ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Tecnologías

Programa de Especialización Tecnológica
en Electricidad, Electrónica y Telecomunicaciones

PROYECTO DE GRADO

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN CON SISTEMAS DE SEGURIDAD Y CONTROL, DE ACCESO FISICO Y REMOTO AL SISTEMA DE LA EMPRESA IMPORTADORA ARICAMERLUIZ.

Previo a la obtención del Título de:

TECNÓLOGO EN SISTEMAS DE TELECOMUNICACIONES

Presentado por:
Rafael Moroni Lara Gómez

Guayaquil - Ecuador

2014

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Tecnologías

Programa de Especialización Tecnológica en Electricidad, Electrónica y Telecomunicaciones

PROYECTO DE GRADO

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN CON SISTEMAS DE SEGURIDAD Y CONTROL, DE ACCESO FISICO Y REMOTO AL SISTEMA DE LA EMPRESA IMPORTADORA ARICAMERLUIZ.

Previo a la obtención del Título de:

TECNÓLOGO EN SISTEMAS DE TELECOMUNICACIONES

Presentado por:
Rafael Moroni Lara Gómez

Guayaquil - Ecuador

2014

AGRADECIMIENTO

Agradezco a Dios quien me ha guiado, inspirado, y acompañado en todo momento de mi vida física y espiritualmente. A mis padres por su incomparable amor, dedicación y consejo, quienes han logrado que considere a los estudios, parte fundamental en mi vida. Amigos y compañeros de universidad con los que he podido adquirir mayor dedicación y esfuerzo en las tareas asignadas. A nuestros docentes que nos han compartido su conocimiento de tal forma que han sembrado ese deseo de querer aprender, descubrir e innovar en la tecnología.

Rafael Lara Gómez

DEDICATORIA

Dedico el presente trabajo a mis Padres y hermanas por tener siempre la predisposición en ayudarme con lo necesario en mi vida universitaria y personal. A mis grandes amigos con los cuales me he relacionado frecuentemente dándome sabios consejos para alcanzar mis metas personales, educativas y laborales.

Rafael Lara Gómez

TRIBUNAL DE SUSTENTACIÓN

Lcdo. Celso Daniel Jiménez
DELEGADO DEL INTEC

Lcdo. Luis Fernando Franco
DIRECTOR DEL PROYECTO

Lcdo. Diego Armando Muso
VOCAL

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Proyecto de Grado, corresponde exclusivamente al autor; y el patrimonio intelectual del mismo a la Escuela Superior Politécnica del Litoral.

Rafael Moroni Lara Gómez

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

CAPÍTULO 1
INFORMACIÓN GENERAL

1.1 ANTECEDENTES

La compañía Aricamerluiz establecida en el año 1987 tiene como misión principal contribuir al desarrollo social del país, suministrando productos de calidad en una amplia gama de artículos, tales como: electrodomésticos, productos electrónicos, útiles escolares, productos de bazar, juguetería y demás, contando con experiencia, prestigio y acogida de diferentes clientes.

Elementos primordiales que se deben tomar en cuenta en una empresa es la arquitectura de una red, confiabilidad, disponibilidad y seguridad de la información. Uno de los objetivos es lograr que la empresa mantenga niveles de desempeño adecuados en el control y acceso a la información en sus bases de datos, para lo cual se realizará lo siguiente: mantenimiento preventivo del servidor y de los PC de los usuarios, instalación y configuración del servidor en la plataforma Windows Server 2008, creación del dominio aricamerluiz.com, instalación de un biométrico para control de empleados, instalación de cámaras IP para mayor seguridad.

Se ha elaborado una propuesta para la empresa Aricamerluiz en la cual se recomienda equipos de red tales como: servidor, router y switches, para incrementar la optimización y acceso a los datos que se dará mediante el sistema. Se diseñará un nuevo esquema de direccionamiento IP, llevando un control más eficiente y seguro, implicando la utilización de subredes para una adecuada segmentación.

1.2 OBJETIVO GENERAL.

Garantizar el acceso a la información de la empresa Aricamerluiz en sus diferentes departamentos con un nuevo diseño e implementación de red lan, basado en estándares y protocolos, otorgando sistemas de seguridad y protección.

1.3 OBJETIVOS ESPECÍFICOS.

Realizar el diseño lógico y físico de la red con sus respectivas medidas de distancia para la interconexión de los equipos.

Instalar el cableado para los diferentes puntos de red hacia el switch, conexiones del router, conexión de cámaras IP al switch, tomando en cuenta las normas y procedimientos para un buen desempeño de la red.

Suministrar conectividad de usuario a usuario y de usuario a aplicación a una velocidad y confiabilidad razonables.

Facilitar el acceso a recursos compartidos, equipos, programas, drivers que se encuentren en el servidor con limitaciones correspondientes a cada empleado.

Presentar un presupuesto de los equipos e implementos recomendados para tomar en cuenta la arquitectura y escalabilidad de la empresa.

Admitir sistemas de control de asistencia para los empleados mediante biométricos dactilares.

Proporcionar sistemas de monitoreo y supervisión de los empleados permanente y remotamente por medio de cámaras IP configuradas e instaladas en lugares estratégicos.

CAPITULO 2
MARCO TEÓRICO

2.1 REDES DE DATOS

Una red son múltiples computadoras conectadas entre ellas que utilizan sistemas de comunicaciones. El objetivo de una red es que las computadoras se comuniquen y compartan archivos. Las primeras redes de datos estaban limitadas a intercambiar información basada en caracteres entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos, a los diferentes tipos de dispositivos. Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona acceso a una amplia variedad de métodos de comunicación alternativos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

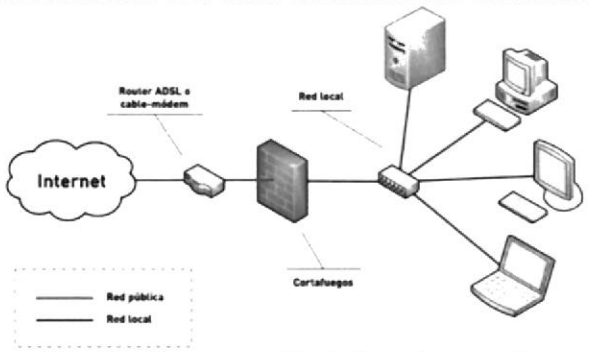


Fig. 2.1: Representación de las redes actuales.
Fuente: http://holomannovoa.blogspot.com/

2.1.1 REDES CONVERGENTES

Los avances de la tecnología nos permiten consolidar las redes dispersas en una única plataforma: una plataforma definida como una red convergente. El flujo de voz, vídeo y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas. En una red convergente todavía hay muchos puntos de contacto y muchos dispositivos especializados (por ejemplo: computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas) pero una sola infraestructura de red común.

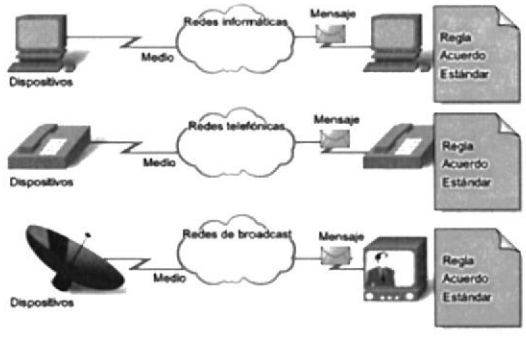


Fig. 2.2: Redes convergentes.
Fuente: http://argentows.blogspot.com/

ARQUITECTURA DE RED

El término arquitectura de red, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

TOLERANCIA A FALLAS

Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo.

ESCALABILIDAD

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica.

CALIDAD DE SERVICIO (QoS)

Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad. Los nuevos requerimientos para admitir esta calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas de red.

SEGURIDAD

Las expectativas de privacidad y seguridad que se originan del uso de internetworks para intercambiar información empresarial crítica y confidencial exceden lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red.

2.1.2 MEDIOS DE RED

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.
Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:

- Hilos metálicos dentro de los cables,

- Fibras de vidrio o plásticas (cable de fibra óptica), y
- Transmisión inalámbrica.

La codificación de señal que se debe realizar para que el mensaje sea transmitido es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- la distancia en la cual el medio puede transportar exitosamente una señal,
- el ambiente en el cual se instalará el medio,
- la cantidad de datos y la velocidad a la que se deben transmitir, y
- el costo del medio y de la instalación.

