: [8 de Diciembre de 2008, 17:33pm].

Tabla 3. Requisitos mínimos de máquina Microsoft Office PowerPoint 2007[25]

Para usar Microsoft Office PowerPoint 2007, se necesitará:

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 500 Megahercios (Mhz) o superior
Memoria	256 Megabytes (MB) de RAM como mínimo
Disco Duro	1 Gigabytes (GB); una parte de este espacio se liberará después de la instalación si se elimina el paquete de descarga original del disco duro
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 1024 X 768 o superior
Sistema Operativo	Sistema Operativo Microsoft Windows XP con Service Pack (SP) 2, Windows Server 2003 con Service Pack 1 o posterior. Algunas características de entrada manuscrita requieren la ejecución de Microsoft Windows XP Tablet PC Edition o posterior. La funcionalidad de reconocimiento de voz requiere un micrófono para hablar de cerca y un dispositivo de salida de audio; las funciones de Information Rights Management requieren acceso a un servidor Windows 2003 Server con SP 1 o posterior que ejecute los Servicios de Windows Rights Management.
Otros	Para algunas funciones de colaboración avanzada, se requiere conectividad a Microsoft Windows Server 2003 con SP1 o posterior ejecutando Windows SharePoint Service. Las bibliotecas de diapositivas de PowerPoint requieren Office SharePoint Server 2007. Internet Explorer 6.0 o posterior, sólo exploradores de 32 bits. La funcionalidad de Internet requiere acceso a Internet (puede estar sujeto a cuotas).
Adicional	Los requisitos y funcionalidad reales del producto pueden variar en función del sistema operativo y la configuración del sistema.

Microsoft Word: Es un procesador de texto y se usa para elaborar cartas y trabajos. En el caso de APP MACHINES Ltda., lo usan para escribir todo tipo de cartas, para los formatos de cotizaciones, informes entre otros.

[25] Ibid., PowerPoint. Consultado: [8 de Diciembre de 2008, 17:33pm].

Tabla 4. Requisitos mínimos de máquina Microsoft Office Word 2007[26]

Para usar Microsoft Office Word 2007, se necesitará:

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 500 Megahercios (Mhz) o superior
Memoria	256 Megabytes (MB) de RAM como mínimo *
Disco Duro	1,5 Gigabytes (GB); una parte de este espacio se liberará después de la instalación si se elimina el paquete de descarga original del disco duro
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 1024 X 768 o superior
Sistema Operativo	Sistema Operativo Microsoft Windows XP con Service Pack (SP) 2, Windows Server 2003 con Service Pack 1 o posterior. Algunas características de entrada manuscrita requieren la ejecución de Microsoft Windows XP Tablet PC Edition o posterior. La funcionalidad de reconocimiento de voz requiere un micrófono para hablar de cerca y un dispositivo de salida de audio.
Otros	Las publicaciones se pueden enviar usando Office Outlook 2007, Outlook Express 6.0 o Windows Live Mail; los destinatarios pueden verlas en diversos clientes de correo electrónico y servicios basados en Web. Internet Explorer 6.0 o posterior, sólo exploradores de 32 bits. La funcionalidad de Internet requiere acceso a Internet (puede estar sujeto a cuotas).
Adicional	Los requisitos y funcionalidad reales del producto pueden variar en función del sistema operativo y la configuración del sistema.

* El corrector gramatical y ortográfico contextual de **Word** no se activa si el equipo no tiene 1 GB de memoria como mínimo.

Microsoft Outlook: Es el cliente de e-mail de Microsoft, APP MACHINES Ltda., lo usa para revisar, redactar y leer el correo de la empresa, el cual está configurado para funcionar con este paquete.

Para utilizar Microsoft Office Outlook 2007, se necesitará:

[26] Ibid., Word. Consultado: [8 de Diciembre de 2008, 17:33pm].

Tabla 5. Requerimientos mínimos de máquina Microsoft Outlook 2007[27]

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 500 Megahercios (MHz) o superior
Memoria	Procesador de 500 Megahercios (MHz) o superior
Disco Duro	1,5 Gigabytes (GB); una parte de este espacio se liberará después de la instalación si se elimina el paquete de descarga original del disco duro.
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 1024x768 o superior
Sistema Operativo	Sistema operativo Microsoft Windows XP con Service Pack (SP) 2, Windows Server 2003 con SP1 o posterior. Algunas características de entrada manuscrita requieren la ejecución de Microsoft Windows XP Tablet PC Edition o posterior; la funcionalidad de reconocimiento de voz requiere un micrófono para hablar de cerca y un dispositivo de salida de audio; las funciones de Information Rights Management requieren acceso a un servidor Windows 2003 Server con SP1 o posterior que ejecute los Servicios de Windows Rights Management.
Otros	Para algunas funciones avanzadas de Outlook 2007, se necesita conectividad a Microsoft Exchange Server 2000 o posterior. Para la búsqueda instantánea, se necesita Microsoft Windows Desktop Search 3.0. Los calendarios dinámicos requieren conectividad del servidor. Para algunas funciones de colaboración avanzada, se necesita conectividad a Microsoft Windows Server 2003 con SP1 o posterior ejecutando Microsoft Windows SharePoint Services. Para algunas funciones avanzadas se requiere Microsoft Office SharePoint Server 2007. Internet Explorer 6.0 o posterior, sólo exploradores de 32 bits. La funcionalidad de Internet requiere acceso a Internet (puede estar sujeto a cuotas).
Adicional	Los requisitos y la funcionalidad reales del producto pueden variar en función del sistema operativo y la configuración del sistema.

Acrobat Standard: Se utiliza para leer documentos con extensión PDF. Además sirve para crear formularios. La empresa lo usa para crear archivos con firmas, manuales de las maquinas y leer archivos en formato PDF,

Para usar Acrobat Standard, se necesitará:

[27] Ibid., OutLook. Consultado: [08 de Diciembre de 2008, 08:40pm].

Tabla 6. Requerimientos mínimos de máquina Acrobat Standard[28]

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 1,3 Gigahercios (Ghz) o más rápido.
Memoria	256 Megabytes (MB) de RAM (se recomienda 512 MB)
Disco Duro	1,5 Gigabytes (GB); una parte de este espacio se liberará después de la instalación si se elimina el paquete de descarga original del disco duro
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 1024 X 768
Sistema Operativo	Microsoft Windows XP Home, Profesional o Tablet PC Edition con Service Pack 2 o 3 (32 bits y 64 bits). Windows Server 2003 (con Service Pack 2 Para 64 bits). Windows Vista Home Basic, Home Premium, Business, Ultimate o Enterprise con o sin Service Pack 1 (32 bits y 64 bits)
Otros	Aceleración del hardware de video (opcional)

Msn Messenger: Es un programa de mensajería con el cual se pueden compartir archivos y charlas con las demás personas. APP MACHINES Ltda., usa este paquete para establecer conversaciones con los proveedores, con los posibles clientes, los clientes ya establecidos, además también se usa para prestar soporte. Sin embargo, aunque todos los equipos tienen instalada la aplicación solo hacen uso de la aplicación los departamentos que tienen salida a Internet, como se puede ver en la Figura 3 Mapa de conexión a Internet, de la página 68.

Para usar Msn Messenger, se necesitará:

[28] Adobe "Requisitos del Sistema para Acrobat Estándar" Disponible en: http://www.adobe.com/es/products/acrobatstd/systemreqs/ Consultado: [8 de Diciembre de 2008, 17:44pm]

Tabla 7. Requerimientos mínimos de máquina Msn Messenger 7.5[29]

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador Pentium a 233 Megahercios (Mhz) o más. Lo recomendado para la última versión de Messenger 7.5 es de 500 MHz.
Memoria	Para el nuevo Messenger 7.5 se necesita un mínimo de 64 Megabytes (MB) de RAM, aunque lo recomendado es 128 MB.
Disco Duro	Se necesitan 50 MB libres de espacio en Disco Duro para la instalación.
Pantalla	Monitor con una resolución de 800 X 600
Sistema Operativo	Sistema Operativo Microsoft Windows 98, 2000, Millenium o XP.
Otros	Se debe tener una tarjeta gráfica SVGA, aunque se puede utilizar una VGA de 256 colores o superior. Se tiene que tener instalado Microsoft Internet Explorer 6.0 o una versión posterior, aunque no sea el explorador predeterminado.
Adicional	Opcionalmente se puede instalar Windows Media Player, si se quiere utilizar el nuevo Messenger 7.5 con Webcam, micrófonos o altavoces.

Skype: Este programa sirve para llamar gratis a otras personas en cualquier lugar del mundo, las personas se pueden comunicar entre usuarios Skype o se puede llamar a teléfonos fijos o celulares con su respectiva tarifa, además si se tiene cámara Web se pueden realizar video llamadas con el mismos sistema.

Las llamadas tienen muy buena calidad de sonido, y son seguras, ya Skype cifra en forma automática las llamadas, conversaciones y transferencias de archivos antes de enviarlas por Internet para que nadie pueda interceptar tu llamada, tus conversaciones de texto o transferencia de archivos.

APP MACHINES Ltda., usa Skype para establecer conversaciones con los proveedores, con los posibles clientes, los clientes ya establecidos, además también se usa para prestar soporte, es muy importante para comunicarse de forma segura con proveedores que no viven en Colombia como son los miembros de Pfeiffer Vacuum Alemania, o Pfeiffer Vacuum Latinoamérica.
Para usar Skype, se necesitará:

[29] MSN Messenger "Requisitos Mínimos del Sistema" Disponible en: http://www.mundodescargas.com/messenger7/messenger_7_5_requisitos.htm Consultado: [8 de Diciembre de 2008, 17:52pm].

Tabla 8. Requerimientos mínimos de máquina Skype.[30]

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 1000 GHz.
Memoria	256 Megabytes (MB) de RAM
Disco Duro	Se necesitan 50 MB libres de espacio en Disco Duro para la instalación.
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 1024 X 768 o superior
Sistema Operativo	Sistema Operativo Microsoft Windows 2000, XP o Vista. (Los usuarios con Windows 2000 deben tener instalado DirectX 9.0 para poder realizar video llamadas).
Otros	En la conexión a Internet lo ideal es contar con Banda Ancha (GPRS no admitido en conversaciones de voz). Para video llamadas de alta calidad se necesita un software u una cámara web de alta resolución y un equipo informático con procesador de doble núcleo y conexión de banda ancha de alta velocidad (384 Kbps)
Adicional	Altavoces y micrófono incorporados o externos.

Detalles Técnicos: Versión 3.8.0.188, tamaño de archivo 21 MB. Lanzamiento oficial en Noviembre 19 de 2008 con el nombre de "SkypeSetup.exe"

Internet Explorer: Es un navegador Web producido por Microsoft para el sistema operativo Windows desde 1995. APP MACHINES Ltda., usa este paquete como navegador Web para visitar páginas de Internet.

Para usar Internet Explorer, se necesitará:

[30] SKYPE "Requisitos Mínimos de Máquina" Disponible en: http://www.skype.com/intl/es/download/skype/windows/ Consultado: [8 de Diciembre de 2008, 17:55pm].

Tabla 9. Requerimientos mínimos de máquina Internet Explorer 7.[31]

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 233 Megahercios (Mhz) o superior (se recomienda un Procesador Pentium)
Memoria	Si se utiliza Windows XP Service Pack 2 (SP2): 64 MB de RAM.
	Si se utiliza Windows XP Professional (64 Edition): 128 MB de RAM.
	Si se utiliza Windows Server 2003 Service Pack 1 (SP1): 64 MB de RAM
	Si se utiliza Windows Server 2003 Service Pack 1 ia64: 128 MB de RAM
	Cualquier equipo con la cantidad de memoria recomendada para Windows (por ejemplo, 128 MB para Windows Xp y 256 para Windows XP Professional x64) cubrirá los requisitos de memoria para Internet Explorer 7.0.
Disco Duro	Se necesitan 50 MB libres de espacio en Disco Duro para la instalación.
Unidad	Unidad de CD-ROM (si se realiza la instalación desde un CD - ROM)
Pantalla	Monitor Super VGA (800 x 600) o de mayor resolución con 256 colores.
Sistema Operativo	Sistema Operativo Microsoft Windows XP con Service Pack 2(SP2), Windows XP Professional x 64 Edition y Windows Server 2003 con Service Pack 1 (SP1).
Otros	
Adicional	Modem o conexión a Internet; mouse Microsoft, Microsoft IntelliMouse o dispositivo señalador compatible.

Mozilla Firefox: Es un navegador Web de la familia Mozilla. Se dice que es el segundo más popular en el mundo. APP MACHINES Ltda., usa este paquete como navegador Web para visitar páginas de Internet.

Para usar Mozilla Firefox, se necesitará:

[31] INTERNET EXPLORER "Requisitos Mínimos del Sistema) Disponible en: http://www.microsoft.com/spain/windows/downloads/ie/sysreq.mspx Consultado: [8 de Diciembre de 2008, 18:00pm].

Tabla 10. Requerimientos mínimos de máquina para Mozilla Firefox[32]

COMPONENTE	REQUISITO
Equipo y Procesador	Procesador de 233 Megahercios (Mhz) (recomendado 500 MHz o superior)
Memoria	64 Megabytes (MB) de RAM (recomendado 128 MB o superior)
Disco Duro	52 Mb de espacio libre en disco
Unidad	Unidad de CD-ROM o DVD
Pantalla	Monitor con una resolución de 800 X 600
Sistema Operativo	Sistema Operativo Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista.
Otros	
Adicional	

Luego de confrontar las aplicaciones del cliente y los requisitos de máquina se puede afirmar que las máquinas de APP MACHINES Ltda., cumplen todos los requisitos mínimos para instalar configurar y manejar las aplicaciones anteriormente descritas, esto se encuentra más detallado en los informes anexos extraídos de los equipos por medio del programa Everest (Ver Anexo C. Informes y demás).

Actualmente las aplicaciones que hacen uso de la red son todas las que se necesitan para navegación de Internet como el MSN Messenger, el Skype, el Internet Explorer, el Mozilla Firefox y finalmente el Microsoft Outlook, pues las demás aplicaciones se trabajan localmente. Sin embargo, el diseño final tendrá la capacidad de integrar nuevas aplicaciones requeridas por el Cliente. Este aspecto se trata con más detalle en el numeral 4.1.10 (Nuevos Requerimientos de Red).

4.1.3 Documentar los Protocolos. Para documentar los protocolos existen herramientas de uso público o privado las cuales, permiten capturar tramas de red con el fin de analizarlas. Igualmente, brinda la posibilidad de observar cada protocolo y su comportamiento. Estas se denominan analizadores de protocolos.

Se utilizó WireShark para analizar y documentar los protocolos de la empresa APP MACHINES Ltda., el paquete se instaló en un Host PC y se corrió durante un día de trabajo, para realizar la captura respectiva, el momento para capturar los

[32] Mozilla FireFox "Requisitos Mínimos de Máquina" Disponible en: http://www.mozilla-europe.org/es/firefox/system-requirements/ Consultado: [8 de Diciembre de 2008, 18:06pm].

protocolos fue un día laboral cualquiera en el que se instaló el paquete en una máquina y se puso a funcionar para tomar los respectivos datos.

Los datos recopilados por el analizador de protocolos provienen de un tráfico de salida de Internet, más no de un tráfico local o interno pues la compañía no tiene una red de datos a la cual se le pueda aplicar el analizador. Después de analizar los datos se obtuvo la siguiente tabla:

Tabla 11. Listado de protocolos

Nº	Nombre del Protocolo	Tipo de Protocolo	# de usuarios	Comentarios
1	UDP	Capa de Transporte	12	No orientado a conexión
2	TCP	Capa de Transporte	12	Orientado a Conexión
3	ICMP	Capa de Internet	12	No orientado a conexión
4	DNS	Capa de Aplicación	12	puerto TCP/UDP 53
5	IGMP	Capa de Internet	12	No orientado a conexión
6	SMB	Capa de Aplicación	12	C/S compartir archivos puerto TCP/UDP 3978
7	DCERPC	Cliente / Servidor	12	C/S por rpc
8	SRVSVC	Cliente / Servidor	12	C/S por rpc
9	RX	Capa de Red	12	puerto TCP/UDP 7001
10	NBSS	Servicio Sesiones Samba	12	Servicio para Samba
11	DHCP	Capa de Aplicación	12	puerto TCP/UDP 6768
12	Bootstrap protocol	Capa de Transporte	12	servidor Bootstrap
13	http	Capa de Aplicación	12	puerto TCP/UDP 80
14	SSDP	Servicio de Windows TCP/UDP	12	puerto TCP/UDP 1900
15	IP	Capa de Red	12	TCP/UDP
16	ARP	Capa de Red	12	protocolo resolución direcciones
17	LANMAN	LAN man	12	puerto TCP/UDP 139
18	BROWSE	Capa de Aplicación	12	Aplicación junto con http
19	TPKT	Capa de Transporte	12	TCP datos primitivos
20	TDS	Capa de Red	12	Subredes Ip
21	MSNMS	Servicio Msn Messenger	12	puerto TCP 80, 443, 1863
22	https	Capa de Aplicación	12	puerto TCP/UDP 80
23	SSLv3	Capa de Transporte	12	puerto TCP 443, 3944
24	Netbios	Capa de Aplicación	12	puerto TCP/UDP 139
25	dbcontrol_agent	Servicio de Oracle	12	Agente Oracle
26	Fjitsuappmgr	protocolo sesión alternativa	12	Puerto TCP 2425
27	SNMP	Capa de Aplicación	12	Puerto TCP/UDP 80
28	ov-nnm-websrv	Servicio Web	12	Puerto TCP/UDP 3443
29	netbios-ssn	Capa de Aplicación	12	Servicio netbios
30	wms-messenger	Servicio Msn Messenger	12	puerto TCP 80, 443, 1863
31	Radius	Capa de Red	12	Puerto TCP/UDP 1813
32	Mailprox	Servicio mail	12	Puerto TCP/UDP 3936

Después de explorar con el analizador de protocolos, se encontró que a nivel de capa de aplicación se observaron Http, SNMP, DHCP, DNS, a nivel de Transporte el protocolo UDP si se trabaja con algún stream de video o un sistema de nombres de dominios (DNS), TCP que maneja exploradores Web, e-mail, además de los puertos de origen y destino; por los lados de la capa de red se encuentra el protocolo IP, la dirección IP origen y la dirección IP destino, en la capa de enlace se ubica Ethernet como protocolo y como control de acceso al medio CSMA/CD para conexiones alámbricas y CSMA/CA para conexiones inalámbricas, finalmente en la capa física se encuentra la dirección MAC. Todo esto ayuda a conocer cómo viajan los datos por la red, qué puertos están abiertos y si se establecen sesiones locales o saludos en tres vías. Para efectos del proyecto, lo anterior será de gran utilidad buscando un mejor rendimiento o desempeño de la red. De esa manera se puede contemplar dentro del nuevo diseño la configuración de un servidor DNS dentro de la compañía que evite que al momento que se conecte con cualquier servidor, las peticiones o los datos tengan que viajar hasta ese sitio en Internet. La función del servidor será la de recibir todas las peticiones de acceso a Internet y procesar dichas peticiones evitando el flujo de información no necesaria mejorando la utilización del ancho de banda. Otro ejemplo aplicable puede ser el de configurar un servidor de actualizaciones que recoja todas las peticiones el mismo y luego se conecte por ejemplo con el servidor de actualizaciones de Windows, evitando así que cada vez que se encuentre una actualización se genere un broadcast por toda la red inundando el medio y consumiendo ancho de banda inútilmente.

4.1.4 Documentar la red actual (Hardware). Tras realizar la visita de inspección para determinar la cantidad de equipos activos de la empresa APP MACHINES Ltda., se utilizaron herramientas de dominio público como es el Everest o Aida32, esto brinda la posibilidad de tener las características de los equipos que actualmente están a disposición de la empresa, además es de vital importancia saber el inventario de los equipos con los que se cuenta actualmente. Para la toma de estos datos se requirió realizar una visita en un día no laboral para no entorpecer el trabajo de los empleados, esto facilitó la toma de datos rápida y segura. Después de la toma se procedió a desinstalar el paquete.

Se incluyó solo una parte del informe de Everest por máquina haciendo énfasis en tener conocimiento sobre las tarjetas de red pues ellas son las encargadas de transmitir la PDU o trama de capa 2 de un nodo a otro nodo, además pueden ser un punto fundamental en los cuellos de botella debido a la velocidad a la que puedan transmitir los datos, de manera que de nada sirve tener una tarjeta de red que transmita a 1000 Mbps si se tiene por ejemplo un switch que transmita a 10 Mbps

Entonces el hardware con el que cuenta la empresa actualmente se relaciona en los siguientes cuadros consolidados (Tabla 12. Resumen de Equipos de Cómputo, Tabla 13. Resumen de Impresoras, Tabla 14. Resumen de Equipos de Red):

Tabla 12. Resumen de Equipos de Cómputo

Marca	Intel 1.6	Intel 1.8	Intel 2.8	Intel Core 2 Duo	Amd Athlon 64	PENTIUM III	PENTIUM IV	PENTIUM D	TOTAL
DELL	1				1				2
TOSHIBA		1			2				3
CLONES			1	1	2		1	1	6
ACER		1							1
TOTAL	1	2	1	1	5		1	1	12

Tabla 13. Resumen de Impresoras

Marca	Matriz de Punto	Inyección de Tinta	Laser	Total
Epson	1	1		2
Lexmark		1		1
Total	1	2		3

Tabla 14. Resumen de Equipos de Red

Especificaciones	Cantidad
Hub OPCOM 5 puertos 10/100, 100BaseT/Tx	2
Cable UTP Cat 5 Verificado Norma 568 b	8
Router NetGear FS 605	1
Total	11

Tomando como base la misión, visión y metas de APP MACHINES Ltda., se observa que tienen planeado crecer un 10% en cuanto a empleados se refiere, por eso la escalabilidad de una nueva red y la adquisición de nuevos equipos dependerán de la contratación directa de empleados y de la compra de nuevo Hardware y Software. De este tema se hablará a fondo en el numeral 4.1.10 (Nuevos Requerimientos de Red).

4.1.5 Caracterizar los cuellos de Botella. “Es una expresión típica en ingeniería y más en ingeniería de organización. Botella representa el eslabón más débil de una serie de tareas a realizar. En general esta definición se puede aplicar a cualquier situación de la vida cotidiana. Si uno para ir a trabajar tiene que desayunar, ducharse, vestirse, superar el atasco de todas las mañanas y llegar al

trabajo, el cuello de botella sería claramente el atasco, ya que su duración y su criticidad es la más alta y es la que marca el resto de los procesos."[33]

"El acceso simultáneo a recursos compartidos causa cuellos de botella. En general, los cuellos de botella están presentes en todos los sistemas de software y son inevitables. Sin embargo, la demanda excesiva de recursos compartidos causa un tiempo de respuesta largo, y se debe identificar y corregir.

Entre las causas de estos cuellos de botella se incluyen:

- Recursos insuficientes que requieren componentes adicionales o actualizados.

- Recursos del mismo tipo que no distribuyen de forma equilibrada las cargas de trabajo; por ejemplo, cuando un recurso monopoliza un disco.

- Recursos que funcionan incorrectamente.

- Recursos mal configurados."[34]

Un Cuello de Botella se puede producir al momento de navegar en Internet, es en los enlaces WAN donde se pueden generar más frecuentemente, para el caso de APP MACHINES Ltda., donde no existe una red LAN, ni una red para transferencia de archivos, entonces los tipos de red se limitan al uso excesivo de los recursos, como puede ser un cuello de botella por carga extra en una memoria RAM, es decir, cuellos de botella por abrir muchas aplicaciones o ventanas de explorador al tiempo, esto genera sobrecarga en el sistema que termina bloqueando los equipos, actualmente la compañía no maneja archivos muy pesados ni aplicaciones demasiado pesadas con respecto a los procesadores y memorias RAM de los equipos que posee, anexo a este documento (Ver Anexo C. Informes y demás), se encuentran los archivos que resume el programa Everest con la configuración de los equipos de computo actuales, ver de la tabla 2 Requisitos mínimos de máquina Microsoft Office Excel 2007, a la tabla 10 Requisitos mínimos de máquina Mozilla Firefox. A nivel de red, se está sujeto a la velocidad de transferencia de los equipos activos que habitan en esta red, por ejemplo no sirve mantener un router o un switch Giga bit Ethernet, si las tarjetas de red existentes, solo pueden transmitir a una velocidad de 10 Mbps o 100 Mbps, así que se produciría un cuello de botella porque los bits pasarían por el medio del tamaño más pequeño que puede fluir por la red.

[33] Fresqui "¿Qué es el Cuello de Botella? - Ingeniería" Disponible en: http://tec.fresqui.com/que-es-el-cuello-de-botella-enginieria Consultado: [25 de Abril de 2009, 09:40am].
[34] MSDN "Identificar Cuellos de Botella" Disponible en: http://msdn.microsoft.com/es-es/library/ms190994(SQL.90).aspx Consultado: [25 de Abril de 2009, 09:47am].

A nivel de equipos activos (se mencionaron en el numeral 4.1.4) actualmente se posee el Modem-Router que proporciona el ISP y un Hub 10/100 para las conexiones, a nivel de servidores la empresa no posee ninguno actualmente pero está presupuestado adquirir uno o dos dependiendo de las necesidades, de ahí que actualmente no se puedan medir tiempos de respuesta sobre servidores.

Al contemplar el nuevo diseño y con el fin de mermar al máximo la aparición de cuellos de botella, se tendrá que tener en cuenta entre otros, el flujo de tráfico estimado, el espacio, la velocidad de los enlaces, la cantidad de dispositivos por los cual va a tener que transitar el tráfico, la asimetría o la simetría que tengan dichos dispositivos, igualmente es importante ubicar de manera correcta los host de forma Jerárquica (Acceso, Distribución, Núcleo) y en grupos comunes (Propósito, propiedad, ubicación geográfica).

4.1.6 Identificar las limitaciones o restricciones del negocio y las entradas para el diseño de red. Con el ánimo de dar claridad a este punto es de vital importancia hacer énfasis en que este proyecto está enfocado solo en el diseño de la red LAN, por lo que la implementación no está contemplada en dicho proyecto, pero de todos modos es importante dar unas pautas para poder realizar el diseño.

Mediante una carta anexa al documento la empresa APP MACHINES Ltda., ha aprobado un monto de $10.000.000 para usar en tecnología e infraestructura pues basados en la misión, visión y metas del negocio ellos encuentran importante para generar ganancias tener una red de datos y una infraestructura de comunicaciones acorde al crecimiento de la empresa (Ver Anexo B. Correspondencia tramitada con la Empresa APP MACHINES).

Las limitaciones para el diseño apunta al monto que fue otorgado y por eso se trabajará con base en él, como reglas de la compañía la empresa ha solicitado entregar en el diseño 3 (tres) cotizaciones con equipos activos, pasivos y enlaces de conexión, incluidos los cuartos de equipos y algún PC que se necesite comprar (Ver Anexo C. Informes y demás.).

4.1.7 Caracterizar la disponibilidad de la red actual. "Disponibilidad significa tener la seguridad de acceder de forma confiable y oportuna a los servicios de datos para usuarios autorizados."[35] En APP MACHINES Ltda., la disponibilidad que se va a analizar, es de la red actual por tanto esta se traduce a la cantidad de veces que opera la red ante la solicitud de un servicio como puede ser el acceso a Internet, al no poseer una red para transferir y compartir archivos, la disponibilidad se mide en la cantidad de veces que se puede caer el servicio de Internet

[35] CISCO Networking Academy "CCNA Exploration 4.0 Aspectos Básicos de Networking" Capitulo 1.4.5.2 Consultado: [25 de Abril de 2009, 11:10am].

adquirido a un ISP que para el proyecto es Telmex Colombia, del volumen de ventas el 70% corresponde a la comercialización de equipos y marcas de los socios estratégicos, de este 70%, el 25% de la comercialización se realiza vía correo electrónico o corresponde a visitas de clientes a la página Web. Por otro lado en la parte de mercadeo es de vital importancia que el enlace de Internet esté disponible pues es por este medio por el que se realizan los contactos con los proveedores extranjeros, ya sea por correo electrónico, por Msn Messenger o por Skype, así que es de vital importancia tener el enlace con Internet pues aunque su uso no es constante la falta de él puede generar pérdida de ganancias para la empresa, igualmente surge la necesidad de crear una red de datos para compartir archivos como de interés común entre los diferentes departamentos y en diferentes formatos como son .doc .exe .ppt entre otros, y también que se encuentre disponible en todo momento, con el fin de prevenir caídas del sistema que se vean reflejadas en pérdidas económicas para la empresa.

4.1.8 Caracterizar el uso de la red. En este momento no existen dentro de la compañía el uso de perfiles ni de roles, pues cada persona se sienta en su puesto de trabajo con su host definido a elaborar sus tareas diarias, igual mente no hay una segmentación de los equipos por lo tanto todos los equipos están en el mismo dominio de broadcast por esto es una preocupación de la Gerencia, definir perfiles de usuario puesto que existen documentos de uso público y documentos de uso privado que como su nombre lo dice no deben ser vistos, ni utilizados ni mucho menos alterados por el personal. Para esto la red debe contemplar dentro de su diseño la segmentación de la red por propósito y por seguridad. Por propósito debido a que dentro de las políticas de gestión encontraremos la necesidad de dividir por perfiles de usuario el ancho de banda de la red. Por seguridad para proteger los documentos, para limitar el acceso a documentos o carpetas por perfiles y finalmente para la salida a Internet.

Para conocer como está actualmente la empresa APP MACHINES Ltda., en cuanto a planta física, disposición de equipos y forma de conexión a Internet, se adelantó una visita para levantar la información concerniente a la planta física (Ver Figura 1. Mapa de planta física P.65), distribución de equipos (Ver Figura 2. Mapa de distribución de equipos. P.65) y la conexión a Internet (Ver Figura 3. Mapa de conexión de Red. P. 66). Estas figuras se elaboraron a escala en Autocad 2007 y Microsoft Visio 2007.

Figura 1. Mapa de planta física de la empresa.

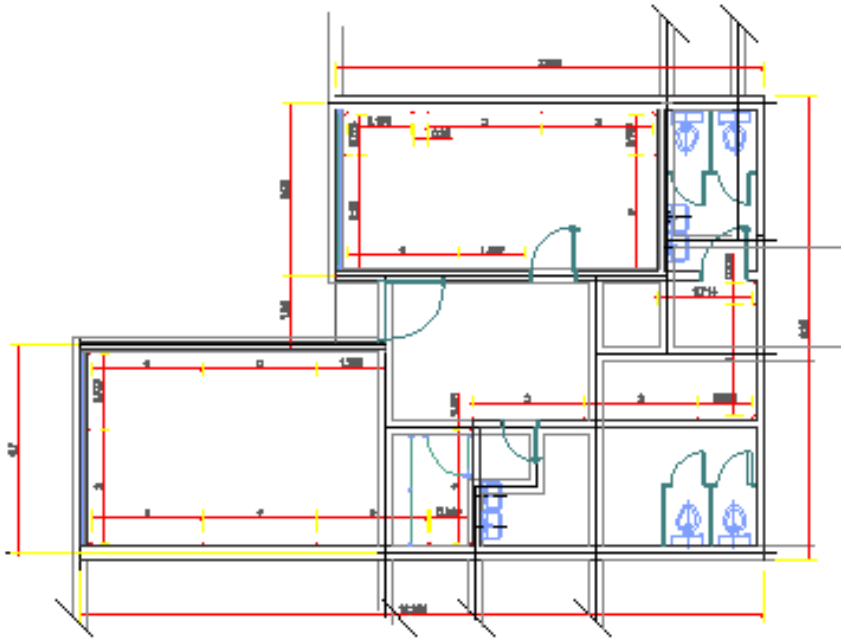
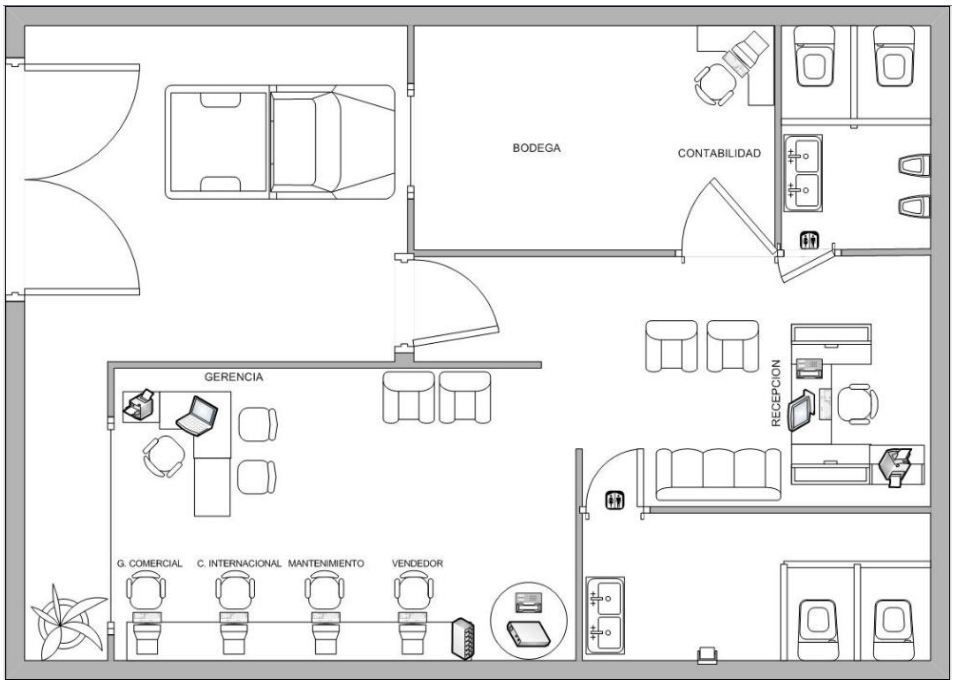


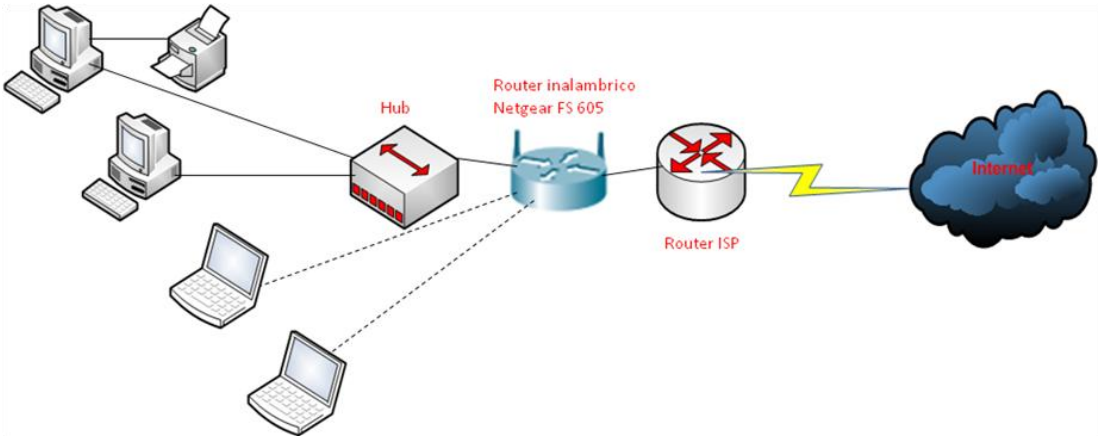
Figura 2. Mapa de distribución de los equipos.



La conexión hacia Internet se hace de la siguiente manera:

Internet llega a APP MACHINES Ltda., por medio del modem o router que otorga en comodato el ISP, para este caso es Telmex, la señal de aquí tiene dos formas de llegar a los equipos, la primera es vía inalámbrica y la segunda es la que se conecta a un Patchcord del Router al Hub y así mismo el Hub distribuye la señal a los host conectando el otro extremos del patchcord a la tarjeta de red de los equipos.

Figura 3. Mapa de conexión a Internet



Los siguientes test de velocidad fueron realizados desde www.testdevelocidad.es y estos resultados se comparan con el contrato con la empresa prestadora del servicio en este caso

Figura 4. 1erTest de velocidad a las 7:30 am 3 abril 2009

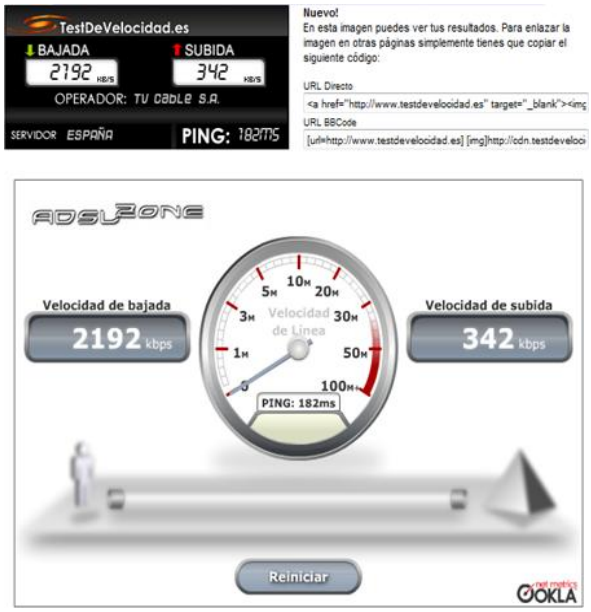


Figura 5. 2do Test de velocidad a las 2 12:00 pm 3 de abril 2009

Figura 6. 3er Test de velocidad a las 5:30 pm 3 de abril del 2009

La nueva Red debe ser pensada para soportar tráfico de Internet, tráfico local, Programas de Diseño de máquinas, Programas de simulación de software de ultrasonido, Voz sobre IP, además debe de garantizar rendimiento, confiabilidad, escalabilidad, también debe soportar las aplicaciones actuales y el tráfico actual que maneja considerando el crecimiento y una posible aumento de las personas que hagan uso de la red. Esto con el fin de garantizar la confiabilidad de la red.

4.1.9 Caracterizar el rendimiento de la red. Para caracterizar la disponibilidad de la red actual, existen herramientas como analizadores de tráfico, Ping y Traceroute. En el desarrollo de esta tarea se utilizó Ping para evaluar el rendimiento ya que es una herramienta que se encuentra a la mano y los datos que arrojan son de fácil comprensión tanto para el que toma los datos como para el cliente que solicita el estudio.

“Ping es una utilidad para probar la conectividad IP entre hosts. Ping envía solicitudes de respuestas desde una dirección host específica. Usa un protocolo de capa 3 que forma parte del conjunto de aplicaciones TCP/IP llamado Control

Message Protocol (Protocolo de mensajes de control de Internet, ICMP). Ping usa un datagrama de solicitud de eco ICMP.
Si el host en la dirección especificada recibe la solicitud de eco, éste responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el ping mide el tiempo requerido para la respuesta.

A medida que se recibe cada respuesta, el ping muestra el tiempo entre el envío del ping y la recepción de la respuesta. Ésta es una medida del rendimiento de la red. Ping posee un valor de límite de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el ping abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las peticiones, la utilidad de ping provee un resumen de las respuestas. Este resumen incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

De igual manera se utilizó Traceroute (tracert), esta es una utilidad que permite observar la ruta entre un host y otro. El rastreo genera una lista de saltos alcanzados con éxito a lo largo de la ruta.

Esta lista puede suministrar información importante para la verificación y el diagnóstico de fallas. Si los datos llegan a destino, entonces el rastreador menciona la interfaz en cada router que aparece en el camino.

Si los datos fallan en un salto durante el camino, se tiene la dirección del último router que respondió al rastreo. Esto indica el lugar donde se encuentra el problema o las restricciones de seguridad.

4.1.9.1 Tiempo de ida y vuelta (RTT). El uso de traceroute proporciona el tiempo de ida y vuelta (RTT) para cada salto a lo largo del camino e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta (RTT) es el tiempo que le lleva a un paquete llegar al host remoto y a la respuesta regresar del host. Se usa un asterisco (*) para indicar la pérdida de un paquete.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si tenemos altos tiempos de respuesta o pérdidas de datos de un salto particular, ésta es una indicación de que los recursos del router o sus conexiones pueden estar estresados.

4.1.9.2 Tiempo de vida (TTL). "Traceroute hace uso de una función del campo Tiempo de vida (TTL) en el encabezado de Capa 3 y Mensaje excedido en tiempo ICMP. El campo TTL se usa para limitar la cantidad de saltos que un paquete

puede cruzar. Cuando un paquete ingresa a un router, el campo TTL disminuye en 1. Cuando el TTL llega a cero, el router no envía el paquete y éste es descartado.

Además de descartar el paquete, el router normalmente envía un mensaje de tiempo superado de ICMP dirigido al host de origen. Este mensaje de ICMP estará conformado por la dirección IP del router que respondió."[36]

Después de explicar el funcionamiento de Ping y Traceroute, se procede a observar cada host de la red, identificando el tiempo potencial y el rendimiento de cada uno de ellos.

Esto se hace realizando un ping desde cada PC así mismo y a todos los demás. Al no existir una red de datos para comunicarse entre host, la red que encontramos es para salir a internet por lo cual el ping se debe realizar a páginas de Internet que visitan los miembros de la empresa para medir el rendimiento del canal de Internet que APP MACHINES Ltda., tiene contratado, el ISP es Telmex Colombia con el cual han estipulado 2.000K o 2 Megas de velocidad.

Los Pings y sus resultados se tomaron en dos tandas, la primera en uso normal de recursos del canal de Internet y la segunda con un uso excesivo del canal que supone un usuario descargando películas o algún stream de video en Youtube; los resultados se consolidan así:

[36] Ibid., Capitulo 6.6.4.1 Consultado: [13 de Mayo de 2009, 14:10pm].