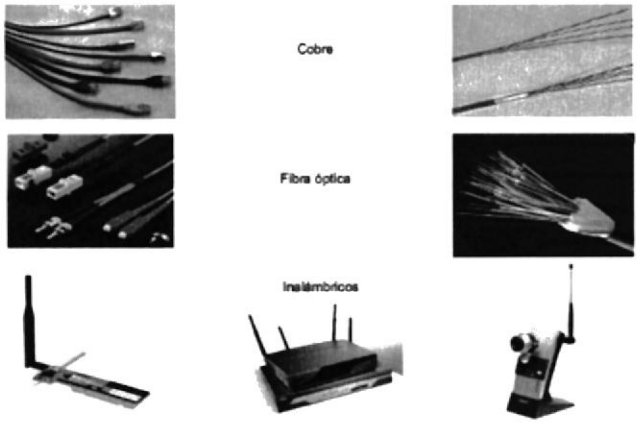


Fig. 2.3: Medios de red.
Fuente: www.cisco.com

2.1.3 MODELO DE PROTOCOLO TCP/IP

Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo ***TCP/IP*** es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

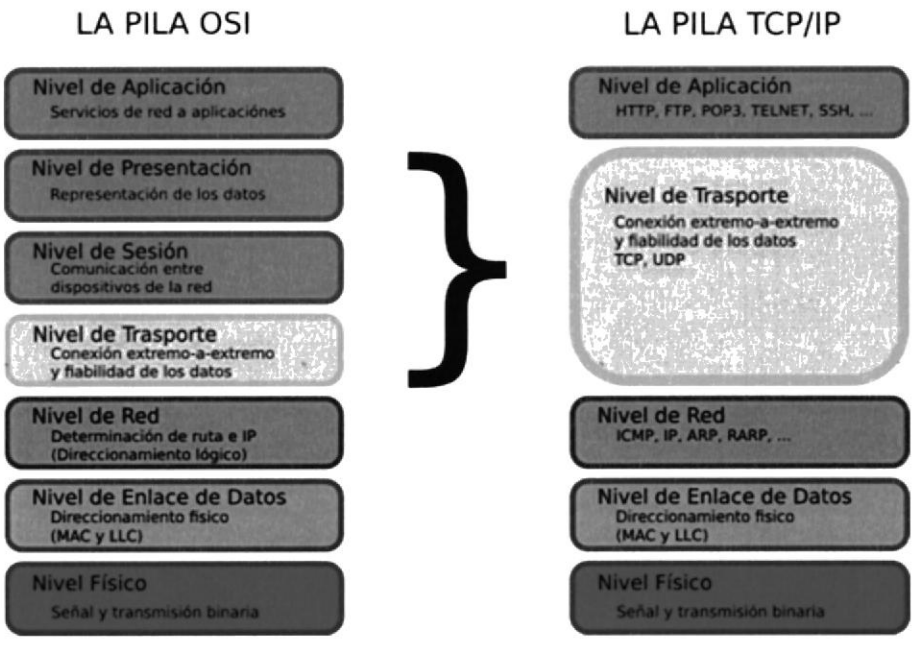


Fig. 2.4: Modelos de Referencia y Protocolo (OSI-TCP/IP)
Fuente: purogeek.wordpress.com

SERVIDORES

Un servidor generalmente es una computadora que contiene información para ser compartida con muchos sistemas de cliente. Por ejemplo, páginas Web, documentos, bases de datos, imágenes, archivos de audio y vídeo pueden almacenarse en un servidor y enviarse a los clientes que lo solicitan. Diferentes tipos de aplicaciones del servidor tienen diferentes requerimientos para el acceso de clientes. Algunos servidores pueden requerir de autenticación de la información de cuenta del usuario para verificar si el usuario tiene permiso para acceder a los datos solicitados o para utilizar una operación en particular.

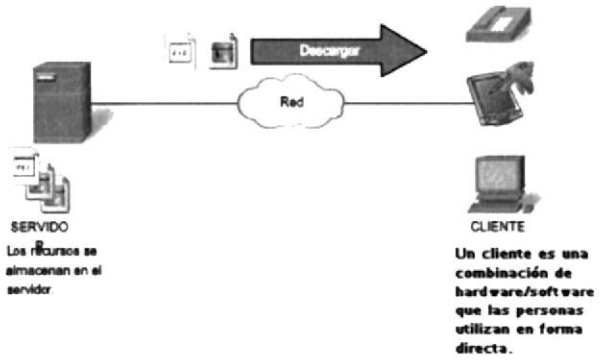


Fig. 2.5: Modelo Cliente-Servidor
Fuente: www.cisco.com

ANCHO DE BANDA

La capacidad que posee un medio de transportar datos se describe como el ancho de banda de los datos sin procesar de los medios. El ancho de banda digital mide la cantidad de información que puede fluir desde un lugar hacia otro en un período de

tiempo determinado. El ancho de banda generalmente se mide en kilobits por segundo (kbps) o megabits por segundo (Mbps).

El ancho de banda práctico de una red se determina mediante una combinación de factores: las propiedades de las tecnologías y los medios físicos elegidos para señalizar y detectar señales de red.

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = fundamental unit of bandwidth
Kilobits por segundo	kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

Fig2.6: Unidades de ancho de banda.
Fuente: www.cisco.com

2.1.4 CABLE DE PAR TRENZADO NO BLINDADO (UTP)

El cableado de par trenzado no blindado (UTP), como se utiliza en las LAN Ethernet, consiste en cuatro pares de alambres codificados por color que han sido trenzados y cubiertos por un revestimiento de plástico flexible. Los códigos de colores identifican los pares individuales con sus alambres y sirven de ayuda para la terminación de cables.

El trenzado cancela las señales no deseadas. Cuando dos alambres de un circuito eléctrico se colocan uno cerca del otro, los campos electromagnéticos externos crean la misma interferencia en cada alambre. Los pares se trenzan para mantener los alambres lo más cerca posible. Cuando esta interferencia común se encuentra en los alambres del par trenzado, el receptor los procesa de la misma manera pero en forma opuesta. Como resultado, las señales provocadas por la interferencia electromagnética desde fuentes externas se cancelan de manera efectiva.

TIPOS DE CABLE UTP

El cableado UTP, con una terminación de conectores RJ-45, es un medio común basado en cobre para interconectar dispositivos de red, como computadoras, y dispositivos intermedios, como routers y switches de red.

Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados. Esto significa que los alambres individuales del cable deben conectarse en diferentes órdenes para distintos grupos de pines en los conectores RJ-45. A continuación se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado: [1]

- Cable directo de Ethernet
- Cruzado de Ethernet
- Consola

Tipo de cable	Estándar	Aplicación
Cable directo de Ethernet	Un extremo T568A, otro extremo T568B	Conexión de un host de red a un dispositivo de red como un switch o hub.
Cruzado Ethernet	Un extremo T568A, otro extremo T568B	Conexión de dos hosts de red. Conexión de dos dispositivos intermediarios de red (switch a switch o router a router).
Transpuesto	Propietario de Cisco	Conecte el puerto serial de una estación de trabajo al puerto de consola de un router utilizando un adaptador.

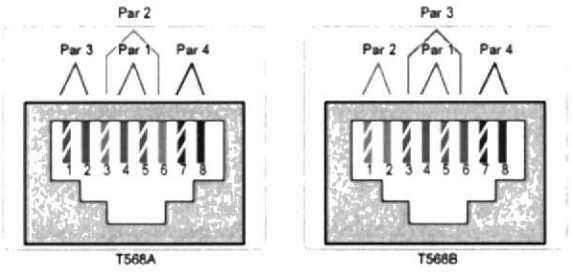


Fig2.7: Tipos de cable directo, conexión cruzada y transpuesto.
Fuente: www.cisco.com

2.2 RED DE AREA LOCAL (LAN)

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina Red de área local. Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

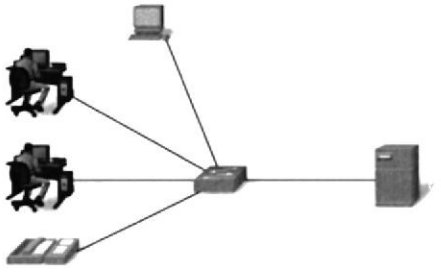


Fig. 2.8: Red de área local (LAN)
Fuente: www.cisco.com

2.2.1 CONEXIONES LAN

La Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) establecen las conexiones del cableado UTP.

El conector RJ-45 es el componente macho engarzado al extremo del cable. Cuando se observan desde el frente, los pines se numeran del 8 al 1. Cuando se observan desde arriba con la entrada de apertura frente a usted, los pines se enumeran del 1 al 8, de izquierda a derecha. Es importante recordar esta orientación al identificar un cable.

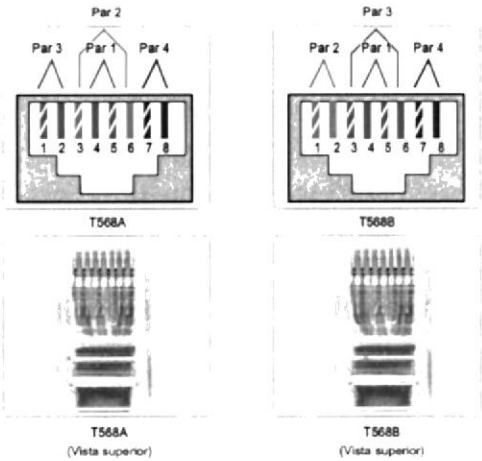


Fig2.9: Rj45 T568A y terminación T568B.
Fuente: www.cisco.com

TIPOS DE INTERFACES

En una LAN Ethernet, los dispositivos utilizan uno de los dos tipos de interfaces UTP: MDI o MDIX.

La MDI (interfaz dependiente del medio) utiliza un diagrama de pines normal de Ethernet. Los pines 1 y 2 se utilizan como transmisores y los pines 3 y 6 como receptores. Dispositivos como computadoras, servidores o routers tendrán conexiones MDI.
Los dispositivos que proporcionan la conectividad a la LAN (por lo general, hubs o switches) habitualmente utilizan conexiones MDIX (Interfaz cruzada dependiente del medio).

Los cables MDIX intercambian los pares transmisores internamente. Este intercambio permite que los dispositivos finales se encuentren conectados a un hub o switch utilizando un cable de conexión directa.

En general, cuando conecte diferentes tipos de dispositivos, utilice un cable de conexión directa. Cuando conecte el mismo tipo de dispositivo, utilice un cable de conexión cruzada.

2.2.2 CABLES UTP DE CONEXIÓN DIRECTA

Un cable de conexión directa tiene conectores en cada extremo y su terminación es idéntica conforme a los estándares T568A o T568B.
La identificación del estándar del cable utilizado le permite determinar si cuenta con el cable correcto para un determinado trabajo. Más importante aún, es normal utilizar los mismos códigos de color en toda la LAN para lograr consistencia en la documentación.

Utilice cables directos para las siguientes conexiones:
- Switch a puerto Ethernet del router
- Equipo a switch
- Equipo a hub

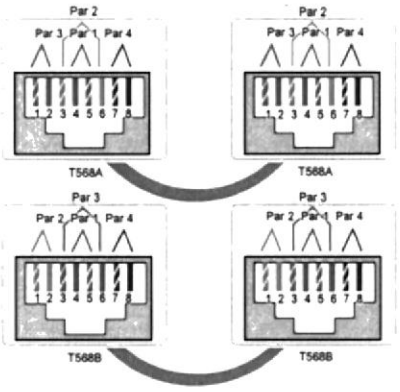


Fig2.10: Cables de conexión directa con terminaciones T568A y T568B.
Fuente: www.cisco.com

2.2.3 CABLES UTP DE CONEXIÓN CRUZADA

Para que los dos dispositivos se comuniquen a través de un cable directamente conectado entre los dos, el terminal transmisor de uno de los dispositivos necesita conectarse al terminal receptor del otro dispositivo.

El cable debe tener una terminación para que el pin transmisor, Tx, que toma la señal desde el dispositivo A en un extremo, se conecte al pin receptor, Rx, en el dispositivo B.

De manera similar, el pin Tx del dispositivo B debe estar conectado al pin Rx del dispositivo A. Si el pin Tx de un dispositivo tiene el número 1 y el pin Rx tiene el número 2, el cable conecta el pin 1 en un extremo con el pin 2 en el otro extremo. Este tipo de cable se denomina "de conexión cruzada" por estas conexiones de pin cruzadas.

Para alcanzar este tipo de conexión con un cable UTP, un extremo debe tener una terminación como diagrama de pin EIA/TIA T568A y el otro, como T568B.

En resumen, los cables de conexión cruzada conectan directamente los siguientes dispositivos en una LAN:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a conexión del puerto Ethernet del router
- Equipo a equipo
- Equipo a puerto Ethernet del router

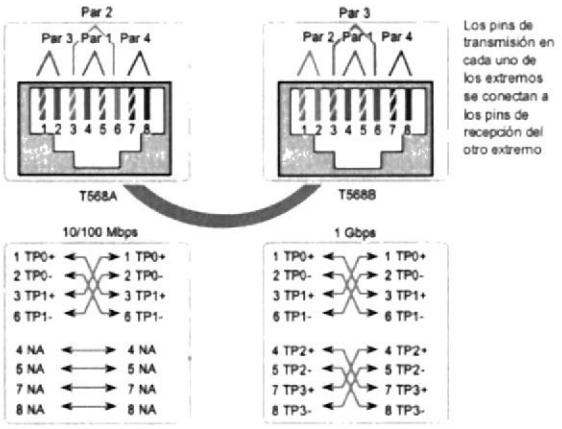


Fig2.11: Conexión Cruzada T568A y T568B del otro extremo.
Fuente: www.cisco.com

2.2.4 MEDIOS INALÁMBRICOS

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. Los dispositivos y usuarios que no están autorizados a ingresar a la red pueden obtener acceso a la transmisión, ya que la cobertura de la comunicación inalámbrica no requiere el acceso a una conexión física de los medios. Por lo tanto, la seguridad de la red es el componente principal de la administración de redes inalámbricas.

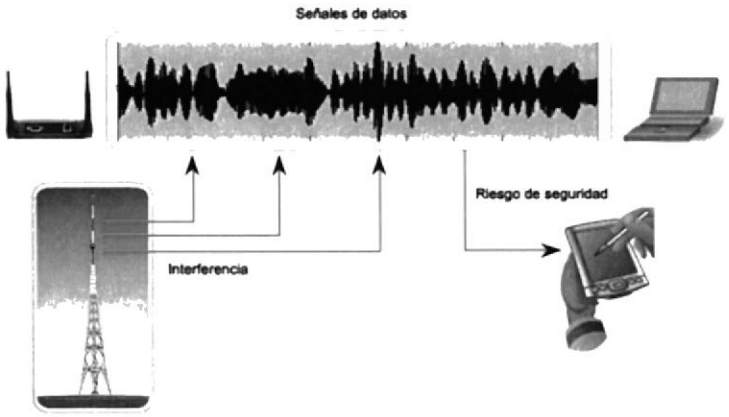


Fig2.12: Seguridad y señales de medios inalámbricos.
Fuente: www.cisco.com

LAN INALÁMBRICA

Una implementación común de transmisión inalámbrica de datos permite a los dispositivos conectarse en forma inalámbrica a través de una LAN. En general, una LAN inalámbrica requiere los siguientes dispositivos de red:
Punto de acceso inalámbrico (AP): Concentra las señales inalámbricas de los usuarios y se conecta, generalmente a través de un cable de cobre, a la infraestructura de red existente basada en cobre, como Ethernet.

Adaptadores NIC inalámbricos: Proporcionan capacidad de comunicación inalámbrica a cada host de la red. [11]

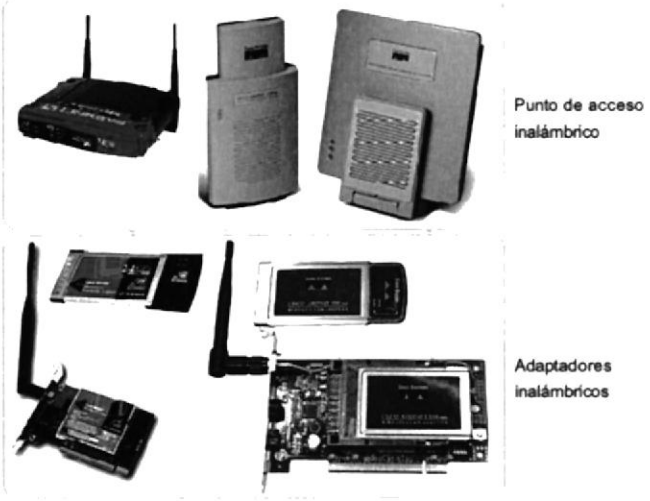


Fig2.13: Adaptadores y puntos de acceso de una red inalámbrica.
Fuente: www.cisco.com

2.3 ETHERNET

Ethernet es en la actualidad la tecnología LAN preponderante a nivel mundial, se compone de estándares en las capas inferiores, puede decirse que en términos generales se entiende mejor con referencia al modelo OSI. El modelo OSI separa las funcionalidades de la capa de Enlace de datos de direccionamiento, entramado y acceso a los medios desde los estándares de la capa física de los medios. Los estándares de Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. Si bien las especificaciones de Ethernet admiten diferentes medios, anchos de banda y otras variaciones de Capa 1 y 2, el formato de trama básico y el esquema de direcciones son los mismos para todas las variedades de Ethernet.

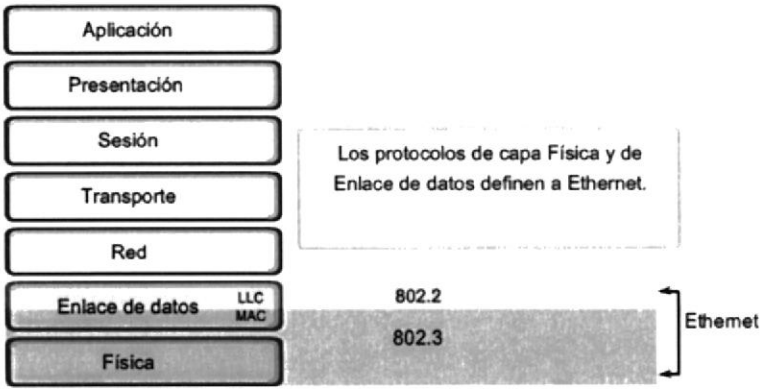


Fig2.14: Estándares e Implementación.
Fuente: www.cisco.com

Ethernet opera a través de dos capas del modelo OSI. El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se conoce como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

Ethernet en la Capa 1 implica señales, streams de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones.

Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación.

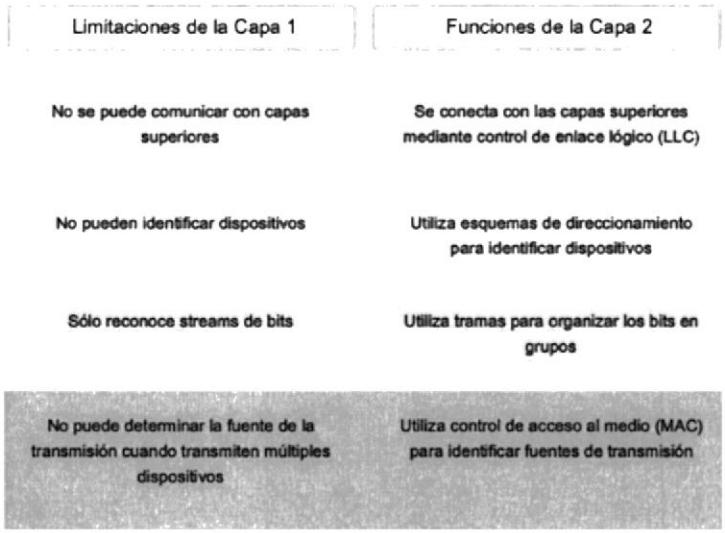


Fig2.15: Funciones de la capa 2, limitaciones de la capa 1.
Fuente: www.cisco.com

CONTROL DE ACCESO AL MEDIO (MAC)

El Control de acceso al medio (MAC) es la subcapa de Ethernet inferior de la capa de Enlace de datos. El hardware implementa el Control de acceso al medio, generalmente en la Tarjeta de interfaz de red (NIC).

ENCAPSULACIÓN DE DATOS

La encapsulación de datos proporciona tres funciones principales:

- Delimitación de trama
- Direccionamiento
- Detección de errores

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir una trama. Cuando forma una trama, la capa MAC agrega un encabezado y un tráiler a la PDU de Capa 3. La

utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor.

El proceso de encapsulación también posibilita el direccionamiento de la capa de Enlace de datos. Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.