4.1.9.3 Resultados en utilización normal del canal:

Figura 7. Ping a www.appmachines.com

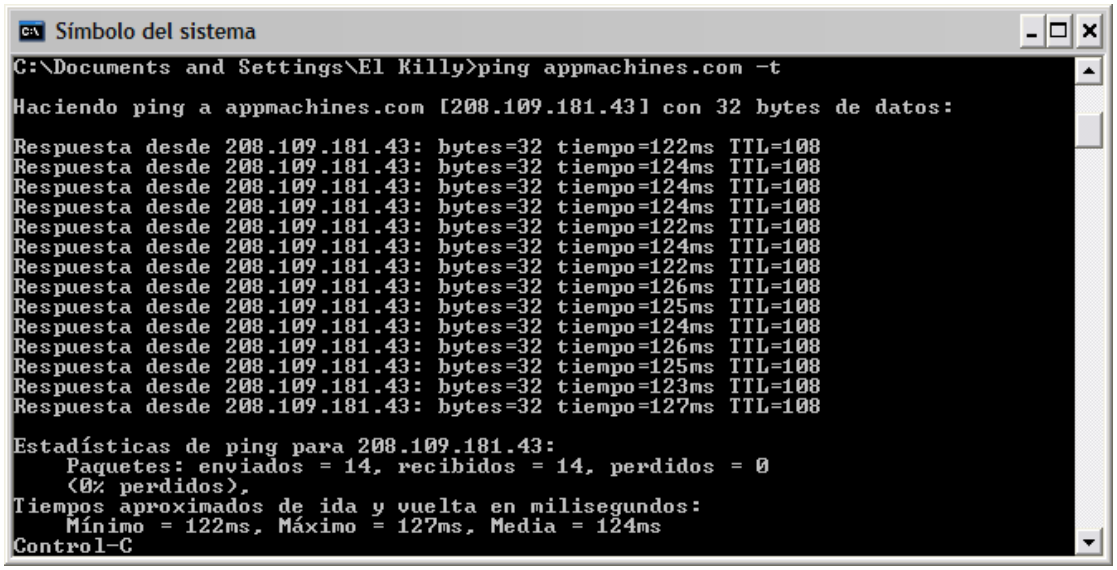


Figura 8. Ping a www.portafolio.com.co

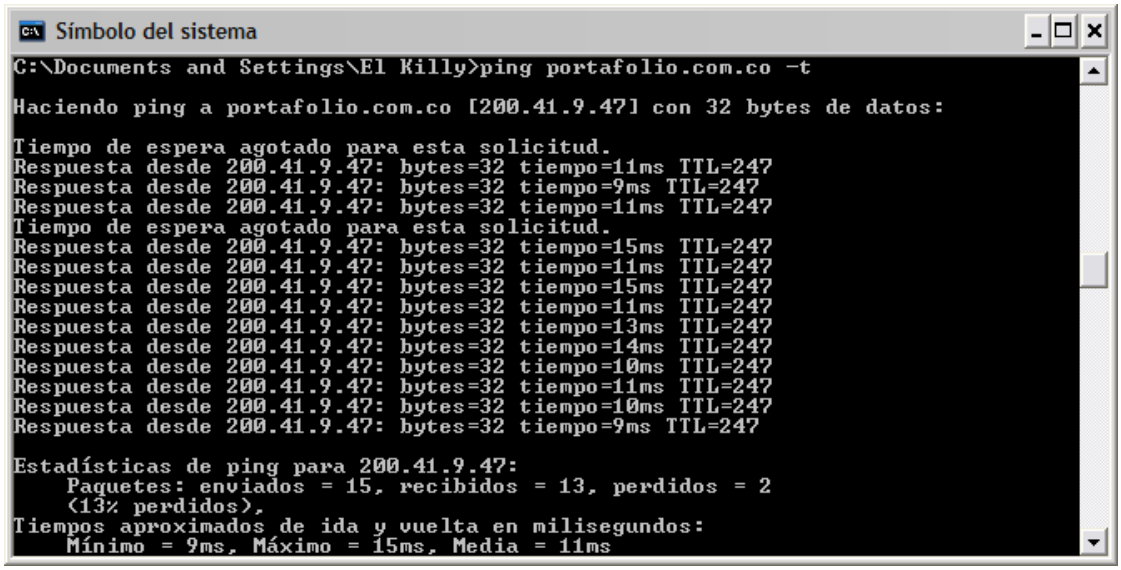


Figura 9. Ping a www.labomed.com

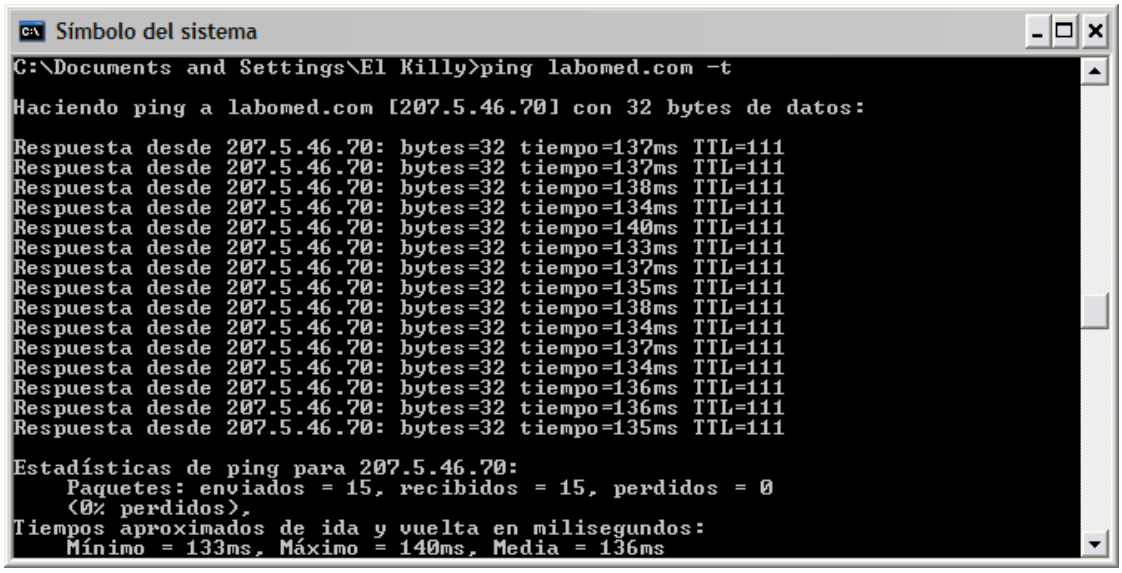


Figura 10. Ping a www.keiyu-ndt.com.tw

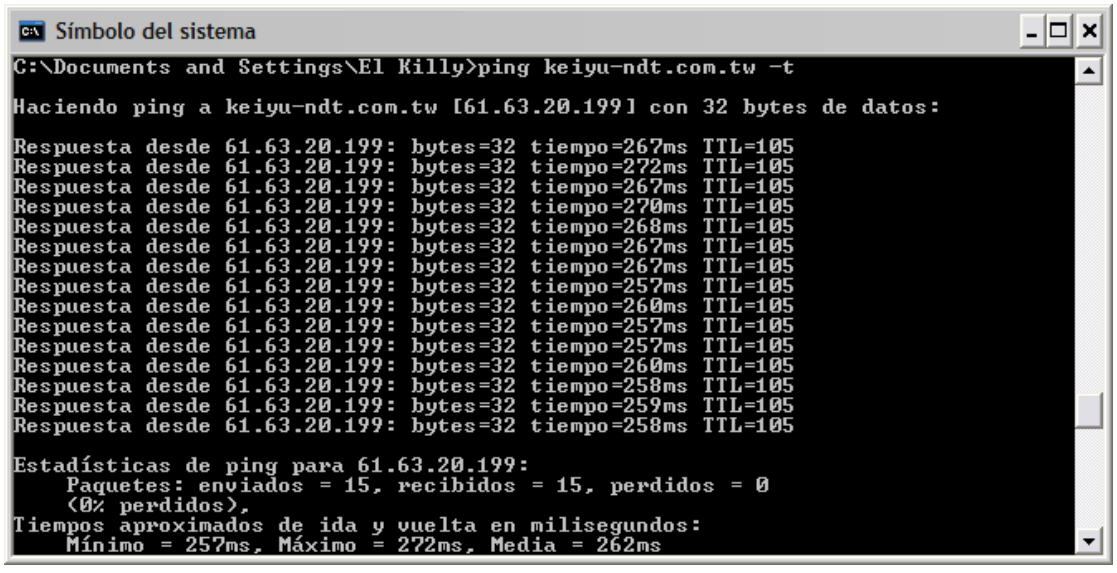


Figura 11. Ping a www.xe.com

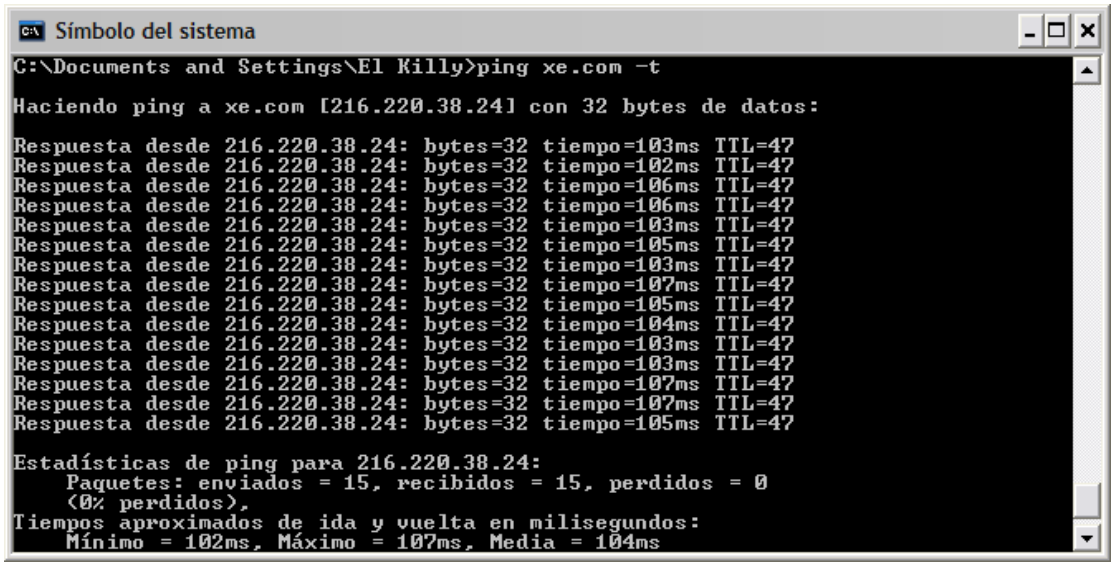


Figura 12. Traza a www.portafolio.com.co

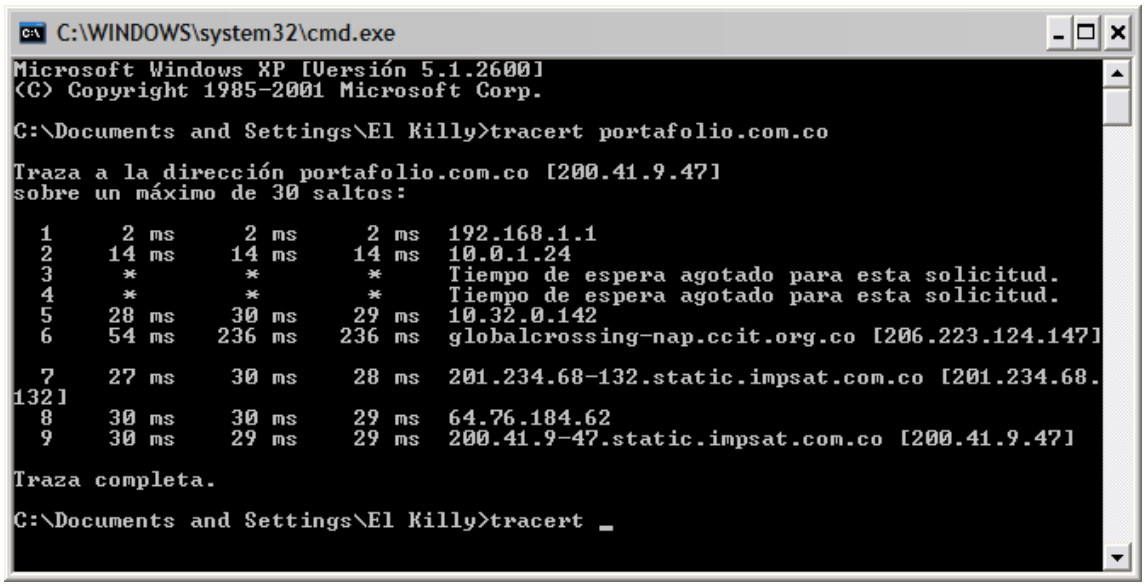
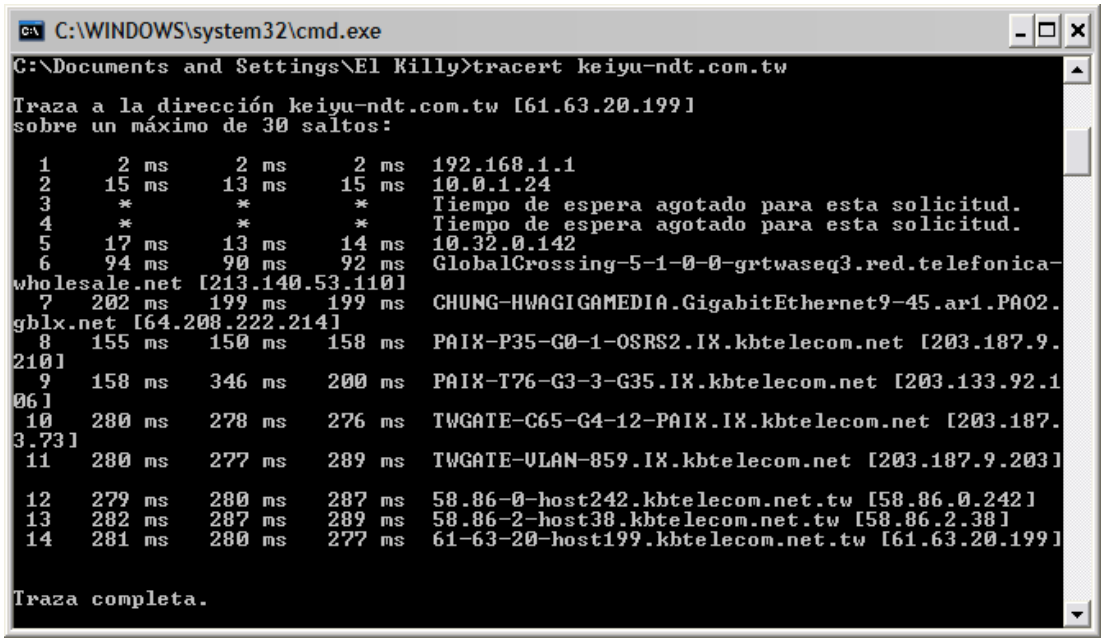


Figura 13. Traza a www.keiyu-ndt.com.tw



4.1.9.4 Resultados en utilización excesiva del canal:

Figura 14. Ping www.appmachines.com

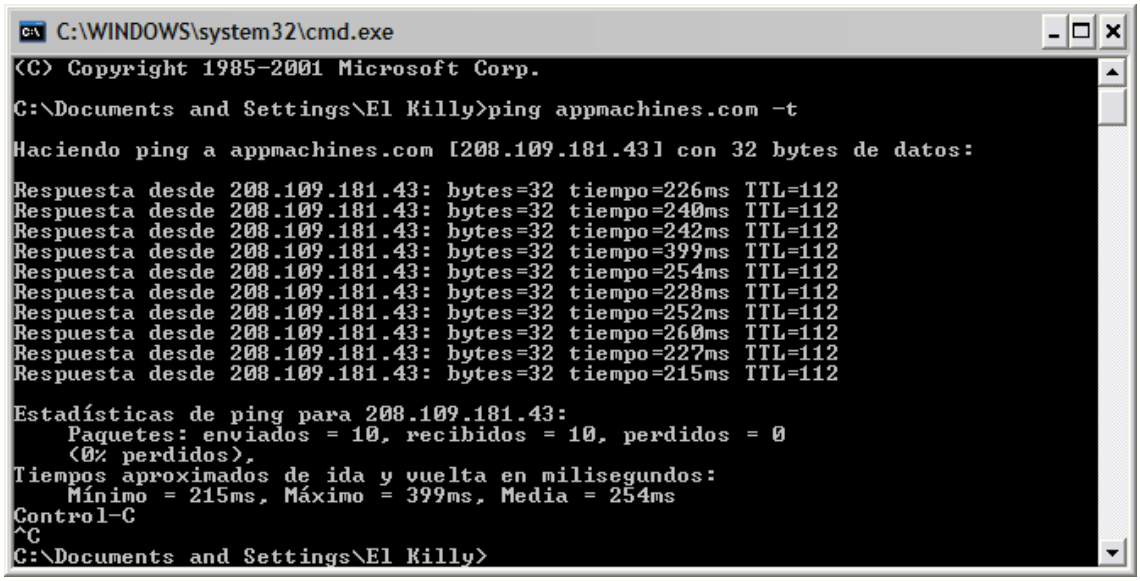


Figura 15. Ping a www.portafolio.com.co

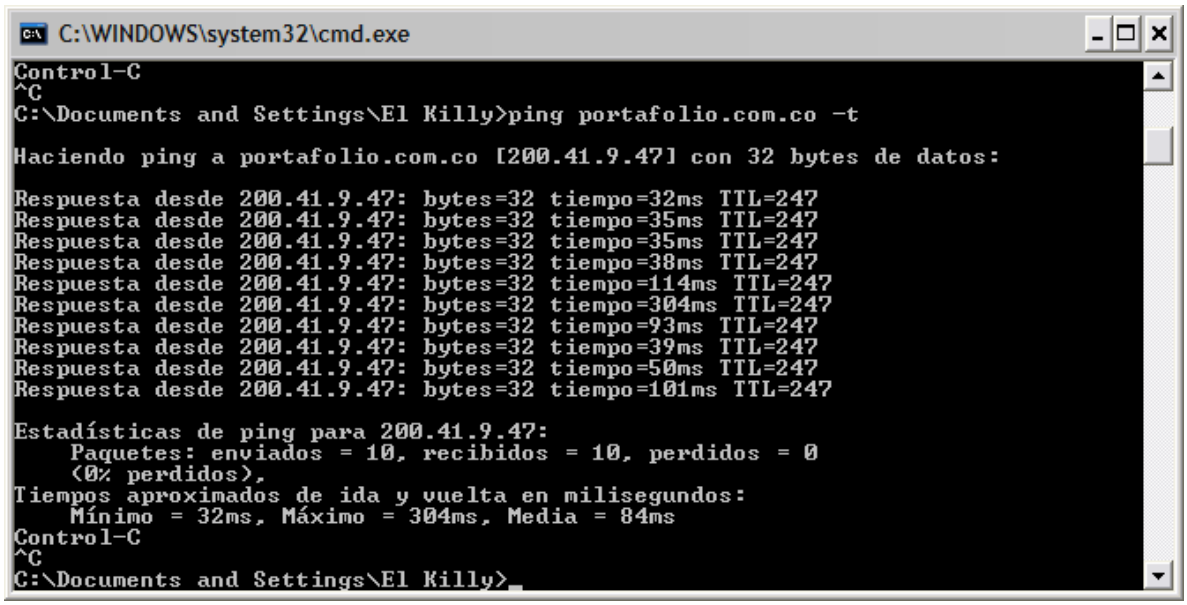


Figura 16. Ping a www.labomed.com

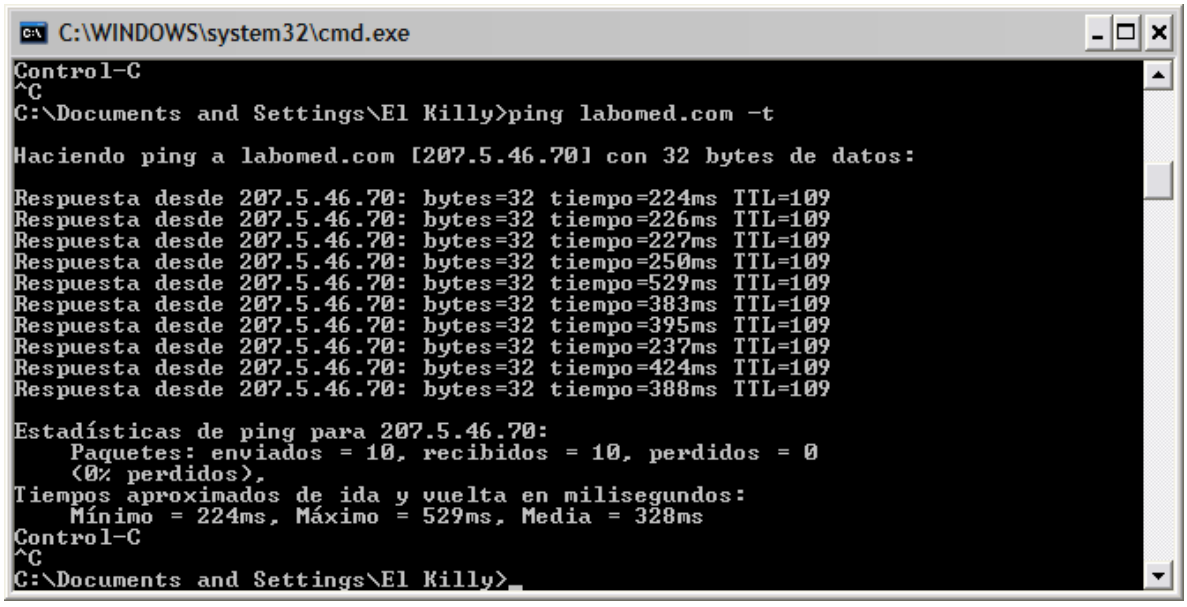
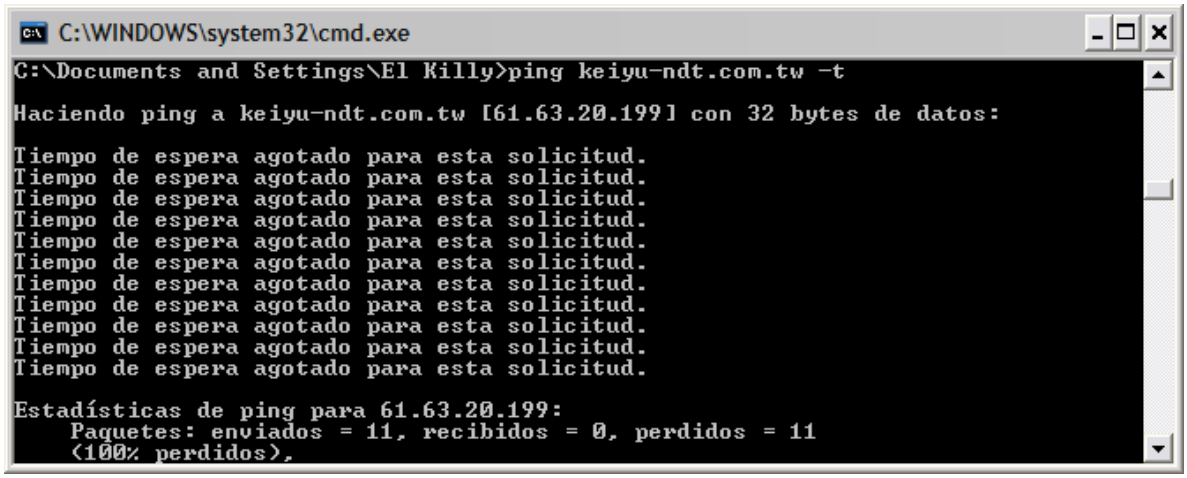


Figura 17. Ping a www.keiyu-ndt.com.tw*



* No todas las páginas de Internet responden a los mensajes ICMP por seguridad, pero esto no significa que no exista conexión con la página.

Figura 18. Ping a www.xe.com

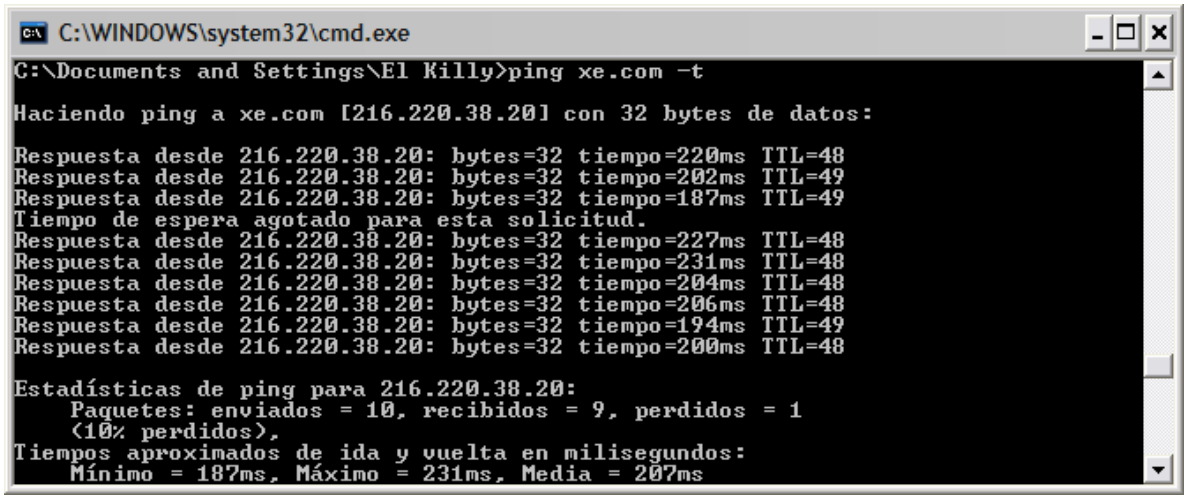


Figura 19. Traza a www.portafolio.com.co

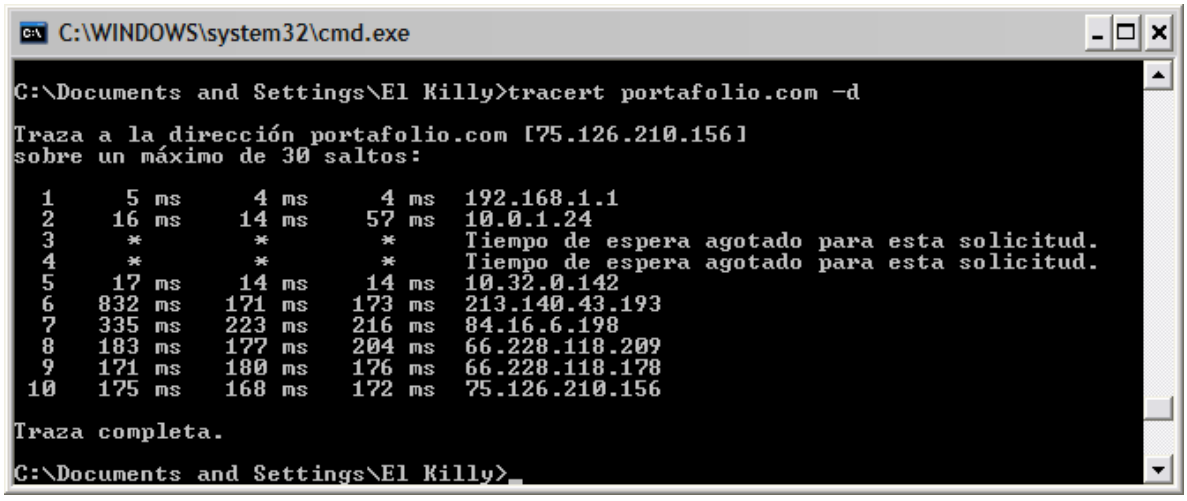
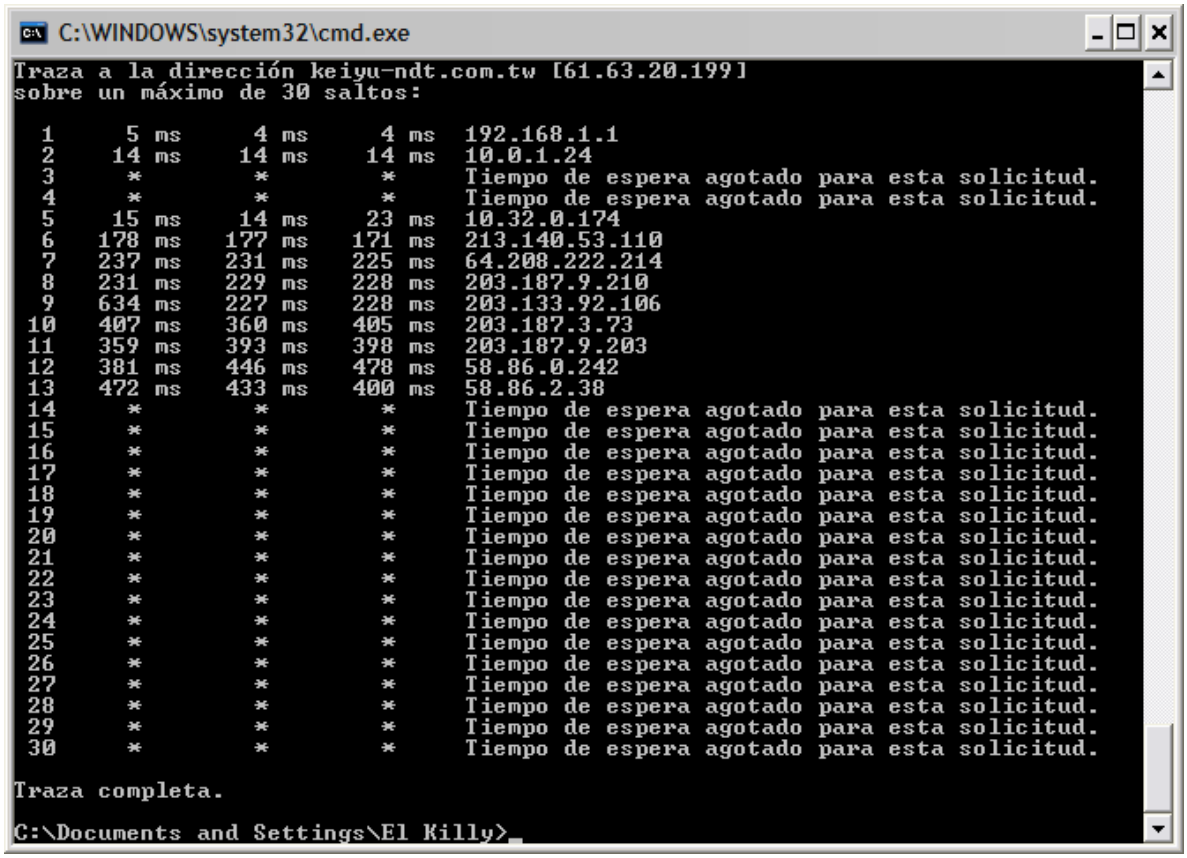


Figura 20. Traza a www.keiyu-ndt.com.tw



El siguiente cuadro contiene agrupados los datos con la utilización normal y excesiva del canal, además de la diferencia entre ambas siendo este cuadro un patrón de análisis para el rendimiento de la red o canal de Internet dentro de APP MACHINES Ltda.

Tabla 15. Estadísticas de Ping con diferentes usos del Canal.

Tipo	Dirección WEB	Utilización Normal del Canal			Utilización Excesiva del Canal			Total
		Mínimo	Máximo	Media	Mínimo	Máximo	Media	
Ping	www.appmachines.com	122	127	124	215	339	254	130
Ping	www.portafolio.com.co	9	15	11	32	304	84	73
Ping	www.labomed.com	133	140	136	224	529	328	192
Ping	www.keiyu-ndt.com.tw	257	272	262	Pp	Pp	Pp	sin M
Ping	www.xe.com	102	107	104	187	231	207	103

* El total es la diferencia de la media de utilización normal del canal y la media de utilización excesiva del canal.

Se puede concluir que el rendimiento de la red actual de APP MACHINES está en los promedios normales de envío y respuesta de los pings, el más rápido fue a portafolio y el más lento fue a Keiyu debido a la distancia y al número de saltos que tiene que dar para llegar hasta esa red, además hay una variación importante en los tiempos en general cuando se está haciendo uso excesivo del ancho de banda, esto es un impacto negativo que el nuevo diseño por medio del control de contenido y la asignación de ancho de banda debe volver a parámetros normales garantizando así un buen diseño de red.

4.1.10 Nuevos Requerimientos de Red. Para los nuevos requerimientos de red se realizó una entrevista con el Gerente de la empresa, para determinar la evolución de la misma en los próximos tres años. El resultado de esta entrevista, se adjunta al presente proyecto como soporte de los datos recopilados. Después de analizar los resultados de la entrevista se obtuvieron los siguientes requerimientos:

- **Personal.** Se contempla la posibilidad de contratar tres personas adicionales como mínimo en el transcurso de los siguientes tres años, para satisfacer el crecimiento y las necesidades de la empresa. De cumplir con esto, se deberán de adquirir los equipos de cómputo respectivos para dicho personal.

- **Aplicaciones.** Dentro de los requerimientos se encuentran aplicaciones a futuro. La primera es un aplicativo de base de datos llamado SAMM. Este paquete

sirve para organizar y manejar el seguimiento a clientes, igualmente sirve para establecer trabajos o tareas cronológicamente. La segunda es un software de diseño de máquinas como Autocad o SolidEdge y tercero un software para el manejo de equipos que trabajan con ultrasonido llamado UTSIM.

- **Equipos de Impresión y Otros.** Aunque las impresoras que se poseen en el momento se consideran suficientes, el gerente puede proyectar la adquisición de impresoras que hagan parte del diseño de la nueva red teniendo su propio punto de datos y su dirección IP. Igualmente se podría pensar en adquirir software para telefonía IP o teléfonos IP. Adicionalmente es necesario adquirir algunas UPS (Fuente de poder ininterrumpido), con el fin de mantener los servidores y los equipos prendidos por lo menos mientras se guardan las configuraciones al momento de alguna interrupción de energía.

- **Servicios y Perfiles de Usuario.** Los perfiles de usuario se manejarán en el mediante el servicio Proxy, al momento de configurar los grupos de trabajo y dentro de la división de host y equipos activos por propósito, ubicación geográfica o propiedad.

- **Consecución de nuevos PC.** Esto depende estrictamente de la llegada de nuevo personal o de la consideración directa de la gerencia por cambiar o actualizar un equipo dependiendo de las necesidades de la empresa.

- **Instalación y configuración de servidores.** Pensando en el nuevo diseño, se considera la instalación y configuración de un servidor instalando servicios de Base de Datos, Aplicaciones, Proxy y posiblemente DNS o DHCP.

4.2 DISEÑAR LA RED LAN TENIENDO EN CUENTA LAS NORMAS TÉCNICAS Y LEGALES QUE SE REQUIEREN

4.2.1 Consideraciones generales. Una vez realizado todo lo correspondiente a la caracterización de la red actual, se tienen datos claros acerca de las aplicaciones que la empresa utiliza diariamente, además, de las aplicaciones que se tienen pensadas utilizar con miras al nuevo diseño. Igualmente, se tiene conocimiento de los protocolos que corren dentro de su red (conexión a INTERNET) siendo este un parámetro importante pues la mayoría del tráfico que circula por una red es debido a protocolos y actualizaciones de estado de las mismas. Al mismo, tiempo se tiene la información de que equipos y cuantos se tienen actualmente. Este es sin duda otro factor importante en el nuevo diseño pues se debe justificar la adquisición de nuevos equipos pensando no solo en el crecimiento de la empresa sino en los avances tecnológicos y la escalabilidad de la nueva red. En cuanto a los cuellos de botella, siempre es una preocupación dar un equilibrio entre seguridad y

rendimiento. Así mismo, el tratar de disminuir los cuellos de botella se vuelve un reto para cualquier diseñador de redes. Además, todas las conclusiones extraídas del capítulo anterior deben ser un punto de arranque para el nuevo diseño que debe ofrecer garantías en cuanto a un ancho de banda robusto, tener redundancia en los equipos de las capas de núcleo y acceso del diseño, ofrecer alternativas solidas para la seguridad de la información y de la red, llegando a ser un diseño confiable en todos los aspectos, teniendo en cuenta los requerimientos del cliente, las normas y estándares que rigen el diseño de redes.

4.2.2 Antecedentes. Cisco propone en su libro Desingning Cisco Networks, Volumen 1. Versión 2.0 alrededor de doce capítulos para tener en cuenta en el diseño de redes. Los más relevantes son:

- Caracterizar la red existente
- Extraer los nuevos requerimientos del cliente
- Diseñar la topología
- Provisión de hardware y de los medios de comunicación para la LAN
- Provisión de hardware y de los medios de comunicación para la WAN
- Diseñar un modelo de direccionamiento de capa de red
- Seleccionar los protocolos de enrutamiento
- Características del software a disposición
- Seleccionar una estrategia de administración de la red
- Escribir un documento del diseño
- Validar el diseño de la red

La información que se puede obtener de estos capítulos es importante para el proyecto, haciendo la aclaración de que se toman solo como una guía y no se está ceñido totalmente a lo que diga Cisco pues algunos factores pueden cambiar de acuerdo al diseño que se necesita para este proyecto.

Una vez hecho el levantamiento de toda la información, el siguiente paso es realizar el diseño físico de la red, donde se tendrá en cuenta entre otras, áreas de trabajo, instalaciones eléctricas, instalaciones de datos, equipos activos, equipos pasivos, adquisición de nuevos computadores o impresoras y por supuesto el cableado estructurado que se necesite.

Es importante conocer cómo se encuentra actualmente la oficina con el fin de poder determinar si se va a hacer reingeniería de lo que se tiene, o por el contrario se va a empezar el diseño desde cero. Para esto se ha levantado un plano con el

área de trabajo que se tiene disponible para trabajar y otro plano de cómo están ubicados los equipos actualmente y como se logra tener conexión a INTERNET.

Durante el desarrollo de este capítulo se tendrán en cuenta varios planos para dar entendimiento y desarrollo a dicho punto. Los planos que aparecen en este trabajo se desarrollaron en AUTOCAD 2007 y son una fiel copia de los planos originales suministrados por la firma constructora de la edificación, los cuales se tomaran como referencia para el avance de todo el trabajo. Así mismo, para dar sentido a los planos anexos al documento (Ver Anexo A. Figuras, Mapas y Planos P. 159), se numerarán las diferentes salas que se encuentran en el plano para facilitar la identificación de cada área cada vez que se haga mención a la misma. De esta manera, la numeración quedará de la siguiente manera: (Ver Anexo A, Figura 21 Zonificación áreas de trabajo existentes. P. 160)

- Oficina y área de trabajo actual – Zona 1
- Bodega actual – Zona 2
- Recepción actual – Zona 3
- Oficina 1. (Nuevo diseño) – Zona 4
- Oficina 2. (Nuevo diseño) – Zona 5
- Recepción (Nuevo diseño) – Zona 6

La Figura 22 (Ver Anexo A, Figura 22 Áreas disponibles actualmente. P. 161) permite observar dos áreas bien definidas y de tamaño suficientemente grande para ubicar los equipos y los cuartos de telecomunicaciones que se necesiten para el diseño. Estas áreas están correctamente acotadas.

La Figura 2 (Mapa de distribución de los equipos. P. 67), muestra la forma como se encuentran distribuidos los equipos actualmente, donde se observa que son menos de los que se tiene pensado instalar, pues el diseño está orientado a un crecimiento mínimo de tres años. Así mismo, se observa cómo están conectados los equipos y la forma como se lleva la corriente a cada uno de ellos. La infraestructura de la oficina cuenta con un montaje eléctrico por dentro del muro, pero no cuenta con la cantidad suficiente de tomas y derivaciones para los equipos que se desean instalar. Actualmente, la conexión eléctrica de los equipos se hace a través de extensiones y tomas múltiples. De esta figura se concluye que es necesario hacer un diseño integrado para llevar la energía a cada uno de los equipos lo mismo que los cables de datos para cada uno de ellos. Esto implica la utilización de canaletas para llevar la corriente a cada uno de los equipos y la instalación suficientes de toma corrientes dobles. Igualmente, los cables de datos se transportaran por canaletas independientes de las anteriores y se terminarán en tomas de datos sencillos.

Para la elaboración del nuevo diseño se deben tener en cuenta los estándares y las normas que rigen este tipo de diseño. Por eso es importante saber la utilidad y la aplicación que pueden llegar a tener dentro del proyecto.

Tabla 16. Normas Nacionales e Internacionales Aplicables al proyecto

Norma	Fin de la norma	Tipo
ANSI/EIA/TIA 568a	Las topologías, la distancia máxima de los cables, el rendimiento de los componentes, las tomas y los conectores de telecomunicaciones.	Internacional
ANSI/EIA/TIA 568b	Estándar de cableado para telecomunicaciones en edificios comerciales, requerimientos generales, balance del cable par trenzado, estándar de componentes para cableado de fibra óptica	Internacional
ANSI/EIA/TIA 569b	Rutas y espacios para cables de telecomunicaciones en una edificación, reconoce tres conceptos, los edificios son dinámicos, los sistemas de telecomunicaciones son dinámicos y las telecomunicaciones son más que voz y datos	Internacional
ANSI/EIA/TIA 606ª	Estándar de administración para la infraestructura de telecomunicaciones en edificios comerciales	Internacional
ANSI/EIA/TIA 607ª	Sistema de puesta a tierra para telecomunicaciones	Internacional
ICONTEC NTC 4353	Telecomunicaciones, cableado estructurado, cableado para telecomunicaciones en edificios comerciales	Nacional
ICONTEC NTC 2050	Reglamento técnico de instalaciones eléctricas	Nacional
ISO/IEC 17799	Tecnología de la Información – Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información	Internacional

4.2.3 Diseño Físico de la Red. Con relación a este punto es importante justificar el por qué el diseño va a ser una red cableada y no una red inalámbrica. Una red inalámbrica puede presentar problemas, como: desconexión de los medios, interferencias debido a otras redes, caídas por estados climáticos, en la calidad de la señal y en la velocidad de transmisión dentro de la misma LAN. Se puede decir, que la posibilidad de caídas de una red inalámbrica, no es solo problema del ISP que presta el servicio sino que influyen factores externos que hacen que por ahora la red cableada esté un paso adelante, pues depende únicamente del ISP, que de factores externos. Además, una red inalámbrica puede resultar más costosa que una cableada, debido al costo que implica la compra de antenas o tarjetas de red inalámbricas para cada computador e impresora. Un factor específico de APP MACHINES es la solicitud de adelantar un estudio acerca del espectro electromagnético en las cercanías de la empresa, pues la misma queda cercana a la sede principal de la DIJIN, quienes cuentan con gran cantidad de equipos de

telecomunicaciones instalados en sus dependencias con sus respectivas antenas, que interfieren en gran medida las comunicaciones en este sector de la ciudad. Igualmente, a unos doscientos metros aproximadamente de la sede de la empresa, existe instalada una celda de un operador de telefonía móvil con sus correspondientes interferencias.

Como primer paso, se levantó el plano de la planta física de la oficina para determinar los espacios disponibles y elaborar el diseño físico. El plano se elaboró en AUTOCAD versión 2007, tomado como modelo el plano real que posee la empresa de la edificación, teniendo en cuenta las medidas y distribuciones actuales según el citado plano (Ver Anexo A. Figura 22 Áreas disponibles actualmente. P.161).

Descripción de la planta física (Ver Anexo A. Figura 21. Zonificación áreas de trabajo existentes. P 160): La planta física se encuentra en un solo piso el cual se divide en dos grandes oficinas, la primera denominada como oficina 2, con medidas de 5.60 m x 2.85m para un área de 15.96 $m^{2,}$ la segunda nombrada como oficina 1 tiene medidas de 6.85m x 3.50m para un área de 23.97 m^2; están separadas por un pasillo señalado como recepción posee medidas de 6.85m x 2.50m de área de 17.125 m^2, así mismo cuenta con 2 baños uno de ellos con medidas de 2.25m x 5.07m para un área de 11.40 m^2 y el otro 1.82 m x 2.85 m para un área de 5.187 $m^{2,}$ finalmente un garaje de 4.25 m x 4.55 m para un área de 19.33 m^2.

Toda la edificación está sustentada en muros de bloque sellado con cemento aparte de ello cuenta con ventanales en cada una de las oficinas para así garantizar ventilación e iluminación. Se concluye que se cuenta con una planta física de un área total de 54.48 m2 para adelantar el diseño de la red.

La infraestructura cuenta con un montaje eléctrico por dentro del muro, pero no cuenta con la cantidad de tomas y derivaciones suficientes para la cantidad de equipos que se desean implementar, lo cual lleva a la planeación y diseño de una infraestructura eléctrica externa e independiente de la red eléctrica actual. En el momento la conexión de los equipos se hace a través de extensiones y tomas múltiples (Ver Anexo A. Figura 23, Mapa Eléctrico Actual. P 162). Esta Figura permite observar que en total existen cinco tomas dobles de corriente distribuidas dos en la sala principal o oficina 1, dos tomas dobles de corriente en la bodega y una más en la recepción, de ahí que a ellas se conecten multitomas para poder suplir las necesidades de corriente de todos los equipos en funcionamiento que son alrededor de quince dispositivos eléctricos tales como computadores de escritorios, computadores portátiles, impresoras, fuentes, entre otros.

El nuevo diseño necesita tener en cuenta entre otros, organización de puestos de trabajo ya sea por dependencia, por propósito o utilización de la red; además es

importante realizar un cableado estructurado de acuerdo con las normas legales establecidas, de la misma manera es vital hacer modificaciones en las oficinas 1 y 2, para ubicar en ellas además de las canaletas, los puntos de red, los puntos eléctricos y los cuartos de equipos.

Como punto de arranque del diseño, y teniendo en cuenta el amplio espacio disponible en la oficina 1, es necesario llevar a cabo la construcción de un cuarto con todas las normas de seguridad, para que funcione desde ahí la Sala de Telecomunicaciones Principal. Este será un cuarto independiente con acceso restringido, donde será instalado un gabinete de piso que contendrá los equipos de red, como el Servidor, Routers, Switches y HUB. Desde este sitio se hará la distribución de puntos de red a la oficina 1, la recepción e interconectar los Switches entre sí. (El ubicado en la oficina 1 con el ubicado en la oficina 2). Es de anotar que tanto el acceso al cuarto como al gabinete se hará mediante llaves de seguridad.

En la oficina 2 será ubicado un rack de pared tipo gabinete para montar en él un Switch y un Pacth Panel y distribuir desde ahí el cableado a los equipos de esa oficina. Esto teniendo como base conceptos de economía en la distribución del cableado general de datos y facilitar las labores de mantenimiento.

4.2.3.1 Instalaciones Eléctricas

Dado que las instalaciones de la oficina se encuentran en arriendo y que las grandes modificaciones a la planta física deben ser aprobadas por el dueño del predio, la gerencia no encuentra adecuada la compra e instalación de techos o pisos falsos para la instalación de cables de red o de energía. Por esta razón, es necesario acoger la opción de instalar canaletas plásticas para el transporte seguro de la energía y datos hacia los equipos de cómputo.

Para el proyecto, se instalarán dos tipos distintos de canaletas, así:

- Canaletas plásticas de 40x40 mm, para el tendido de cables de alimentación de energía.

- Canaletas plásticas de 60x40 mm, para el tendido de cables de datos.

Para el caso del tendido eléctrico, se tiene en cuenta la Norma NTC 2050 (Código Eléctrico Colombiano), de Noviembre 25 de 1998. Esta norma encaja dentro del enfoque que deben tener los reglamentos técnicos y que tiene plena aplicación en el proceso de utilización de la energía eléctrica. Se declaran de obligatorio cumplimiento los primeros siete capítulos de la Norma:

Cap. 1. Definiciones y requisitos generales para instalaciones eléctricas.

Cap. 2. Los requisitos de alambrado y protecciones.

Cap. 3. Los métodos y materiales de las instalaciones.

Cap. 4. Los requisitos de instalación para equipos y elementos de uso general.

Cap. 5. Los requisitos para ambientes especiales.

Cap. 6. Los requisitos para equipos especiales.

Cap. 7. Las condiciones especiales de las instalaciones.

Es de anotar, que la citada norma está enfocada principalmente en los aspectos de seguridad y protección a los usuarios.

En el proceso de diseño, se determinó que las canaletas para el tendido eléctrico se instalarán a una altura de 18 cm del nivel del piso o por encima del guarda escoba y deberán cumplir con las siguientes reglas:

- Ningún tomacorriente deberá estar instalado a una distancia menor a 30 cm del borde de la pared.

- Los tomacorrientes deberán estar separados entre sí por una distancia que no sea menor a 80 cm ni mayor a 100 cm como límites.

- Se deben instalar los tomacorrientes de tal forma que el terminal de neutro quede arriba en las instalaciones horizontales.

Las canaletas se instalarán en todo el contorno del área disponible, es decir, debe abarcar todo el área correspondiente a la oficina 1 y 2 y parte del área de la recepción. (Ver Anexo A, Figura 24. Medición de las Canaletas P. 163 y Figura 25. Instalación canaletas a través del perímetro. P. 164). El total de canaletas alcanza los 42 m. y se instalarán 22 tomas dobles en todo el contorno.

La distribución a cada uno de los tomacorrientes se realizará a través de canaletas plásticas y conductores eléctricos del tipo GPT 12 AWG diferenciándose las fases y la línea a tierra con los colores rojo (línea viva), negro (línea neutro) y amarillo (línea a tierra), de acuerdo a las normas del Código Eléctrico Nacional.

Puesto que el cableado eléctrico es de vital de importancia para que los equipos electrónicos que componen la red, funcionen correctamente y teniendo en cuenta

que en este campo no se cuenta con la experiencia necesaria para garantizar un buen desempeño de las nuevas instalaciones, se dará curso a la gerencia de la empresa de la solicitud de que el diseño de instalación de la red eléctrica se contraté con una entidad experta en la rama, tal como lo exige la norma NTC 2050 y el RETIE.

El diseño de cumplir con las directrices expuestas anteriormente en este numeral.

4.2.3.2 Cableado de datos. Para realizar el cableado estructurado de la empresa, se deben tener en cuenta los estándares para realizar usa solución completa de conectividad donde se pueda garantizar la utilización de servicios de datos y de voz sin afectar el rendimiento y la confiabilidad de la red, ya sea diariamente o a largo plazo. Igualmente se debe tener en cuenta una planificación a futuro pues el cable a instalar debe satisfacer estas necesidades, potencialmente se debe tener en cuenta soluciones de categoría 5e y 6 pues está implementación trae consigo la admisión de tecnologías actuales y futuras, Ver Anexo A. Figura 28. Cableado UTP par trenzado P.167.

Siguiendo los lineamientos de Cisco, en sus indicaciones de cableado estructurado acompañados por Panduit, existen siete subsistemas relacionados con el cableado estructurado y cada uno tiene una función específica para proveer servicios de datos y voz dentro de una empresa, es importante resaltar que Cisco es la compañía líder en equipamiento de redes y administración de redes, por eso el proyecto busca referirse a Cisco y sus lineamientos:

1. Punto de demarcación (PDM)

2. Sala de equipamiento (ER)

3. Sala o cuarto de telecomunicaciones (TR)

4. Cableado de backbone, conocido como cableado vertical

5. Cableado de distribución o cableado horizontal

6. Área de Trabajo (WA)

7. Administración

De estos subsistemas se van a tener en cuenta el número 1, el 3, 4, el 5 y 6 aclarando que APP MACHINES es una empresa pequeña, no siendo necesario para este diseño hacer la implementación de cableado vertical, pero si hay que tener en cuenta algo del cableado denominado como cableado de Backbone, pues su aplicación se verá reflejada en la conexión que se hará entre los Switches Sw1 y Sw2.

Por otro lado esta red debe ser escalable tanto en el cableado, en el cuarto de telecomunicaciones y en el área de trabajo, esto se hace para poder adaptarse a cambios posteriores ya sean de diseño o por cambios de la gerencia, así que deberá tenerse en cuenta hacer el tendido de cable extra, por ejemplo tender un cable adicional hacia cada estación de trabajo o escritorio ofreciendo de esta manera redundancia por falla en el cable o en los pares del cableado. En el cuarto de equipos debe tenerse en cuenta el tender o agregar un 20% del cable tendido para prevenir futuras fallas del cableado. Para el área de trabajo deberían utilizarse placas de pared multipuerto para prevenir requerimiento de derivaciones de cableado de red. Los estándares de administración requieren que todos estos circuitos o dispositivos estén claramente detallados para facilitar el entendimiento de las conexiones y el posible diagnostico de fallas.

4.2.3.3 Punto de demarcación. Punto establecido en un edificio o un complejo para separar los equipos del cliente de los equipos del proveedor de servicios[37]. Realmente este es el punto donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios, siendo de vital importancia para una empresa pues si sucede un problema es importante saber si el problema es responsabilidad de la compañía o del proveedor de servicio.

En el proyecto el punto de demarcación es donde los dos hilos de cable que provienen de la acometida externa se juntan con el filtro que provee el ISP para dividir por una lado la señal telefónica y por otro lado la señal de ADSL, luego se conecta un cable con terminación RJ11 desde el filtro hasta el modem que brinda la señal de Internet. Por consiguiente el punto de demarcación y la sala o cuarto de comunicaciones deben ir de la mano pues en dicho cuarto debe encontrarse un filtro para llevar al modem la señal de Internet y de ahí a los otros dispositivos que el diseño disponga. Debido a esto, para efectos del proyecto el punto de demarcación estará ubicado en la sala o cuarto de telecomunicaciones que será ubicada en la oficina 1 u oficina principal

4.2.3.4 Sala de equipamiento. Tiene la misma función que la sala o cuarto de telecomunicaciones, pero la sala de equipamiento se considera cuando se trabaja en un edificio grande con varias salas de telecomunicaciones y una sala de equipamiento central, para el proyecto no aplica este concepto porque la edificación es de un solo piso y solo tendrá un cuarto de telecomunicaciones. La norma TIA/EIA 606A define para la administración de infraestructura de telecomunicaciones en edificios comerciales cuatro clases:

[37] CISCO Networking Academy “CCNA Exploration 4.0 Acceso a la WAN” Capitulo 1.2.2.1

“Clase 1.

- Un solo cuarto de equipos, que hace la función de sala de equipamiento.
- No existen cuartos adicionales de telecomunicaciones.
- No existe cableado vertical.
- Rutas de cable simples que no necesitan de administración.”[38]

Este modelo es el que aplica a los requerimientos de la empresa APP MACHINES debido al tamaño de la edificación y las necesidades.

4.2.3.5 Sala o cuarto de telecomunicaciones. En ella está ubicado el punto de demarcación pues una vez que el cable ingresa a la edificación, se dirige hacia la instalación de entrada. Ya en la sala de telecomunicaciones, ella es el centro de la red de datos y voz, pues alberga los equipos de distribución como Routers, Switches, servidores, PBX telefónicos, equipos de Internet de alta velocidad entre otros.

Debido a que la empresa no tiene ningún cuarto de telecomunicaciones, se tiene la necesidad de crear un cuarto que pueda salvaguardar equipos de telecomunicaciones que se usaran en el posterior diseño entre los que se encuentran, un Router R1, un Switch Sw1, un servidor, una UPS. La finalidad de estos equipos es llevar datos a ambas oficinas dentro de la empresa y también gestionar la red cuando el diseño esté montado totalmente. La sala o cuarto de telecomunicaciones del proyecto se diseñará y se construirá dentro de la oficina 1, estimaría dimensiones de 2.25 metros de largo por 1.20 metros de ancho, de esta forma, la norma TIA/EIA 569A, dice que para instalar un gabinete se requiere de por lo menos 76.2cm de espacio libre para que la puerta pueda abrir, por lo cual el cuarto de equipos se ajusta a los parámetros establecidos. Se pondrá una pared en cemento a lo largo de los 2.25 metros y se asentará una puerta de acceso a dicho cuarto con sus respectivas llaves de ingreso.

Para el proyecto, la sala de comunicaciones tendrá instalados el Router R1 conectado al modem, que suministra el proveedor de servicios o punto de demarcación, el Switch principal Sw1 y el servidor. Desde el Switch Sw1 se conectará un cable cruzado hasta el otro Switch Sw2, para dar conectividad a la oficina 2. Dicho Switch Sw2 puede estar montado contra una pared con bisagra

[38] Pdf “Suplemento sobre cableado estructurado” Disponible en: http//www.espoch.edu.ec/descargas/noticias/dacee2_CCNA1_CS_Structured_Cabling_es.pdf P. 27 Consultado: [11 de Agosto de 2009, 10:00 am]

para un bastidor de distribución o un rack de pared, para Panduit esto puede ser considerado como Cableado vertical o cableado de Backbone y la norma recomienda que la distancia máxima de esta conexión sea de 300 metros, por lo que va de acuerdo con la TIA/EIA 568A.

4.2.3.6 Cableado Vertical o Cableado Backbone. Cualquier cableado instalado entre la MC Conexión cruzada principal y otra TR sala de telecomunicaciones se conoce como cableado backbone. Los estándares establecen con claridad la diferencia entre el cableado horizontal y backbone. El cableado backbone también se denomina cableado vertical. Está formado por cables backbone, conexiones cruzadas principales e intermedias, terminaciones mecánicas y cables de conexión o jumpers usados para conexiones cruzadas de backbone a backbone.[39] El cableado de backbone incluye lo siguiente:

• TR en el mismo piso, MC a IC e IC a HC

• Conexiones verticales o conductos verticales entre TR en distintos pisos, tales como cableados MC a IC

• Cables entre las TR y los puntos de demarcación

• Cables entre edificios, o cables dentro del mismo edificio, en un campus compuesto por varios edificios.

La distancia máxima de los tendidos de cable depende del tipo de cable instalado. Para el cableado backbone, el uso que se le dará al cableado también puede afectar la distancia máxima. Por ejemplo, si un cable de fibra óptica monomodo se utiliza para conectar la HC a la MC, entonces la distancia máxima de tendido de cableado backbone será de 3000 m (9842,5pies). Algunas veces la distancia máxima de 3000 m (9842,5 pies) se debe dividir en dos secciones. Por ejemplo, en caso de que el cableado backbone conecte la HC a la IC y la IC a la MC. Cuando esto sucede, la distancia máxima de tendido de cableado backbone entre la HC y la IC es de 300 m (984 pies). La distancia máxima de tendido de cableado backbone entre la IC y la MC es de 2700 m (8858 pies)[40]

Para la aplicación del proyecto como ya se dijo anteriormente en este capítulo, el cableado Backbone será el cableado que irá desde el TR cuarto de telecomunicaciones ubicado en la oficina 1 hasta el rack de pared ubicado en la

[39] Ibid., P. 21.
[40] Ibid., P. 22.

oficina 2, dicho cableado será una conexión cruzada entre los Switches Sw1 y Sw2 para llevar señal de datos a dicha oficina y permitir el paso de las VLAN entre ambos Switches.

Para este diseño se necesitan dos (2) switches, que dentro de las especificaciones, cada uno tenga entre dos (2) y cuatro (4) puertos Gigabit Ethernet, para interconectarlos entre sí, dando un ancho de banda elevado que garantice una mejor disponibilidad de los servicios de red. Así mismo se puede dejar abierta la posibilidad de configurar Etherchannel o crear agregación de enlaces.

De la misma manera cada Switch debe cumplir el requerimiento de tener veinticuatro (24) puertos Fast Ethernet, para tener redundancia por puerto, con el fin de poder reemplazar un puerto si este se cae o se daña, sin afectar así el trabajo de la persona perjudicada por la caída de dicho puerto. Aproximadamente van a ser utilizados en total nueve (9) puertos en el Switch Sw1 y seis (6) puertos en el Switch Sw2, dejando quince (15) puertos para utilizarse como redundancia para el Switch Sw1 y diecinueve (19) para redundancia en el Switch Sw2, dicha redundancia tendrá injerencia importante cuando dentro del diseño lógico se desarrolle la creación de VLAN por dependencia, pues cada VLAN tendrá asociada tres (3) puertos en cada uno del los Switch.

4.2.3.7 Cableado de distribución o cableado horizontal. Se debe utilizar un esquema de cableado uniforme en todo el sistema del panel de conexión. Por ejemplo, si se utiliza un plan de cableado T568-A para tomas o jacks de información, se deben usar paneles de conexión T568-A. Esto también se aplica para el plan de cableado T568-B.

Los jacks que se usan para este tipo de conexión son RJ-45 y el cable que se usa es par trenzado no blindado (UTP), que define como tipo de conexión como ya se indico anteriormente RJ-45, define como lógica del conector que los pares 2 y 3 se usan para la comunicación de los datos y el par 1 y 4 son neutros.

Para los cables directos y el plan de cableado se utilizará la norma T568-A como parámetro, dejando claro que tanto la norma anteriormente indicada como la T568-B son óptimas para el proyecto, indicando además que las redes no usan los cuatro pares (8 cables) en total, utilizan 4 cables, dos para transmitir y dos para recibir. Del mismo modo para los cables cruzados que se utilizaran para interconectar los Switches Sw1 y Sw2 entre sí, serán en un extremo con plan T568-A y en el otro extremo T568-B.

4.2.3.8 Área de trabajo. El área de trabajo es a donde la sala o cuarto de equipos le presta servicio. Por lo general ocupa un piso o parte de un piso en un edificio.[41] La distancia de cableado horizontal máxima es de 90 metros, desde el punto de terminación en la sala de telecomunicaciones hasta la terminación en la toma del área de trabajo. La ANSI/TIA/EIA-568-B establece que puede haber cinco (5) metros de cable de conexión para interconectar los paneles de conexión del equipamiento, y cinco (5) metros de cable desde el punto de terminación del cableado en la pared hasta el teléfono o el computador. Este máximo adicional de diez (10) metros de cables de conexión agregados al enlace permanente se denomina canal horizontal. La distancia máxima para un canal es de cien (100) metros. El máximo enlace permanente, es de noventa (90) metros más diez (10) metros como máximo de cable de conexión, (ver anexo Figura 29, Distancias de cableado según la NTC 4353. P 167).

Para los servicios del área de trabajo es útil usar cables de conexión cuando con frecuencia se producen cambios en la conectividad. Es mucho más fácil conectar un cable desde la toma del área de trabajo a una nueva posición en la sala de telecomunicaciones que quitar hilos terminados de aparatos ya conectados, y volver a terminarlos en otro circuito. Los cables de conexión también son utilizados para conectar el equipo de networking a las conexiones cruzadas en una sala de telecomunicaciones. Los cables de conexión están limitados por el estándar TIA/EIA-568-B.1 a cinco (5) metros.

El área de trabajo en la compañía se encuentra distribuida en tres partes, la oficina 1 ó principal, la oficina 2 y la recepción, la sala o cuarto de telecomunicaciones debe encargarse de irrigar datos a estos tres sitios buscando tener en red todos los equipos que la empresa posee de manera que todos puedan interactuar si lo requieren. De esta manera, el área de trabajo en la oficina 1, después de quitar el espacio requerido para construir el cuarto de telecomunicaciones quedaría de 5.32 metros de largo por 3.5 metros de ancho aproximadamente, el área de trabajo de la recepción sería aproximadamente de 6.59 metros de largo por 2.5 metros de ancho, finalmente el área de la oficina 2 tendría aproximadamente 5.60 metros de largo por 2.85 metros de ancho, teniendo en total un aproximado de 17.51 metros por 8.85 como área de trabajo para distribuir los puntos de datos y los puntos de corriente.

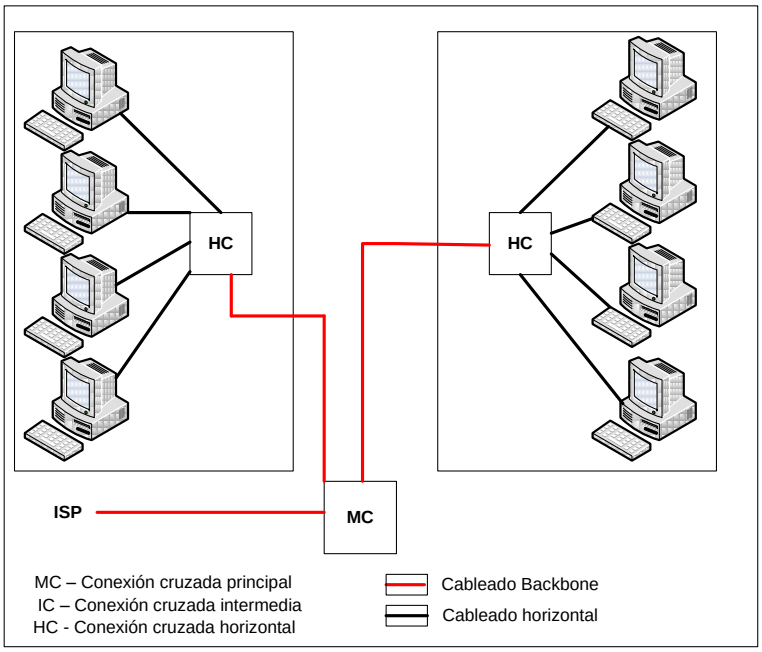
Por disposición de la gerencia la ubicación de los equipos dentro de la edificación se hará conforme a grupos estratégicos, de esta manera la oficina 1 acogerá

[41] Ibid., P. 14.

equipos del área de la gerencia, sistemas, contabilidad y comercio exterior, mientras que en la oficina 2 serán ubicados equipos del área de ventas, mantenimiento y jurídica, dejando en el hall la recepción.

Para el diseño físico se va a denominar una conexión cruzada principal y una conexión cruzada horizontal como lo muestra la Figura 32 (Conexión cruzada principal y conexión cruzada horizontal).

Figura 32 Conexión cruzada principal y conexión cruzada horizontal



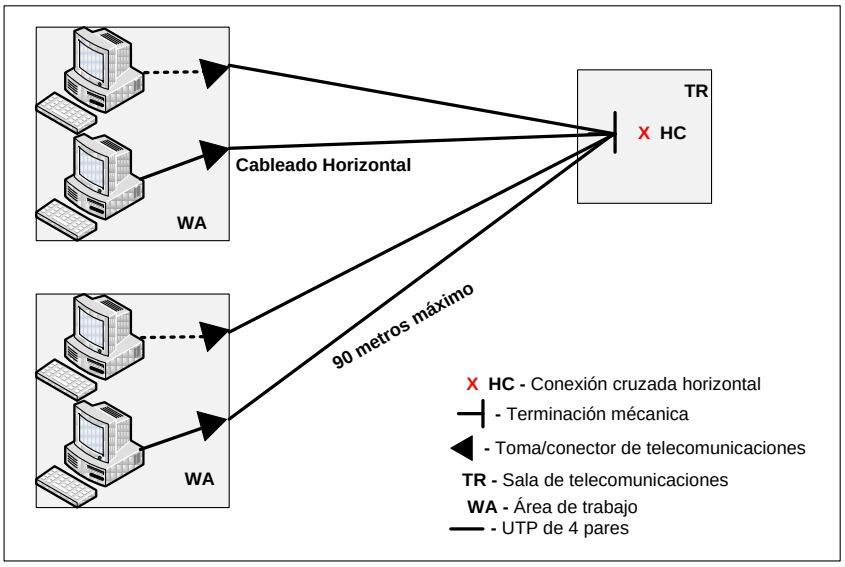
La conexión cruzada horizontal (HC) es la sala de telecomunicaciones más cercana a las áreas de trabajo. La HC por lo general es un panel de conexión o un bloque de inserción a presión. La HC puede también contener dispositivos de networking como repetidores, hubs o switches. Puede estar montada en un bastidor en una habitación o gabinete. Dado que un sistema de cableado horizontal típico incluye varios tendidos de cables a cada estación de trabajo, puede representar la mayor concentración de cables en la infraestructura del edificio.[42]

[42] Ibid., p. 22.

Para el proyecto la MC o conexión cruzada principal es el cuarto de telecomunicaciones que está ubicado en la oficina 1, la HC o conexión cruzada horizontal del cuarto de telecomunicaciones es la que distribuye cableado a la oficina 1, siendo el Switch Sw1, la otra HC o conexión cruzada horizontal es el rack que contiene el Switch Sw2 de distribución de la oficina 2 para distribuir cableado a la oficina anteriormente mencionada.

Como se acaba de indicar la HC de la oficina 2 contiene su Switch para distribuir los datos en ese sitio de la empresa como se observa en la Figura 33, (Conexión cruzada horizontal en la oficina 2).

Figura 33. Conexión cruzada horizontal en la oficina 2



Finalmente el cableado de datos será tendido de dos formas, la primera ira desde la sala de telecomunicaciones hasta la oficina Nº1 ubicando ocho puntos de datos en ocho tomas sencillas, estas tomas se distribuirán separadas a 30 centímetros de la pared, la siguiente toma debe estar entre 80cm y 100 cm separada la una de la otra con el fin de evitar interferencia electromagnética. De la misma forma se va a tender un cable hasta una toma doble de datos ubicada en la recepción. La segunda distribución ira desde la sala de comunicaciones hasta el panel de distribución conectándose al Switch y este mismo distribuirá el cableado de datos a ocho puntos de datos conectados a ocho tomas sencillas que tendrán aplicada

la misma norma que se utilizo para la distribución de las tomas en la oficina 1, (Ver AnexoA. Figura 27. Cableado de Datos P.165 y Figura 26, Detalle Frontal Canaletas P.164).

4.2.4 Diseño Lógico de la red. Antes de empezar con el diseño lógico hay que resaltar que es importante recordar que la empresa exige un mínimo de tres cotizaciones, para poder ejecutar órdenes de compra.

En los anexos se encuentran cotizaciones de elementos Cisco, 3com y Trendnet.

Para el estudio de las cotizaciones se van a usar matrices de selección y de viabilidad, para escoger finalmente el dispositivo que se usará en el diseño. (Estas matrices y su desarrollo son tomadas en apuntes de clase de la materia Análisis de Sistemas I, dictada por el entonces profesor Javier Arango Pardo).

Las matrices son armadas de acuerdo a criterios de evaluación que propone la empresa pues para ellos es importante en primer lugar la parte económica, funcionalidad, escalabilidad y desempeño del dispositivo que se escoja. El criterio se ponderará de acuerdo a las pautas que posee la empresa para escoger otro tipo de dispositivos donde el factor es una numeración de 1 a 5. Para el caso del proyecto se tomará 5 como la escala más alta, llenando a tope lo que se pide en los requerimientos del cliente, el 3 en la escala marcará un punto medio de la selección donde se puede considerar que falte o que sobre según el criterio analizado, finalmente el 1 en la escala marca que no llena las expectativas respecto a lo que la empresa solicita. Nos basamos en las pautas que tienen establecidas en APP MACHINES para evaluar con criterio las cotizaciones que entran a estudio.

La matriz de selección tomará cada opción por aparte tomando como criterios de selección:

1. Económico: Este ítem tiene un porcentaje del 30% sobre la decisión final, debido a que el precio debe estar sujeto a la parte económica de la empresa y al cumplimiento de los requisitos que la compañía requiere.

- Calificación: 5, 3, 1; donde 5 es la mayor probabilidad de compra, 3 la media y 1 la menor probabilidad de compra, comparando la rentabilidad que ofrece el producto de acuerdo a su precio.

2. Operativo: Este ítem tiene un porcentaje del 5% sobre la decisión final, debido a la compatibilidad que tiene el dispositivo con los sistemas operativos que se

encuentran en el mercado. Así se garantiza que el dispositivo que se adquiera, funcione con cualquier sistema operativo.

- Calificación: 5, 3, 1; donde 5 significa el total acuerdo con los sistemas operativos que soporta el dispositivo, 3 significa que no están acorde con lo que ofrece el producto de acuerdo a los sistemas operativos que soporta y 1 que están en total desacuerdo con los sistemas operativos que soporta el dispositivo.

3. Técnico: Este ítem tiene un porcentaje del 20% sobre la decisión final, teniendo en cuenta la implementación de la red comparada con el tipo y numero de puertos que el dispositivo posee pensando en los requerimientos de la empresa.

- Calificación: 5, 3, 1; donde 5 expresa que cumple de mejor manera los requerimientos de la empresa, 3 cumple con las especificaciones técnicas con gran amplitud, generando esto sobrevaloración y subutilización y 1 que no se ajusta a los requerimientos técnicos exigidos por la empresa.

4. Protocolos: Este ítem tiene un porcentaje del 15% sobre la decisión final, puesto que según el diseño, el ambiente puede ser multiprotocolo y es necesario que soporte protocolos propietarios como no propietarios.

- Calificación: 5, 3, 1; donde 5 expresa que cumple de mejor manera los requerimientos en cuanto a protocolos soportados por el dispositivo, 3 cumple con las especificaciones en cuanto a protocolos y 1 que los protocolos que soporta el dispositivo no cumplen los requerimientos exigidos por la empresa.

5. Servicios: Este ítem tiene un porcentaje del 20% sobre la decisión final, ya que para el diseño es importante la cantidad y calidad de servicios que preste el dispositivo, pensando en una red convergente.

- Calificación: 5, 3, 1; donde 5 expresa que los servicios ofrecidos por el dispositivo cumplen a cabalidad los requerimientos pensando en una red convergente, 3 los servicios cumplen parcialmente con los requerimientos de una red convergente y 1 que los servicios no se ajustan a los principios de una red convergente.

6. Facilidad de configuración: Este ítem tiene un porcentaje del 10% sobre la decisión final, al que ofrezca una mejor y mayor posibilidad de configuración del dispositivo.

- Calificación: 5, 3, 1; donde 5 cumple a cabalidad con la mayor y mejor posibilidad de configuración con respecto al dispositivo, 3 ofrece opciones normales de

configuración y 1 que no ofrece mayor posibilidad de configuración para lo requerido en la empresa.

Tras especificar los criterios a tener en cuenta en la matriz de selección para el Router, los resultados están referenciados en la Tabla 17.

Tabla 17. Matriz de selección para el Router

CRITERIOS	CANDIDATO 1 TRENDNET TW100BRV304	%	CANDIDATO 2 CISCO 1841	%	CANDIDATO 3 CISCO 2821	%	Total %
ECONÓMICO	$600.000 (5)	1.500	$1'400.000 (3)	0.900	$6'636.000 (1)	0.3	30%
OPERATIVO	Compatible con los sistemas Windows 95/98/ME/NT/2000/XP, Unix y Mac (5)	0.25	Compatible con los sistemas Windows 95/98/ME/NT/2000/XP, Unix y Mac (5)	0.25	Compatible con los sistemas Windows 95/98/ME/NT/2000/XP, Unix y Mac (5)	0.25	5%
TÉCNICO	3 puertos 10/100, 1 puerto WAN 10/100 (1)	0.2	2 puertos 10/100, 1 puerto de consola, 1 puerto auxiliar, 2 slost modulares (5)	1	2 puertos 10/100/1000, 1 puerto de consola, 1 puerto auxiliar, 4 slots modulares, 1 puerto USB (3)	0.6	20%
PROTOCOLOS	NAT, PPPoE, NTP, SMTP, HTTP, TFTP, DHCP, TCP/IP, PAP, CHAP, RIP1, RIP2, DDNS (3)	0.45	NAT, PPP, HDLC, SMTP, PAP, CHAP, HTTP, DHCP, RIP V1, RIP V2, EIGRP, 802.1Q (5)	0.75	NAT, PPP, HDLC, SMTP, PAP, CHAP, HTTP, DHCP, RIP V1, RIP V2, EIGRP, 802.1Q (5)	0.75	15%
SERVICIOS	VPN Firewall (3)	0.6	VPN, VLAN, ACL (5)	1	VPN, VLAN, QoS, ACL (5)	1	20%
FACILIDAD DE CONFIGURACIÓN	http, https (3)	0.3	Consola, http, https, auxiliar (5)	0.5	Consola, http, https, auxiliar (5)	0.5	10%
Total	Opción 1	3.300	Opción 2	4.400	Opción 3	3.4	100%

4.2.4.1 Matriz de Viabilidad para el Router. Está matriz tiene como fin indicar por qué se escogió la alternativa 2 como opción para el diseño.

Tabla 18. Matriz de Viabilidad para el Router

Criterio	Candidato 2 Router Cisco 1841
Económico	$1'400.000
Operativo	Compatible con los sistemas Windows 95/98/ME/NT/2000/XP, Unix y Mac

Técnico	2 puertos 10/100, 1 puerto de consola, 1 puerto auxiliar, 2 slost modulares
Protocolos	NAT, PPPoE, NTP, SMTP, HTTP, TFTP, DHCP, TCP/IP, PAP, CHAP, RIP1, RIP2, DDNS
Servicios	VPN Firewall
Facilidad de configuración	http, https , consola, auxiliar

Según el análisis de la tabla se escoge el candidato 2, debido a que cumple a cabalidad con todos los criterios y requerimientos que pide el diseño y la empresa.

Tras especificar los criterios a tener en cuenta en la matriz de selección para los Switches, los resultados están referenciados en:

Tabla 19. Matriz de selección para los Switches

	Switch Cisco Catalyst 2960 24 puertos 10/100, 2 puertos 10/100/1000	%	Switch Trendnet 24 puertos Giga, TEGS240 TX	%	Switch 3com 24 puertos giga, 3CRBSG2893	%	Total %
ECONÓMICO	$1'900.000 (3)	0.900	$1'200.000 (3)	0.900	$1'500.000 (3)	0.9	30%
TÉCNICO	24 puertos 10/100, 2 puertos 10/100/1000 (3)	0.6	24 puertos 10/100/1000 (3)	0.6	24 puertos 10/100/1000, 4 puertos 10/100/1000 SFP (5)	1	20%
PROTOCOLOS	SNMP, 802.1Q CDP (5)	1	SNMP (1)	0.2	SNMP (1)	0.2	20%
SERVICIOS	Avanzado QoS, ACL, VLAN, 802.1x, VoIP, Port security, 4 colas de prioridad (5)	1	VLAN (1)	0.2	802.1x VLAN, ACL (3)	0.9	20%
FACILIDAD DE CONFIGURACIÓN	Consola, CLI, basado en WEB (5)	0.5	Basado en WEB (3)	0.3	Basado en WEB, consola (5)	0.5	10%
Total	Opción 1	4.000	Opción 2	2.200	Opción 3	3.5	

4.2.4.2 Matriz de Viabilidad para los Switches. Está matriz tiene como fin indicar por qué se escogió la alternativa 2 como opción para el diseño.

Tabla 20. Matriz de Viabilidad para los Switches.

Criterio	Switch Cisco Catalyst 2960 24 puertos 10/100, 2 puertos 1000
Económico	$1'900.000
Técnico	24 puertos 10/100, 2 puertos 1000
Protocolos	SNMP, 802.1Q, CDP, STP

Servicios	Avanzado QoS, ACL, VLAN, 802.1x, VoIP, Port security, 4 colas de prioridad
Facilidad de configuración	Consola, CLI basado en WEB, auxiliar

4.2.4.3 Direccionamiento IP. La empresa en la actualidad tiene contratado el servicio de internet con el ISP (TELMEX), la cual otorga concesiones en las direcciones IP solamente por 8 días. Por lo tanto, la persona encargada del área de sistemas tendría que realizar un trabajo de configuración de IP, indagando que dirección le fue asignada cada vez que la empresa prestadora del servicio en este caso (TELMEX) cambie las direcciones para poder ofrecer salida de internet a la compañía. Lo cual conlleva pérdida de tiempo, sobrecarga de trabajo en el área de sistemas. Por esta la recomendación de adquirir con el ISP, una dirección IP fija , con el fin de que pueda ser utilizada permanentemente con la traducción de la salida a internet con los diferentes tipos de NAT existentes. "Algunas de las ventajas que conlleva ello son conservar el esquema de direccionamiento legalmente registrado, aumenta la flexibilidad de las conexiones con la red pública, brinda regularidad para esquemas de direccionamiento de redes internas y brinda seguridad de red"[43].

Se va a utilizar direccionamiento privado para asignárselo a los equipos que pertenece la empresa, tal cual como queda referenciado en la tabla 21, se debe dejar claro que para efectos del diseño en cada Red o subred se dejaran libres o por fuera de la asignación de las mismas por DHCP las primeras 10 direcciones con el fin de asignarlas a elementos que necesitan direcciones IP fijas, como pueden ser servidores, teléfonos IP, impresoras, fax, pbx al mismo tiempo se incluirán aquí las direcciones de administración de los equipos de red, Switches y routers, pensando de igualmente en la escalabilidad de la red y el posible crecimiento de la empresa.

El servicio del direccionamiento IP fijo tiene un costo mensual de $5.000. Por lo cual a nivel económico no es relevante y es de fácil acceso para la empresa.

Tabla 21. Direccionamiento IP General

[43]CISCO Networking Academy "CCNA Exploration 4.0 Acceso a la WAN", Capitulo 7.2.3

Clase	Dispositivos de Red o Conexión	Dirección IP	Máscara de subred	1ra Dirección Disponible	Última dirección Disponible	Dirección de Broadcast	Siguiente dirección de subred
A	de R1 a ISP	200.69.32.0/30	255.255.255.252	200.69.32.1	200.69.32.2	200.69.32.3	200.69.32.4
C	Vlan 10	192.168.0.0/24	255.255.255.0	192.168.0.1	192.168.0.254	192.168.0.255	192.168.1.0
C	Vlan 15	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.254	192.168.1.255	192.168.2.0
C	Vlan 20	192.168.2.0/24	255.255.255.0	192.168.2.1	192.168.2.254	192.168.2.255	192.168.3.0
C	Vlan 25	192.168.3.0/24	255.255.255.0	192.168.3.1	192.168.3.254	192.168.3.255	192.168.4.0
C	Vlan 30	192.168.4.0/24	255.255.255.0	192.168.4.1	192.168.4.254	192.168.4.255	192.168.5.0
C	Vlan 35	192.168.5.0/24	255.255.255.0	192.168.5.1	192.168.5.254	192.168.5.255	192.168.6.0
C	Vlan 40	192.168.6.0/24	255.255.255.0	192.168.6.1	192.168.6.254	192.168.6.255	192.168.7.0
C	Vlan 99	192.168.99.0/24	255.255.255.0	192.168.99.1	192.168.99.254	192.168.99.255	192.168.100.0

4.2.4.4 Router. A continuación la Tabla 22 explica las características a utilizar por parte de un Router Cisco de la serie 1800, este dispositivo tendrá como fin hacer enrutamiento hacia Internet y llevando Internet a todos los dispositivos que lo requieran dentro de la compañía, igualmente el dispositivo hará enrutamiento INTERVLAN para que algunos miembros en VLAN diferente se puedan comunicar o puedan tener acceso entre sí con otras VLAN.

Tabla 22. Router Cisco serie 1800.

Nombre y modelo del dispositivo	Nombre de la interfaz	Dirección MAC	Dirección IP/mascara de subred	Protocolos de enrutamiento
R1, Cisco 1841	fa0/0	0050.0F38.0C01	200.68.32.1/30	
	fa0/1	0050.0F38.0C02	192.168.99.1/24	

De la tabla 22 se puede conocer que el Router R1, posee dos puertos Fast Ethernet, el puerto Fast Ethernet0/0 va conectado al Router ISP o Modem que brinda el ISP, el puerto Fast Ethernet 0/1 va conectado al puerto giga1/1 del Switch Sw1, las funciones principales del router son hacer enrutamiento INTERVLAN y llevar Internet a las estaciones de trabajo.

4.2.4.5 Switches. Se van a utilizar y configurar dos Switches Catalyst 2960, estos dispositivos poseen 24 puertos Fast Ethernet y dos puertos Gigabit Ethernet, dichos dispositivos tendrán conectados a sus puertos, el Router R1, entre sí los dos Switches, el Servidor SRV1 y las estaciones de trabajo de la compañía. Quedan alrededor de 17 puertos sin equipos conectados pero asociados a las VLAN que se configurarán, estos garantiza redundancia por puerto y la posibilidad de escalar la red sin importar la dependencia que crezca.

En las tablas 23 y 24 se muestra cómo se van a configurar los Switches, los puertos que van a ser utilizados y los que se dejarán disponibles, de la misma manera los puertos que tienen conectados estaciones de trabajo, el servidor se dejan en modo de acceso, también los puertos que están disponibles para equipos que se pueden conectar a las diferentes VLAN se dejan en modo de acceso y se dejaran administrativamente abajo. Finalmente los puertos que comunican los Switches Sw1, Sw2 y el Router R1 se encuentran en modo troncal para permitir el paso de las VLAN y el enrutamiento INTERVLAN.