Una función adicional de la encapsulación de datos es la detección de errores. Cada trama de Ethernet contiene un tráiler con una comprobación cíclica de redundancia (CRC) de los contenidos de la trama. Una vez que se recibe una trama, el nodo receptor crea una CRC para compararla con la de la trama. Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

2.3.1 TOPOLOGÍA ESTRELLA

Lo más usual en esta topología es que en un extremo del segmento se sitúe un nodo y el otro extremo se termine en una situación central con un concentrador. La principal ventaja de este tipo de red es la fiabilidad, dado que si uno de los segmentos tiene una falla, afectará solo al nodo conectado a él. Otros usuarios de los ordenadores de la red continuarán operando como si ese segmento no existiera. 10BASE-T Ethernet y fast Ethernet son ejemplos de esta topología.

TOPOLOGÍA LÓGICA

La topología lógica subyacente de Ethernet es un bus de multiacceso. Esto significa que todos los nodos (dispositivos) en ese segmento de la red comparten el medio. Esto significa además que todos los nodos de ese segmento reciben todas las tramas transmitidas por cualquier nodo de dicho segmento.

Debido a que todos los nodos reciben todas las tramas, cada nodo debe determinar si debe aceptar y procesar una determinada trama. Esto requiere analizar el direccionamiento en la trama provisto por la dirección MAC.

Ethernet ofrece un método para determinar cómo comparten los nodos el acceso al medio. El método de control de acceso a los medios para Ethernet clásica es el Acceso múltiple con detección de portadora con detección de colisiónes (CSMA/CD).

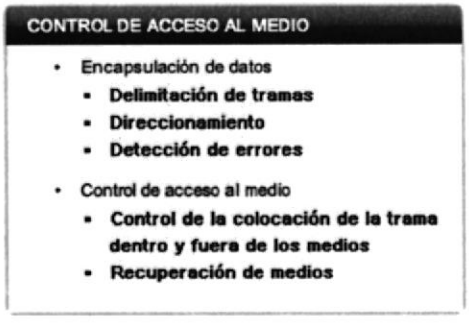


Fig2.16: Proceso de cómo llevar los datos a los medios.
Fuente: www.cisco.com

2.3.2 ETHERNET ACTUAL

Un desarrollo importante que mejoró el rendimiento de la LAN fue la introducción de los switches para reemplazar los hubs en redes basadas en Ethernet. Este desarrollo estaba estrechamente relacionado con el desarrollo de Ethernet 100BASE-TX. Los switches pueden controlar el flujo de datos mediante el aislamiento de cada uno de los puertos y el envío de una trama sólo al destino correspondiente (en caso de que se lo conozca) en vez del envío de todas las tramas a todos los dispositivos.

El switch reduce la cantidad de dispositivos que recibe cada trama, lo que a su vez disminuye o minimiza la posibilidad de colisiones. Esto, junto con la posterior introducción de las comunicaciones full-duplex (que tienen una conexión que puede transportar señales transmitidas y recibidas al mismo tiempo), permitió el desarrollo de Ethernet de 1 Gbps y más.

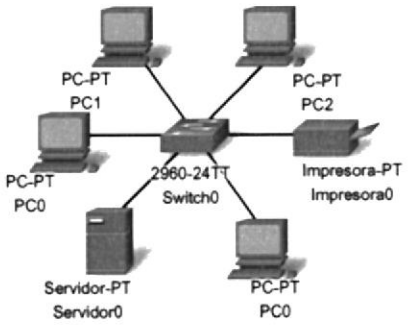


Fig2.17: Ethernet actual basada en SWITCH.
Fuente: www.cisco.com

LATENCIA

La señal eléctrica que se transmite requiere una cantidad determinada de tiempo (latencia) para propagarse (viajar) a través del cable. Cada hub o repetidor en la ruta de la señal agrega latencia a medida que envía los bits desde un puerto al siguiente.

Este retardo acumulado aumenta la probabilidad de que se produzcan colisiones, porque un nodo de escucha puede transformarse en señales de transmisión mientras el hub o repetidor procesa el mensaje. Debido a que la señal no había alcanzado este nodo mientras estaba escuchando, dicho nodo pensó que el medio estaba disponible. Esta condición produce generalmente colisiones.

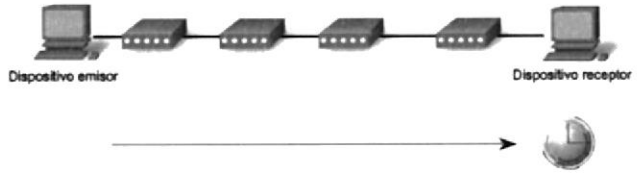


Fig2.18: Retardo Ethernet (latencia)
Fuente: www.cisco.com

DESCRIPCIÓN GENERAL DE LA CAPA FÍSICA DE ETHERNET

Las diferencias que existen entre Ethernet estándar, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet tienen lugar en la capa física, generalmente denominada *Ethernet PHY*.

La Ethernet se rige por los estándares IEEE 802.3. Actualmente, se definen cuatro velocidades de datos para el funcionamiento con cables de fibra óptica y de par trenzado:

Tipo de Ethernet	Ancho de banda	Tipo de cable	Duplex	Distancia máxima
10Base-5	10 Mbps	Coaxial thicknet	Half	500 m
10Base-2	10 Mbps	Coaxial thinnet	Half	185 m
100Base-TX	10 Mbps	UTP Cat3/Cat5	Half	100 m
100Base-TX	100 Mbps	UTP Cat5	Half	100 m
100Base-TX	200 Mbps	UTP Cat5	Full	100 m
100Base-TX	100 Mbps	Fibra multimodo	Half	400 m
1000Base-T	200 Mbps	Fibra multimodo	Full	2 km
1000Base-TX	1 Gbps	UTP Cat5e	Full	100 m
1000Base-SX	1 Gbps	UTP Cat6	Full	100 m
1000Base-LX	1 Gbps	Fibra multimodo	Full	550 m
10GBase-CX4	1 Gbps	Fibra monomodo	Full	2 km
10GBase-T	10 Gbps	Twinaxial	Full	100 m
10GBase-LX4	10 Gbps	UTP Cat6a/Cat7	Full	100 m
10GBase-LX4	10 Gbps	Fibra multimodo	Full	300 m
10 Mbps	10 Gbps	Fibra monomodo	Full	10 km

Fig2.19: Tipos de Ethernet.
Fuente: www.cisco.com

100 Mbps - FAST ETHERNET

Entre mediados y fines de la década de 1990 se establecieron varios estándares 802.3 nuevos para describir los métodos de transmisión de datos en medios Ethernet a 100 Mbps. Estos estándares utilizaban requisitos de codificación diferentes para lograr estas velocidades más altas de transmisión de datos.

La Ethernet de 100 Mbps, también denominada Fast Ethernet, puede implementarse utilizando medios de fibra o de cable de cobre de par trenzado. Las implementaciones más conocidas de la Ethernet de 100 Mbps son:
100BASE-TX con UTP Cat5 o mayor
100BASE-FX con cable de fibra óptica

Ya que las señales de mayor frecuencia que se utilizan en Fast Ethernet son más susceptibles al ruido, Ethernet de 100 Mbps utiliza dos pasos de codificación por separado para mejorar la integridad de la señal.

100BASE-TX

100BASE-TX fue diseñada para admitir la transmisión a través de dos hilos de fibra óptica o de dos pares de cable de cobre UTP de Categoría 5. La implementación 100BASE-TX utiliza los mismos dos pares y salidas de pares de UTP que la 10BASE-

T. Sin embargo, la 100BASE-TX requiere UTP de Categoría 5 o superior. La codificación 4B/5B se utiliza para la Ethernet 100BASE-T.

1000 Mbps - Gigabit Ethernet

El desarrollo de los estándares de Gigabit Ethernet dio como resultado especificaciones para cobre UTP, fibra monomodo y fibra multimodo. En redes de Gigabit Ethernet, los bits se producen en una fracción del tiempo que requieren en redes de 100 Mbps y redes de 10 Mbps. Gracias a que las señales se producen en menor tiempo, los bits se vuelven más susceptibles al ruido y, por lo tanto, la temporización tiene una importancia decisiva. La cuestión del rendimiento se basa en la velocidad con la que el adaptador o la interfaz de red puedan cambiar los niveles de voltaje y en la manera en que dicho cambio de voltaje pueda detectarse de un modo confiable a 100 metros de distancia en la NIC o la interfaz de recepción.

2.3.3 UTILIZACIÓN DE SWITCHES

En los últimos años, los switches se convirtieron rápidamente en una parte fundamental de la mayoría de las redes. Los switches permiten la segmentación de la LAN en distintos dominios de colisiones. Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto. Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

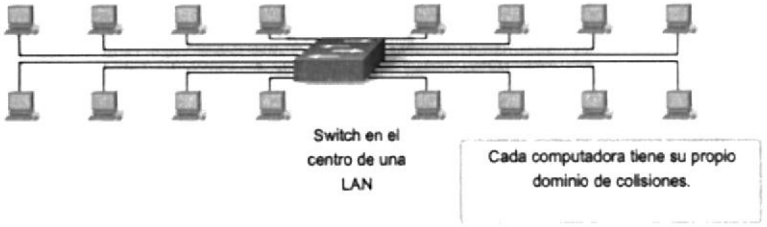


Fig2.20: Lan que utiliza un switch .
Fuente: www.cisco.com

2.3.4 ROUTER

Son los dispositivos principales utilizados para interconectar redes. Cada puerto de un router se conecta a una red diferente y realiza el enrutamiento de los paquetes entre las redes.
Los routers tienen la capacidad de dividir dominios de broadcast y dominios de colisiones. También pueden utilizarse para interconectar redes que utilizan diferentes tecnologías. Los routers pueden tener interfaces LAN y WAN.