Tabla 23 Características del Switch Sw1

Nombre del Switch, modelo dirección ip	Nombre del puerto	Velocidad	Duplex	Estado STP (Reenviar / Bloquear)	Puerto rápido	Estado troncal	Canal Ether (L2 o L3)	Clave
Sw1, WS-C2960-24TT, 192.168.1.254/24	fa0/1	100	Full	Reenviar	Si	On	L2	Conectado con R1
	fa0/2	100	Automático	No	Si	Off	L2	Conectado con PC0
	fa0/3	100	Automático	No	Si	Off	L2	Conectado con PC1
	fa0/4	100	Automático	No	Si	Off	L2	Conectado con PC4
	fa0/5	100	Automático	No	Si	Off	L2	Conectado con PC2
	fa0/6	100	Automático	No	Si	Off	L2	Conectado con PC3
	fa0/7	100	Automático	No	Si	Off	L2	No Conectado
	fa0/8	100	Automático	No	Si	Off	L2	No Conectado
	fa0/9	100	Automático	No	Si	Off	L2	No Conectado
	fa0/10	100	Automático	No	Si	Off	L2	No Conectado
	fa0/11	100	Automático	No	Si	Off	L2	No Conectado
	fa0/12	100	Automático	No	Si	Off	L2	No Conectado
	fa0/13	100	Automático	No	Si	Off	L2	No Conectado
	fa0/14	100	Automático	No	Si	Off	L2	Conectado con PC9
	fa0/15	100	Automático	No	Si	Off	L2	No Conectado
	fa0/16	100	Automático	No	Si	Off	L2	No Conectado
	fa0/17	100	Automático	No	Si	Off	L2	Conectado con PC10
	fa0/18	100	Automático	No	Si	Off	L2	No Conectado
	fa0/19	100	Automático	No	Si	Off	L2	No Conectado
	fa0/20	100	Automático	No	Si	Off	L2	No Conectado
	fa0/21	100	Automático	No	Si	Off	L2	No Conectado
	fa0/22	100	Automático	No	Si	Off	L2	No Conectado
	fa0/23	100	Automático	No	Si	Off	L2	Conectado con SRV1
	fa0/24	100	Automático	No	Si	Off	L2	No Conectado
	Giga1/1	1000	Automático	Reenviar	No	On	L2	Conectado con Sw2
	Giga1/2	1000	Automático	No	No	Off	L2	No Conectado

Tabla 24 Características del Switch Sw2

Nombre del Switch, modelo dirección ip	Nombre del puerto	Velocidad	Duplex	Estado STP (Reenviar / Bloquear)	Puerto rápido	Estado troncal	Canal Ether (L2 o L3)	Clave
Sw2, WS-C2960-24TT, 192.168.2.254/24	fa0/1	100	Automático	No	Si	Off	L2	No Conectado
	fa0/2	100	Automático	No	Si	Off	L2	No Conectado
	fa0/3	100	Automático	No	Si	Off	L2	No Conectado
	fa0/4	100	Automático	No	Si	Off	L2	No Conectado
	fa0/5	100	Automático	No	Si	Off	L2	No Conectado
	fa0/6	100	Automático	No	Si	Off	L2	No Conectado
	fa0/7	100	Automático	No	Si	Off	L2	No Conectado
	fa0/8	100	Automático	No	Si	Off	L2	Conectado con PC5
	fa0/9	100	Automático	No	Si	Off	L2	Conectado con PC6
	fa0/10	100	Automático	No	Si	Off	L2	No Conectado
	fa0/11	100	Automático	No	Si	Off	L2	Conectado con PC7
	fa0/12	100	Automático	No	Si	Off	L2	Conectado con PC8
	fa0/13	100	Automático	No	Si	Off	L2	No Conectado
	fa0/14	100	Automático	No	Si	Off	L2	No Conectado
	fa0/15	100	Automático	No	Si	Off	L2	No Conectado
	fa0/16	100	Automático	No	Si	Off	L2	No Conectado
	fa0/17	100	Automático	No	Si	Off	L2	No Conectado
	fa0/18	100	Automático	No	Si	Off	L2	No Conectado
	fa0/19	100	Automático	No	Si	Off	L2	No Conectado
	fa0/20	100	Automático	No	Si	Off	L2	Conectado con PC11
	fa0/21	100	Automático	No	Si	Off	L2	No Conectado
	fa0/22	100	Automático	No	Si	Off	L2	No Conectado
	fa0/23	100	Automático	No	Si	Off	L2	No Conectado
	fa0/24	100	Automático	No	Si	Off	L2	No Conectado
	Giga1/1	1000	Automático	Reenviar	No	On	L2	Conectado con Sw1
	Giga1/2	1000	Automático	No	No	Off	L2	No Conectado

4.2.4.6 Sistema Final (Estaciones de Trabajo). Las estaciones de trabajo se encuentran distribuidas en las dos oficinas que se encuentran reseñadas en la Figura 21, ver anexo. Según dispone la gerencia en la oficina principal se encontrarán las estaciones de trabajo referentes al departamento de Gerencia, el departamento de Sistemas y el departamento de Comercio exterior. La oficina secundaria Tendrá alojadas estaciones de trabajo concernientes al departamento de Ventas, el departamento de Mantenimiento y el departamento de Jurídica. El cuarto principal de comunicaciones que como ya se ha indicado anteriormente estará en la oficina 1 u oficina principal, tendrá el Servidor, el cual estará ubicado en un rack o gabinete de piso que tendrá instalados también el Router R1 y el Switch Sw1. En la tabla 25 está descrito el sistema final de la compañía, en dicha tabla se encuentran reseñados cada estación de trabajo con características, entre las cuales se encuentran el nombre del dispositivo que sirve para asociar el equipo a la dependencia a la que pertenece, esto además es de gran ayuda debido a que será un factor importante para la creación y configuración de VLANs, el tipo de sistema operativo que tiene instalado la máquina, el rango de dirección IP en el que se encuentra el dispositivo, el Gateway por defecto, la dirección del servidor de nombres o DNS y sus aplicaciones de red, todo esto tiene como fin dejar

documentado el diseño para hacer más sencilla la corrección de errores en el futuro.

Tabla 25 Sistema final

Nombre del dispositivo, (objetivo)	Sistema operativo/versión	Dirección IP/mascara de subred	Dirección de Gateway Predetermina	Dirección del servidor DNS	Aplicaciones de red
SRV (servidor de administracion)	Linux Centos 5	192.168.0.2/24	192.168.99.1/24	200.21.200.80	http
PC0 (PC del usuario: Gerencia)	Windows XP Home SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC1 (Pc del usuario: Gerencia)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC2 (Pc del usuario: Depto Sistemas)	Windows XP Professional SP3	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http, telnet
PC3 (Pc del usuario: Depto de Sistemas)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http, telnet
PC4 (Pc del usuario: Recepción)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC5 (Pc del usuario: Ventas)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC6 (Pc del usuario: Ventas)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC7 (Pc del usuario: Mantenimiento)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC8 (Pc del usuario: Mantenimiento)	Windows XP Professional SP2	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC9 (Pc del usuario: Contabilidad)	Windows XP Professional SP3	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC10 (Pc del usuario: Comercio ext.)	Windows XP Professional SP3	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http
PC11 (Pc del usuario: Jurídica)	Windows XP Professional SP3	Asignada por dhcp	192.168.99.1/24	200.21.200.80	http

4.2.4.7 Creación y configuración de las VLAN. La segmentación de la red dentro de APP MACHINES, se hará mediante VLAN y no comprando un Switch, por cada red a segmentar, debido a que esta opción es extremadamente costosa. (ejemplo: un Switch de CISCO catalyst 2960 puede admitir hasta 255 VLAN de rango normal y extendido).

Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada. Para que las computadoras se comuniquen en la misma VLAN, cada una debe tener una dirección IP y una máscara de subred consistente con esa VLAN. En el switch deben darse de alta las VLANs y cada puerto asignarse a la VLAN correspondiente.

Entre las ventajas de trabajar con VLAN como tecnología están:

- **“Seguridad:** Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

- **Reducción de costo:** el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

- **Mejor rendimiento:** la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

- **Mitigación de la tormenta de broadcast:** la división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast.

- **Mayor eficiencia del personal de TI:** las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.” [44]

La idea del diseño es dividir la red de la compañía por propósito o por dependencia, creando y configurando VLANs por cada departamento, como se cito anteriormente las VLAN ayudan a tener una red segura, es menos costoso que adquirir un Router o un Switch por cada red o subred, mejora el rendimiento de la red y ayuda para que usuarios del mismo tipo trabajen en el mismo segmento de red compartiendo esos recursos.

Las VLAN que se van a crear en este diseño tendrán asignados tres puertos en cada Switch con el fin de manejar redundancia de puertos por futuras caídas o fallos de un puerto en alguna de las VLAN, para la comunicación entre VLANS es importante configurar los puertos involucrados como puertos troncales en los Switches, estos puertos permiten que la información de las VLANs pasen sin etiquetar, mientras que los puertos asociados a las VLAN como tal o a los computadores son denominados puertos de acceso.

En la tabla 26 se muestra el direccionamiento utilizado para cada VLAN, el nombre de cada una y los puertos asociados a las mismas, en cada Switch hay puertos libres que para el diseño actual no serán asignados a ninguna VLAN.

[44] CISCO Networking Academy “CCNA Exploration 4.0 Conmutación y conexión inalámbrica de LAN” Capitulo 3.1.1

Para transferir información de las VLAN, se va a crear un Dominio VTP con un Cliente VTP y un Servidor VTP, para que esto se dé, los Switches deben estar en el mismo dominio y tener la misma contraseña.

Con el fin de garantizar que el diseño funcione con tecnologías avanzadas, los puertos fa0/2 y fa0/3 se configuraran para trabajar dentro de una VLAN de voz. Esto asegura un ancho de banda para la calidad de la voz, que el tráfico en este puerto este etiquetado dentro de la VLAN de voz. Por consiguiente, se puede decir, que el puerto queda configurado para admitir un teléfono IP y así el tráfico de voz tendrá prioridad sobre la red.

Tabla 26 Constitución de las VLAN

Switch Nº	VLAN Nº	Nombre	Dirección IP	Puertos Asociados
Sw1	VLAN 10	Gerencia	192.168.0.0/24	fa0/2, fa0/3, fa0/4, fa0/22
	VLAN 15	Sistemas	192.168.1.0/24	fa0/5, fa0/6, fa0/7
	VLAN 20	Ventas	192.168.2.0/24	fa0/8, fa0/9, fa0/10
	VLAN 25	Mantenimiento	192.168.3.0/24	fa0/11, fa0/12, fa0/13
	VLAN 30	Contabilidad	192.168.4.0/24	fa0/14, fa0/15, fa0/16
	VLAN 35	Comercio Ext.	192.168.5.0/24	fa0/17, fa0/18, fa0/19
	VLAN 40	Jurídica	192.168.6.0/24	fa0/20, fa0/21, fa0/22
	VLAN 45	Voz		fa0/2, fa0/3
	VLAN 99	Administrativa	192.168.99.0/24	
Puertos Libres				fa0/23, fa0/24
Sw2	VLAN 10	Gerencia	192.168.0.0/24	fa0/1, fa0/2, fa0/3, fa0/4
	VLAN 15	Sistemas	192.168.1.0/24	fa0/5, fa0/6, fa0/7
	VLAN 20	Ventas	192.168.2.0/24	fa0/8, fa0/9, fa0/10
	VLAN 25	Mantenimiento	192.168.3.0/24	fa0/11, fa0/12, fa0/13
	VLAN 30	Contabilidad	192.168.4.0/24	fa0/14, fa0/15, fa0/16
	VLAN 35	Comercio Ext.	192.168.5.0/24	fa0/17, fa0/18, fa0/19
	VLAN 40	Jurídica	192.168.6.0/24	fa0/20, fa0/21, fa0/22
	VLAN 99	Administrativa	192.168.99.0/24	
Puertos Libres				Fa0/23, fa0/24

Cada VLAN tiene mínimo un puerto disponible para crecimiento pensando en la escalabilidad que pueda llegar a tener esta red durante 3 años o un poco más, al

utilizar enrutamiento INTERVLAN las estaciones de trabajo en redes o VLAN diferentes podrán comunicarse pues el Router hará el enrutamiento debido para que el paquete encuentre la red del siguiente salto. Por cada departamento que tiene la empresa se creara una VLAN y cada departamento tiene como mínimo un Host, de acuerdo con la tabla 26 se observa las diferentes VLAN y su distribución.

Las VLAN sirven para segmentar las redes conmutadas basadas en equipos de proyectos, funciones o departamentos. Esto por ejemplo, permite al administrador implementar políticas de acceso y seguridad para grupos o VLANs en particular. Para APP MACHINES se ha segmentado la red en 8 subredes o VLAN porque con esto se busca que cada departamento trabaje por aparte manejando su propio flujo de datos, teniendo en cuenta que el departamento de Ventas, y la Gerencia necesitan tener un canal estable para tener contacto tanto con proveedores en el extranjero como para los clientes que se contactan vía WEB, entonces la segmentación ayudara a la empresa que cada departamento tenga su VLAN independiente con su tráfico de igual manera.

4.2.4.8 Listas de Acceso (ACL). La ACL es una configuración de Router que controla si un Router permite o deniega paquetes según el criterio encontrado en el encabezado del paquete.[45] Las ACL inspeccionan los paquetes de la red según un criterio, como dirección de origen, de destino, protocolos y números de puerto. Además de permitir o denegar el tráfico, una ACL puede clasificar el tráfico para darle prioridad en la línea. Esta capacidad es similar a tener un pase VIP para un concierto o evento deportivo. Las ACL extendidas filtran los paquetes IP en función de varios atributos, por ejemplo: tipo de protocolo, direcciones IP de origen, direcciones IP de destino, puertos TCP o UDP de origen, puertos TCP o UDP de destino e información opcional de tipo de protocolo para una mejor disparidad de control.[46]

Para el diseño se van a utilizar listas de acceso extendidas, estas listas además de lo nombrado anteriormente deben implementarse cerca al origen de los paquetes, además proporcionan un control mayor ya que comparan el paquete con más parámetros que una lista de acceso estándar, otra cosa que es importante resaltar es que solo se puede tener una lista de acceso por cada interfaz, es decir por interfaz se puede tener una ACL de entrada y una ACL de salida. La creación de estas listas de acceso tiene como fin bloquear o permitir el

[45] Ibid., capitulo 5.1.3.
[46] Ibid., capitulo 5.1.5.

acceso a ciertas redes, a ciertos servicios como navegación WEB o transferencia de archivos, además para este proyecto las ACL están fuertemente ligadas a las políticas de gestión de la red, pues las listas de acceso ayudarán al rendimiento de la red, a la seguridad de la red siendo los usuarios de la red los que más deben estar enterados de la denegación o de que se permita el acceso a la red o a ciertos servicios dentro de la empresa.

La tabla 27 hace referencia a las Listas de Acceso que se piensan implementar en el diseño

Tabla 27. Listas de Acceso (ACL)

Tipo	Nombre ACL	Descripción	Interfaz	Forma ACL
Reflexiva	SinIntrusos	Utilizando established dentro de la ACL se permite tráfico ICMP entrante y saliente pero solo se permite el tráfico TCP que se inició desde el interior de la red	Int fa0/0	De Entrada
Estándar	NoTelnetR1	Denegar el acceso a las lineas VTY de R1 a todas las redes menos a la VLAN de Sistemas	No Aplica	De Entrada
Estándar	NoTelnetSw1	Denegar el acceso a las lineas VTY de Sw1 a todas las redes menos a la VLAN de Sistemas	No Aplica	De Entrada
Estándar	NoTelnetSw2	Denegar el acceso a las lineas VTY de Sw2 a todas las redes menos a la VLAN de Sistemas	No Aplica	De Entrada

4.2.4.9 Descripción del Diseño. Para hacer más fácil el entendimiento del diseño, este se dividirá en 4 puntos importantes.

1. Cuarto de equipos o telecomunicaciones

El cuarto de equipos o telecomunicaciones estará ubicado en un cuarto aparte al lado de la oficina 1, en él habrá un rack de 120mm de altura donde estarán instalados, un Router Cisco serie 1800 (R1), un Switch Cisco Catalyst de 24 puertos Fast Ethernet y dos puertos Gigabit Ethernet (Sw1), el servidor con su teclado y mouse, el patch panel y una UPS para dotar de energía los dispositivos que se encuentran en este cuarto. El Switch Sw1 irá conectado con el Router R1 por un cable UTP categoría 6, de este cuarto saldrá cableado UTP categoría 5e para la oficina 1 o principal, cableado UTP categoría 5e para la recepción y cableado UTP categoría 6 para interconectar entre sí los Switches Sw1 y Sw2

2. Oficina 1 o principal

Tendrá ocho puntos de datos que conectan con el Switch Sw1 del cuarto de equipos

3. Gabinete de equipos oficina 2

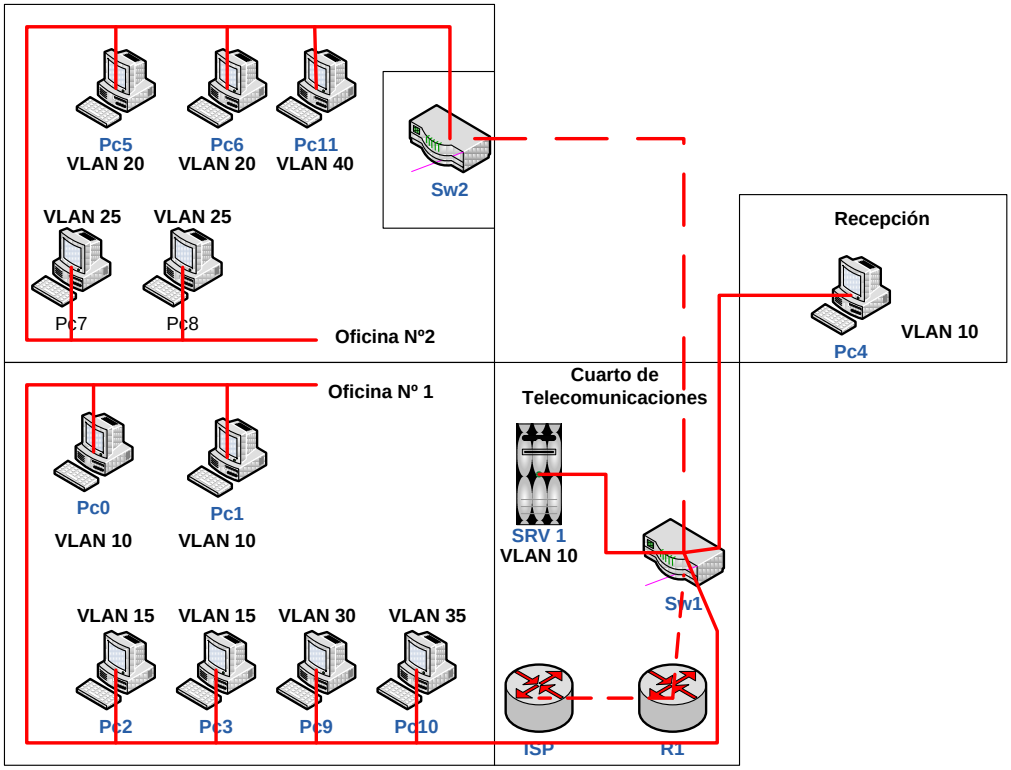
Existirá un rack de pared de 50mm en el que se situaran un Switch Cisco Catalyst de 24 puertos Fast Ethernet y dos puertos Gigabit Ethernet (Sw2), desde ahí se enviara cableado de datos para la oficina 2 y también existirá un cable UTP categoría 6 conectando entre sí Sw1 y Sw2.

4. Oficina 2

Tendrá instalado el Rack de telecomunicaciones del que saldrá cableado UTP categoría 5e para las ocho tomas de datos ubicados en esa oficina. (Ver Anexo Figura 29. Cableado de datos).

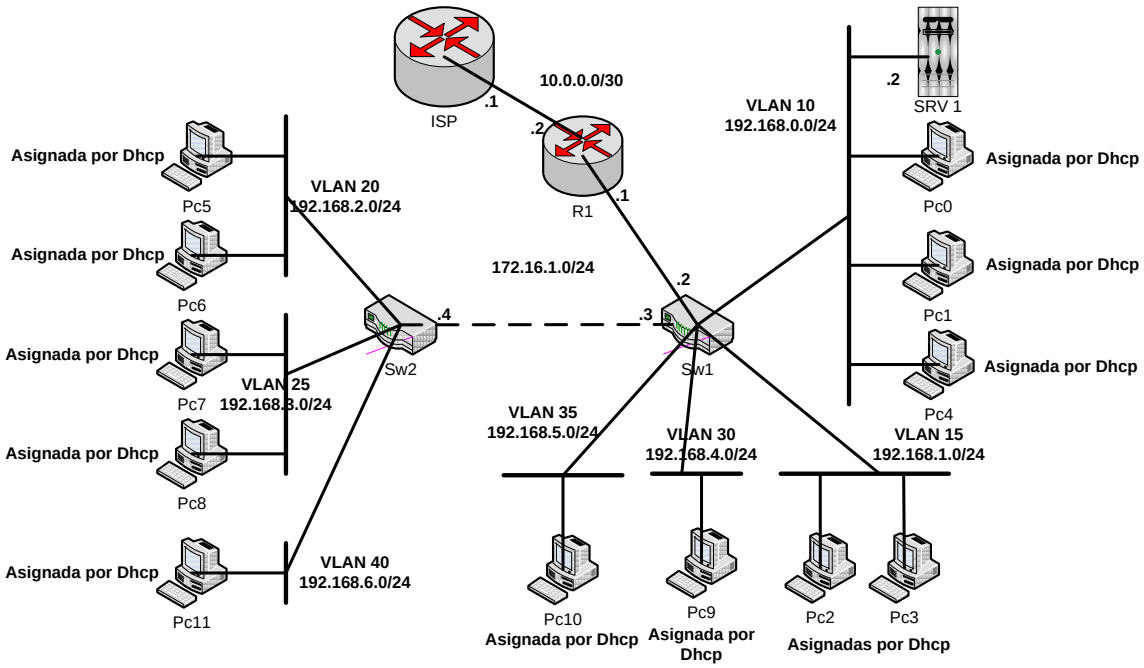
Las Figuras 34 y 35 contienen el diseño lógico con la información de las tablas anteriormente mencionadas de forma que ilustra claramente como estará dividida cada dependencia por subred y por VLAN, de manera que el direccionamiento tendrá parte estática reservada para equipos de administración como Routers, Switches, servidores y parte dinámica asignada por DHCP para las estaciones de trabajo.

Figura 34. Diseño Lógico por oficina



- La empresa seguirá con el contrato que tiene en la actualidad para su conexión de internet

Figura 35. Diseño Lógico



- **Modelo Core-Distribution-Access.** "La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez."[47]

Este tipo de modelos hace que las redes se vean separadas en capas, de manera que cada capa tenga funciones diferentes y específicas, además es importante conocer que la aplicación de este tipo de modelos ayuda a encontrar beneficios para los diseños de red, entre los que encontramos:

"**Escalabilidad:** Las redes jerárquicas pueden expandirse con facilidad.

Redundancia: A nivel de núcleo y distribución asegura disponibilidad de la ruta.

[47] Ibid. , Capítulo 1.1.1.1.

Rendimiento: El agregado del enlace entre los niveles de núcleo de alto rendimiento y Switches de nivel de distribución permite casi la velocidad del cable en toda la red.
Seguridad: seguridad de puerto a nivel de acceso y las políticas en el nivel de distribución hacen que la red sea más segura.

Facilidad de Administración: La consistencia entre los Switches en cada nivel hace que la administración sea más simple.

Facilidad de Mantenimiento: La modularidad del diseño jerárquico permite que la red escale sin volverse demasiado complicada."[48]

Este modelo es de tres capas:

- **Acceso:** Está compuesta por interfaces con dispositivos finales como PC, impresoras o teléfonos IP, encargándose de proveer acceso al resto de la red. Puede tener Routers, Switches, puentes, hubs y puntos de acceso inalámbricos.

En esta capa encontramos factores importantes que la identifican:

- Agregación de enlace
- Etherchannel
- VLAN
- FastEthernet / GigabitEthernet
- PowerOver Ethernet (PoE)
- QoS

- **Distribución:** "Agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las VLAN definidas en la capa de acceso."

Los factores importantes que se encuentran en esta capa son:

- L3 Switching
- Tasa de envió alta
- GigabitEthernet / 10GigabitEthernet

[48] Ibid. Capítulo 1.1.1.3

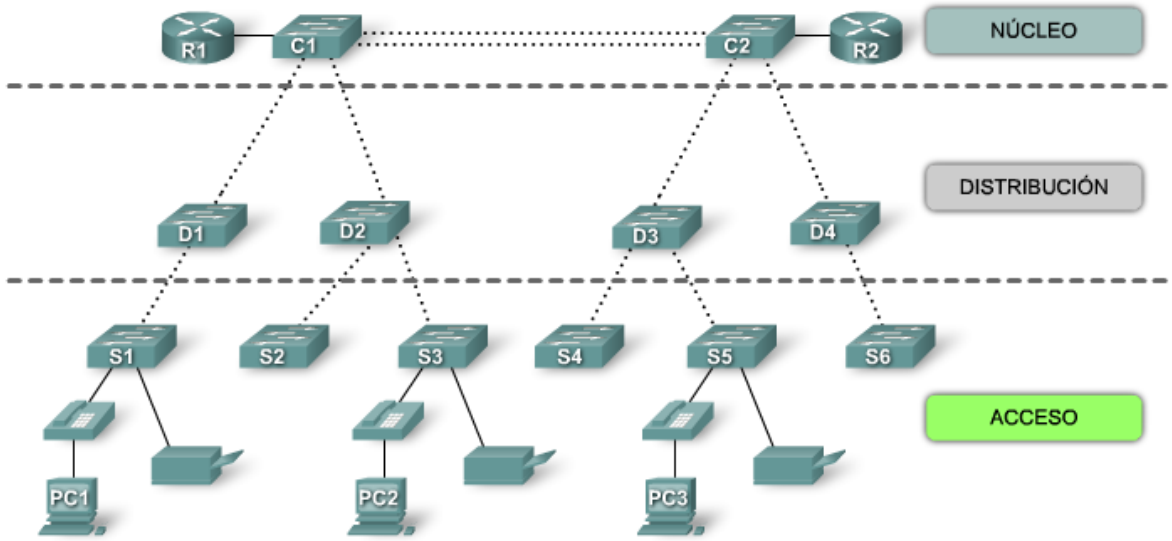
- Componentes redundantes hacia el núcleo
- ACL
- Agregación de enlaces
- QoS

- **Núcleo:** Es la capa de más alta velocidad, tiene injerencia en la interconexión de los equipos de distribución y debe ser sumamente disponible y redundante, además está parte del modelo es la que se conecta a Internet y debe estar en capacidad de poder reenviar grandes cantidades de datos rápidamente.

Los factores importantes que se encuentran son:

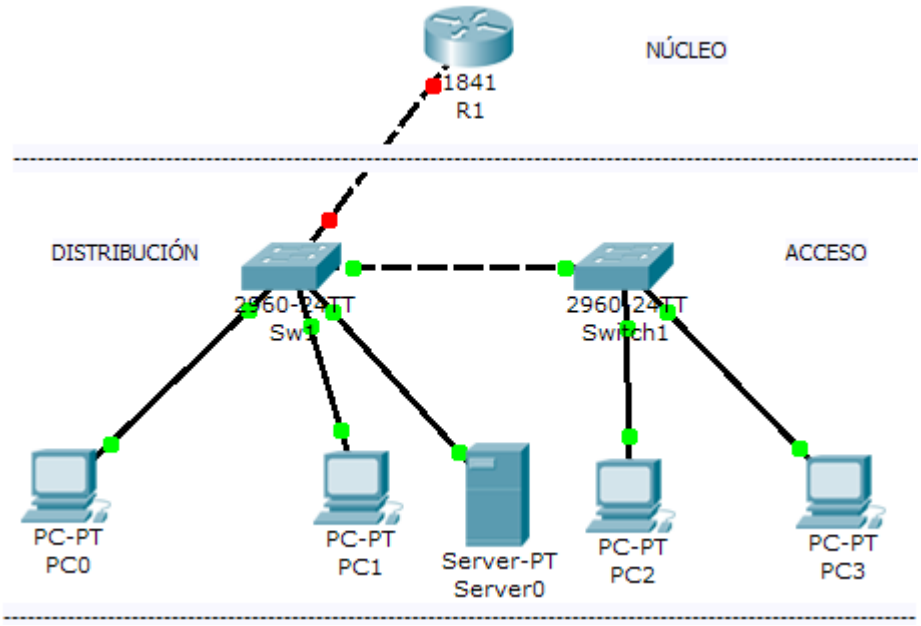
- L3 Switching
- Tasa de envió muy alta
- GigabitEthernet / 10GigabitEthernet
- QoS a nivel de Internet
- Equipos costosos y de alta disponibilidad
- Agregación de enlaces y Etherchannel

Figura 36. Modelo Jerárquico de una Red (Core-Distribution-Access)



La aplicación del modelo al diseño de la red para APP MACHINES está supeditada en primer lugar al tamaño de la empresa y al de la red, debido a que el presupuesto en APP MACHINES y las necesidades no van acordes a comprar equipos de gran envergadura además no maneja tantos usuarios como para comprar por ejemplo un Switch en capa de acceso, uno en distribución, mínimo dos routers y un Switch en capa de núcleo, asumiendo que los Swtches debiera ser multicapas para asegurar la velocidad requerida.

Figura 37. Diseño de APP MACHINES



- **Modelo de Redundancia.** El libro Designing Cisco Networks, versión 2, recomienda cuatro (4) tipos de redundancia para aplicar en un diseño de red:

  - **Entre estación de trabajo y Router**.

Para los equipos de cómputo conectados a una red es importante saber la ruta o el camino para salir de la red, en este caso es el router por defecto, cuando la red posee varios routers podemos utilizar protocolos de enrutamiento para conocer las redes no conectadas directamente, se puede utilizar de la misma forma el protocolo ARP que almacena dirección IP y dirección MAC, en este proyecto existe un solo router que se encarga de realizar el enrutamiento INTERVLAN para que los equipos de cómputo conozcan las diferentes redes.

En el libro nombrado anteriormente Cisco recomienda la implementación de Routers Fantasmas, estos dispositivos están configurados de la misma manera que el router activo, de manera que si el router activo queda fuera de línea el router fantasma entrá transparentemente a hacer la función del router activo, esto

se debe a que el router activo está periódicamente enviando tramas con las direcciones que conoce.

Debido a los costos la empresa no contempla por ahora realizar adquisiciones de routers de reserva, pero se recomienda implementarlo en el futuro con el crecimiento de la empresa.

- **Redundancia en los servidores.**

La importancia de salvaguardar los archivos que maneja la empresa a diario, brinda la posibilidad de crear discos espejo o manejar discos que dupliquen la información con el fin de poder crear copias de seguridad, además es importante darle organización al manejo de los back-up estableciendo personal encargado y horarios para la realización de los mismo, siendo la gerencia la encargada de establecer estas normas.

- **Redundancia en las rutas o en el enrutamiento**.

Este concepto es de utilidad para hacer balanceo de cargas y minimizar los efectos de las posibles caídas. Si es una red enrutada (Routers) se pueden utilizar los protocolos de enrutamientos para evitar loops de enrutamiento. De ser una red conmutada (Switches), existen mecanismo como Spanning-tree para evitar los loops de enrutamiento cuando existe más de una ruta a una red.

Para establecer redundancia en las rutas el router adquirido es modular, lo que permite adquirir tarjetas adicionales para enlaces FastEthernet o WAN, los Switches poseen 24 puertos cada uno que podrían servir para crear rutas redundantes si el caso lo requiere.

- **Redundancia en la media**.

Su importancia está a nivel de enlaces WAN y respaldo para los mismos, pero en el momento y en un futuro próximo APP MACHINES no piensa utilizar enlaces WAN para conectar diversas sucursales.

- **Modelo de Seguridad**

Con el crecimiento de los sistemas, las redes, Internet y las aplicaciones, cada vez se vuelve más complicado encontrar un equilibrio entre estar aislado y abierto, esto exige soluciones de seguridad perfectamente integradas, más transparentes y flexibles. La importancia es encontrar un equilibrio entre acceso y seguridad en una red, ya que este equilibrio es el más difícil de configurar y administrar, se hace

más difícil acceder a los recursos para los usuarios finales y una red segura puede llegar a ser bastante costosa.

El modelo de Seguridad recomendado por Cisco en su libro Designing Cisco Networks, versión 2. Está basado en configuración de Firewall o contrafuegos. “Un firewall protege una red de otra red”[49]. Por lo que es de gran importancia para el diseño pensar en la implementación del mismo para proteger su red empresarial de los peligros que trae consigo Internet.

El firewall puede ser configurado en un Router o en un Switch y funciona inspeccionando las cabeceras de los paquetes, por lo que se puede realizar filtrado de los mismos.

Para APP MACHINES el modelo de seguridad va a estar enfocado a ACL, al Servidor de administración y finalmente a las políticas de gestión.

Las ACL que se van a configurar dentro del diseño cumplen la tarea de impedir el acceso a las líneas VTY de los dispositivos activos, únicamente tendrá acceso el personal del departamento de Sistemas. Asimismo por medio de una lista reflexiva se permitirá el tráfico IP en sesiones originadas en la red empresarial y denegará el tráfico IP originado por fuera de la red.

Igualmente se recomienda al departamento de sistemas estar al tanto de las actualizaciones de los antivirus en los equipos, pues este tipo de negligencias podría producir daños en la red.

Entre los delitos informáticos que se pueden evitar mediante una buena administración se encuentran:

- **Abuso interno de acceso a Internet:** Al navegar con proxy se puede evitar la navegación en páginas indebidas tratando de disminuir al máximo el abuso en el acceso a Internet y acostumbrando al usuario a navegar para lo estrictamente necesario.
- **Denegación de servicio:** la idea del agresor es desactivar o dañar la red, el sistema o los servicios. Puede ser tomado como un acto de piratería informática pero a la vez es el ataque más temido a una red. La idea en este punto es tener la red lo más equilibrada posible en cuanto a los daños como saturación en los servidores o en los equipos activos por sobrecargas

[49] CISCO System. op. cit., P. 4-28

en los mismos, sobrecargas que serian manipuladas desde afuera de la red empresarial.

- **Detección de contraseñas:** Las contraseñas deben ser solidas y se debe evitar dejarlas anotadas en lugares visibles, se recomienda hacer actualización de contraseñas periódicamente para evitar detección a las mismas, un ataque sería un algoritmo que descifre la contraseña por medio de ataque de diccionario por ejemplo, esto pondría en riesgo la red y la información de la compañía.

"Autosecure de Cisco utiliza un único comando para desactivar procesos y servicios no esenciales del sistema y elimina amenazas de seguridad potenciales."[50] Esto ayuda a brindarle más seguridad a la red de APP MACHINES debido a que Autosecure bloquea los puertos que no se utilizan, activa el firewall por defecto del Router, activa SSH si se necesita y bloquea algunos protocolos como CDP, esto se hace de modo interactivo de manera que el usuario lo configuré como desee.

Finalmente la solución para APP MACHINES estará representada en el servidor, el firewall, el Autosecure y las listas de acceso; estos factores asegurarán en gran medida que la red del diseño sea lo más segura posible.

4.3 DETERMINAR LAS POLÍTICAS DE GESTIÓN DE LA RED EN BASE A LOS REQUERIMIENTOS DE LA EMPRESA

Al momento de hablar de gestión en una red es casi que obligatorio hablar del protocolo SNMP (Simple Network Managment Protocol). "SNMP es un protocolo del nivel de aplicación que proporciona un formato de mensajes para el intercambio de información entre gestores y agentes de SNMP"[51]
SNMP posee tres partes:

Gestor SNMP: Es el sistema encargado de monitorear y controlar la actividad de los componentes de red.

Agente SNMP: Es un componente de software dentro del dispositivo que se va a gestionar.

[50] Ibid, capítulo 4.3.3.1
[51] Practica_final_h.pdf. p. 2 Apuntes de clase Materia Gestión de Redes dictada por el profesor Hugo Malaver

La MIB (base de datos de información de administración): Son los objetos de información de gestión, estos objetos están ubicados en los dispositivos que se van a gestionar al igual que los agentes SNMP.

"El protocolo SNMP funciona según el modelo cliente/servidor. El proceso servidor se ejecuta en los agentes, donde se mantiene a la escucha de peticiones por parte del gestor SNMP. El servidor SNMP (en el agente) emplea el puerto 161 de UDP. Por otro lado, las notificaciones que genera el agente se envían al gestor al puerto UDP 162, donde debe existir un proceso gestor de interrupciones (*trap manager*) que las procese."[52]

De esa manera es importante decir que se puede configurar SNMP para que realice envíos como interrupciones o alarmas como por ejemplo, tráfico excesivo, finalmente su aplicación será desarrollada según necesidades de la empresa.

Al mismo tiempo hay que hablar del modelo de administración de redes, dicho modelo se compone de tres partes, Organizacional, técnico y funcional.

Organizacional: Aplicado al proyecto la empresa deberá definir quién o quiénes van a llevar a cabo la gestión de la red, esta persona tiene que tener las contraseñas de administración de los dispositivos, las llaves de acceso al cuarto de telecomunicaciones. Además debe determinar cada cuanto se realizaran las revisiones de los informes de navegación, el personal escogido tendrá que estar pendiente de las alarmas que se generen en el servidor, en los equipos activos o en las estaciones de trabajo.

Técnico: Define las herramientas a utilizar por parte de la empresa para desarrollar la gestión de la red, como la utilización de SNMP depende de las necesidades de la empresa, la parte técnica del modelo tendrán injerencia en la administración de los dispositivos, la gestión de los informes de navegación, la gestión del servicio WEB, el seguimiento del tráfico interno y las otras opciones posibles de gestionar en la red de APP MACHINES.

Funcional: son funciones propias de gestión. Si la empresa lo requiere, se podría crear un modelo de FCAPS (Configuración, fallos, prestaciones, seguridad y contabilidad). El personal designado en la parte organizacional se deberá encargar de la definición de tareas en cada área del modelo FCAPS.

Después de efectuadas varias reuniones con el gerente de APP MACHINES, en las que se extrajeron los requerimientos nuevos de la empresa. Basados en ellos

[52] Ibid., p. 3.

se hizo el desarrollo del diseño de la red, ahora en este capítulo se efectuará un escrito que sirva de guía para las políticas de gestión para aplicar a la red y a los usuarios que hagan uso de ella.

Como ya se indicó en el capítulo anterior el manejo del tráfico se hará con base en la separación de Host según el propósito (uso relativamente común de software, herramientas y tráfico), adicional a esto las VLAN se crearon por área o dependencia de trabajo (Gerencia, Ventas, Mantenimiento).

Para la definición de las políticas de la gestión de la red en APP MACHINES se tendrá como guía parcial la norma ISO/IEC 17799 de la que se tomarán como ejemplo parágrafos como:

- Gestión de las comunicaciones y operaciones.

- Gestión de la seguridad en la red.

- Controles de redes.

- Seguridad de los servicios de red.
- Gestión de medios, medios removibles.

- Política de control de acceso, registro del usuario.

- Gestión de privilegios, gestión de las claves secretas de los usuarios.

- Responsabilidades del usuario.

- Control de acceso a la red, políticas sobre los usos de los servicios de la red, control de conexión a la red y control del routing de la red.

Para desarrollar estas políticas de gestión es importante tener involucrado en todo momento al usuario final, que para este caso serían las personas que laboran dentro de la empresa y que harán uso de la red. Debido a esto es importante formular medidas claras y concisas sin que ellas tengan vacios para no generar malas interpretaciones, evitando así un posterior desacató de la norma o abuso por parte de los dueños de la empresa contra sus trabajadores.

4.3.1 Políticas de Gestión APP MACHINES. La gestión de la red en APP MACHINES se deberá regir en gran medida por esta norma de convivencia que vincula, dispositivos activos, computadoras, medios extraíbles y personal.

Dicha norma está dividida en:

4.3.1.1 Seguridad del cableado

Objetivo: Es importante tener en cuenta que todo el cableado debe estar protegido contra la intercepción o daño, ya que este lleva consigo datos o dan soporte a los servicios de información. Para lograr esto se debieran tener en cuenta los siguientes lineamientos:

1. En APP MACHINES el cableado de red y eléctrico estará protegido por canaletas plásticas evitando las rutas a través de áreas públicas, tal como sugiere la norma TIA/EIA 569-B.
2. Los cables de energía debieran estar separados de los cables de comunicaciones como lo dictan apartes de las normas EIA/TIA 568-A y la NTC 2050, esto con el fin de evitar interferencia electromagnética.

3. Se deberán utilizar marcadores para identificar tanto los cables como los equipos claramente, esto con el fin de minimizar errores en la manipulación, como un empalme accidental de los cables de red equivocados. Apoyarse en la norma EIA/TIA 606-A.
4. Como norma de seguridad y administración de los puertos que no se estén usando dentro del Switch, estarán administrativamente abajo, con el fin de que no los puedan usar.

5. Los puertos del Switch que tengan equipos conectados, sin importar la Vlan a la que pertenezcan, tendrán configurado port-security sticky con un máximo de una dirección MAC, de manera que si se conecta otro equipo diferente, el puerto se caerá automáticamente.

6. Para la seguridad de cableado en sistemas sensibles o críticos se debieran considerar más controles como:

    - La instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación, acogidos a la norma EIA/TIA 569-B.
    - El acceso controlado a los paneles y cuartos de cableado con el fin de evitar manipulaciones malintencionadas o pérdidas de información, esto incluye el acceso al cuarto de telecomunicaciones de la oficina principal y el acceso al rack de pared de la oficina 2.

7. Al momento de la instalación del cable, se recomienda tener en cuenta el tendido de dos o más cables para cada estación, esto con el fin de prevenir el daño de un cable instalado y su posterior cambio por el dejado como repuesto.

8. Se recomienda adquirir o subcontratar analizadores de cable, con el fin de hacerle seguimiento a los mismos en el futuro. Es importante realizar un mantenimiento preventivo para evitar daños inesperados en la estructura del cable.

4.3.1.2 Gestión de las comunicaciones y operaciones

Objetivo: "Asegurar la operación correcta y segura de los medios de procesamiento de información". [53] Con el fin de asegurar una buena gestión en las comunicaciones y operaciones se deben preparar procedimientos documentados, tales como:

Prender y apagar los computadores, realizar copias de seguridad, mantenimiento de equipos, manejo de medios y cuarto de cómputo.

Se deberán detallar las instrucciones para la ejecución de cada trabajo así:

1. Documentar correctamente la red actual, con el fin de hacer mantenimientos preventivos, cambios o mejoras en el diseño.

2. Poseer documentación sobre contactos que hagan el debido soporte en caso de dificultades operacionales o técnicas inesperadas.

3. Procedimientos de reinicio y recuperación del sistema, en el evento de una falla de la red.

4. Mantener documentados los horarios de realización de copias de seguridad en los servidores.

5. Informar el manejo de formateo de los equipos de cómputo con el fin de que los trabajadores realicen copias de seguridad para no perder información confidencial de la empresa.

6. Estipular formalmente un día para realizar mantenimiento preventivo a las máquinas, con el fin de mantener un sistema saludable.

7. Los medios de respaldo se deben probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesario en caso de emergencia.

[53] Estándar Internacional ISO/IEC 17799 p. 62.

4.3.2.3 Gestión de la seguridad de la red

Objetivo: "Asegurar la protección de la información en redes y la protección de la infraestructura de soporte. Las redes debieran ser adecuadamente manejadas y controladas para poder proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red".[54]

1. Se deben implementar controles para asegurar la seguridad de la información dentro de la red y proteger los servicios de accesos no autorizados.

2. Se deben tratar los problemas de redes y cómputo diferenciadamente.

3. La documentación de la red se deberá almacenar de una manera segura

4. La documentación, los archivos confidenciales, que se mantienen en red, deben estar adecuadamente protegidos con contraseñas o con los controles pertinentes.

5. Cuando es importante la confidencialidad, las copias de respaldo deberán ser protegidas por medio de un plan de encriptación o codificación.

6. Las actividades de gestión de la red deben estar estrechamente coordinadas para optimizar el servicio y garantizar que los controles sean aplicados correctamente.

7. Con el fin de garantizar una red segura, se controlará el personal que navegue en la red empresarial y en Internet por medio de métodos como autenticación, control de contenido en páginas WEB y generación de informes de navegación.

8. De ser necesario, por órdenes de la gerencia, se tomaran medidas de restricción del tiempo de navegación en Internet, basados en estadísticas.

9. De ser necesario, por órdenes de la gerencia, se limitará o se suspenderá el ancho de banda a perfiles de usuarios que demuestren mal uso de los recursos de la red como descargas de videos, películas, warez, mp3, mp4.

[54] Ibid., p. 75.

4.3.2.4 Gestión de medios y de la información

Objetivo: Los medios se deben proteger y controlar físicamente. Asimismo deben existir procedimientos de gestión para los medios removibles.

1. Se debe hacer un inventario general de los archivos o los datos que se necesiten borrar, identificando los ítems que podrían requerir una eliminación segura. Los encargados de indicar que archivos pueden ser borrados, serán los que en previa reunión definan las directivas de la empresa.

2. Cuando sea posible se debiera tener un inventario (de no más de un año), de los archivos confidenciales eliminados, para mantener un registro de si el archivo se perdió o fue borrado.

3. Se deberán tomar medidas necesarias para el acceso de medios removibles a los computadores de la empresa, esto con el fin de evitar el espionaje industrial.

4. Cualquier medio removible deberá ser objeto de revisión de un antivirus para garantizar la salud del equipo de cómputo y de la red.

5. Se recomienda realizar un formato de ingreso y salida de medios extraíbles con el fin de ejercer control sobre el movimiento de dichos elementos y la información de la empresa, evitando así el espionaje empresarial.

6. Cualquier medio removible (memoria USB, Discos externos) podrá ser objeto de revisión por parte del departamento de sistemas y el personal de seguridad privada de la empresa, si el caso lo requiere.
7. Mantener la distribución de información por medio de dispositivos extraíbles en el punto mínimo posible.

8. De ser requerido por la gerencia, los correos electrónicos que se envíen desde el correo corporativo, deberán ser enviados como copia oculta a la gerencia para garantizar la confidencialidad de la información que saldrá.

9. De no ser acatado el numeral anterior, la gerencia cambiara las características del cuadro de CCO (Con copia oculta), pasando de escritura

y lectura a solo lectura, imponiendo ahí la dirección de correo de la gerencia.

"Recomendación: estos procedimientos se aplican a la información en documentos; sistemas de cómputo; redes; computación móvil; comunicaciones móviles; comunicaciones vía correo, correo de voz y voz en general; multimedia; servicios/medios postales; uso de maquinas de fax y cualquier otro ítem confidencial; por ejemplo cheques en blanco y facturas".[55]

4.3.2.5 Control de acceso

Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a la red.

1. Identificar toda la información relacionada con las aplicaciones, la red y los riesgos que enfrenta la información.
2. Los perfiles de acceso de usuario estándar para los puestos de trabajo comunes.

3. Cada trabajador sin excepción deberá tener un nombre de acceso y una contraseña para poder acceder a los equipos y a la navegación a Internet, dichos datos quedaran grabados en el servidor de administración y gestión de la red.

4. La empresa requerirá una autorización formal para las solicitudes de acceso.

5. La empresa deberá hacer una revisión periódica de los controles de acceso.

6. Con base en estudios previos, la empresa podrá revocar los derechos de acceso a los servicios o a la red.

4.3.2.6 Control de acceso del usuario

Objetivo: Se debieran establecer procedimientos formales para controlar la asignación de los derechos de acceso a la red y a las carpetas compartidas. Cuando sea apropiado, se debiera prestar atención especial a la necesidad de

[55] Ibid., p. 78.

controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles de la red.

1. “Utilizar IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones; sólo se debiera permitir el uso de IDs grupales cuando son necesarios por razones comerciales u operacionales, y debieran ser aprobados y documentados”.[56]

2. Los ID de usuario tendrán el patrón nombre.apellido a menos de que exista una redundancia entre algunos nombres.

3. “Proporcionar a los usuarios un enunciado escrito de sus derechos de acceso”.[57] Se recomienda realizar una reunión en la que por medio de acta, se comuniquen los derechos de acceso a los empleados, debido a que no se pueden cambiar los contratos ya firmados.
4. “Requerir a los usuarios que firmen los enunciados indicando que entienden las condiciones de acceso”.[58]

5. Mantener un registro formal de todas las personas registradas para utilizar la red y los servicios.

6. Eliminar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto o trabajo han dejado la organización.

4.3.2.7 Gestión de las claves secretas de los usuarios

Objetivo: Se deberán tener parámetros para la asignación, el manejo y el cambio de claves grupales y personales, asimismo se deberá hacer énfasis en la confidencialidad de las mismas.

1. "Cuando se requiere que los usuarios mantengan sus propias claves secretas, inicialmente se les debiera proporcionar una clave secreta temporal segura, la cual están obligados a cambiar inmediatamente”.[59]

2. Se recomienda a la gerencia, cambiar las claves por lo menos una (1) vez al mes o según considere conveniente.

[56] Ibid., p. 96
[57] Ibid., p. 96
[58] Ibid., p. 97
[59] Ibid., p. 98

3. El patrón de construcción de una contraseña deberá ser no menor de cinco (5) dígitos, ni mayor de diez (10) dígitos, los caracteres a utilizar serán números, letras (Mayúsculas o minúsculas) y caracteres especiales, exceptuando el espacio.

4. “Establecer procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta nueva, sustituta o temporal”.[60]

5. La primer clave o contraseñas será obtenida por un generador de contraseñas, de ahí en adelante el usuario podrá cambiar la contraseña por la que él desee, manteniendo el patrón de construcción de las mismas.

6. “Las claves secretas temporales debieran ser únicas para la persona y no debieran de ser fáciles de adivinar”.[61] Para esto se usara el generador de contraseñas.
7. El generador de contraseñas será administrado por el departamento de sistemas.

8. “Las claves secretas nunca debieran ser almacenadas en los sistemas de cómputo de una forma desprotegida.

9. Se debiera chequear la asignación de privilegios a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados”.[62]

4.2.3.8 Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no autorizados, para impedir poner en riesgo la integridad de la red, los servicios que presta, la información confidencial y los equipos de cómputo.

1. El departamento de sistemas es el único departamento encargado de las funciones de los equipos de cómputo y de los equipos activos de la red, por lo tanto ellos son los únicos que tendrán acceso a la sala de telecomunicaciones.

[60] Ibid., p. 98
[61] Ibid., p. 98
[62] Ibid., p. 99

2. La oficina dispone de una recepción por lo tanto es restringido el acceso a personal no autorizado, para poder ingresar deberá existir autorización de la gerencia.
3. Los usuarios debieran estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

4. El usuario deberá respetar la norma de seguridad que presta el servidor proxy. La única manera que deberá utilizar para salir a Internet dentro de la empresa será haciendo uso de este servidor.

5. El usuario deberá respetar el control de contenido que el servidor haga a las páginas WEB que visitan. Por ningún motivo deberá tratar de ingresar a páginas indebidas sin la respectiva autorización.

6. El usuario deberá cerrar la sesión en el equipo en el que trabaja cada vez que se ausente del puesto de trabajo, a no ser que tenga un mecanismo de cierre apropiado, por ejemplo un protector de pantalla asegurado por clave.

7. Si el usuario se encuentra prestando servicios de mantenimiento en un equipo diferente al suyo, deberá terminar la sesión apenas acabe el trabajo, de manera que la cuenta de administrador del equipo no quede abierta, evitando riesgos o pérdidas de información.

8. El usuario deberá cuidar su cable de red, ya que el port-security en el Switch estará configurado para admitir una sola dirección MAC, de manera que si conecta el cable equivocado esto generará la caída del puerto en el Switch.

9. Se informará a los empleados acerca de las responsabilidades que tienen para no comprometer a le empresa en casos de difamación, hostigamiento, suplantación, reenvió de correos electrónicos y compras no autorizadas.

10. No dejar información confidencial o critica en medios impresos; por ejemplo, copiadoras, impresoras y maquinas de fax; ya que el personal no autorizado puede tener acceso a ellas.[63]

[63] Ibid., p. 81 núm j.

4.2.3.9 Uso de claves secretas

Objetivo: El usuario de la red deberá seguir buenas prácticas de seguridad en la selección y uso de las claves secretas.

1. Mantener confidenciales las claves secretas.

2. Evitar mantener un registro (por ejemplo, papel, archivo en software o dispositivo manual) de las claves secretas, a no ser que este se pueda mantener almacenado de manera segura y el método de almacenaje haya sido aprobado.

3. Cambio de claves secretas cuando haya el menor indicio de un posible peligro en el sistema o la clave secreta.

4. Seleccionar claves secretas de calidad con el largo mínimo suficiente que sean:

    a) Fáciles de recordar

    b) No se basen en nada que otro pueda adivinar fácilmente u obtener utilizando la información relacionada con la persona; por ejemplo, nombres, números telefónicos y fechas de nacimiento, entre otros.

    c) No sean vulnerables a los ataques de diccionarios (es decir, que no consista de palabras incluidas en los diccionarios).

    d) En lo posible conservar el patrón de números, letras mayúsculas y minúsculas y caracteres especiales exceptuando el espacio.

5. Cambiar la clave temporal en el primer ingreso

6. No compartir las claves secretas individuales.

4.3.2.10 Control de acceso a la red

Objetivo: Evitar el acceso no autorizado a los servicios de red.

1. El control del acceso a la red es obligatorio.

2. La autenticación para acceder a Internet es obligatoria.

3. Los mecanismos de autenticación deben ser apropiados para el usuario y el equipo.

4. La restricción del tiempo de navegación en páginas de sano entretenimiento, se hará en horario laboral comprendido de las 08:00am hasta las 12:00m y de la 01:00pm hasta las 05:00pm, de esta manera se podrá hacer uso de la red para efectos no corporativos a horas diferentes a las anteriormente indicadas.

5. Deberán tomarse medidas pertinentes para hacer uso de conexiones remotas, el uso de VPN's, canales seguros, o https deberá ser la opción más apropiada.

6. El acceso a la configuración de los dispositivos activos de la red, deberá estar restringida por contraseñas y tendrá gran injerencia sobre el diseño del cuarto de telecomunicaciones.

7. El acceso remoto a los dispositivos activos de la red deberá estar bloqueado por medio de contraseñas, que solo deberán poseer los encargados.

8. Sólo se mantendrán abiertos los puertos estrictamente necesarios, esto con el fin de dar seguridad a la red interna en el router de borde.

9. Se creará una lista de acceso reflexiva (Stablished) con el fin de denegar el tráfico IP en sesiones que se originan fuera de la red.

4.3.2.11 Políticas sobre el uso de los servicios de la red

Objetivo: Los usuarios solo deberán tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

Los usuarios deberán hacer uso respetuoso de los recursos de red, con el fin de no sobrecargar el tráfico en la misma.

1. De ser necesario se asignaran anchos de banda dependiendo de los perfiles de usuario comparados con las necesidades de la empresa.

2. La gerencia deberá determinar si la asignación de ancho de banda se hace por dependencias o perfiles de usuarios.

3. El acceso a las conexiones de red y a los servicios, necesitará de autenticación.

4. Se crearan listas de acceso (ACL), con el fin de permitir o denegar servicios en la red, según los requerimientos de la gerencia.

4.3.2.12 Identificación del equipo en la red

Objetivo: La identificación automática del equipo se debiera considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.

1. Todos los equipos deberán tener un único nombre que los identifique en la red, esto será un factor importante, cuando se necesite que la comunicación solo sea iniciada desde una ubicación o equipo especifico.

2. Los nombres en la red podrán ser de utilidad para indicar si un equipo está autorizado a conectarse a una red o a una subred.

3. En algunos casos el nombre del equipo podrá ser asociado a una cuenta de usuario, esto con el fin de hacer seguimiento con el informe de navegación.

4. Dentro del diseño deberá tenerse en cuenta, realizar la respectiva documentación acerca del equipo de cómputo, los cables de datos conectados a él, la dirección MAC, el usuario que lo utiliza, la red a la que pertenece, esto podría ser útil cuando se haga mantenimiento o se necesite identificar qué equipo está caído en la red.

4.3.2.13 Control de conexión a la red

Objetivo: Los derechos de acceso a la red de los usuarios se debieran mantener y actualizar conforme lo requiera la política de control de acceso.

1. Se puede restringir la capacidad de conexión de los usuarios a través de gateways de la red que filtran tráfico por medio de listas de acceso. Por ejemplo, transferencias de archivos o acceso a las aplicaciones.

2. Se debiera considerar vincular los derechos de acceso a la red con ciertos días u horas.

3. Como control de acceso a la red, será obligatorio autenticarse con un usuario y una contraseña validos para la red.

4. Las conexiones remotas a la red deberán estar reglamentadas por la gerencia de la empresa, indicando los parámetros de conexión.

4.3.2.14 Control del Routing de la red

Objetivo: "Se debieran implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales".[64]

1. Se emplearán tecnologías de proxy y traducción de direcciones para el enrutamiento de la red.

2. Se deberán tener en cuenta las fortalezas y las debilidades de este tipo de implementaciones.

3. Los requerimientos para el control del routing de la red se debieran basar en las políticas de control de acceso.

4. En la documentación del diseño deberán quedar indicados todos los protocolos de enrutamiento que usa el diseño.

4.3.2.15 Monitoreo

Objetivo: Supervisar la información que se obtiene de la gestión, con el fin de organizar, cambiar o mejorar la gestión en la red empresarial.

1. La frecuencia con que se revisan los resultados de las actividades de monitoreo dependerá de los riesgos involucrados. Los factores de riesgo a considerarse incluyen:

   a) Grado crítico de los procesos de aplicación

   b) Valor, sensibilidad y grado crítico de la información involucrada

   c) Antecedentes de infiltración y mal uso del sistema, y la frecuencia con la que se explotan las vulnerabilidades

[64] Ibid., p. 108.

d) Extensión de la interconexión del sistema (particularmente las redespúblicas)

e) Desactivación del medio de registro

f) Otra información

2. La gerencia podrá exigir informes de las páginas WEB visitadas, semanal o mensualmente, según lo requiera.

3. Los informes de las páginas WEB visitadas podrán ser tenidos en cuenta por la gerencia para emitir memorandos o llamados de atención.

4. “Es necesaria la utilización de procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados”.[65]

5. Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a la red. Se debieran establecer procedimientos formales para controlar la asignación de los derechos de acceso a la red y a las carpetas compartidas. Cuando sea apropiado, se debiera prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles de la red.

6. Hacer uso de SNMP con el fin de gestionar la red.

Como ayuda y soporte para las políticas de gestión se instalará, se configurará y se adicionará al diseño un servidor cuyo fin será el de prestar servicios que ayuden a ejercer control sobre la red y los grupos de usuarios asociados a ella, a continuación se hará una explicación de lo que se desarrollara para APP MACHINES Ltda.

El montaje e implementación del servidor en sistema operativo Linux Centos 5, no se ha podido desarrollar en primer lugar a que la empresa APP MACHINES no incluyo el equipo de cómputo destinado para ser configurado, en segundo lugar, la parte económica es un factor importante pues la citada empresa, no tiene pensado en este momento ejecutar el diseño de red desarrollado en este proyecto, debido a esto la empresa puede considerar un gasto innecesario el adquirir un equipo de cómputo que no entrará a operar apenas se haga la respectiva configuración. Si

[65] Ibid., p. 91

APP MACHINES decide implementar el diseño, seguramente la adquisición del equipo se hará y posteriormente se configurará e instalará.

Los requerimientos del cliente incluyen la insatalacion de el paquete SAMM y UTSIM y los requerimeintos minimos de maquina son:

Requisitos Servidor
Sistema Operativo Linux distribuciones Redhat, Sistema operativo OpenSolaris, Sistema Operativo Microsoft Windows 2000 Server with Service Pack (SP) 4 or later; Windows 2000 Professional with SP 4 or later; Windows XP with SP 2 or later; Windows Server 2003 Standard Edition, Enterprise Edition, or Datacenter Edition with SP 1 or later; Windows Small Business Server 2003 with SP 1 or later; Microsoft Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition with SP 1 or later; Windows XP Professional x64 Edition or later running in Windows on Windows
Procesador Pentium III 1.8 GHz (Mínimo)
Espacio disponible en disco 10Gb Mínimo, Recomendado 20Gb o superior
Memoria RAM Mínimo 512Mb (Recomendado 1Gb)
Monitor SVGA Resolución Mínima 800X600 (1024 X 768 Recomendado)
Tarjeta de video Mínimo 8Mb
Mouse Requerido
Tarjeta de Red Mínimo 10Mbps (recomendado 100Mbps).
Unidad de CD ROM Necesario para la Instalación

Requisitos Clientes
Sistema Operativo Linux distribuciones Redhat, Sistema operativo OpenSolaris, Sistema Operativo Win 98, XP home, XP professional, 2000 professional, Server. Win NT4 sp6.
Procesador Pentium III 1.8 GHz (Mínimo)
Espacio disponible en disco 1 Gb mínimo
Memoria RAM Mínimo 256RAM (512 Recomendado)
Monitor SVGA Resolución Mínima 800X600 (1024 X 768 Recomendado)
Tarjeta de video Mínimo 8 Mb
Mouse Requerido
Tarjeta de Red Mínimo 10Mbps (recomendado 100Mbps).
Unidad de CD ROM Necesario para la Instalación

VERSION SAMM WEB.

Requisitos Servidor

Sistema Operativo Linux distribuciones Redhat, Sistema operativo OpenSolaris, Sistema Operativo Microsoft Windows 2000 Server with Service Pack (SP) 4 or later; Windows XP Professional with SP 2 or later; Windows Server 2003 Standard Edition, Enterprise Edition, or Datacenter Edition with SP 1 or later; Windows Small Business Server 2003 with SP 1 or later; Microsoft Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, or Datacenter x64 Edition with SP 1 or later; Windows XP Professional x64 Edition or later running in Windows on Windows.
Servidor Web Internet Information Services 5.0 o superior
Procesador Pentium IV 1.8 GHz (Mínimo). Recomendado varios núcleos.
Espacio disponible en disco 2Gb Mínimo. Recomendado 10Gb o superior
Memoria RAM Mínimo 2Gb. Recomendado 4Gb o superior.
Velocidad de Red 100Mbps o superior.
Conexión a Internet Necesaria para la Instalación

Requisitos Clientes
Explorador de Internet
(en orden de recomendación) Firefox 3.0+, Google Chrome 2.0+, Internet Explorer 7.0+, Safari 4.0+
Procesador Pentium IV 1.5 GHz (Mínimo)
Memoria RAM Mínimo 1 GB
Monitor Resolución Mínima 1024 X 768
Mouse Requerido
Velocidad de Red Mínimo 10Mbps (recomendado 100Mbps).

REQUISITOS MÍNIMOS PARA UTSIM

the minumum requirement for UTsim is a pentium 2 runing windows 3.2. However it will run on windows XP or windows Vista or windows 7 or Linux.

- **Requerimientos del sistema**

Se debe contar con la suficiente cantidad en memoria y un microprocesador en buen estado. Con casi cualquier distribución comercial de Linux. El ambiente grafico necesitara al menos 192 MB RAM, y 650-800 MB de espacio en disco duro

para la instalación mínima. Para contar con la menor cantidad de aplicaciones prácticas, se requieren al menos 800 MB adicionales de espacio en disco duro repartido en al menos dos particiones. Se recomienda un microprocesador 80586 (Pentium o equivalente) a 200MHz. Sin ambiente grafico, como es el ambiente de un servidor, o bien solo aplicaciones para modo texto, 64 MB RAM y un microprocesador 80586 a 100MHz serán suficientes.

El servidor de video puede funcionar con sólo 64 MB RAM; pero su desempeño será muy lento. Algunas aplicaciones para modo grafico necesitan escalar 64 MB, 128 MB, 256 MB de RAM adicional. El mínimo recomendado para utilizar GNOME 2.x es de 192 MB RAM; se recomiendan 256 MB. El óptimo es de 512 MB RAM.

Si desea instalar Linux en una computadora personal con las suficientes aplicaciones como para ser totalmente funcional y productivo y contar con el espacio necesario para instalar herramientas de oficina (OpenOffice.org), se recomienda contar con al menos 2 GB de espacio, al menos 256 MB RAM y un microprocesador AMD K6, K6-II, K6-III, Athlon, Duron, Pentium, Pentium MMX, Pentium II, Pentium III, Pentium 4 o Cyrix MII a cuando menos 300MHZ o más.

- **Servicio de páginas Web (Apache)**

Un servidor web es un programa que implementa el *protocolo HTTP* (*hypertext transfer protocol*). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

El servidor web es un programa que se ejecuta continuamente en el servidor manteniéndose a la espera de peticiones por parte de un cliente (un navegador de Internet) y que responde a estas peticiones adecuadamente, mediante una *página web* que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error.

Se dispondrá de este servidor para insertar una página o un sistema de información Interno para usar vía Web, igualmente si la gerencia lo desea podrá insertar la página Web de la empresa al servidor evitando el pago de hospedaje por la misma, como la página se encuentra dentro de la compañía esto genera una sola solicitud al servidor para acceder a ella y no será necesario desplazarse hasta Internet para poder realizar una consulta. La empresa considera importante la utilización del servidor debido a las razones expuestas anteriormente.

- **Servicio Proxy Cache (Squid y Squid-Guard)**

El servidor proxy es un intermediario entre los equipos de una red de área local e Internet y actúa como "representante" de una aplicación efectuando solicitudes en Internet. De esta manera, cuando un usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un servidor proxy, la aplicación primero se conecta con el servidor proxy y le da la solicitud a éste. El servidor proxy se conecta entonces al servidor externo al que la aplicación del cliente desea conexión y le envía la solicitud., para que posteriormente, el servidor externo le envíe la respuesta al proxy y este a su vez la envía a la aplicación del cliente.

El proxy también permite mejorar la velocidad de acceso a Internet almacenado localmente las páginas más consultadas por los usuarios de la empresa, evitando las conexiones directas con los servidores remotos, así como la utilización innecesaria de ancho de banda.

Una vez los usuarios hallan configurado su navegador web para dirigir sus accesos al servicio proxy-caché, el servidor proxy-caché se encarga de proporcionarle la página pedida bien obteniéndola de su caché o accediendo al documento original; al dar servicio a muchos usuarios la caché contendrá muchos documentos beneficiándose toda la organización de ello. Se evitan transferencias innecesarias y con ello se aumenta la velocidad en la carga de las páginas, ya que no es necesario pedir una página cuando ya esté almacenada en la caché (porque otro la había pedido antes).

Squid y Squid Guard, son los servidores que se van a utilizar realizar los servicios que va a manejar el sistema operativo Linux Centos 5, lo más importante es que tanto el sistema operativo como los paquetes son de licenciamiento libre, igualmente siendo confiables y robustos. Los servicios que tendrá inmerso el servidor son:

- **Autenticación**

Debido a que el Proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, se utiliza para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña para navegar en Internet.

- **Control de Contenido o filtrado**

Al utilizar un servidor proxy, las conexiones de la red interna pueden rastrearse al crear *registros de actividad (logs)* para guardar sistemáticamente las peticiones de los usuarios cuando solicitan conexiones a Internet.

Gracias a esto, las conexiones de Internet pueden filtrarse al analizar tanto las solicitudes del cliente como las respuestas del servidor. El filtrado que se realiza comparando la solicitud del cliente con una lista de solicitudes autorizadas se denomina *lista blanca*; y el filtrado que se realiza con una lista de sitios prohibidos se denomina *lista negra*. Finalmente, el análisis de las respuestas del servidor que cumplen con una lista de criterios (como palabras clave) se denomina *filtrado de contenido*.

Más concretamente el funcionamiento consiste en denegar el acceso a nombres de dominio o direcciones Web que contengan patrones en común. Ejemplos: Porno, Violencia, napster, sex, porn, xxx, adult, warez, entre otros.

Así por ejemplo, si un usuario intenta ingresar a una página cuyo contenido esté relacionado con los patrones antes mencionados, se denegará el acceso a dicha página.

- **Control de Ancho de Banda de descargas**

Con el control de ancho de banda se puede manejar de una manera más eficiente la tasa de transferencia de cada uno de los usuarios, de esta manera evitar que un usuario use todo el ancho de banda dejando a los demás usuarios con una tasa de transferencia lenta y deficiente.

- **Generador de informes de análisis de navegación**

Esta herramienta permite saber dónde han estado navegando los usuarios en Internet. El poder de esta herramienta es increíble, pudiendo saber qué usuarios accedieron a qué sitios, a qué horas, cuantos bytes han sido descargados, relación de sitios denegados, errores de autentificación...entre otros.

Esta función es muy importante, principalmente para las empresas que quieren tener un control de accesos y ancho de banda de acceso a Internet.

Los reportes son mostrados en formato HTML, esto hace que su visualización sea más cómoda y que se pueda acceder a la información desde cualquier otro computador y no necesariamente desde el mismo servidor, la información brindada, es presentada por un rango de fechas, en cada una de ellas se visualiza la transferencia de Bytes que hubo en el periodo.

Como ejemplo, en la Figura 38. Ejemplo de informe de Navegación por usuario. P.133, se puede observar el informe de navegación del usuario cpolo dentro de las fechas de 15 de septiembre al 17 de septiembre del 2009.

Figura 38. Ejemplo de informe de Navegación por usuario.

Periodo:2009Sep14-2009Sep17
Usuario: cpolo
Clasificado por: BYTES, reverse
Usuario reporte

Sitio Accedido	Conexión	Bytes	% Bytes	Entrada-Cache-Salida		Tiempo Utilizado	Milisec	% Hora
mail.appmachines.com.443	66	3,27M	31.52%	0.04%	99.95%	00:04:29	269,172	16.14%
www.portafolio.com.co	108	1,70M	16.44%	0.00%	100.00%	00:00:30	30,918	1.85%
www.xe.com	454	1,51M	14.50%	7.56%	92.44%	00:02:55	175,249	10.51%
www.appmachines.com	29	687,89K	6.63%	32.76%	67.24%	00:00:21	21,915	1.31%
www.facebook.com	13	491,97K	4.74%	0.24%	99.76%	00:00:20	20,329	1.22%
www.telmex.com	37	485,00K	4.67%	52.80%	47.14%	00:00:17	17,783	1.07%
www.labomed.com	33	348,61K	3.35%	9.89%	90.11%	00:00:25	25,208	1.51%
www.youtube.com	49	212,38K	2.05%	1.01%	98.99%	00:00:08	8,501	0.51%
www.eltiempo.com.co	31	201,94K	1.95%	0.00%	100.00%	00:00:28	28,470	1.71%

- **Restricción del tiempo de navegación**

Por medio del Proxy también se puede tener el control de tiempo de navegación, restringiendo el horario en el cual determinados usuarios en la red interna pueden navegar en Internet.

Ejemplo:

Los usuarios Administrador y Gerente pueden navegar en el Horario: lunes, martes, miércoles, jueves y viernes de 10:00-15:00

La restricción del tiempo de navegación se aplica, bien sea por usuario, por grupo de usuarios, por dirección IP o por grupo de direcciones IP.

La aplicación de las políticas de gestión propuestas en este proyecto, sumado a la instalación del servidor deben ayudar en gran medida a mantener una red saludable, con un alto grado de disponibilidad, asegurando la calidad de los servicios que transitan por la red, de manera que el cliente pueda recibir el diseño a satisfacción.

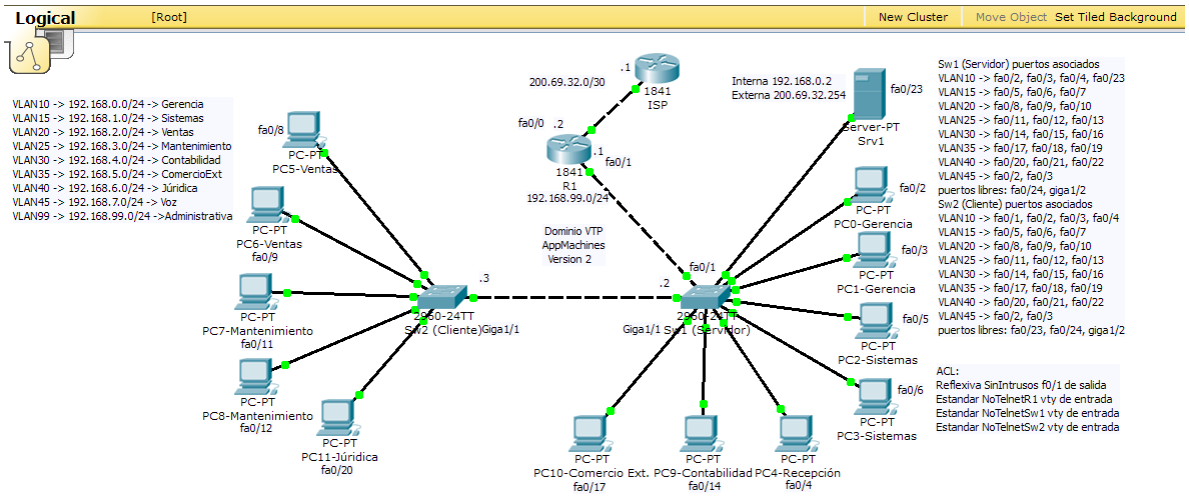
4.4 VALIDAR EL DISEÑO PROPUESTO MEDIANTE UNA SIMULACIÓN

Para realizar la simulación se va a utilizar el programa Packet Tracer 5.2 de la academia de Networking de Cisco. Dicha simulación tiene como fin mostrar pruebas de conectividad entre los diferentes equipos en las VLAN, mostrar las tablas de enrutamiento en los equipos, la creación de las VLAN, el paso de las VLAN a través de un dominio VTP, la aplicación del Router como servidor DHCP, la aplicación de ACL, la aplicación de la seguridad en los puertos de los Switches y la aplicación del servicio de NAT para navegar en Internet.

La ventaja de utilizar Packet Tracer es que utiliza equipos Cisco que fueron tenidos en cuenta para el diseño, por lo cual trata de simular lo más real posible la Red planteada para APP MACHINES.

4.4.1 Escenario 1. La simulación incluye el modem o Router que brinda el ISP, llamado ISP, el router de borde de la empresa llamado R1, dos Switches, Sw1(servidor) y Sw2(Cliente), doce (12) equipos de cómputo y el servidor Srv1, tal como lo puede apreciar en la Figura 39. Topología Simulación Packet Tracer 5.2 (1)

Figura 39. Topología Simulación Packet Tracer 5.2 (1)

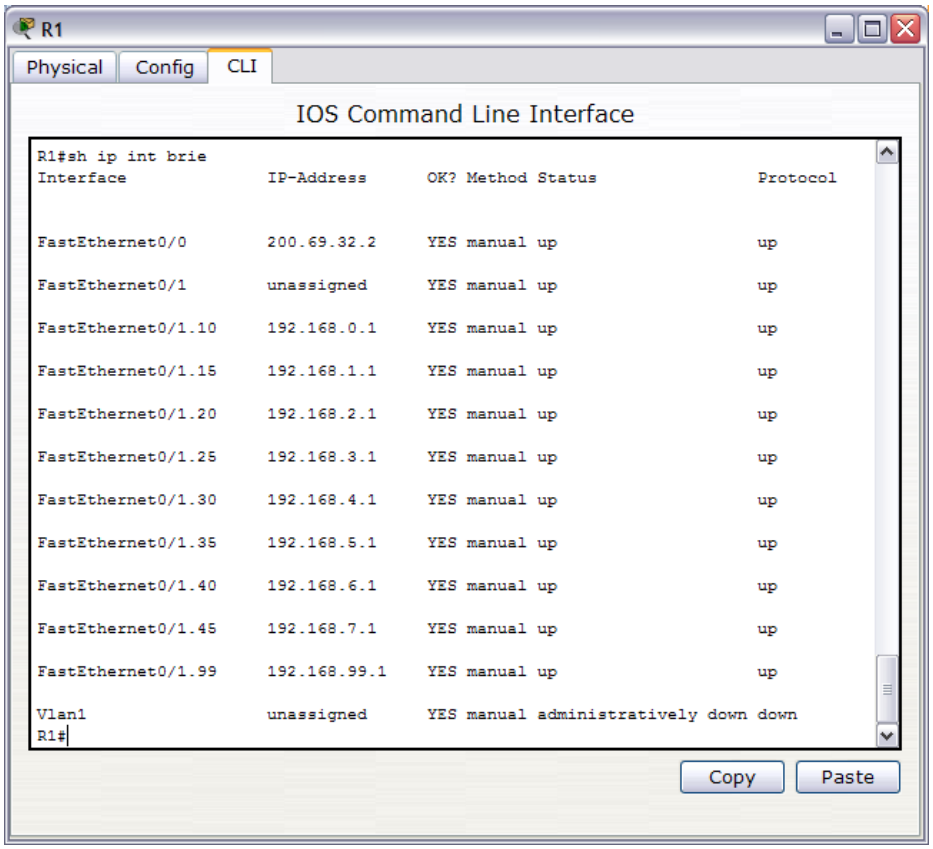


Como anexo al documento se encuentran los comandos de configuración de ISP, R1, Sw1 y Sw2.

Dentro de la simulación Podemos comprobar:

4.4.1.1 Estado de las interfaces en R1. Por medio del comando “Show ip interfaces brief” se puede verificar el estado de las interfaces del dispositivo, se encuentra un resumen que contiene el nombre de las interfaces, la dirección IP y el estado de las mismas. En la figura 40. Estado de las interfaces en R1. P. 135, se observa que R1 tiene dos interfaces físicas, Fa0/0 y Fa0/1, Fa0/0 está conectada hacia ISP, tiene su dirección IP configurada y está arriba por lo que funciona correctamente. La Interfaz Fa0/1 es el enlace troncal hacia Sw1 por lo que no tiene dirección IP pero debe estar arriba, las subinterfaces se crean con respecto a las VLAN creadas en los Switches, cada subinterfaz tiene una dirección IP valida en el rango de cada subred y se encuentran arriba y funcionando correctamente.

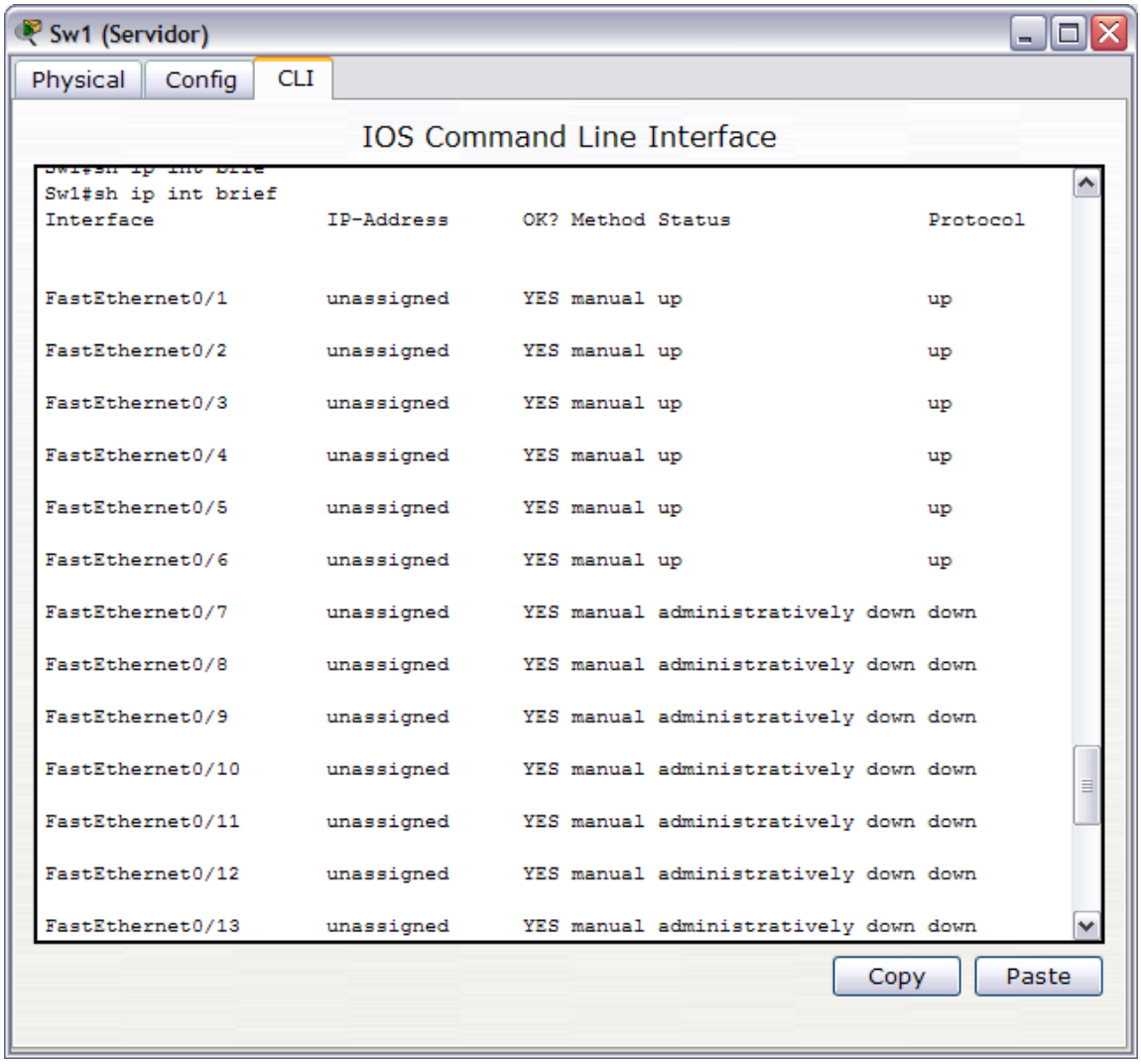
Figura 40. Estado de las interfaces en R1



4.4.1.2 Estado de las interfaces en Sw1. En las figuras 41 y 42, se observa el estado de las interfaces físicas de Sw1, las interfaces que tiene equipos de cómputo conectadas se encuentran arriba, las interfaces que no, se encuentran

administrativamente abajo, cabe aclarar que los puertos son asignados a las VLAN dependiendo de los requerimientos del cliente, pero los puertos Fa0/24 y Giga1/2 se encuentran apagados y sin asignación hacia una VLAN en especial porque no se van a usar inicialmente en el diseño.