Las interfaces LAN del router permiten a los routers conectarse a los medios LAN. Para esto generalmente se utiliza un cableado de UTP (Par trenzado no blindado), pero se pueden agregar módulos con fibra óptica. Según la serie o el modelo del router, puede haber diferentes tipos de interfaces para la conexión del cableado WAN y LAN.

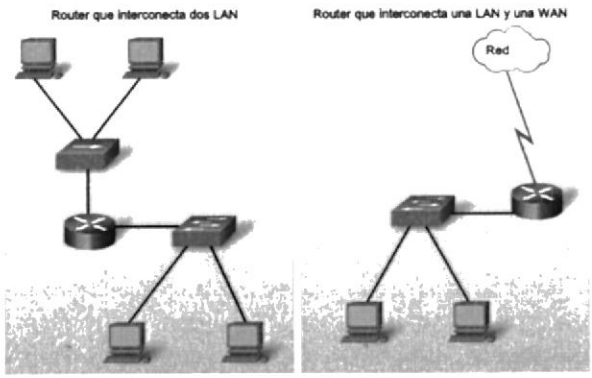


Fig2.21: Conexión de internetwork con un router.
Fuente: www.cisco.com

2.3.5 FIREWALL

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.

En la siguiente ilustración se muestra el funcionamiento de un firewall.

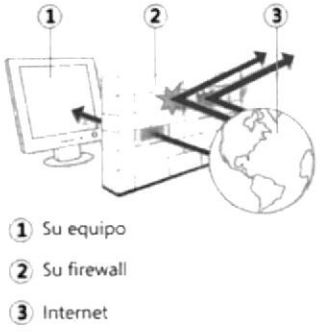


Fig. 2.22: Firewall
Fuente: http://windows.microsoft.com

Un firewall crea una barrera entre Internet y el equipo, igual que la barrera física que constituiría una pared de ladrillos.
Un firewall no es lo mismo que un programa antivirus. Para ayudar a proteger su equipo, necesita tanto un firewall como un programa antivirus y antimalware. [1]

2.4 WINDOWS SERVER 2008

Es un sistema operativo de Microsoft diseñado para servidores, además de ofrecer a las organizaciones la plataforma más productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces de protección de redes. Ofrece una plataforma segura y fácil de administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Del grupo de trabajo al centro de datos, Windows Server 2008 incluye nuevas funciones de gran valor y eficacia y mejores impactantes en el sistema operativo base.

Fig.2.23: Presentación de Windows Server 2008
Fuente: www.microsoft.com

CARACTERÍSTICAS GENERALES

Identificación y acceso a la infraestructura de la red
Seguridad y políticas
Implementación rápida
Servicios de administración sencilla
Soporte para tareas de oficina
Soporte para acceso centralizado a las aplicaciones
Implementación de Servicios y Aplicaciones Web
Confiabilidad
Protección de datos
Incremento de la productividad con Hyper-V

2.4.1 ROLES DE WINDOWS SERVER 2008

Un rol del servidor describe la función principal del servidor. Los administradores pueden optar por dedicar todo un servidor para un rol, o instalar múltiples roles del servidor en un único equipo. Cada rol puede incluir uno o más servicios del rol, u opcionalmente instalar elementos del rol. Los siguientes roles están disponibles en Windows Server 2008 y pueden ser instalados y administrados usando Server Manager: [2]

Nombre del Rol	Descripción
Servicios de Dominio Active Directory	Active Directory Domain Services (AD DS) almacena información sobre usuarios, computadoras, y otros dispositivos de la red. AD DS ayuda a los administradores de seguridad a gestionar esta información.
Servidor de Aplicación	El servidor de aplicación proporciona una solución completa para la organización y gestión de aplicaciones empresariales distribuidas, de alto rendimiento.
Dynamic Host Configuration Protocol (DHCP) Server	El protocolo de configuración dinámica de servidores permite asignar, o arrendar direcciones IP a computadoras y otros dispositivos que estén habilitados como clientes DHCP.
Servidor DNS	Sistema de nombres de dominio (DNS) proporciona un método estándar para asociar los nombres con las direcciones numéricas de Internet.
Servicios de Archivo	Los Servicios de Archivo proporcionan las tecnologías para la administración de almacenamiento, repetición de archivos, gestión de nombres distribuidos, búsqueda rápida de archivos, y racionalizar el acceso de los clientes a los archivos.
Política de Red y Servicios de Acceso	Con los servicios de acceso a la red, usted puede desplegar servidores VPN, servidores de acceso telefónico, enrutadores, y acceso inalámbrico protegido 802.11.
Servicios de Impresión	Los servicios de impresión permiten la administración de servidores de impresión e impresoras.
Servidor Web (IIS)	El servidor Web (IIS) permite el intercambio de información en la Internet, una Intranet, o una extranet. Se trata de una plataforma unificada que integra Web ISS 7.0, ASP.NET, y Windows Comunication Foundation.
Hyper-V	Hyper-V proporciona los servicios que usted puede utilizar para crear y gestionar máquinas virtuales y sus recursos. Cada máquina virtual opera en un entorno de ejecución aislado. Esto le permite ejecutar múltiples sistemas operativos simultáneamente. Disponible únicamente en ediciones de 64 bits, por el momento.

Tabla 2.1: Roles de Windows Server 2008
Fuente: www.microsoft.com

2.5 CÁMARA IP

Una Cámara IP (también conocida como cámara Web o de Red) es una videocámara especialmente diseñada para enviar las señales (video, y en algunos casos audio) a través de Internet desde un navegador (por ejemplo el Internet Explorer, Google Chrome, Safari, etc.) o a través de un concentrador (un HUB o un SWITCH) en una Red Local (LAN).

En este tipo de cámaras se pueden integrar aplicaciones como detección de presencia (incluso el envío de mail si detectan presencia), grabación de imágenes o secuencias en equipos informáticos (tanto en una red local o en una red externa (WAN), de manera que se pueda comprobar el porque ha saltado la detección de presencia y se graben imágenes de lo sucedido.

Entre los elementos que integran una cámara IP podemos citar, además de la cámara propiamente dicha, un compresor de imagen (normalmente a MPEG4), un sistema de procesamiento de datos y un sistema de conexión Ethernet o Wifi, así como los mecanismos y motorizaciones necesarias para su manejo (en el caso de las motorizadas)

Esto reporta una serie de ventajas sobre una webcam normal, tales como la de estar conectada permanentemente al concentrador, y por lo tanto a Internet si tenemos una conexión ADSL, sin que dependa de un PC, requiriendo tan solo la conexión al concentrador o router (ya sea via cable UTP o via Wifi) y una alimentación (que puede ser tanto una toma directa a la red eléctrica como mediante baterías). Estas cámaras son ideales sobre todo cuando queremos controlar un determinado emplazamiento alejado de donde nos encontramos. Su uso más frecuente es el de video vigilancia a través de Internet, lo que nos permite controlar, por ejemplo, un negocio que se encuentra a cientos o miles de kilómetros.

En el mercado hay una gran variedad de este tipo de cámaras, tanto para interior como protegidas para su instalación en exteriores, con sonido e imagen y conectadas mediante cable UTP o via Wifi. También las hay tanto fijas como motorizadas, lo que nos permite controlarlas a través del programa de visualización, con detectores de movimiento, con la posibilidad de conectarle sensores adicionales (de humo, de iluminación...) incluso con la posibilidad de que nos avisen via E-Mail en caso de detectar movimiento en horarios programados. [3]

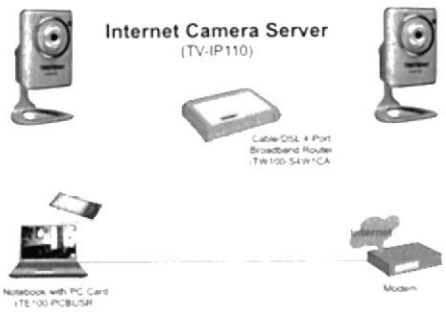


Fig. 2.24: Esquema de conexión de cámaras IP
Fuente: www.trendnet.com

2.6 CONTROL DE ACCESO BIOMÉTRICO

La biometría es una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo, la huella digital, el reconocimiento del patrón venoso del dedo o el reconocimiento facial. La biometría es un excelente sistema de identificación de la persona que se aplica en muchos procesos debido a dos razones fundamentales, la seguridad y la comodidad.

Entre las aplicaciones de identificación con biometría están el control de acceso biométrico, el control de presencia biométrico, el logon biométrico para aplicaciones de software a sistemas operativos o cualquier otra aplicación de identificación mediante la incorporación de un lector biométrico para integración.
La biometría es un sistema que reconoce a la persona basándose en "quién es", no importando "el qué lleva puesto" o "lo que conoce".

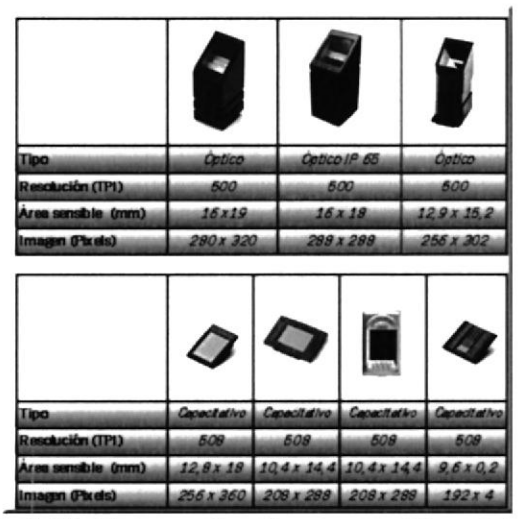
Cosas que puedan llevar, como las llaves y tarjetas de identificación, pueden ser perdidas, sustraídas y/o duplicadas. Cosas que conoce, como passwords y códigos, pueden ser olvidados, sustraídos y/o duplicados.
En lugar de eso, la tecnología biométrica se fija en "quién" es la persona, basándose en una única e inalterable característica humana que no puede ser perdida, olvidada, sustraída o duplicada.