Figura 41. Estado de las interfaces en Sw1



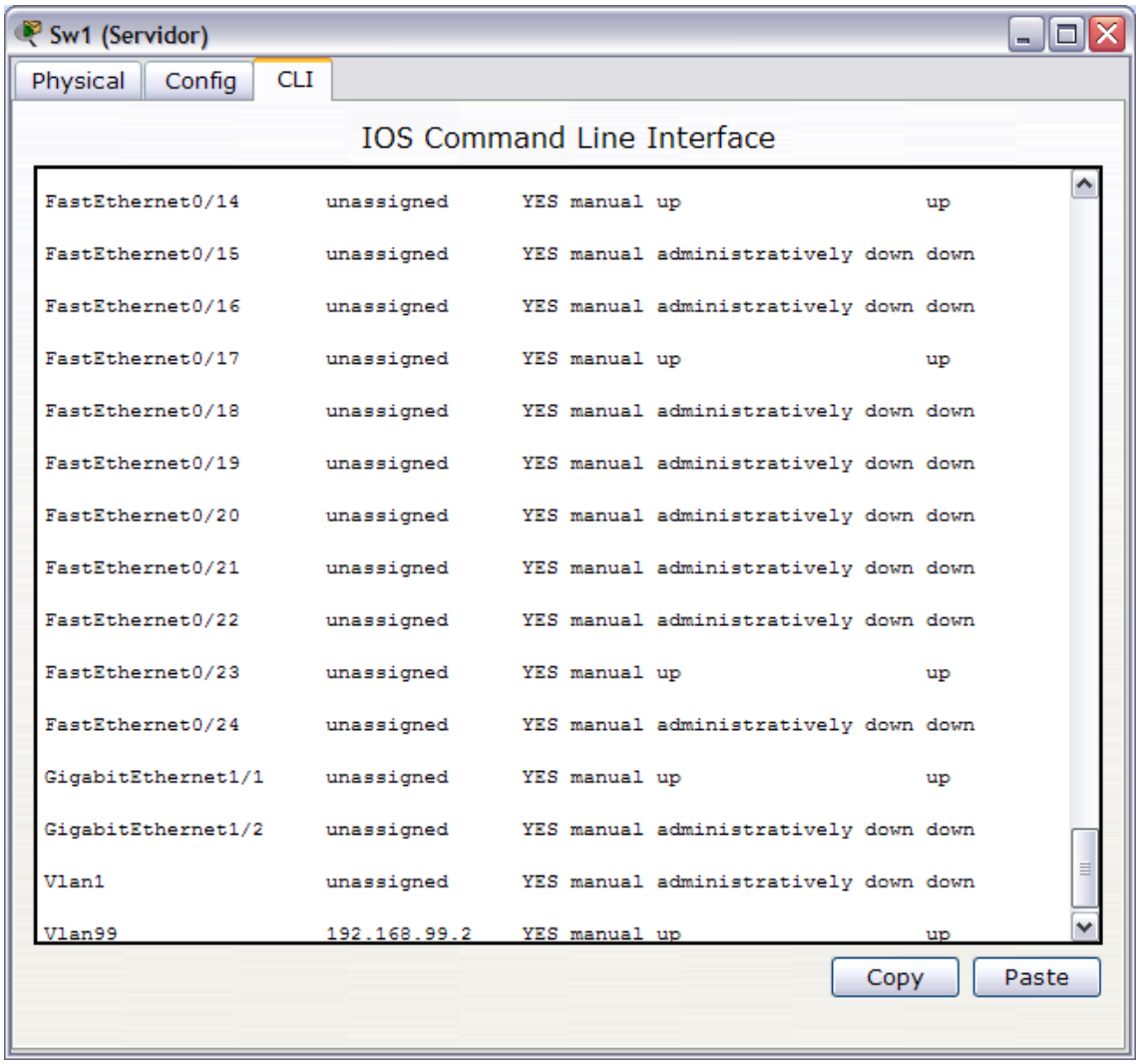


Figura 42. Estado de las interfaces en Sw1

4.4.1.3 Estado de las interfaces en Sw2. En las figuras 43 y 44, se observa el estado de las interfaces físicas de Sw2, las interfaces que tiene equipos de cómputo conectadas se encuentran arriba, las interfaces que no, se encuentran administrativamente abajo, cabe aclarar que los puertos son asignados a las VLAN dependiendo de los requerimientos del cliente, pero los puertos Fa0/23, Fa0/24 y Giga1/2 se encuentran apagados y sin asignación hacia una VLAN en especial porque no se van a usar inicialmente en el diseño.

Figura 43. Estado de las interfaces en Sw2

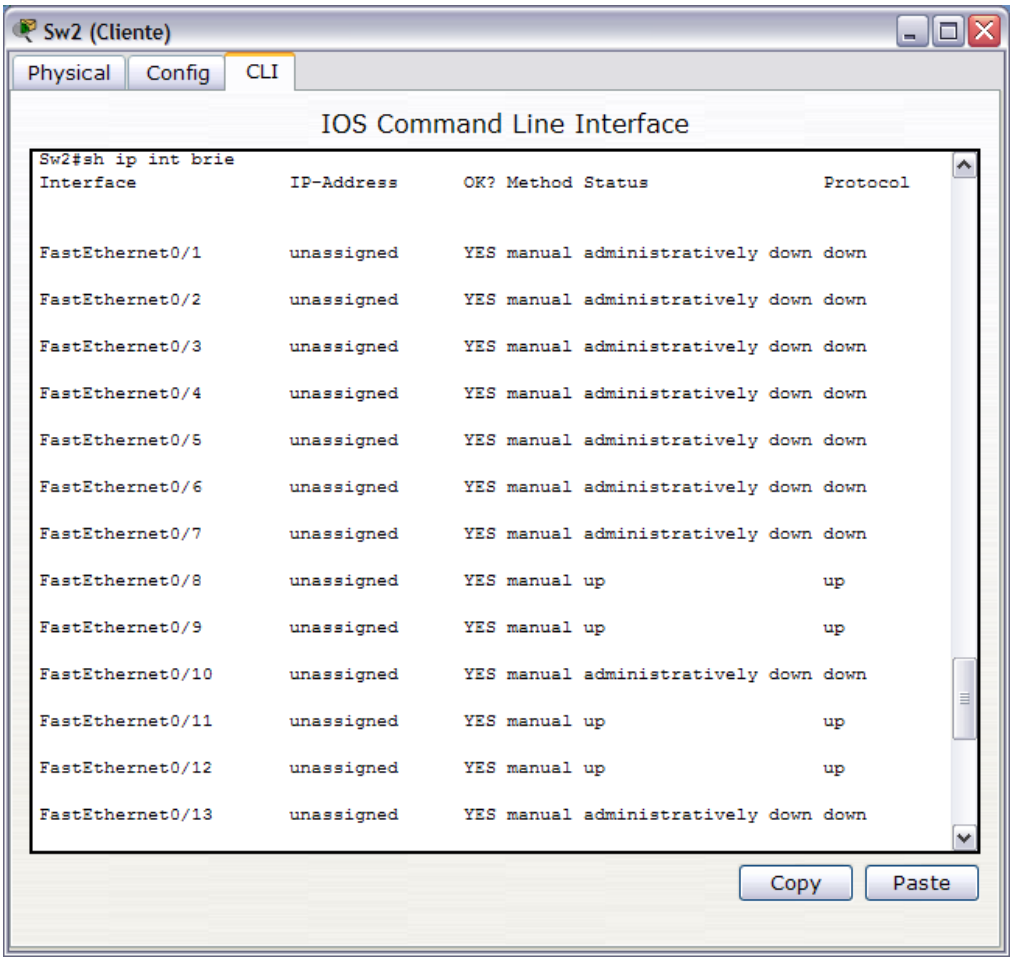
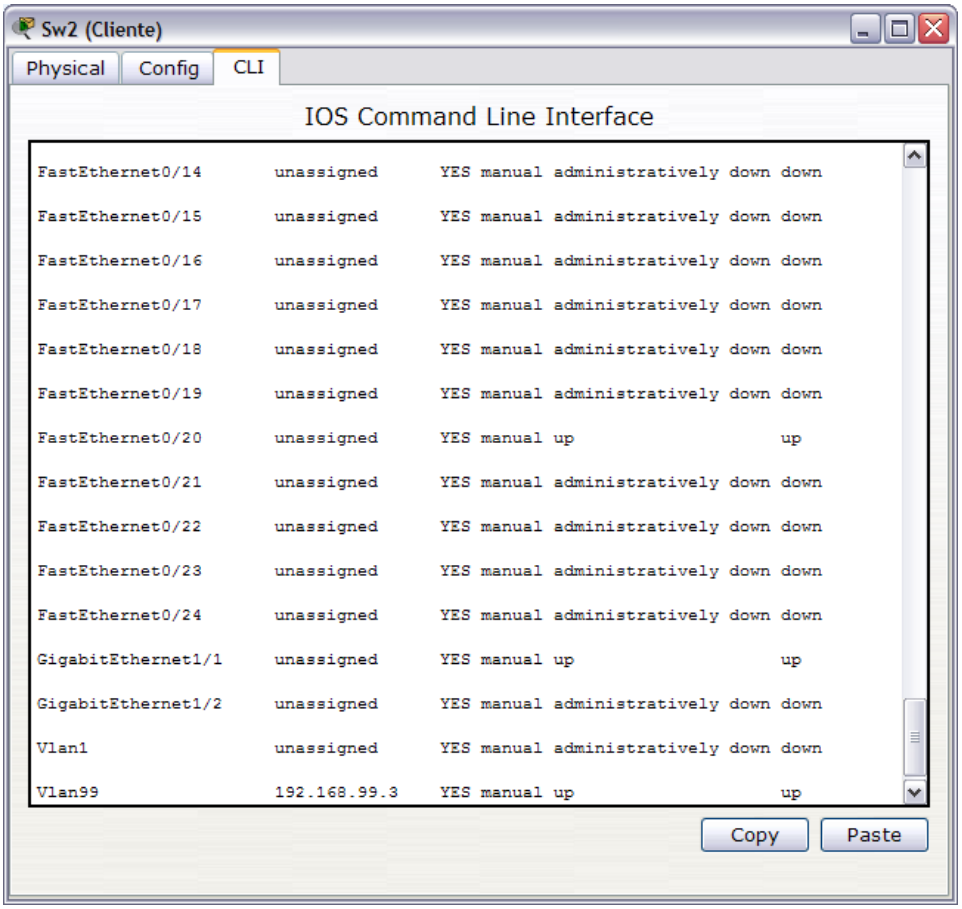


Figura 44. Estado de las interfaces en Sw2 (Continuación)



4.4.1.4 Estado de VTP en Sw1 (Servidor). VTP (Protocolo de enlace troncal de VLAN) permite configurar un Switch en modo servidor para que propague la información de las VLAN, para que esto se cumpla hay tres factores importantes, el primero que deben tener el mismo nombre de dominio VTP, el segundo que tengan la misma contraseña VTP y el tercero es que cuando se conecte el dominio, El cliente debe tener un número de revisión menor o igual que el servidor para que se establezca el enlace troncal y la información acerca de las VLAN se transmita correctamente. En las figuras 45 y 46 se puede observar, la versión de VTP, el número de VLAN existentes, el modo de operación VTP (servidor, cliente, Transparente), el nombre del dominio (APP MACHINES), y el número de revisión el cual es 19 en ambos Switches.

Figura 45. Estado de VTP en Sw1 (Servidor)

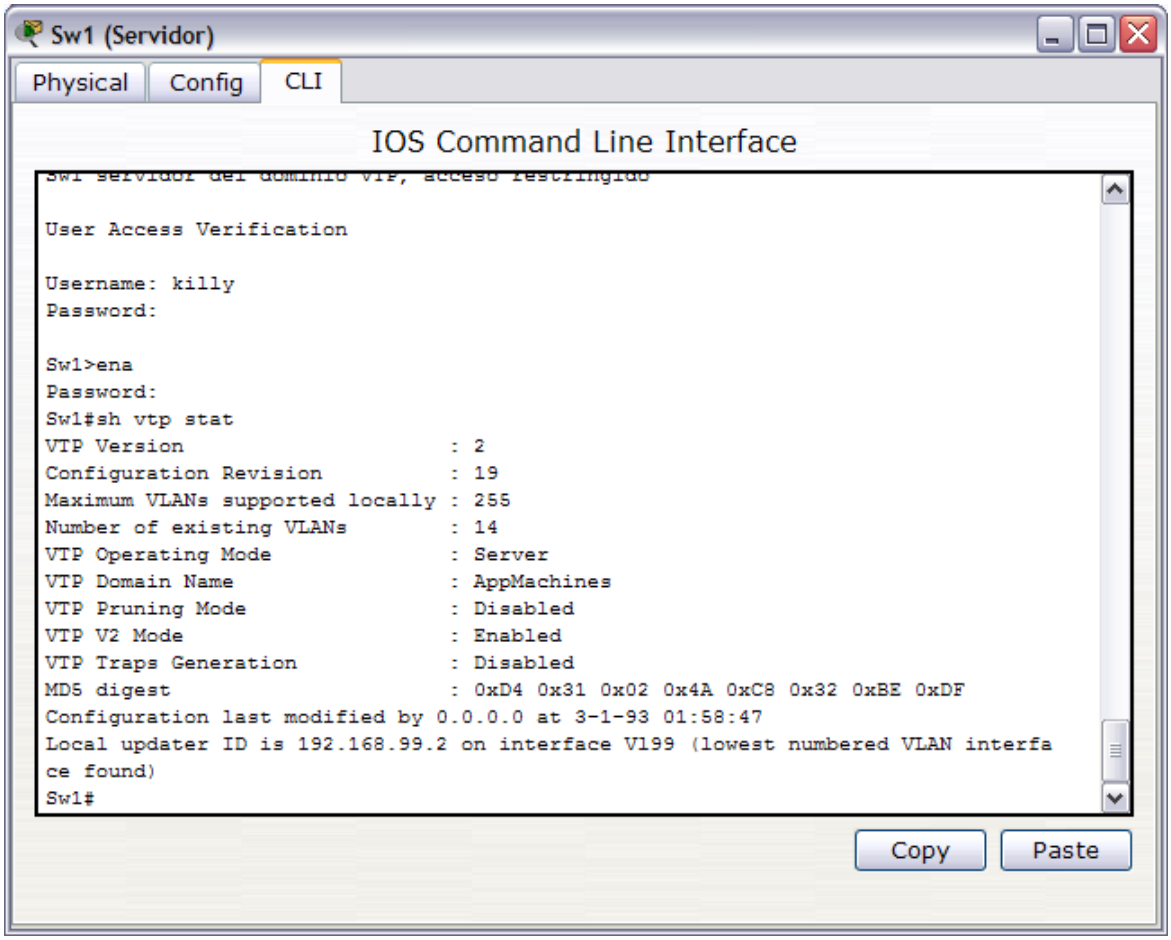
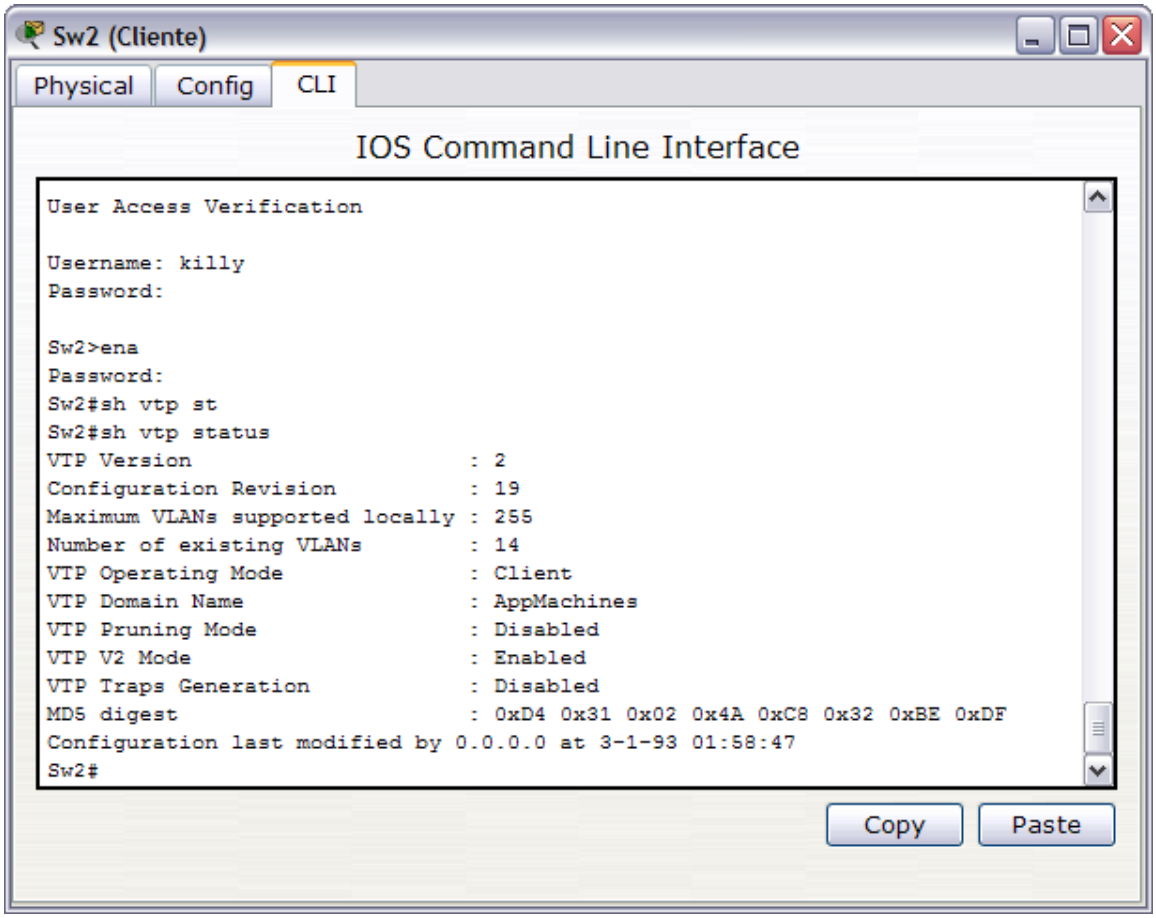


Figura 46. Estado VTP en Sw2 (Cliente)



4.4.1.5 Listado de las VLAN creadas en Sw1. A través del comando “Show vlan brief”, se puede verificar cuantas y que VLAN tiene configurado un Switch, de la misma forma se encuentran, el estado de las VLAN y los puertos que tiene asignados cada VLAN. Cabe aclarar que los puertos que están conectados como enlaces troncales no se observan en el resumen, asimismo aparecen referenciadas las VLAN que los switches tienen creadas por defecto como la 1, fddi-default, token-ring-default.

La figura 47 muestra las VLAN configuradas en Sw1 como servidor del dominio VTP.

La figura 48 demuestra que las VLAN han sido transferidas por medio del dominio VTP y tienen sus respectivos puertos asignados en Sw2.

Figura 47. Listado de las VLAN creadas en Sw1

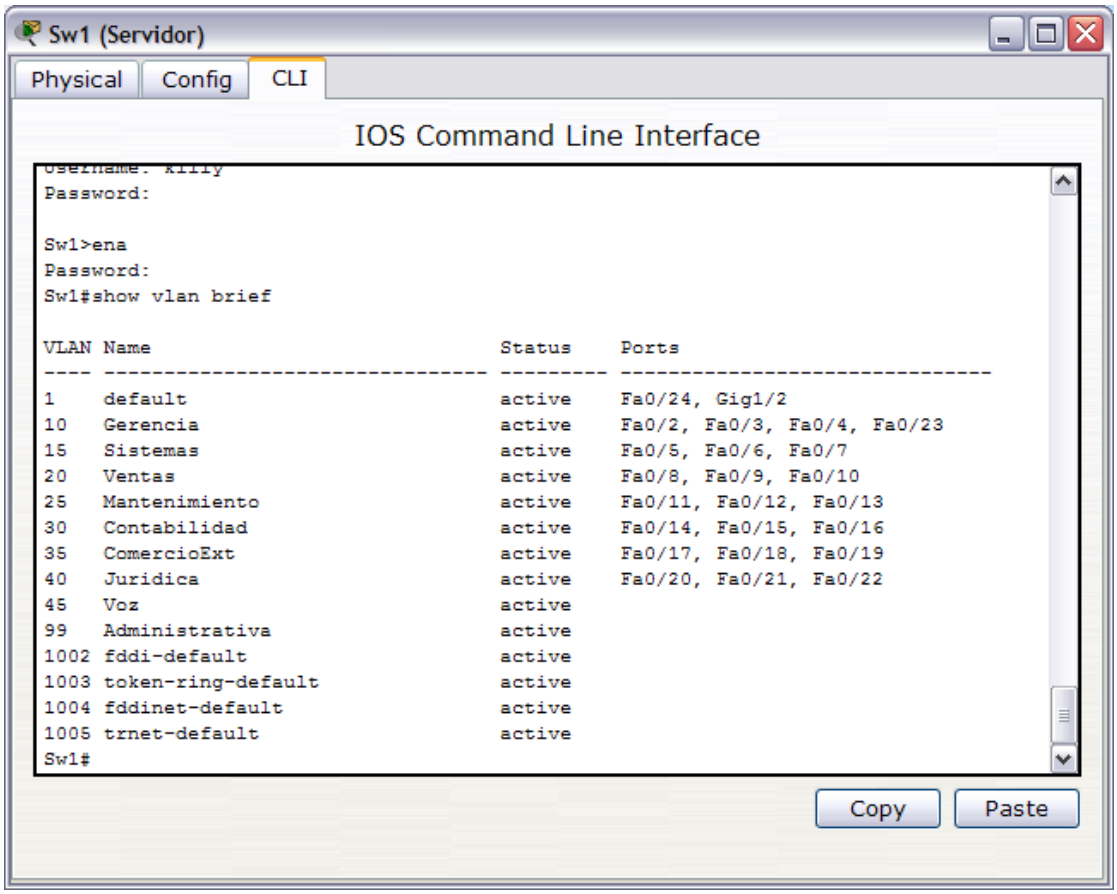
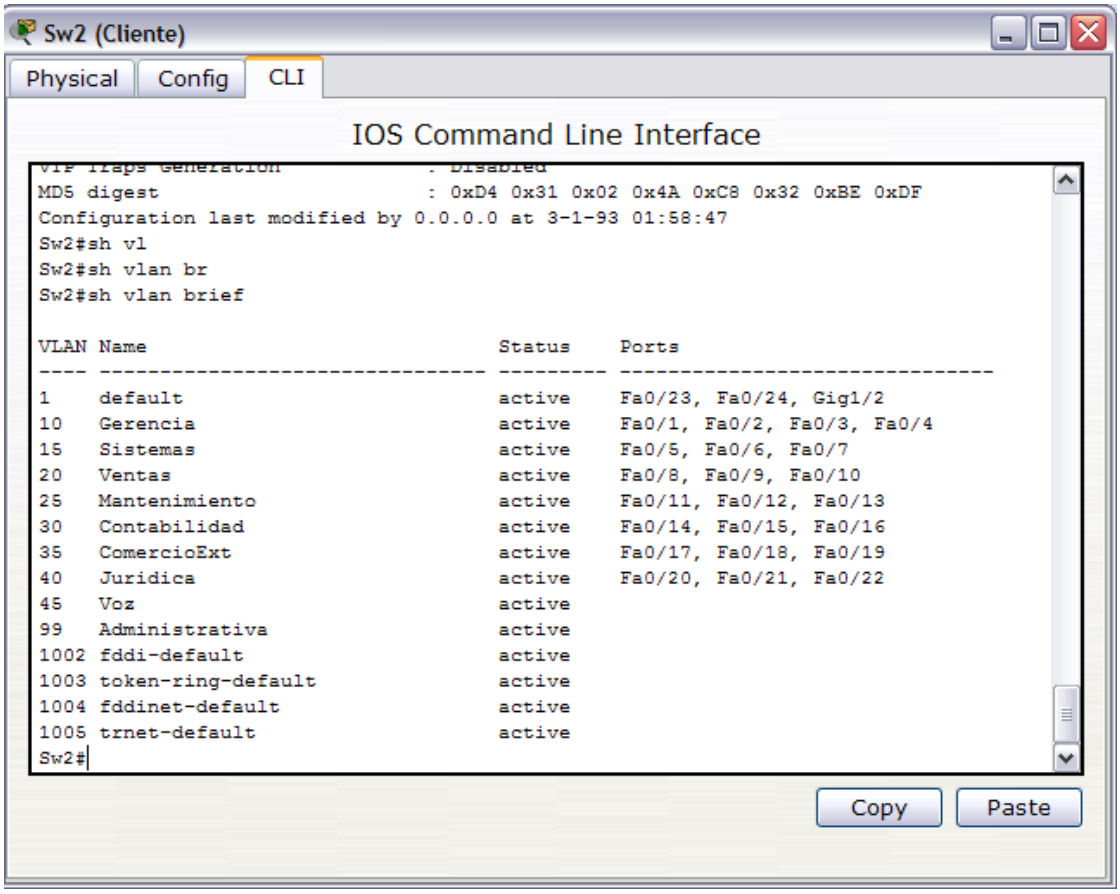


Figura 48. Listado de las VLAN traspasadas a Sw2



4.4.1.6 Estado de los puertos troncales en Sw1. Por medio del comando “Show interface trunk”, se puede verificar el estado de los puertos troncales. Se logra observar que puertos intervienen en el troncal, el modo troncal, el tipo de encapsulación, el estado y la información acerca de la VLAN nativa. La VLAN nativa debe ser igual en los switches que participen del troncal para que este se establezca.

La figura 49 muestra que Sw1 tiene los puertos Fa0/1 y Giga1/1 como puertos troncales, igualmente muestra que el troncal está On, 802.1q como encapsulación y nombra a la VLAN 99 como VLAN nativa.

La figura 50 hace referencia a Sw2, él tiene el pueto Giga1/1 como puerto troncal y muestra la misma información que Sw1, debido a esto, se asume que la

configuración esta correcta y se permite el paso de la información por dichos puertos troncales.

Figura 49. Estado de los puertos troncales en Sw1

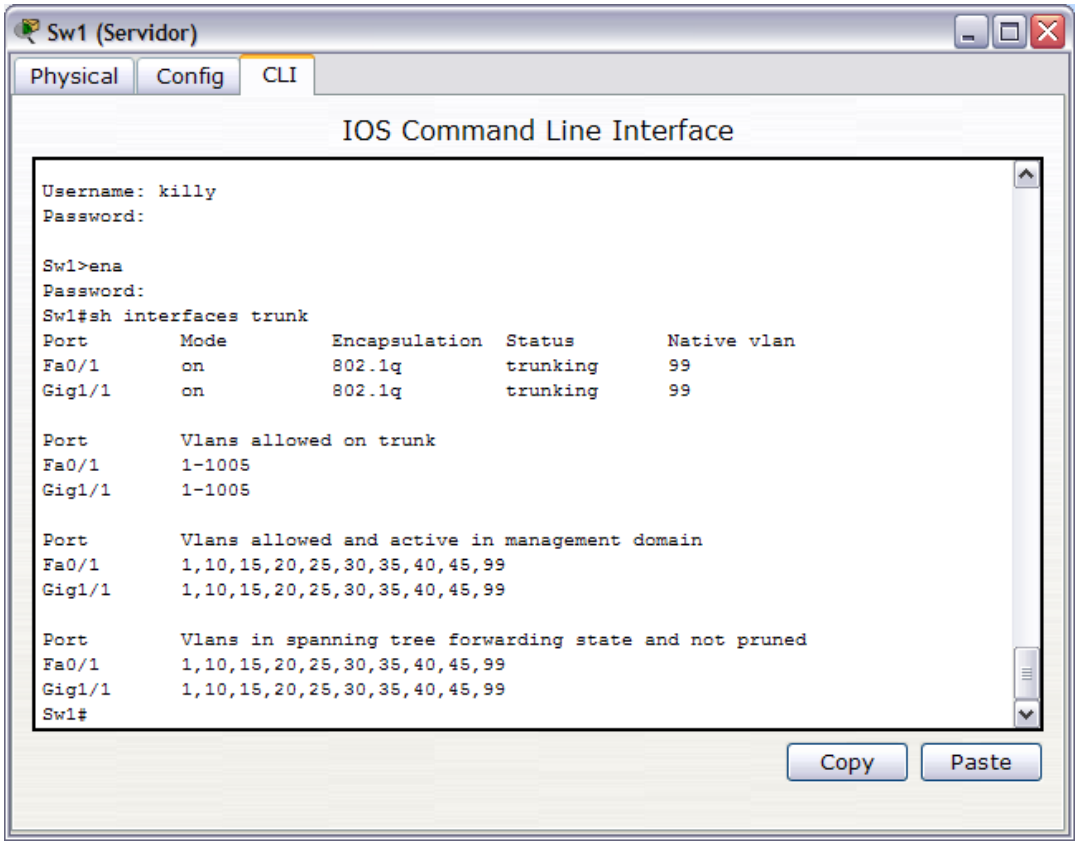
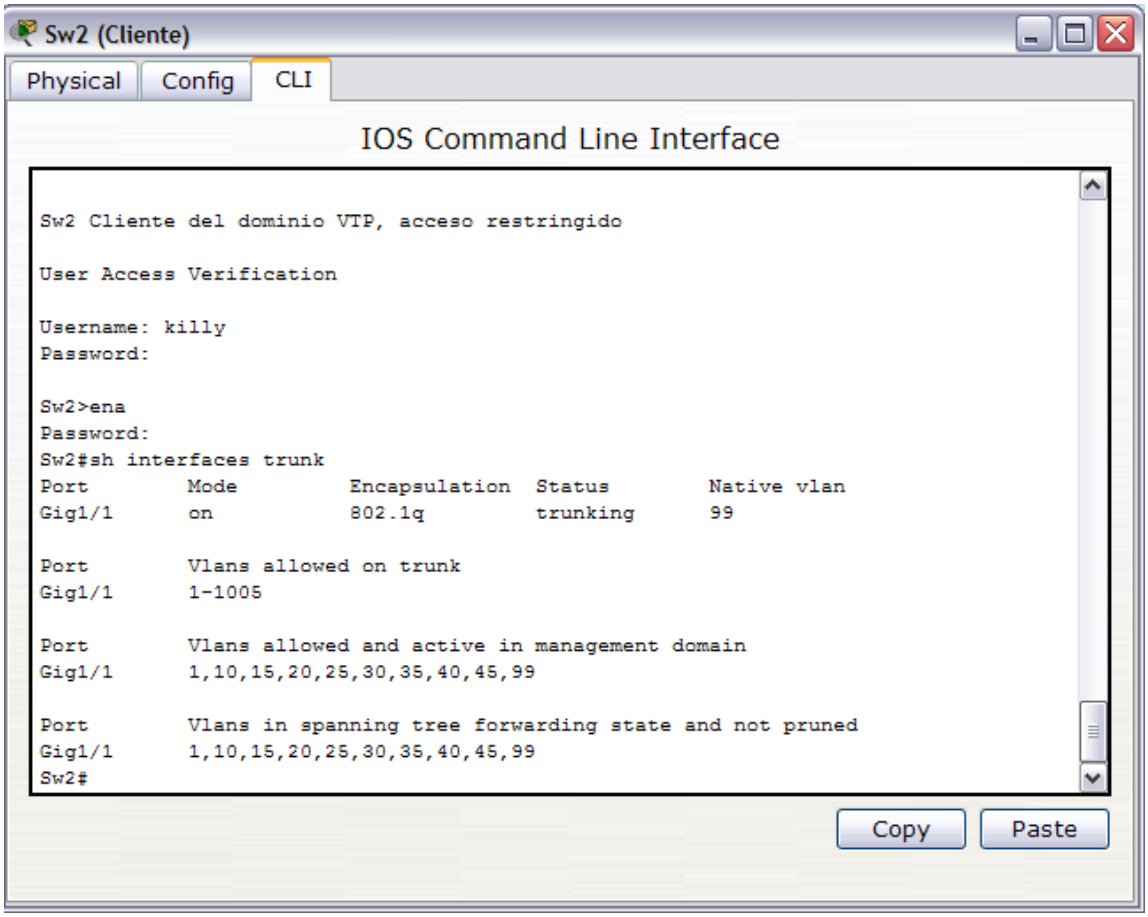


Figura 50. Estado de los puertos Troncales en Sw2



4.4.1.7 Estado DHCP. Tras la configuración de las direcciones excluidas para cada subred IP, se procede a crear un pool de direcciones para ser otorgadas por el servidor DHCP, en la figura 51, el comando “show ip dhcp binding”, muestra que direcciones está otorgando el Router R1 haciendo como servidor de DHCP.

Las figuras 52 y 53 comprueban que los equipos de cómputo están recibiendo dirección por DHCP.

Figura 51. Estado DHCP

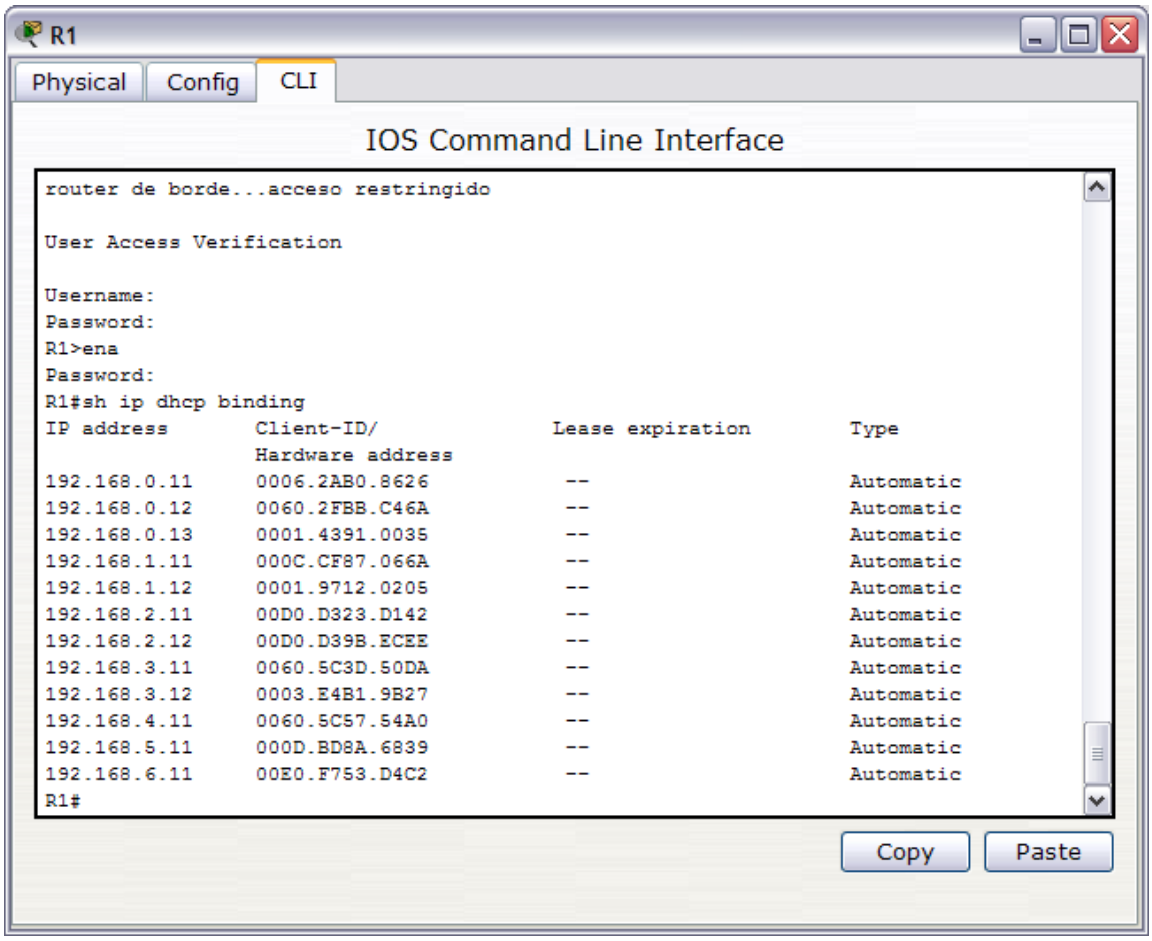


Figura 52. Estado DHCP en equipos de cómputo PC-Gerencia

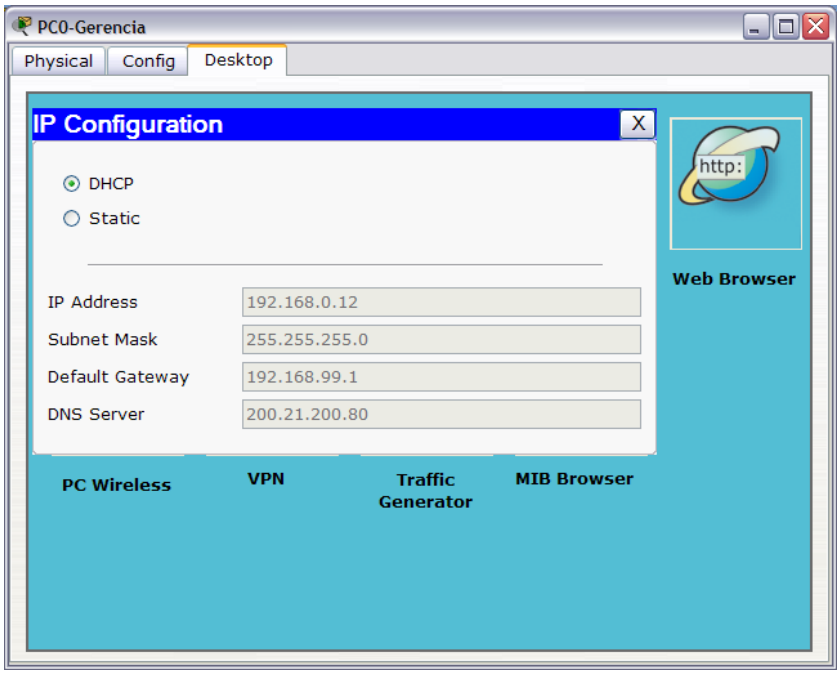
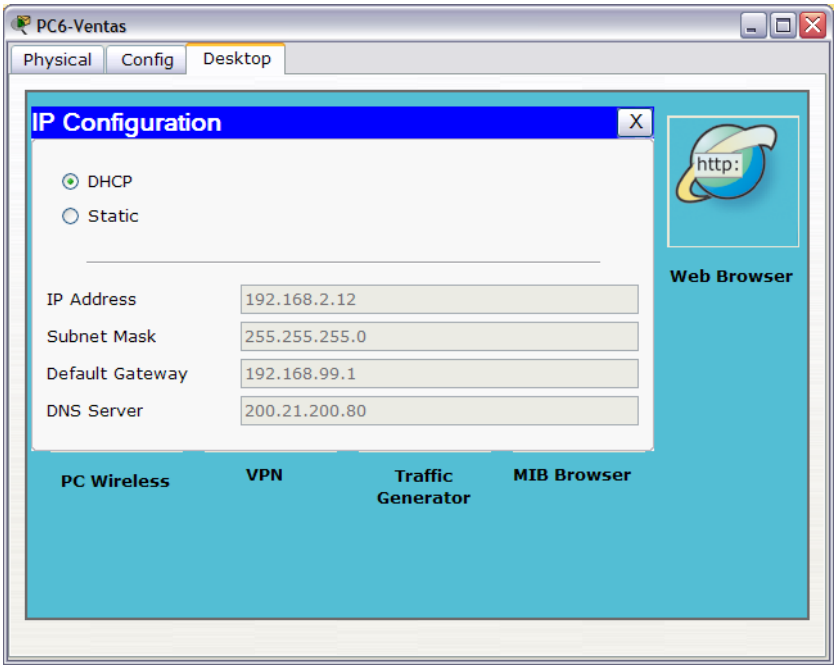
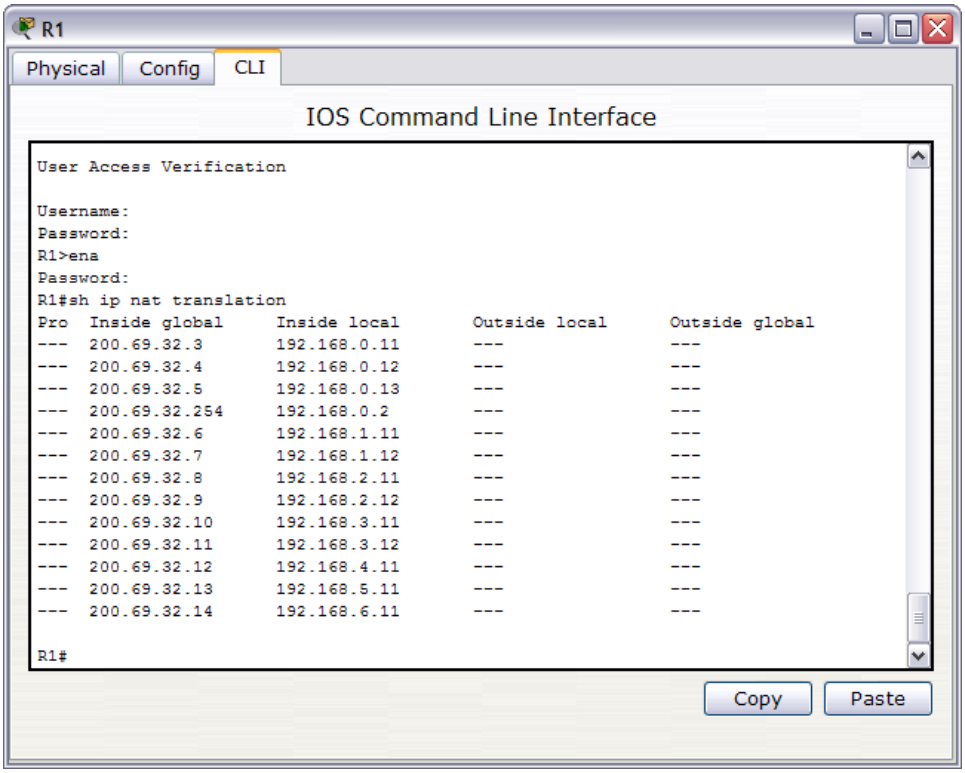


Figura 53. Estado DHCP en equipos de cómputo PC-Ventas



4.4.1.8 Traducciones de NAT. NAT es un protocolo que traduce direcciones privadas en direcciones públicas para poder tener acceso a Internet desde la empresa. Para el proyecto se ha utilizado NAT estático, esto quiere decir que cada equipo tiene una dirección pública para poder navegar en Internet. La figura 54 muestra la asignación de direcciones que cada equipo de cómputo tiene en R1.

Figura 54. Traducciones de NAT



4.4.1.9 ACL Listas de acceso en R1. Las listas de acceso se utilizan para filtrar paquetes y brindar seguridad a la red. las figuras 55, 56 y 57 muestran las ACL configuradas en el bRouter R1, en el Switch Sw1 y en Sw2.

Figura 55. ACL Listas de acceso en R1

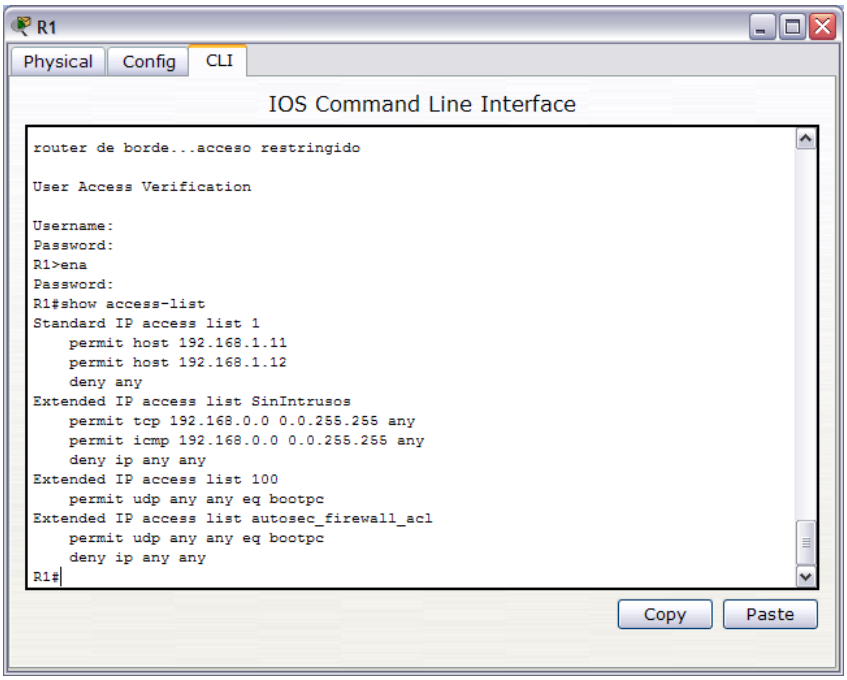


Figura 56. ACL Listas de acceso en Sw1

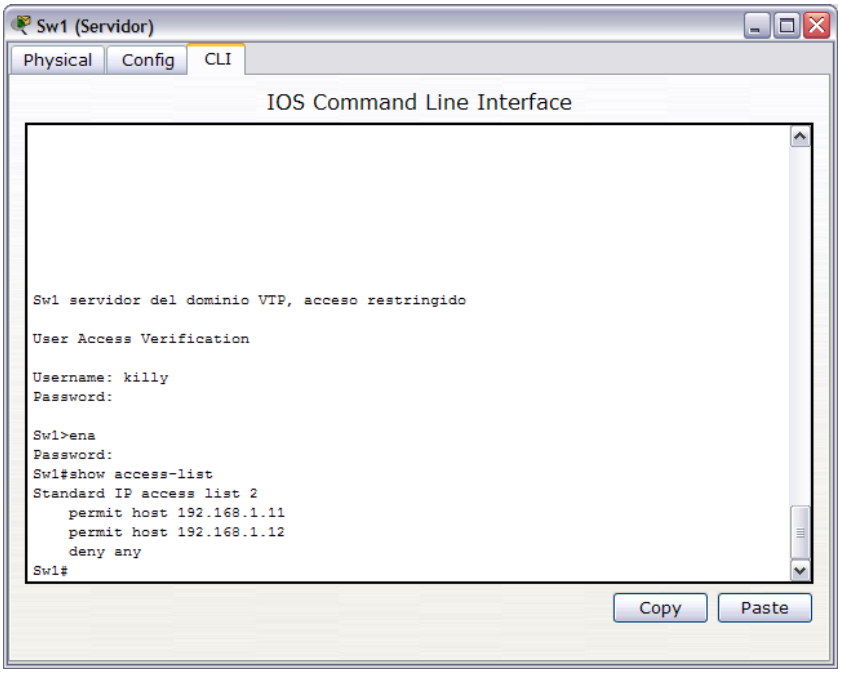
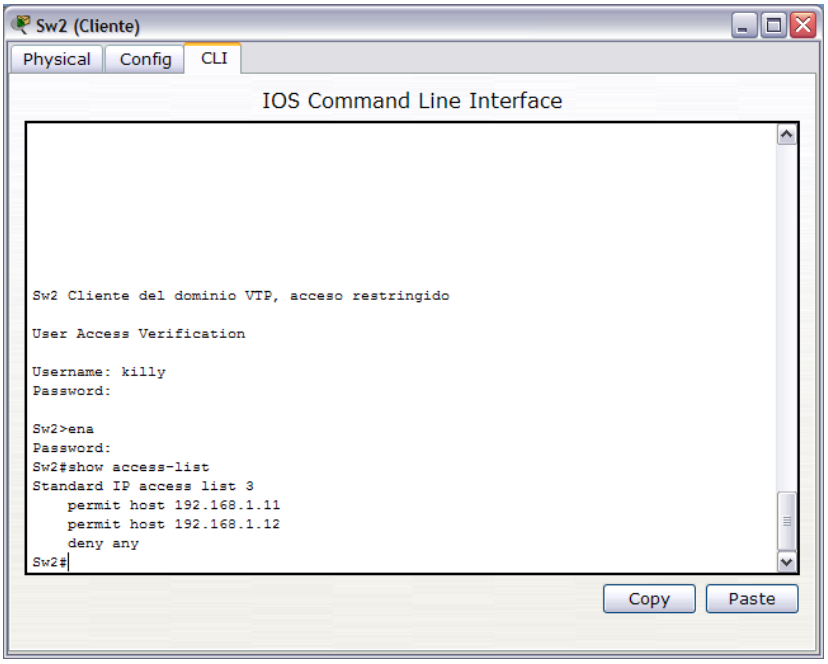
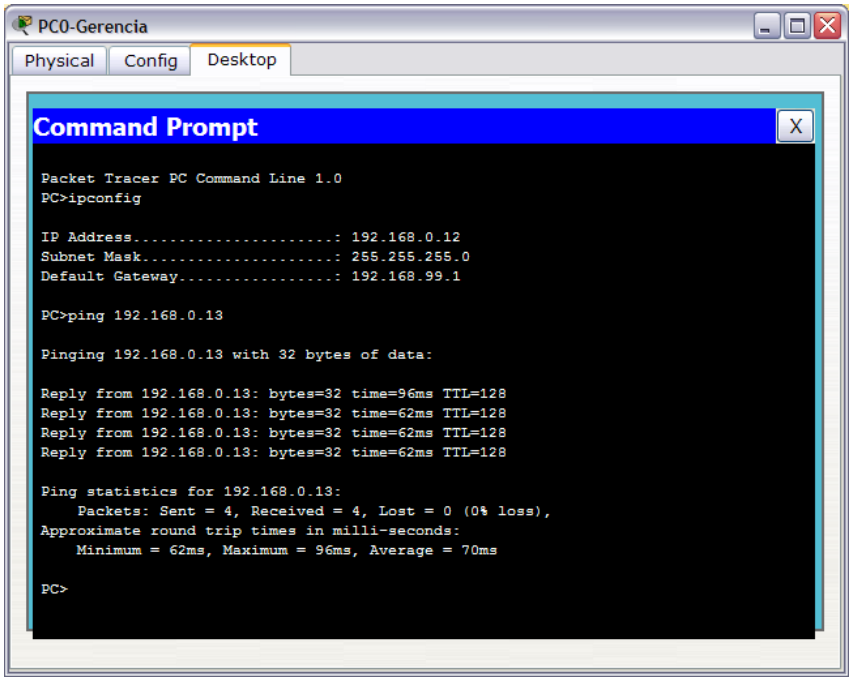


Figura 57. ACL Listas de acceso en Sw2



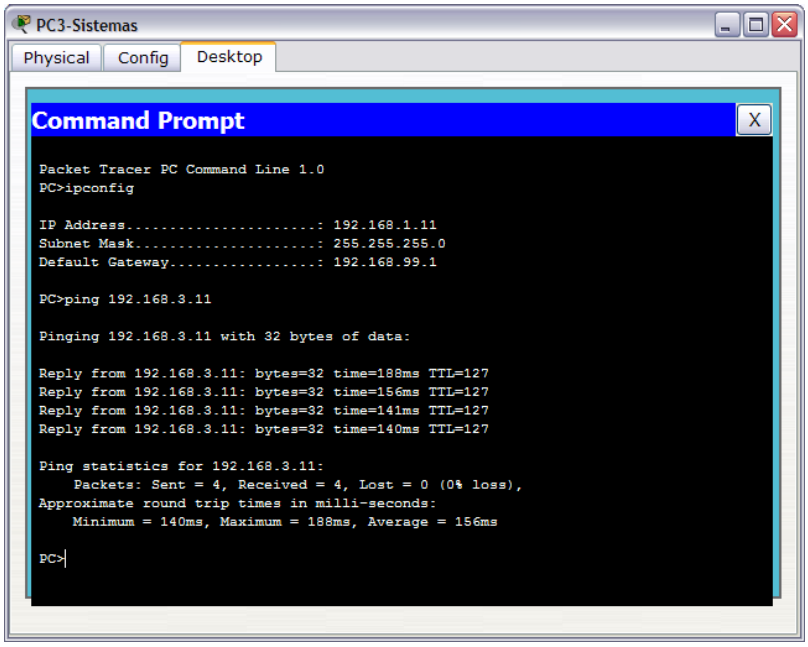
4.4.1.10 Ping para verificar la comunicación de equipos en la misma VLAN. El método para verificar la comunicación dentro de la red es el ping, por medio del protocolo ICMP. La figura 58, muestra que los pings son exitosos entre equipos de la misma VLAN.

Figura 58. Ping para verificar la comunicación de equipos en la misma VLAN



4.4.1.11 Ping para verificar la comunicación de equipos en diferentes VLAN. La Figura 59 muestra los ping exitosos entre equipos en diferentes VLAN. El Router R1, se encarga de hacer el enrutamiento InterVLAN para que la comunicación sea exitosa.

Figura 59. Ping para verificar la comunicación de equipos en diferentes VLAN



4.4.1.12 Ping para comprobar la traducción de direcciones de NAT. Para comprobar la traducción de direcciones, se hace un ping desde el ISP a una dirección pública dentro de la red interna.

En la Figura 60, se observa el ping exitoso entre el ISP y una de las direcciones públicas en la red interna. En el primer intento se pierden los primeros paquetes por la latencia que se da de ir saltando de dispositivo en dispositivo.

En la Figura 61, se muestra la traducción que se hace sobre la dirección que intervino en el ping realizado en la Figura 60.

Figura 60. Ping1 para comprobar la traducción de direcciones de NAT

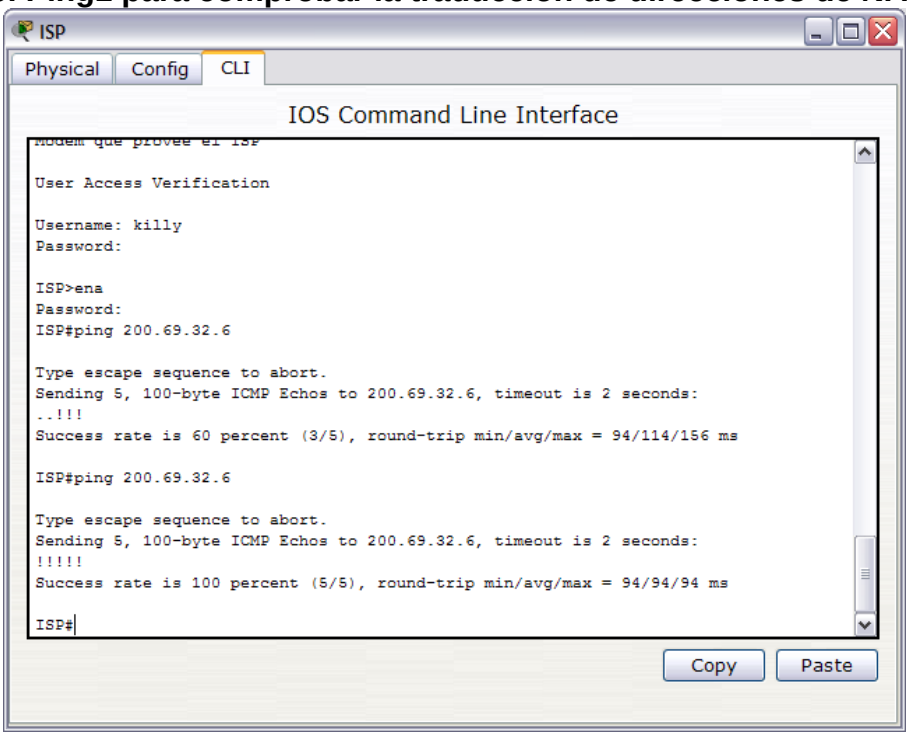
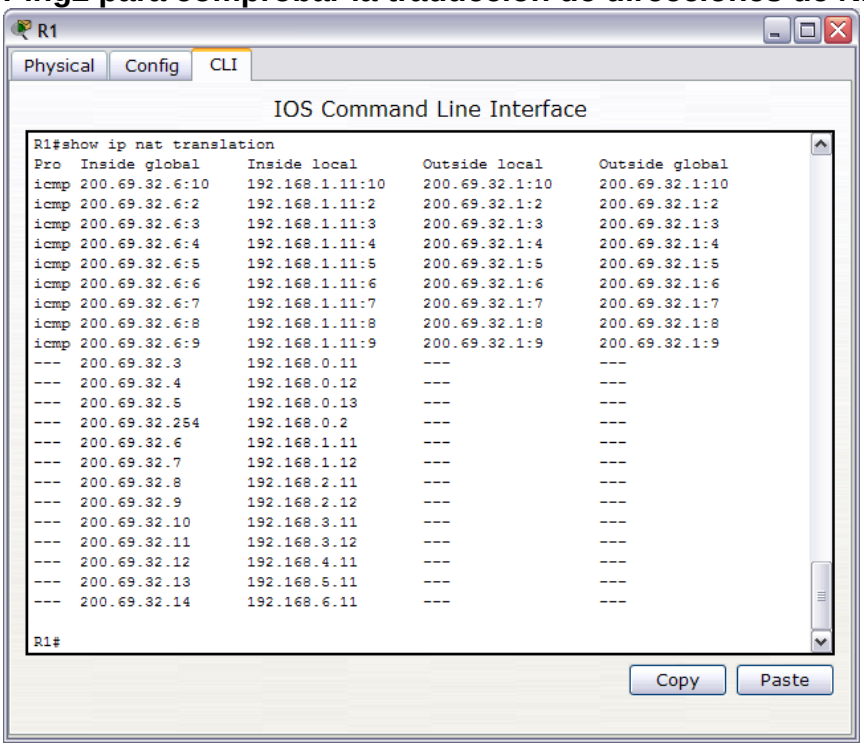
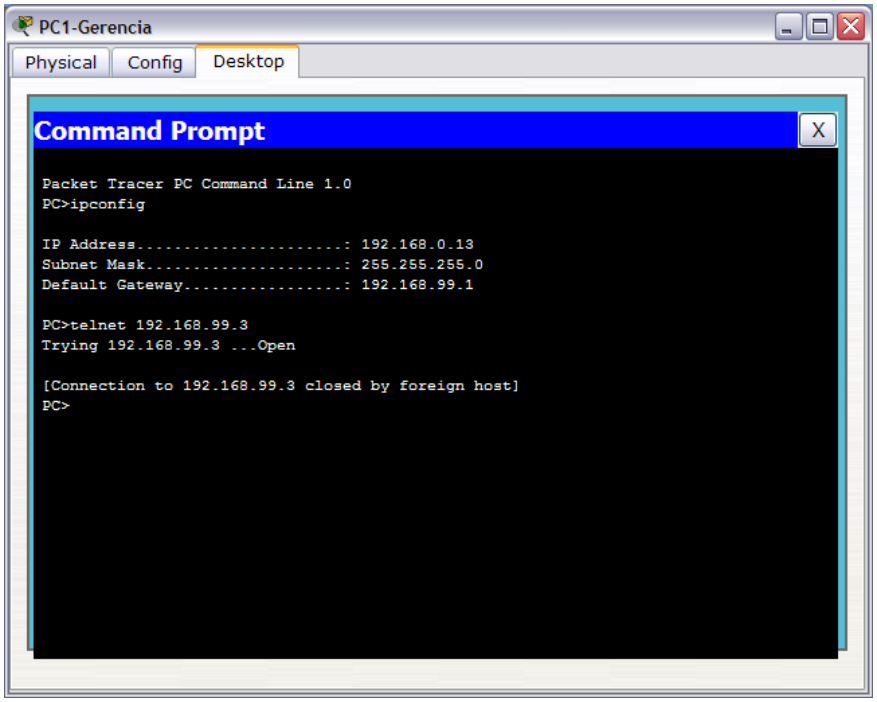


Figura 61. Ping2 para comprobar la traducción de direcciones de NAT



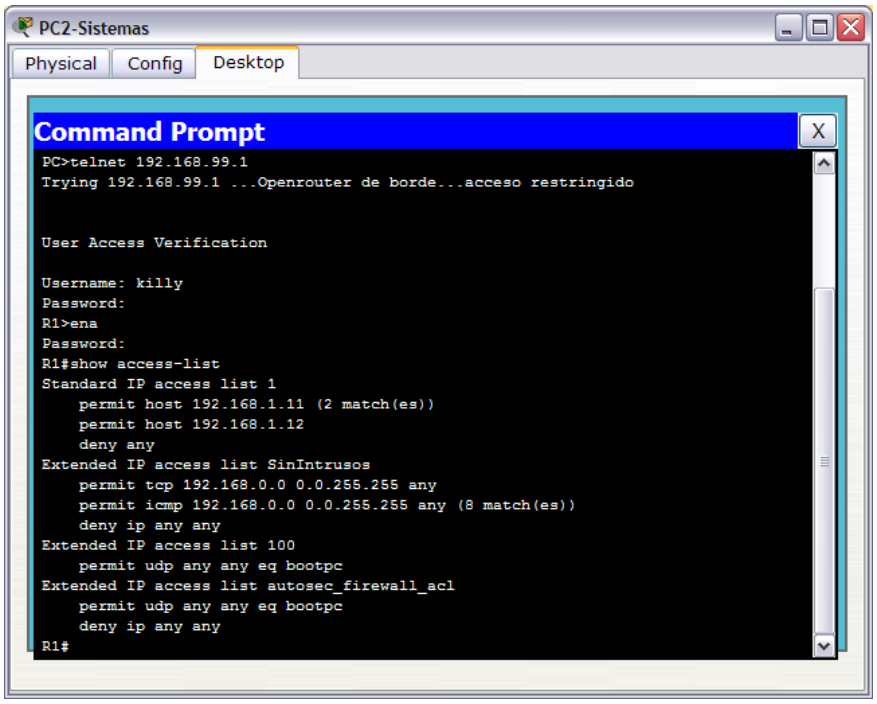
4.4.1.13 Verificación de las listas de acceso ACL. Las líneas VTY de los dispositivos están bloqueadas para todos los miembros de la red menos al departamento de sistemas. La figura 62, muestra como desde un equipo de cómputo en la VLAN de gerencia se tratar de iniciar una sesión de TELNET, pero choca con la ACL impidiendo el acceso.

Figura 62. Verificación de las listas de acceso ACL



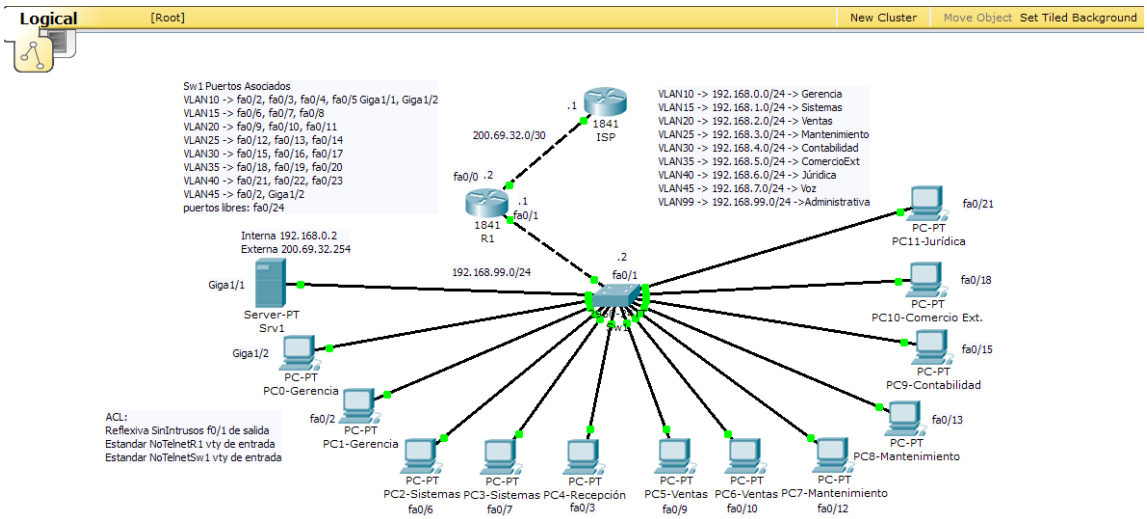
En la Figura 63, se observa cuando un equipo de cómputo del departamento de Sistemas, abre una sesión TELNET con el Router R1, el comando “show Access-list”, muestra la forma en que los paquetes golpean contra las ACL, ya sea denegando o permitiendo según los requerimientos del cliente.

Figura 63. Verificación de las listas de acceso ACL



4.4.2 Escenario 2. La simulación incluye el modem Router que brinda el ISP, llamado ISP, el router de borde de la empresa llamado R1, un Switch, Sw1, doce (12) equipos de cómputo y el servidor Srv1, tal como lo puede apreciar en la Figura 64. Topología Simulación Packet Tracer 5.2 (2)

Figura 64. Topología Simulación Packet Tracer 5.2 (2)

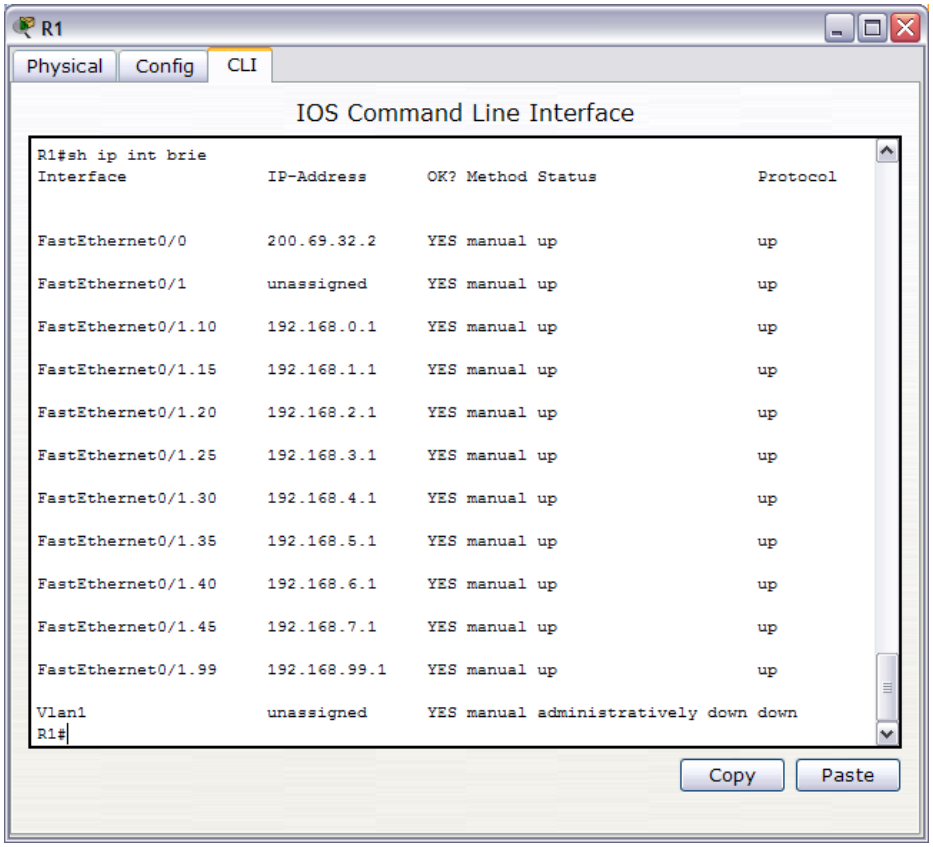


Como anexo al documento se encuentran los archivos de configuración de ISP, R1, Sw1.

Dentro de la simulación Podemos comprobar:

4.4.2.1 Estado de las interfaces en R1. Por medio del comando “Show ip interfaces brief” se puede verificar el estado de las interfaces del dispositivo, se encuentra un resumen que contiene el nombre de las interfaces, la dirección IP y el estado de las mismas. En la figura 65. Estado de las interfaces en R1. P. 135, se observa que R1 tiene dos interfaces físicas, Fa0/0 y Fa0/1, Fa0/0 está conectada hacia ISP, tiene su dirección IP configurada y está arriba por lo que funciona correctamente. La Interfaz Fa0/1 es el enlace troncal hacia Sw1 por lo que no tiene dirección IP pero debe estar arriba, las subinterfaces se crean con respecto a las VLAN creadas en los Switches, cada subinterfaz tiene una dirección IP valida en el rango de cada subred y se encuentran arriba y funcionando correctamente.

Figura 65. Estado de las interfaces en R1



4.4.2.2 Estado de las interfaces en Sw1. En las figuras 66 y 67, se observa el estado de las interfaces físicas de Sw1, las interfaces que tiene equipos de cómputo conectadas se encuentran arriba, las interfaces que no, se encuentran administrativamente abajo, cabe aclarar que los puertos son asignados a las VLAN dependiendo de los requerimientos del cliente, pero el puerto Fa0/24 se encuentra apagado y sin asignación hacia una VLAN en especial porque no se va a usar inicialmente en el diseño.

Figura 66. Estado de las interfaces en Sw1

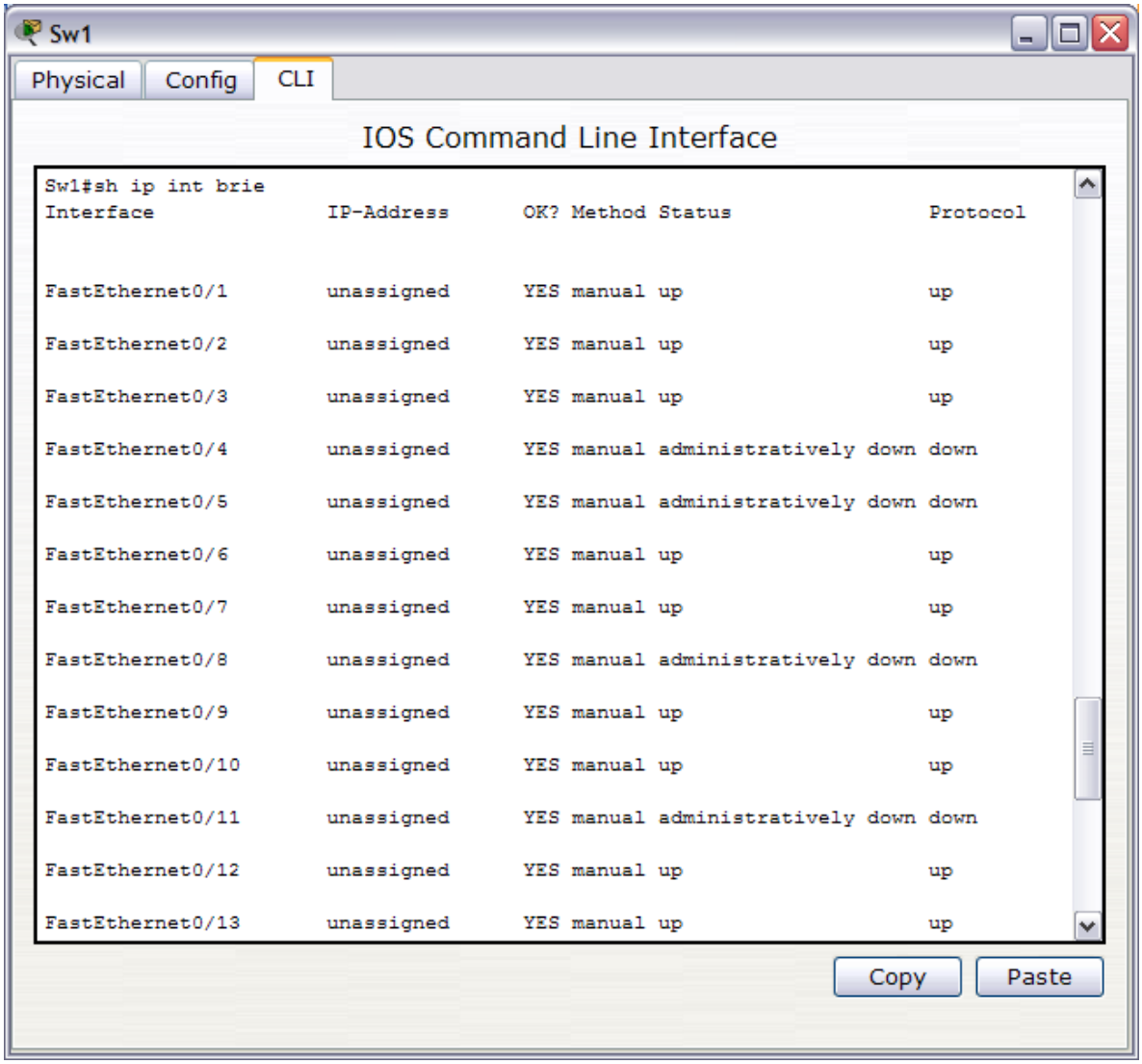
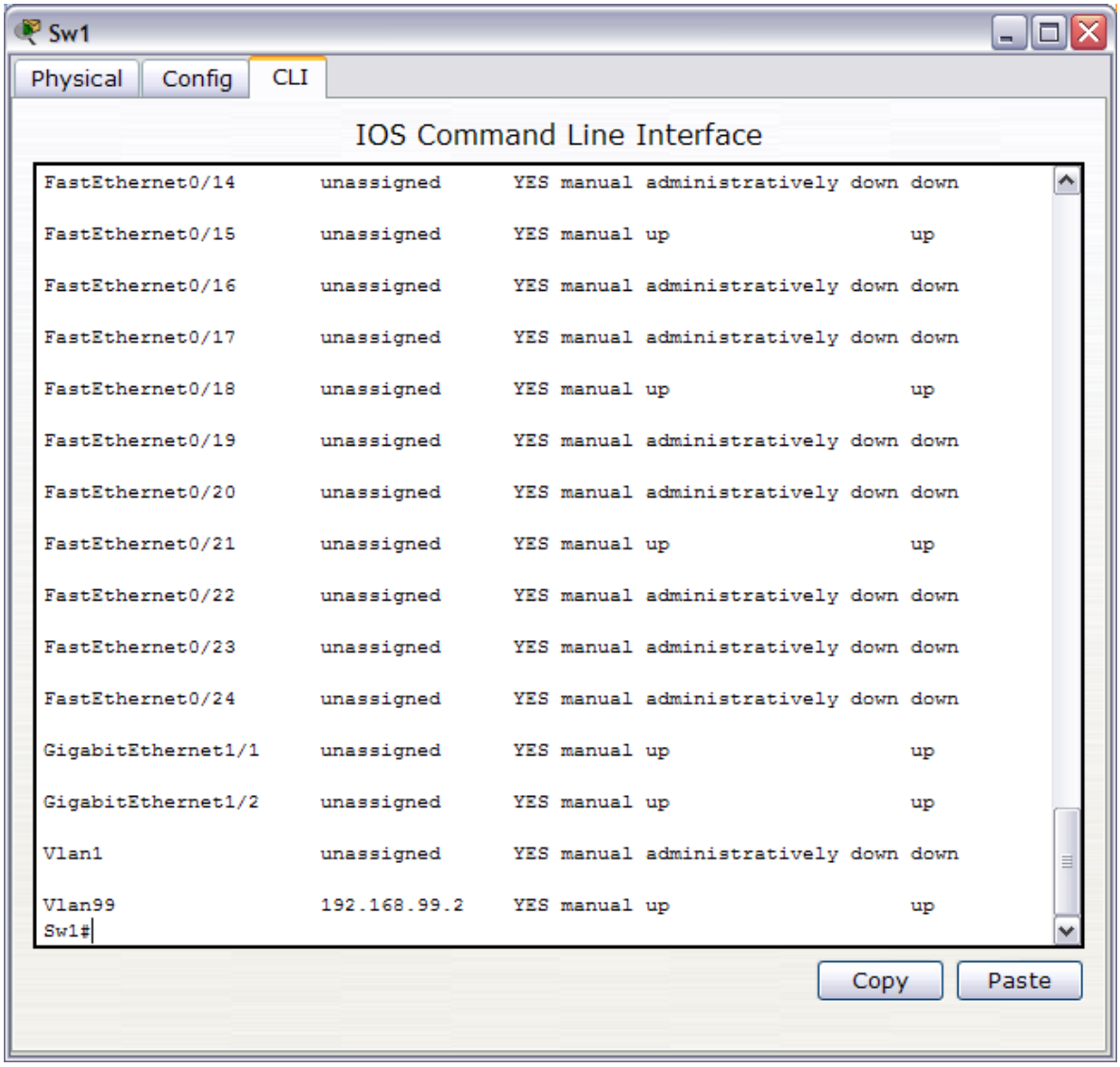


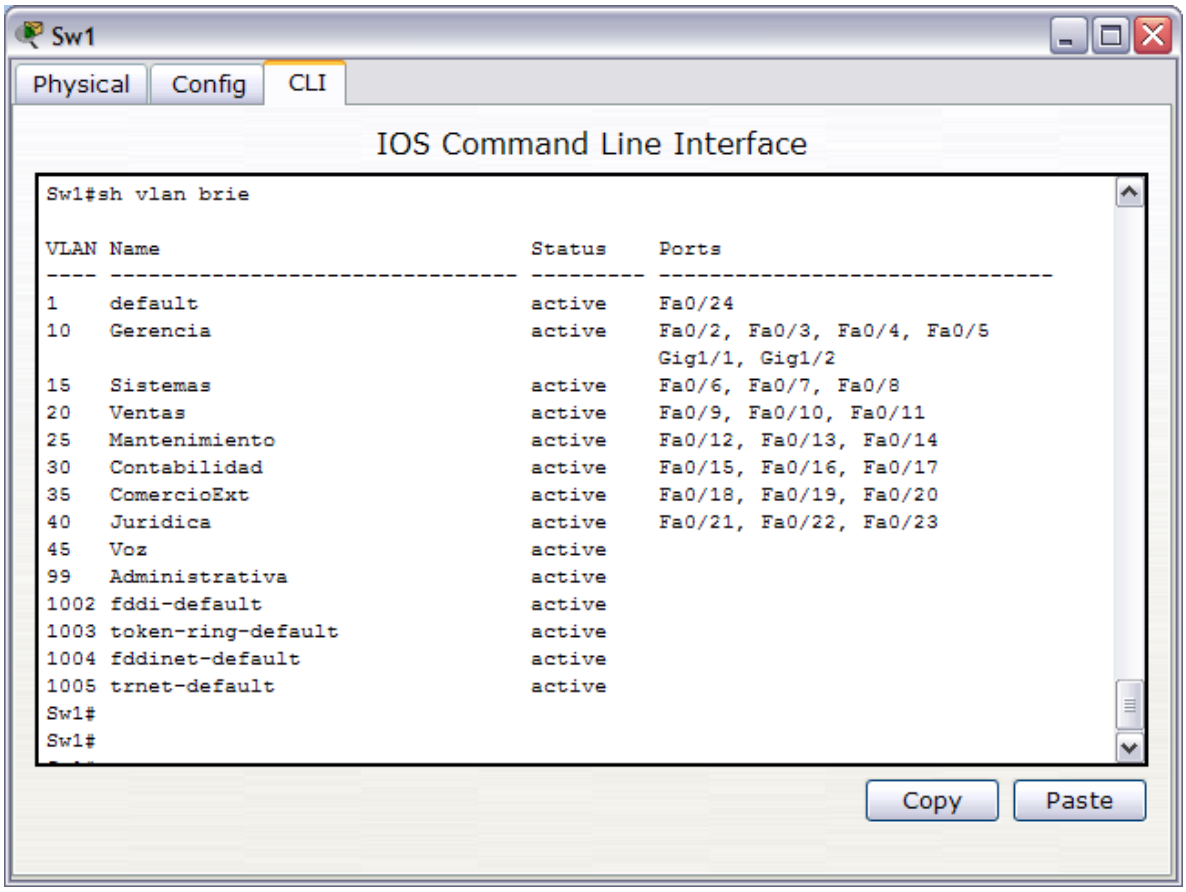
Figura 67. Estado de las interfaces en Sw1 (Continuación)



4.4.2.3 Listado de las VLAN creadas en Sw1. A través del comando “Show vlan brief”, se puede verificar cuantas y que VLAN tiene configurado un Switch, de la misma forma se encuentran, el estado de las VLAN y los puertos que tiene asignados cada VLAN. Cabe aclarar que los puertos que están conectados como enlaces troncales no se observan en el resumen, asimismo aparecen referenciadas las VLAN que los switches tienen creadas por defecto como la 1, fddi-default, token-ring-default.

La figura 68 muestra las VLAN configuradas en Sw1.

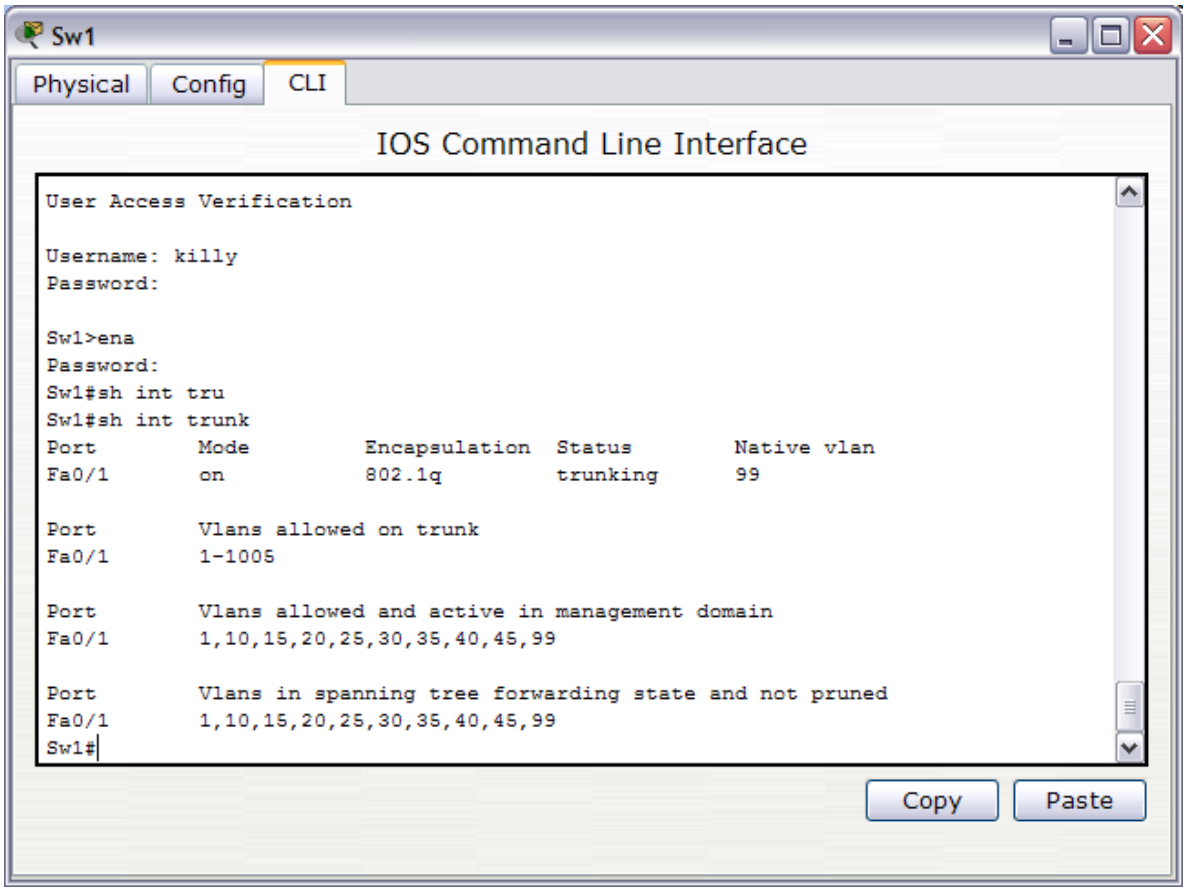
Figura 68. VLAN configuradas en Sw1.



4.4.2.4 Estado de los puertos troncales en Sw1. Por medio del comando “Show interface trunk”, se puede verificar el estado de los puertos troncales. Se logra observar que puertos intervienen en el troncal, el modo troncal, el tipo de encapsulación, el estado y la información acerca de la VLAN nativa. La VLAN nativa debe ser igual en los switches que participen del troncal para que este se establezca.

La figura 69 muestra que Sw1 tiene el puerto Fa0/1 como puerto troncal, igualmente muestra que el troncal está On, 802.1q como encapsulación y nombra a la VLAN 99 como VLAN nativa.

Figura 69. Estado de los puertos troncales en Sw1



4.4.2.5 Estado DHCP. Tras la configuración de las direcciones excluidas para cada subred IP, se procede a crear un pool de direcciones para ser otorgadas por el servidor DHCP, en la figura 70, el comando “show ip dhcp binding”, muestra que direcciones está otorgando el Router R1 haciendo como servidor de DHCP.

Las figuras 71 y 72 comprueban que los equipos de cómputo están recibiendo dirección por DHCP.