Fig. 2.25: Biometría dactilar
Fuente: www.sistemasbiometricos.co

TIPOS DE SENSORES BIOMETRICOS DE HUELLA

El sensor es el dispositivo capaz de leer las características de una huella. Existen dos tecnologías de lectura mediante lectores ópticos o capacitivos. Son muy fáciles de identificar ya que los ópticos tienden a estar iluminados y con filtro de cristal. Los capacitivos, para la lectura, debemos tocar directamente el sensor.

A medida que han mejorado las capacidades de lectura de los sensores han aumentado los niveles de seguridad y disminuido las falsas lecturas permitiendo captar en cada lectura pequeños matices que ayudan a determinar la autenticidad de la huella. Tan solo hace unos años era habitual que los mejores fabricantes dieran como normal más de un 5% de falsas lecturas, hoy en día encontramos fabricantes que están por debajo del 1%.
Es habitual encontrar en grandes instalaciones donde se manejen miles de usuarios y se requiera un gran nivel de seguridad, que los lectores de huella vayan ligados a un identificador adicional tipo teclado o tarjeta, ya que esto permite comparar la huella leída y relacionarla directamente con el PIN, dando como resultado la comparación directa de una sola huella en la base de datos.[4]



Tipo	Óptico	Óptico IP 65	Óptico
Resolución (TPI)	500	500	500
Área sensible (mm)	16 x 19	16 x 18	12,9 x 15,2
Imagen (Pixels)	280 x 320	288 x 288	256 x 302

Tipo	Capacitativo	Capacitativo	Capacitativo	Capacitativo
Resolución (TPI)	508	508	508	508
Área sensible (mm)	12,8 x 18	10,4 x 14,4	10,4 x 14,4	9,6 x 0,2
Imagen (Pixels)	256 x 360	208 x 288	208 x 288	192 x 4

Fig. 2.26: Comparativa de sensores biometricos
Fuente: http://control-accesos.es/

2.7 DIRECCIONAMIENTO IP

Toda la estructura de Internet se basa en los protocolos TCP/IP. La Internet constituye una gran red virtual, ya que consiste en la interconexión de redes físicas mediante enrutadores. Los Enrutadores mantienen ocultas las distintas tecnologías de hardware existentes en la red, es por ello que utilizan un esquema de direccionamiento lógico, que permite encaminar los paquetes dentro de la red.

La función de la dirección IP es identificar simultáneamente tanto la red física a la que pertenece el host así como también al host mismo (estación de trabajo, servidor, enrutador, impresora, etc.)

Información que contiene una dirección IP.
Los primeros 4 bits del primer byte nos dicen la clase de red a la que pertenece la dirección.

Clase	Primer Octeto	Bits fijos	# de Redes	# de Hosts por Red	Máscara de subred por defecto.
A	1 - 126	0	$(2^7) - 2 =$ **126**	$(2^{24}) - 2 = 16777214$	255.0.0.0
B	128 - 191	10	$(2^{14}) =$ **16,384**	$(2^{16}) - 2 = 65,534$	255.255.0.0
C	192 - 223	110	$(2^{21}) =$ **2097152**	$(2^8) - 2 = 254$	255.255.255.0

Fig. 2.27: Información técnica de las clases de redes.
Fuente: www.uca.edu.sv

MÁSCARA DE RED

La mascara de red ayuda a identificar si un host es local o remoto. Esto se hace indicando cuál parte de la dirección IP es la dirección de la red y cuál es la dirección del host. (Network ID vs. Host ID). También ayuda a dividir una red en sub- redes (subnetting).

Los valores por defecto son:
Clase A: 255.0.0.0
Clase B: 255.255.0.0
Clase C: 255.255.255.0

Dichos valores indican que la red no se ha subdividido en subredes.

Una dirección IP codifica la identificación de la red a la cual está conectada el anfitrión y la identificación de un anfitrión único dentro de la red. Cada dirección IP está formada por un par (net id, host id), donde net id identifica una red y host id identifica a un anfitrión dentro de esa red. Por lo tanto los bits de dirección IP de todos los anfitriones en una misma red comparten un prefijo en común. Esta división de la dirección IP en dos partes es para realizar el enrutamiento de manera eficiente.

2.7.1 DIVISIONES DENTRO DE UNA RED

Existen muchas razones para dividir una red en subredes:

Administrar el tráfico de broadcast: Los broadcasts pueden controlarse porque un gran dominio de broadcast se divide en una gran cantidad de dominios más pequeños. No todos los hosts del sistema reciben todos los broadcasts.

Diferentes requisitos de red: Si los diferentes grupos de usuarios requieren servicios informáticos o de red específicos, resulta más sencillo administrar estos requisitos si aquellos usuarios que comparten requisitos se encuentran todos juntos en una subred.
Seguridad: Se pueden implementar diferentes niveles de seguridad en la red basándose en las direcciones de red. Esto permite la administración del acceso a diferentes servicios de red y de datos. [1]

2.8 INTERCONEXIONES ENTRE DISPOSITIVOS

Al planificar la instalación del cableado LAN, existen cuatro áreas físicas que se deben considerar:

Área de trabajo.
Cableado de distribución, también denominado cableado horizontal.

LONGITUD TOTAL DEL CABLE

Para las instalaciones UTP, el estándar ANSI/TIA/EIA-568-B especifica que la longitud combinada total del cable que abarca las cuatro áreas enumeradas anteriormente se limita a una distancia máxima de 100 metros por canal. Este estándar establece que se pueden utilizar hasta 5 metros de patch cable para interconectar los patch panels. Pueden utilizarse hasta 5 metros de cable desde el punto de terminación del cableado en la pared hasta el teléfono o la computadora.

2.8.1 ÁREAS DE TRABAJO

Las áreas de trabajo son las ubicaciones destinadas para los dispositivos finales utilizados por los usuarios individuales. Cada área de trabajo tiene un mínimo de dos conectores que pueden utilizarse para conectar un dispositivo individual a la red. Utilizamos patch cables para conectar dispositivos individuales a estos conectores de pared. El estándar EIA/TIA establece que los patch cords de UTP utilizados para conectar dispositivos a los conectores de pared tienen una longitud máxima de 10 metros.

El cable de conexión directa es el patch cable de uso más común en el área de trabajo. Este tipo de cable se utiliza para conectar dispositivos finales, como computadoras, a una red. Cuando se coloca un hub o switch en el área de trabajo, generalmente se utiliza un cable de conexión cruzada para conectar el dispositivo al jack de pared.

2.8.2 CABLEADO HORIZONTAL

El cableado horizontal se refiere a los cables que conectan los cuartos de telecomunicaciones con las áreas de trabajo. La longitud máxima de cable desde el punto de terminación en el cuarto de telecomunicaciones hasta la terminación en la toma del área de trabajo no puede superar los 90 metros. Esta distancia máxima de cableado horizontal de 90 metros se denomina enlace permanente porque está instalada en la estructura del edificio. Los medios horizontales se ejecutan desde un patch panel en el cuarto de telecomunicaciones a un jack de pared en cada área de trabajo. Las conexiones a los dispositivos se realizan con patch cables.

FACILIDAD DE INSTALACIÓN

La facilidad al instalar un cableado varía según los tipos de cables y la estructura del edificio. El acceso al piso y a sus espacios, además de las propiedades y el tamaño físico del cable, influyen en la facilidad de instalación de un cable en distintos edificios.

En algún punto, las redes inalámbricas requieren de cableado para conectar dispositivos, como puntos de acceso, a la LAN instalada. Los medios inalámbricos a menudo son más fáciles de instalar que un cable de fibra o UTP, ya que se necesitan menos cables en una red inalámbrica. Sin embargo, una LAN inalámbrica requiere de una prueba y planificación más detalladas. Además, varios factores externos, como otros dispositivos de radiofrecuencia o las construcciones, pueden afectar su funcionamiento. [1]

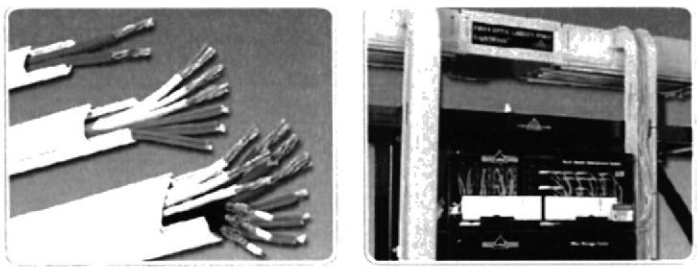


Fig2.28: Facilidad de instalación.
Fuente: www.cisco.com

CAPÍTULO 3
METODOLOGÍA DE DESARROLLO

3.1 PLANIFICACIÓN

Para la planificación de este proyecto se tuvo que realizar un diagnóstico de cómo se encontraban las instalaciones de comunicaciones de la empresa Aricamerluiz.
El edificio de la empresa cuenta con 4 pisos, los cuales están distribuidos de la siguiente manera:

Planta baja para el área de ventas y manejo de Caja, cuenta con 3 computadores de escritorio.

Primer piso para los departamentos de Oficina, los que cuentan con 6 computadores de escritorio y 2 laptops, no poseen un cuarto de telecomunicaciones o cuarto de equipos por lo que el servidor y equipos de red se encontraban instalados en el mismo piso en diferentes ubicaciones.

El segundo, tercer y cuarto piso son las bodegas de los diferentes artículos comercializados, no poseen computadores en ninguno de los pisos mencionados, lo que hace un total de 11 computadores para el uso de la empresa.

ESQUEMA JERÁRQUICO DE LA EMPRESA.