Figura 70. Estado DHCP

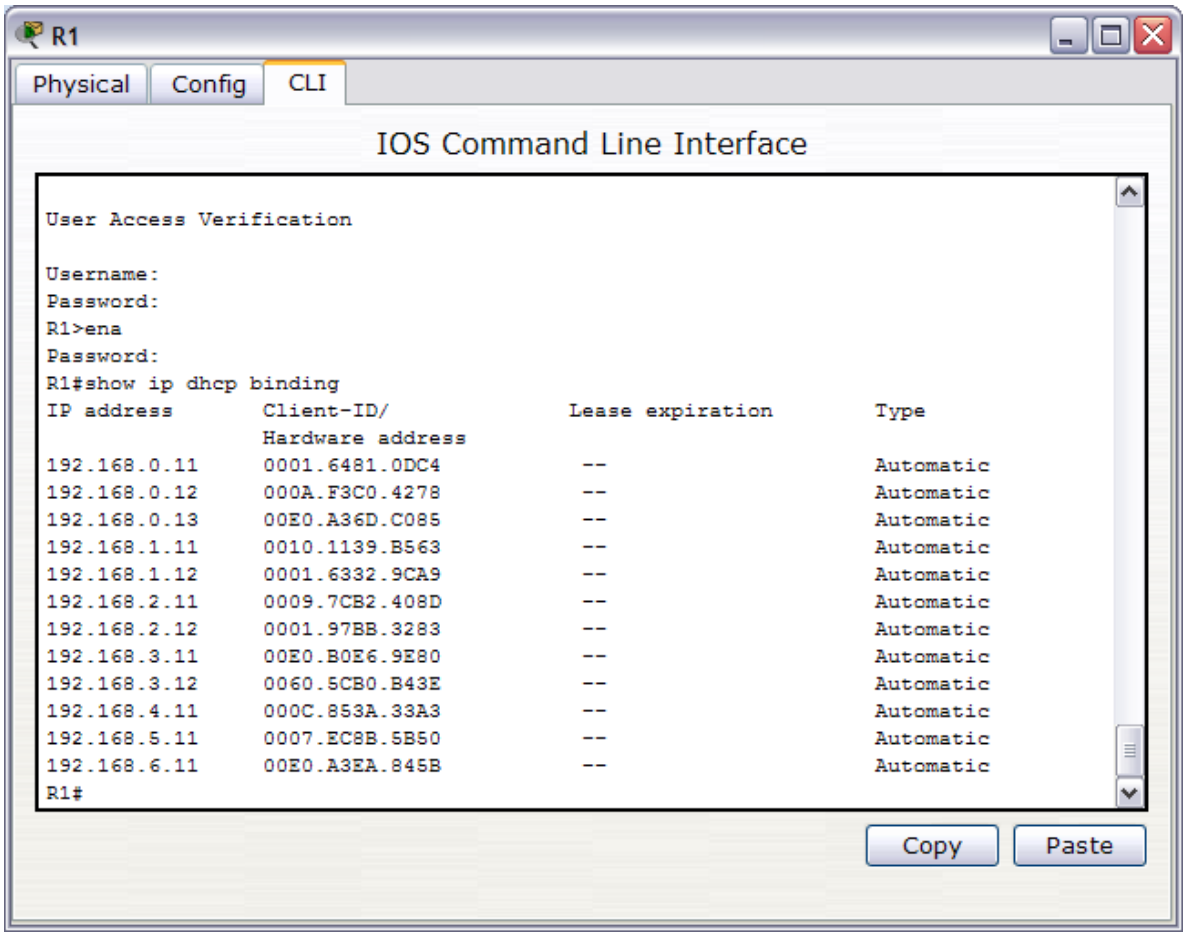


Figura 71. Estado DHCP en equipos de cómputo PC-Gerencia

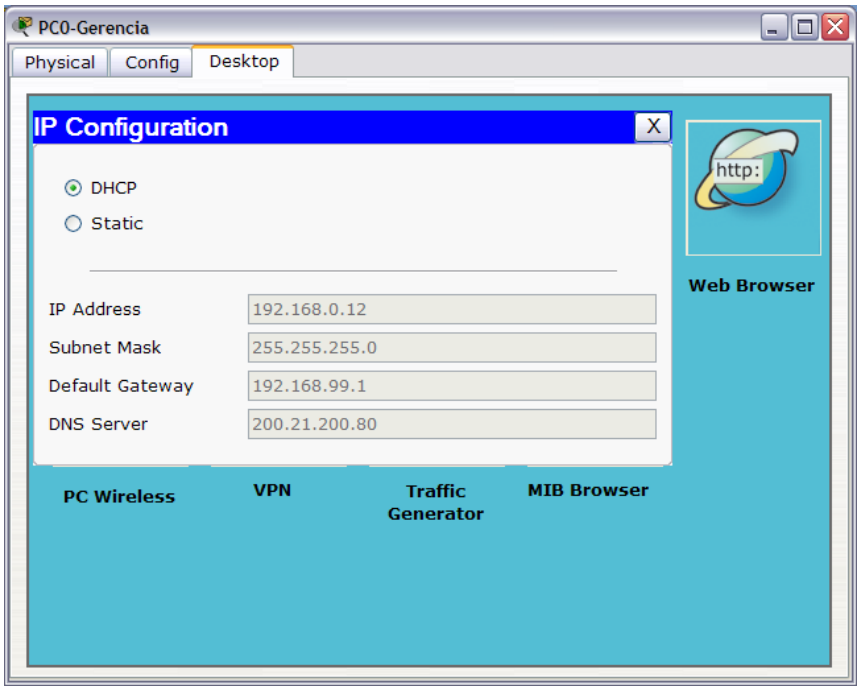
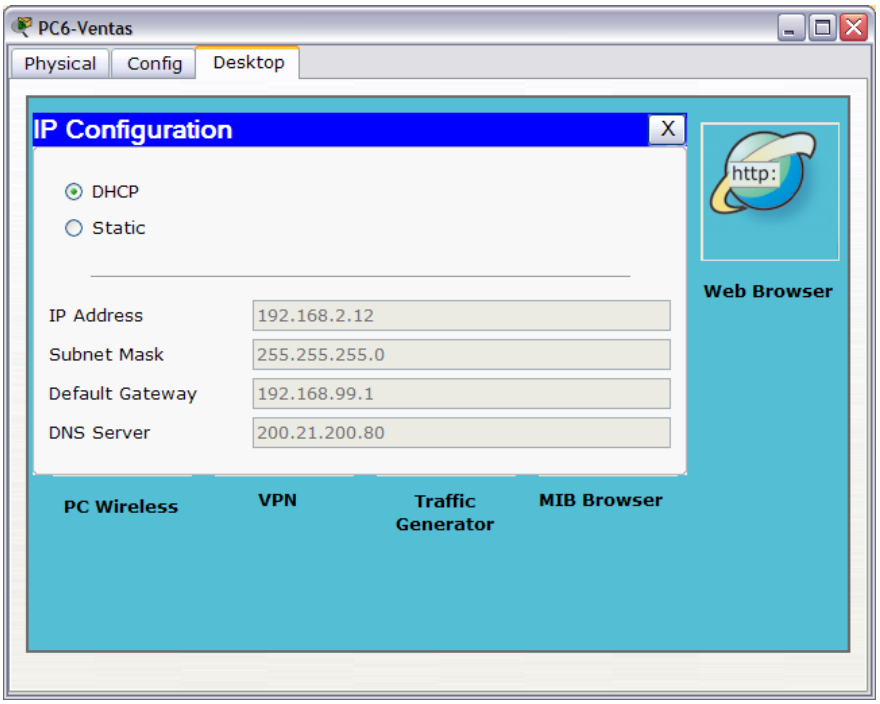
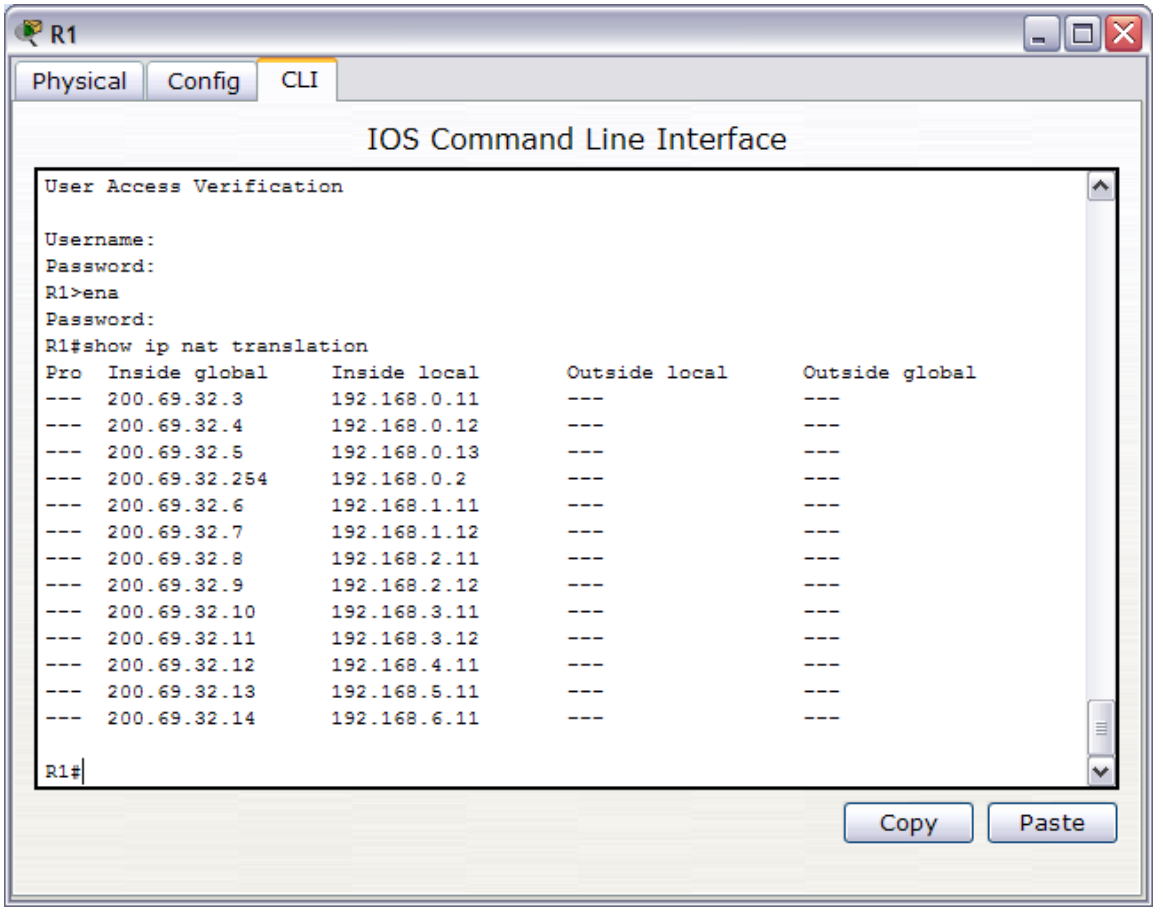


Figura 72. Estado DHCP en equipos de cómputo PC-Ventas



4.4.2.6 Traducciones de NAT. NAT es un protocolo que traduce direcciones privadas en direcciones públicas para poder tener acceso a Internet desde la empresa. Para el proyecto se ha utilizado NAT estático, esto quiere decir que cada equipo tiene una dirección pública para poder navegar en Internet. La figura 73 muestra la asignación de direcciones que cada equipo de cómputo tiene en R1.

Figura 73. Traducciones de NAT



4.4.2.7 ACL Listas de acceso en R1. Las listas de acceso se utilizan para filtrar paquetes y brindar seguridad a la red. las figuras 74, 75 muestran las ACL configuradas en el Router R1, en el Switch Sw1.

Figura 74. ACL Listas de acceso en R1

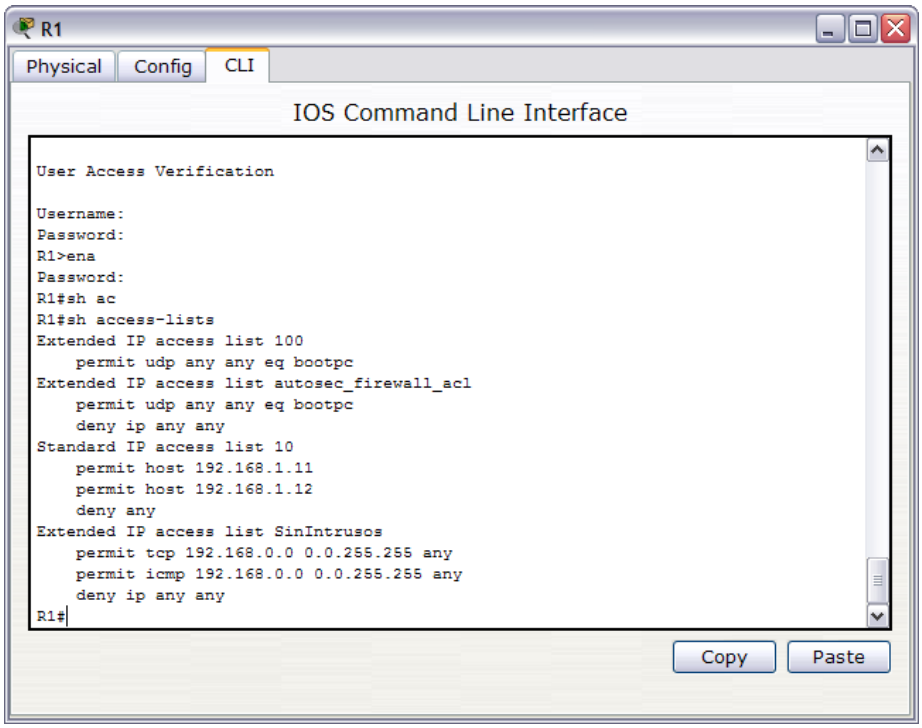
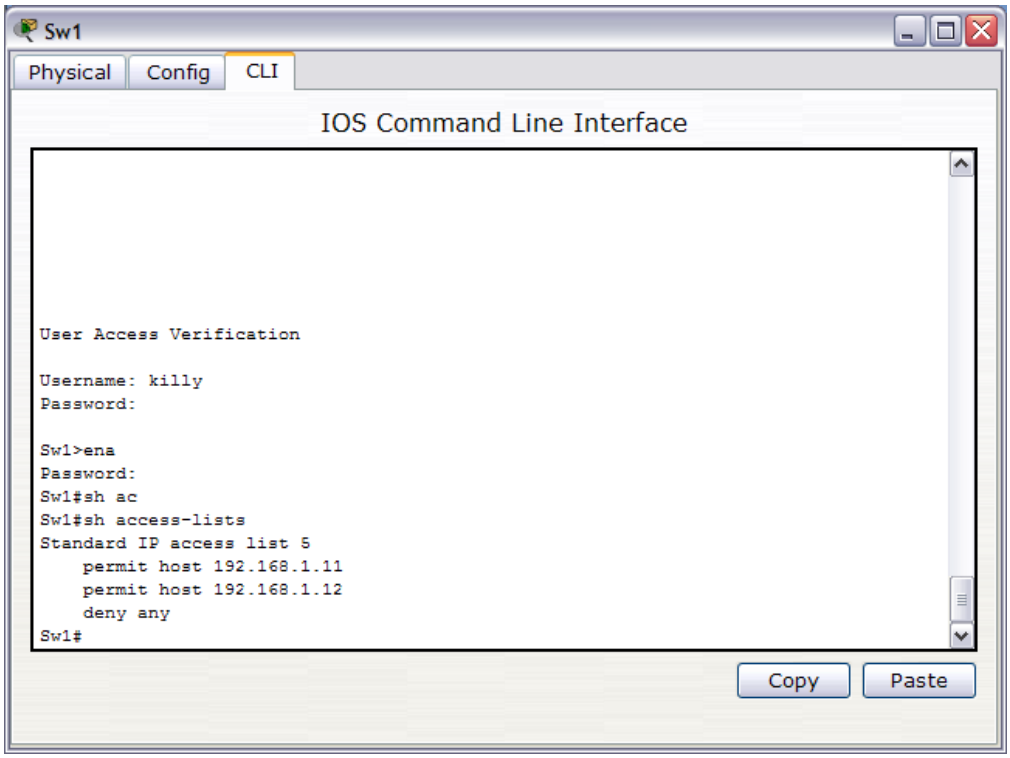
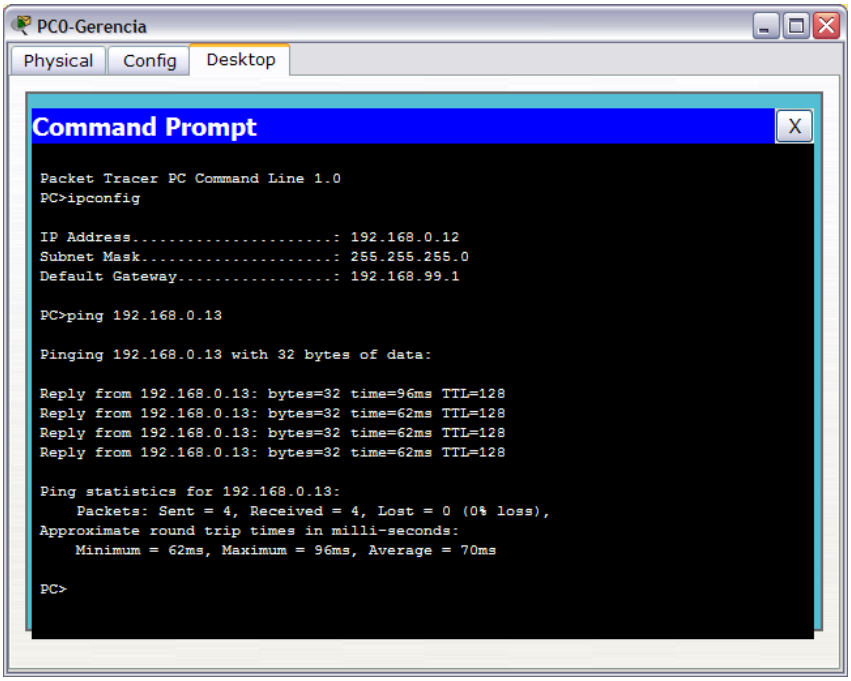


Figura 75. ACL Listas de acceso en Sw1



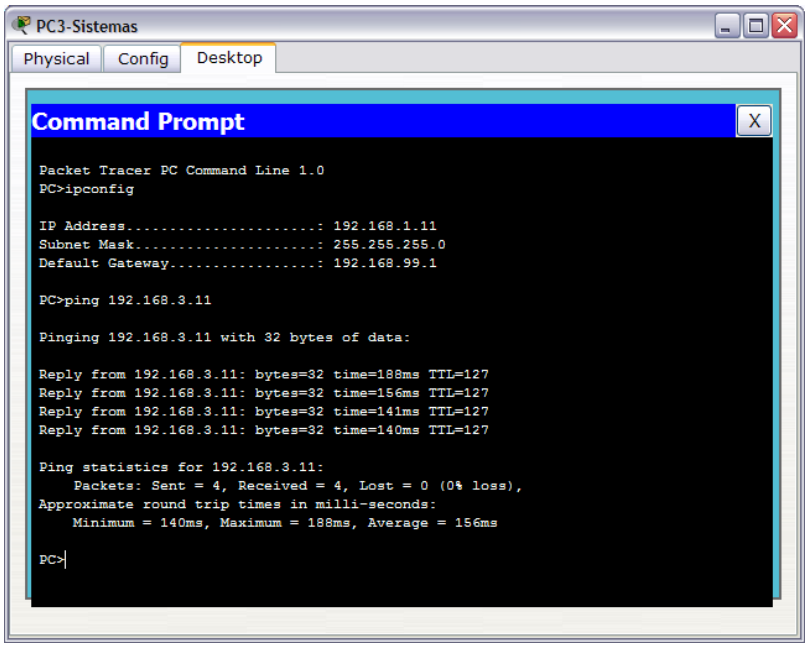
4.4.2.8 Ping para verificar la comunicación de equipos en la misma VLAN. El método para verificar la comunicación dentro de la red es el ping, por medio del protocolo ICMP. La figura 76, muestra que los pings son exitosos entre equipos de la misma VLAN.

Figura 76. Ping para verificar la comunicación de equipos en la misma VLAN



4.4.2.9 Ping para verificar la comunicación de equipos en diferentes VLAN. La Figura 77 muestra los ping exitosos entre equipos en diferentes VLAN. El Router R1, se encarga de hacer el enrutamiento InterVLAN para que la comunicación sea exitosa.

Figura 77. Ping para verificar la comunicación de equipos en diferentes VLAN



4.4.2.10 Ping para comprobar la traducción de direcciones de NAT. Para comprobar la traducción de direcciones, se hace un ping desde el ISP a una dirección pública dentro de la red interna.

En la Figura 78, se observa el ping exitoso entre el ISP y una de las direcciones públicas en la red interna. En el primer intento se pierden los primeros paquetes por la latencia que se da de ir saltando de dispositivo en dispositivo.

En la Figura 79, se muestra la traducción que se hace sobre la dirección que intervino en el ping realizado en la Figura 78.

Figura 78. Ping1 para comprobar la traducción de direcciones de NAT

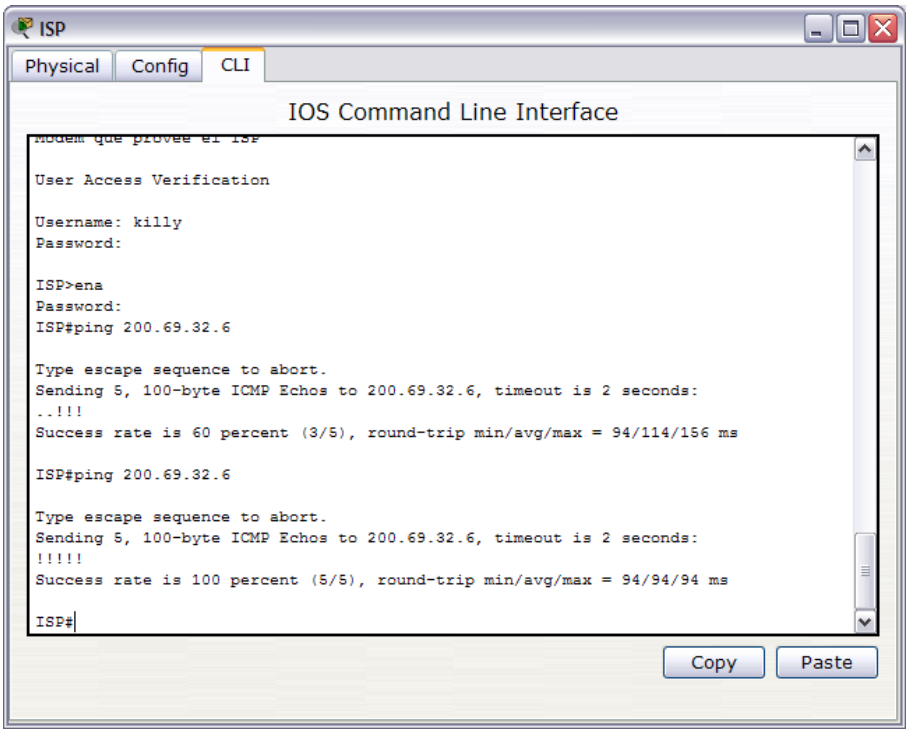
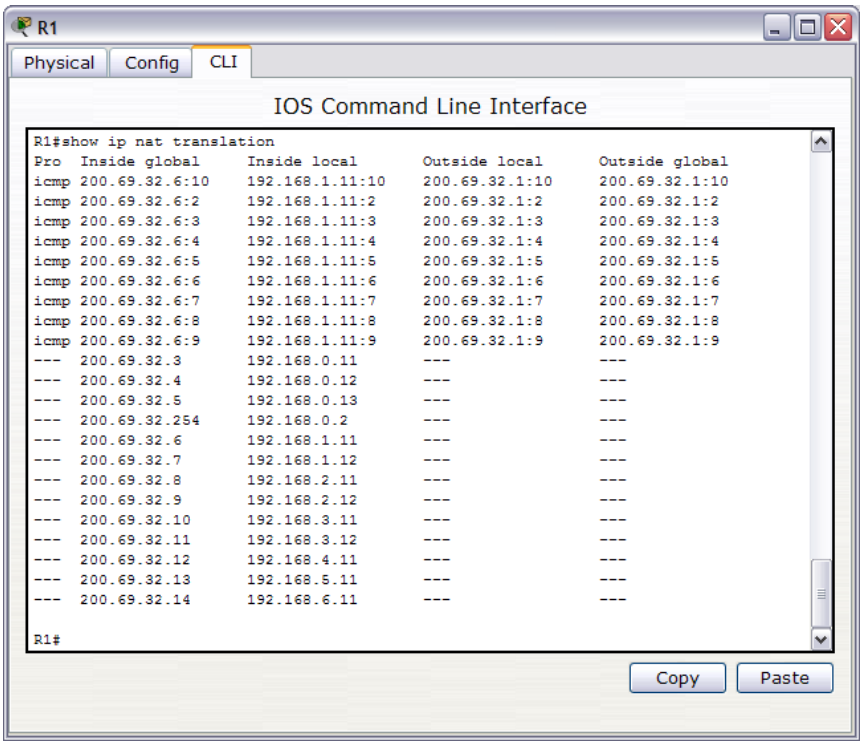
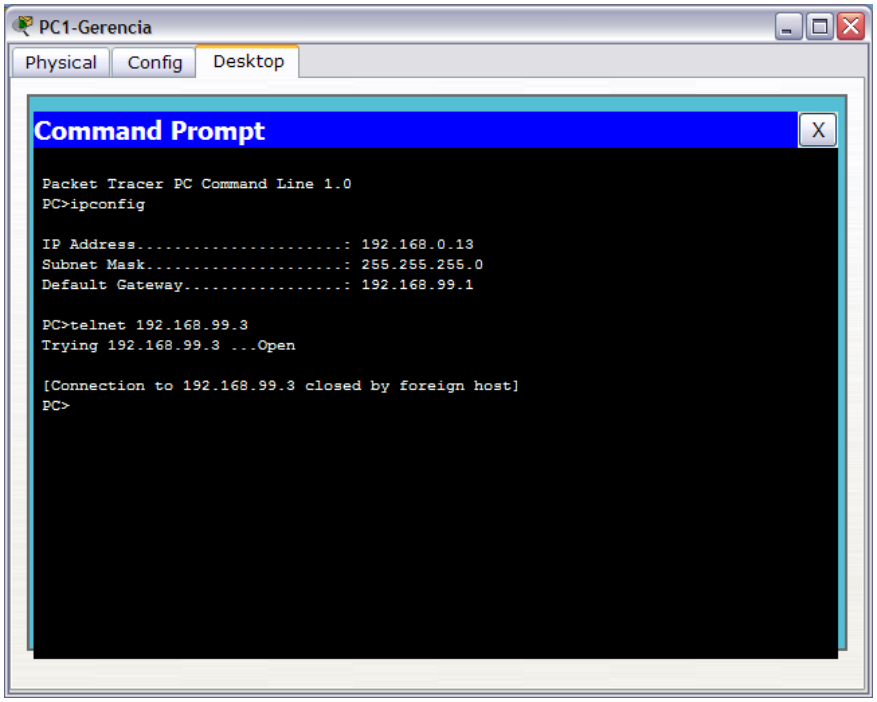


Figura 79. Ping2 para comprobar la traducción de direcciones de NAT



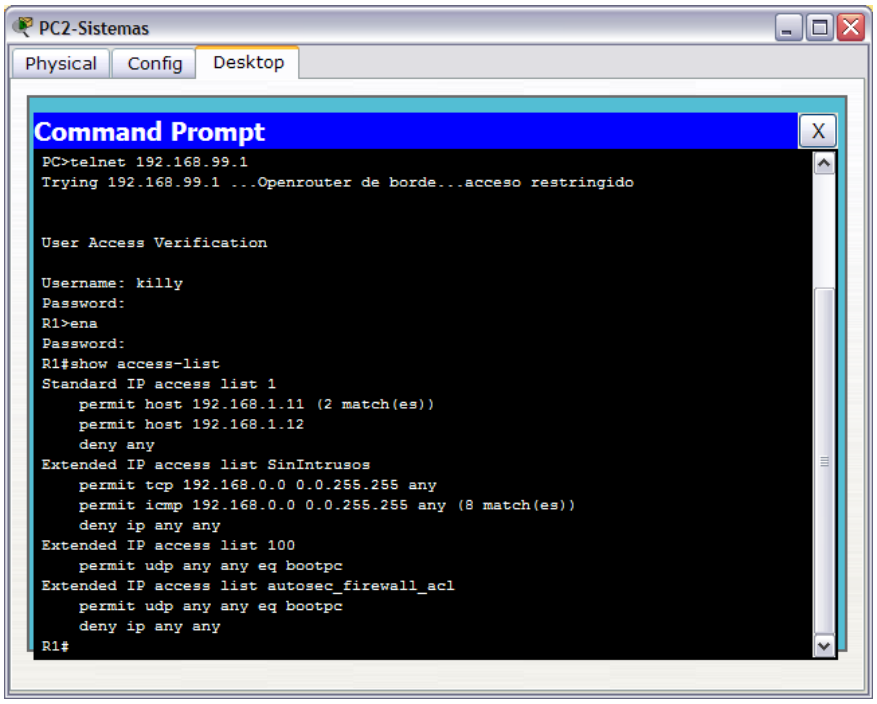
4.4.2.11 Verificación de las listas de acceso ACL. Las líneas VTY de los dispositivos están bloqueadas para todos los miembros de la red menos al departamento de sistemas. La figura 80, muestra como desde un equipo de cómputo en la VLAN de gerencia se tratar de iniciar una sesión de TELNET, pero choca con la ACL impidiendo el acceso.

Figura 80. Verificación de las listas de acceso ACL



En la Figura 81, se observa cuando un equipo de cómputo del departamento de Sistemas, abre una sesión TELNET con el Router R1, el comando “show Access-list”, muestra la forma en que los paquetes golpean contra las ACL, ya sea denegando o permitiendo según los requerimientos del cliente.

Figura 81. Verificación de las listas de acceso ACL



Después de revisar los dos escenarios de simulación se tiene en cuenta el escenario uno (1), porque ofrece gran oportunidad de escalabilidad debido a que un segundo Switch ofrece 24 opciones más de conexión y aunque puede aumentar el costo de implementación para el proyecto, garantiza que VLANs que tienen tres puertos asignados, puedan crecer más debido a que en el Switch2 tendrán otros tres puertos asignados para dicha VLAN, igualmente, si la gerencia lo requiere, el escenario uno (1), ofrece la posibilidad de realizar tareas como agregación de enlaces o Etherchannel.

5 CONCLUSIONES

Se diseñó una red LAN cumpliendo con los estándares y normas técnicas TIA/EIA 568A, TIA/EIA 568B, TIA/EIA 569B, TIA/EIA 606A, garantizando un equilibrio entre acceso y seguridad. Así mismo se utilizó un diseño jerárquico en capas separando el modelo en Núcleo, distribución y acceso, lo que permite una administración más sencilla, una expansión con más facilidad y la resolución de problemas con mayor rapidez. Al momento de diseñar la red de APP MACHINES se buscó una solución total en conectividad, teniendo en cuenta la implementación de los estándares TIA/EIA 568A, TIA/EIA 568B, TIA/EIA 569B, TIA/EIA 606A, para admitir tecnologías actuales y futuras. El cumplimiento de los estándares anteriormente mencionados servirá para garantizar el rendimiento y confiabilidad del proyecto a largo plazo.

Al caracterizar la empresa APP MACHINES Ltda., se encontró que no tenían servidores funcionando ni grupos de trabajo. La conectividad depende del ISP pues al no tener una red para compartir archivos, esta depende de la disponibilidad del canal de Internet. Básicamente la empresa utiliza las aplicaciones de office y navegadores de Internet, por lo que los equipos cumplen los requisitos mínimos de máquina que se necesitan para el diseño.

En el marco de la solución en telecomunicaciones de la empresa APP MACHINES Ltda., se caracterizó la red actual para poder tener un punto de partida en la búsqueda del nuevo diseño, siendo de vital importancia caracterizar todos y cada uno de los elementos que componen una red; se hizo un análisis donde se incluyeron, servidores, grupos de trabajo, conectividad, ancho de banda, tráfico, aplicaciones existentes, además se levantó el inventario de los equipos activos, pasivos y de los enlaces, se buscaron factores de limitaciones, confiabilidad, cuellos de botella, perfiles de los usuarios, para conseguir datos precisos y encontrar los problemas actuales de la empresa y solucionarlos.

El proyecto que se pactó con la empresa APP MACHINES, determinó que el diseño de la red debería ser de forma cableada y no contemplaba la opción de una red inalámbrica. Por esta razón, los análisis se centraron en diseñar una red cableada incluyendo los equipos activos, canaletas, enlaces y equipos de cómputo.

El diseñó sugiere hacer un cambio estructural en la planta física de la empresa. Se necesita crear un cuarto de equipos que cumpla con las normas TIA/EIA 569A y TIA/EIA 606A, el objeto de dicha oficina es salvaguardar los equipos de telecomunicaciones como Servidor, Routers, Switches y UPS, aislándolos de los diferentes sitios de trabajo.

La definición de políticas de gestión de la red para APP MACHINES, surge de la necesidad por mantener una red confiable y disponible, basándose en los requerimientos del cliente. Esto significa un buen aprovechamiento de los recursos. Para ello se crearon y configuraron una VLAN por cada departamento de la empresa, la cual disminuye en un gran porcentaje los dominios de Broadcast, garantizando así que dispositivos que no deben intervenir en la transmisión, procesen el paquete y hagan uso de la red innecesariamente. Esto garantiza una red equilibrada entre seguridad y rendimiento, asegurando alta velocidad y confiabilidad en las conexiones.

Como apoyo al diseño para APP MACHINES se incluye un servidor que debe ser configurado para administrar la red LAN de la empresa. Las políticas de gestión de la red y dicho servidor, deben ofrecer mecanismos de control a los usuarios. Para esto se deberán configurar servicios de autenticación para las estaciones de trabajo, autenticación para navegar en la red, control de contenido en la navegación, control de ancho de banda en las descargas, servicio de servidor de páginas WEB y generación de informes de navegación por usuarios, grupos de usuarios o direcciones IP. Con esto la empresa podrá llevar un control sobre el comportamiento de cada empleado con respecto a la utilización de la red y el desempeño de la misma a lo largo del día, semana o mes. La gerencia de la empresa será la encargada de solicitar los informes al departamento de Sistemas, que servirán para realizar estadísticas o mediciones para controlar el desempeño de los empleados de la empresa.

El diseño se validó mediante la utilización de un programa de simulación llamado Packet Tracer 5.2. Para esto se tuvo en cuenta dos escenarios y se escogió la primera alternativa porque presentaba mayor escalabilidad y permitía la configuración de LINK AGREGATIONS y ETHERCHANNEL.

6 RECOMENDACIONES

Se debe utilizar una metodología de trabajo para recoger la información pertinente para empezar un diseño, incluyendo en todo momento al cliente. Se debe dejar un documento de fácil entendimiento con el fin de que tanto el cliente como los ingenieros puedan comprender la información referenciada.

Se recomienda para la contratación del cableado eléctrico, tener en cuenta el diseño propuesto en este documento, dentro de lo que se encuentran puntos de red, distribución de los equipos de cómputo, sala de telecomunicaciones y equipos activos que se van a utilizar, teniendo en cuenta el diseño propuesto.

El diseño se desarrolló de acuerdo a las normas técnicas vigentes, se recomienda tener en cuenta los diferentes planos para que el diseño trabaje perfectamente, lo que garantiza se eviten en un gran porcentaje los problemas normales de una red.

Con el fin de tener en cuenta a los empleados de la empresa APP MACHINES al momento de poner en práctica las políticas de gestión, se recomienda a la compañía adherir al contrato de trabajo un parágrafo que indique el uso de las políticas de gestión informando los deberes y derechos que cada persona tiene dentro de la red

Dentro del diseño, la parte del cableado eléctrico no se lleva a cabo, debido a que en el campo de la Ingeniería Eléctrica no se tiene la experiencia necesaria para garantizar un buen desempeño de las nuevas instalaciones, por lo que se recomienda a la gerencia de la empresa, la contratación de un entidad experta en el tema, tal como lo exige la norma NTC 2050 y el RETIE.

Se debe capacitar a las personas encargadas de manejar la red de la empresa, estas personas después deberán estar en capacidad de prestar soporte técnico a la red in sitio o en forma remota.

Se debe capacitar el personal de la empresa con el fin de dar claro entendimiento a la aplicación de las políticas de gestión, esto generará que no se encuentren vacios entre los diferentes miembros de la empresa.

Algunos puertos de los Switches han sido configurados para ser puertos de voz. Al momento de incluir VoIP en el diseño, el Dispositivo IP, simplemente se debe conectar al puerto asignado y en dicho puerto habrá prioridad para las tramas de voz ya que irán etiquetadas dentro de la VLAN de voz.

Si la empresa APP MACHINES lo considera conveniente, se recomienda contratar una persona encargada solamente para prestar servicios de soporte a la Red, incluyendo entre otros, monitoreo, generación de informes de navegación, actualización de antivirus, resolver problemas de enrutamiento, problemas de conexión y copias de seguridad periódicas.

Se recomienda a la compañía adquirir los equipos activos propuestos en este diseño, de ser un factor de impedimento la parte económica, se recomienda entonces adquirir equipos con referencias similares de otras marcas.

A la empresa APP MACHINES se recomienda, para que el diseño sea más eficiente, aumentar el valor del presupuesto aprobado, con el fin de mejorar la calidad y la cantidad de los equipos, de manera que se pueda incluir en el diseño, la configuración de un Router fantasma que trabaje silenciosamente al mismo tiempo que el Router R1, garantizando ante un daño en el equipo activo, un reemplazo en caliente, aumentando la confiabilidad y disponibilidad de la red (Redundancia).

La implementación del diseño deberá hacerse lo más pronto posible debido a que las demoras generan que la empresa y la tecnología evolucionen llevando el diseño a un estado en el que no pueda cumplir con los requerimientos del cliente.

Al levantar el inventario de los equipos activos, se encontró que APP MACHINES no tenía un Router para enrutar la red interna de la empresa, la compañía posee un Hub para pegar los equipos al modem que brinda el ISP, por lo que se recomienda la adquisición de uno o varios Switches con el fin de segmentar los dominios de colisión.

Anexo A

Figuras, Mapas y Planos

Anexo B

Correspondencia tramitada con la Empresa APP MACHINES

Anexo C

Informes y demás.

BIBLIOGRAFIA

CISCO System. Desingning Cisco Networks. Cisco System, 1998. 310 P.

ICONTEC, NTC 1486. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Icontec. 2008 p. 115.

ICONTEC, NTC 4353. Telecomunicaciones, cableado estructurado, cableado para telecomunicaciones en edificios comerciales. Icontec. 1997. 130 p.

ISO/IEC, Estándar Internacional ISO/IEC 17799 Segunda edición. 2005. 170 p.

TANENBAUM, Andrew. Redes de computadoras. Amsterdam, The Netherlands. Pearson, 2003. 912 p.

Diccionario Informático "Definición Servidor de Aplicaciones" Disponible en: http://www.alegsa.com.ar/Dic/servidor%20de%20aplicaciones.php Consultado: [12 de Septiembre de 2008, 10:20 am].

Wikipedia "Java Enterprise Edition" Disponible en: http://es.wikipedia.org/wiki**/J2EE** Consultado: **[**12 de Septiembre de 2008, 10:24 am]

Curso Básico de Linux "Linux: Sistema Operativo, Comandos y Utilidad" Disponible en: http://www.senavirtual.edu.co; http://www.gnu.org/software/grub/grub.html Consultado: [12 de Septiembre de 2008, 10:35 am]

ANSI Disponible en: http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1 Consultado: 12 de Septiembre de 2008, 10:45 am

EIA Disponible en: http://www.eia.org/ Consultado: [12 de Septiembre de 2008, 10:45 am]

TIA Disponible en: http://www.tiaonline.org/ Consultado: [12 de Septiembre de 2008, 10:50 am]

IEEE Disponible en:http://www.ieee.org.co/ Consultado: [12 de Septiembre de 2008, 10:53 am]

Pdf. "Redes y Diseño de Cableado Estructurado" disponible en: http://investigacionfitec.googlepages.com/redesydiseodecableadoestructurado.pdf P. 40 Consultado: [12 de Septiembre 2008, 11:00 am]

Microsoft Office Online "Requisitos de la versión Microsoft Office Excel 2007" Disponible en: http://office.microsoft.com/es-hn/word/HA101668653082.aspx Consultado: [8 de Diciembre de 2008, 17:33pm].

Adobe "Requisitos del Sistema para Acrobat Estándar" Disponible en: http://www.adobe.com/es/products/acrobatstd/systemreqs/ Consultado: [8 de Diciembre de 2008, 17:44pm]

MSN Messenger "Requisitos Mínimos del Sistema" Disponible en: http://www.mundodescargas.com/messenger7/messenger_7_5_requisitos.htm Consultado: [8 de Diciembre de 2008, 17:52pm].

SKYPE "Requisitos Mínimos de Máquina" Disponible en: http://www.skype.com/intl/es/download/skype/windows/ Consultado: [8 de Diciembre de 2008, 17:55pm].

INTERNET EXPLORER "Requisitos Mínimos del Sistema) Disponible en: http://www.microsoft.com/spain/windows/downloads/ie/sysreq.mspx Consultado: [8 de Diciembre de 2008, 18:00pm].

Mozilla FireFox "Requisitos Mínimos de Máquina" Disponible en: http://www.mozilla-europe.org/es/firefox/system-requirements/ Consultado: [8 de Diciembre de 2008, 18:06pm].

Fresqui "¿Qué es el Cuello de Botella? - Ingeniería" Disponible en: http://tec.fresqui.com/que-es-el-cuello-de-botella-enginieria Consultado: [25 de Abril de 2009, 09:40am].

MSDN "Identificar Cuellos de Botella" Disponible en: http://msdn.microsoft.com/es-es/library/ms190994(SQL.90).aspx Consultado: [25 de Abril de 2009, 09:47am].

Pdf "Suplemento sobre cableado estructurado" Disponible en: http//www.espoch.edu.ec/descargas/noticias/dacee2_CCNA1_CS_Structured_Cabling_es.pdf P. 27 Consultado: [11 de Agosto de 2009, 10:00 am]

Cisco Networking Academy CCNA Versión 2.1.2 Modulo 1

CISCO Networking Academy "CCNA Exploration 4.0 Aspectos Básicos de Networking"

CISCO Networking Academy "CCNA Exploration 4.0 Conmutación y conexión inalámbrica de LAN"

CISCO Networking Academy "CCNA Exploration 4.0 Acceso a la WAN"