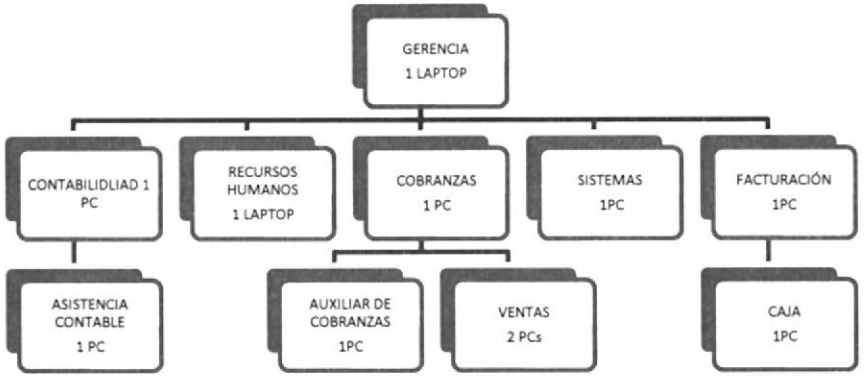


Fig. 3.1: Esquema de los departamentos y cantidad de host.
Fuente: Autor

3.2 ANÁLISIS

Al iniciar el proyecto se tuvo que identificar las falencias que presentaba la interconexión de la red anterior, lo que dio origen al planteamiento para la solución de los diferentes problemas.

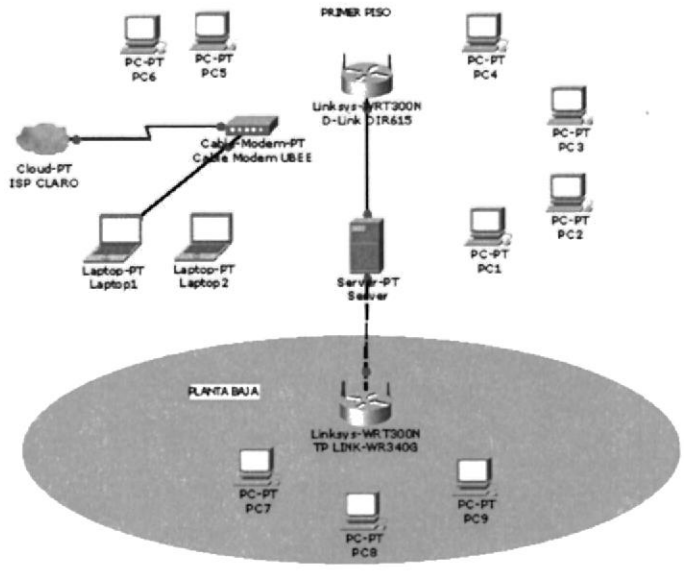


Fig. 3.2: Esquema de la red LAN anterior.
Fuente: Autor

Como se puede observar en la figura 3.1, el esquema de la red anterior no estaba cableada más que para interconectar a los routers con el servidor, y el cable modem con 1 laptop que es del Gerente, además de funcionar prácticamente como una WLAN, para lo cual se habían adquirido e instalado adaptadores USB Wi-Fi para conectarse a internet y al Sistema contable (*Zetalibra*), este fue el principal problema ya que cada vez que deseaban acceder a Internet, tenían que conectarse al SSID (*Service Set Identifier*) del Cable Modem *Ubee U10C037* (también funcionaba como router inalámbrico) y desconectarse del Router *D-Link DIR615* el cual les proporcionaba acceso al sistema antes mencionado, es por esto que no podían tener interconexión tanto al sistema como acceso a internet al mismo tiempo, obteniendo además problemas de desconexión de la red inalámbrica varias ocasiones en el transcurso del día, lo que ocasionaba inconvenientes en el área administrativa como en planta baja donde se presentaban molestias para los empleados de ventas y para los clientes.

En planta baja, el equipo que se encargaba de proporcionar acceso al sistema era el Router *TP-LINK WR340G* el cual estaba conectado al servidor a una tarjeta de red adicional, lo que originaba muchos problemas de desconexión ya que en planta baja no había ningún tipo de seguridad en la red inalámbrica, por no contar con clave de acceso a la misma, y el cable de red que llegaba hasta el servidor no tenía ninguna protección contra ruido e interferencias.

EQUIPOS QUE POSEE LA EMPRESA ACTUALMENTE

CABLE MODEM MOTOROLA 5121

Fig. 3.3: Cable Modem Motorola 5121.
Fuente: http://www.motorolasolutions.com

ESPECIFICACIONES TÉCNICAS
Modem Speed 38Mbps
Interface tipo USB
Compatibilidad con PC, Mac, UNIX, Linux
Requerimientos Windows XP, Windows Me, Windows 2000, Windows 98 SE
Standard Docsis 2.0, 1.1, 1.0
Max Operating Temperature 104° F
Voltage de entrada 220 / 110 volts
Ethernet Speed 100 Base T, 100 BASE TX
Protocolos TCP/IP
SNMP

ROUTER TP-LINK WR340G

Fig. 3.4: Router TP-Link WR340G.
Fuente: www.tp-link.com

ESPECIFICACIONES TÉCNICAS	
Interfaz	4 puertos LAN de 10/100Mbps 1 puerto WAN 10/100Mbps
Suministro de Energía Externa	9VDC/0.6A
Estándares Inalámbricos	IEEE 802.11g, IEEE 802.11b
Antena	Antena omnidireccional fijo de 5dBi
CARACTERÍSTICAS INALÁMBRICAS	
Frecuencia	2.4-2.4835GHz
Velocidad de Señal	11g: hasta 54Mbps (dinámico) 11b: hasta 11Mbps (dinámico)
Funciones Inalámbricas	Activar / Desactivar el radio inalámbrico, Puente WDS
Seguridad Inalámbrica	64/128/152-bit WEP / WPA / WPA2,WPA-PSK / WPA2-PSK
CARACTERÍSTICAS DEL SOFTWARE	
DHCP	DHCP servidor, Cliente, lista de cliente DHCP, Reserva de Dirección
Redireccionamiento de Puertos	Servidor virtual, Port Triggering, UPnP, DMZ
DNS Dinámico	DynDns, Comexe, PeanutHull
Seguridad Firewall (cortafuegos)	DoS, SPI Firewall Filtro Dirección IP / Filtro de dirección MAC / filtro de dominio de Conexiones Direcciones IP y MAC
Management	control de acceso Manejo Local Manejo remoto

SWITCH D-LINK DES1024D

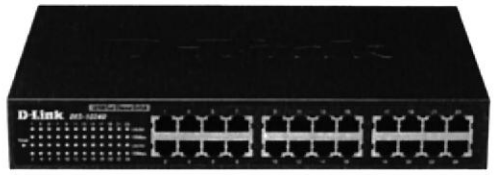


Fig. 3.5: Switch D-LinkDes1024D.
Fuente: www.dlink.com

ESPECIFICACIONES TÉCNICAS	
PUERTOS	**24 puertos RJ-45 10/100Mbps**
ESTÁNDARES	· IEEE 802.3 10Base-T Ethernet · IEEE 802u 100Base-TX Fast Ethernet · ANSI/IEEE 802.3 Nway auto-negotiation
PROTOCOLOS	**CSMA/CD**
MÉTODO DE TRANSMISIÓN	Store-and-Forward
TASA DE TRANSFERENCIA DE DATOS	**Fast Ethernet: 100Mbps (half-uplex), 200Mbps (full-duplex)**
PACKET FILTERING	100BASE-TX: 148,800 pps por Puerto (half-duplex)
PACKET FORWARDING RATES	**100BASE-TX: 148,800 pps por Puerto (half-duplex)**
MAC ADDRESS	Actualización Automática
FILTERING ADDRESS TABLE	**8 K por switch**
MÉTODO DE ACCESO	CSMA/CD
MEDIA INTERFACE EXCHANGE	**Auto MDI-II/MDI-X en cada puerto**
TOPOLOGÍA	Estrella
FUENTE DE PODER	**100~240V AC 50/60Hz Fuente de poder interna**
CONSUMO DE ENERGÍA	10 watts (Max.)
DIMENSIONES FÍSICAS	**280 (Ancho) x 180 (Largo) x 44 (Alto) mm**

SERVIDOR INTEL SC5275

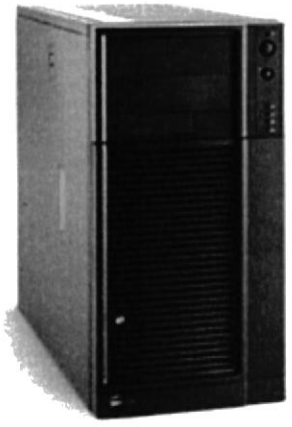


Fig. 3.6: SERVIDOR INTEL
Fuente: http://www.intel.com/

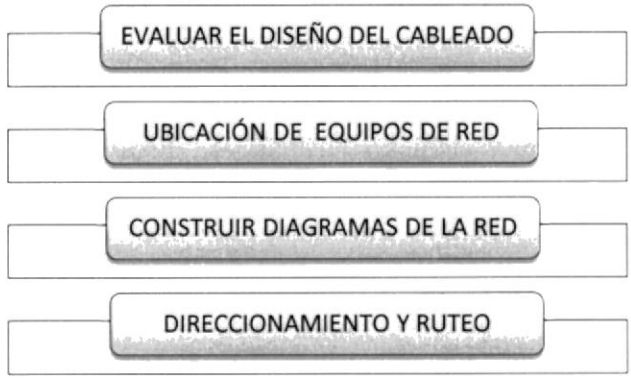
ESPECIFICACIONES TÉCNICAS
INTEL Grand Prairie - SE7525GP2 , dual Xeon 800MHz, dual Serial ATA, RAID 0,1, VGA, 1xPCI Express 16X, 1xPCI Express 4X, 2xPCI-X 64/66, 2xPCI 32/33, up to 8GB DDR memory (PC2100) or 8GB DDR memory (PC2700),LAN 10/100/1000
Pentium Xeon 2800MHz, 1M,800MHZ,FC-mPGA4, BOX
MEMORIA 1GB (2x512MB) DDRAM PC2700 ECC REG KINGMAX
FDD 3.5" SONY
2x 120 GB BARRACUDA Serial ATA 7200.7, 7200rpm,8MB cache,8.5ms(RAID 0)
TECLADO PS/2 LOGITECH DELUXE, MOUSE SCROLL LOGITECH, PAD
CD-ROM 52X TEAC
Carcasa INTEL SC5275E Pilot Point II w/600W PFC Fixed PSU, 2 chassis fans, 1 PSU fan, supports up to 6 tool-free cabled drives, upgradeable to 6 hot-swap drives (SCSI or SATA)

3.3 DISEÑO DE LA RED

El desarrollo de este proyecto tiene como fin diseñar e instalar una red LAN mediante cableado estructurado para interconectar 11 computadores con una IP estática o fija, acceder al sistema contable ininterrumpidamente y permitir la conexión a internet en los departamentos asignados.

ETAPAS DEL DISEÑO FISICO

Este proceso nos permite conocer los diferentes pasos que son necesarios para llevar a cabo la ejecución de proyecto.



3.3.1 EVALUAR EL DISEÑO DEL CABLEADO

Entre los diseños que se podría aplicar tenemos el centralizado y el distribuido, el centralizado es el que vamos a utilizar en este proyecto.
Los componentes medio ambientales que se deben tomar en cuenta tenemos:

Calor, ventilación: El primer piso tiene instalaciones de aire acondicionado que funcionan en los horarios laborales.

Dimensiones, espacio: Los departamentos están ubicados en el primer piso con el espacio considerable para los equipos de red.

Corriente, regulador de voltaje, UPS: El voltaje nominal en el edificio es de 120v AC, todos los equipos cuentan con protección de picos de voltaje (regulador), el servidor cuenta con protección mediante un UPS.

3.3.2 UBICACIÓN DE LOS EQUIPOS DE RED

El emplazamiento de los equipos de red se encuentran en el área de sistemas en un soporte de pared donde están instalados 1 Switch D-Link DES-1024D 24 puertos, 1 Router TP-Link WR340G, 1 cable modem Motorola 5121, los equipos instalados son los que la empresa disponía pero estaban mal ubicados e instalados, el nuevo cable modem lo proporcionó el proveedor de internet Claro.

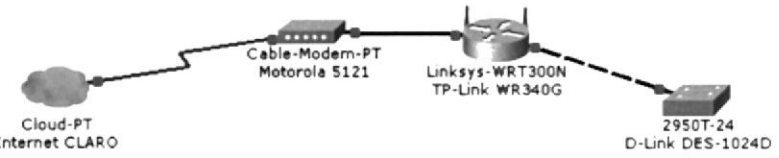


Fig. 3.7: Esquema de los equipos instalados en el área de Sistemas.
Fuente: Autor

Dentro de la ubicación de equipos se debe considerar necesario e importante etiquetar el cableado y los equipos claramente para que sea factible tanto el acceso como la identificación de los mismos por el personal autorizado en horarios de mantenimiento, actualización, cambios en los diseños de la red, o problemas inesperados.

Se debe considerar la siguiente información:
Nombre del sitio o ID
Categoría del sitio (considerar clases)
Nombre y/o número del Campus/Edificio
Número del piso
Número de la pieza
Número del rack
Dirección IP (local y remota)
Números de puerto
Capacidad, ancho de banda, velocidad del circuito, tecnología/servicio Red, enlace de datos, y/o protocolos de ruteo usados.

Fig. 3.8: Identificación de hardware.
Fuente: www.panduit.com

EJEMPLO DE CLASES DE SITIOS TERMINALES EN UNA LAN

Clase 1 (C1). LAN que no tiene conexiones externas (routers). El acceso está limitado a computadores conectados directamente
Clase 2 (C2). LAN conectada a otras LAN vía routers, pero que no tiene computadores conectados directamente
Clase 3 (C3). LAN que tiene tanto computadores conectados directamente como conexiones de routers a otras LANs
Ejemplo:

Nombre sitio, ID Dirección IP remota/Dirección IP local Puerto local-puerto remoto/velocidad/protocolo/clase/servicio

ARICAMERLUIZ, # AH11-SADM 200.124.245.124/192.168.1.30 541-8080/E1/OSPF/C2/RDSI-BE

Esta información deberá guardarse en una base de datos que describa todos los componentes de la red, y ser escrita en etiquetas a ser pegadas a cada componente.

CONSTRUIR DIAGRAMAS DE LA RED

3.3.3 DISEÑO FÍSICO

La topología física de la red se refiere a la forma en que distintos componentes de LAN se conectan entre sí.

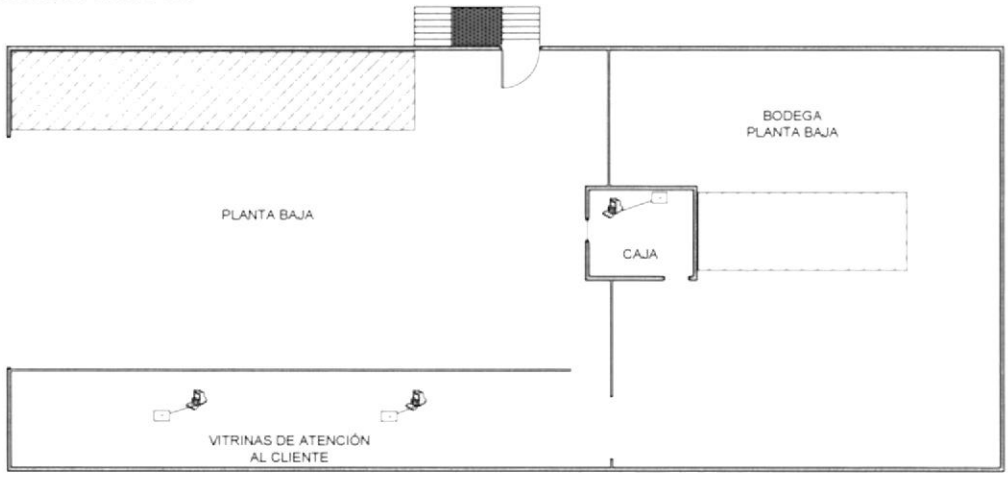


Fig. 3.9: Diseño físico de la planta baja.
Fuente: Autor

Fig. 3.10: Diseño físico del primer piso.
Fuente: Autor

3.3.4 DISEÑO LÓGICO

El diseño lógico de la red se refiere al flujo de datos que hay dentro de una red. También se refiere a los esquemas de nombre y dirección que se utilizan en la implementación de la solución de diseño LAN.

Se ha elaborado un diseño lógico para la empresa considerando los equipos que posee y que se recomendará mas adelante, tomando en cuenta además, los principales servicios que utiliza, los cuales son acceso al sistema contable, archivos compartidos, acceso a internet.

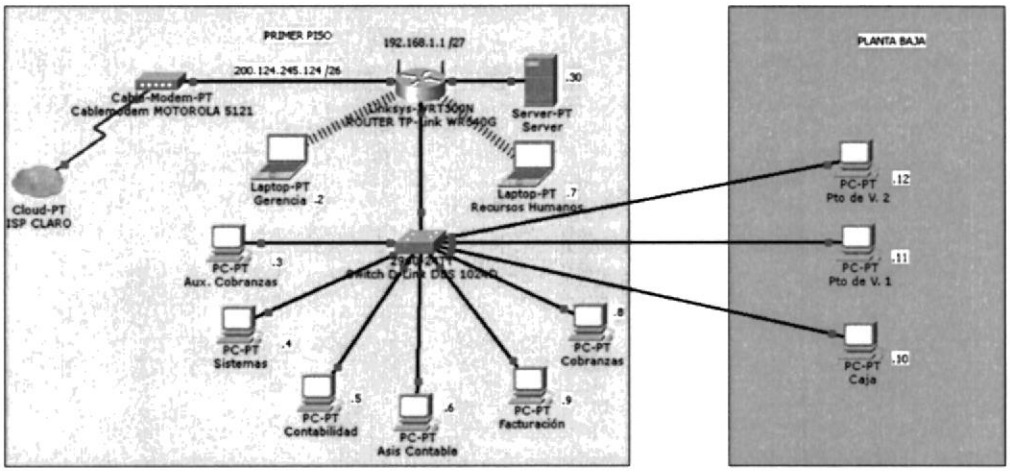


Fig. 3.11: Diseño lógico de la red LAN para la empresa Aricamerluiz.
Fuente: Autor

3.3.5 DIRECCIONAMIENTO Y RUTEO

Para desarrollar el esquema de direccionamiento de la red, se comenzó definiendo la cantidad total de hosts. Considerando que cada dispositivo requerirá una dirección IP, ahora y en el futuro.

Los dispositivos finales que requieren una dirección IP son:

- Equipos de usuarios
- Equipos de administradores
- Servidor

Entre los dispositivos de red que también utilizan una dirección IP se incluyen:

- Interfaces LAN del Router.
- Interfaces (serial) WAN del Router.

Una vez que se ha establecido la cantidad total de hosts que son 12, se debe considerar el rango de direcciones disponibles.

La cantidad de hosts en una red o subred se calcula mediante la fórmula 2 a la enésima potencia menos 2 (2^n - 2), donde n es la cantidad de bits disponibles como bits de host,

y los 2 host sustraídos corresponden a la dirección de red y la dirección de broadcast de la red, y no pueden asignarse a los hosts.

2^5 – 2 equivale a 30 direcciones válidas o utilizables para la red.
Se ha considerado esta cantidad ya que se planea instalar cámaras de seguridad IP, las cuales representan dispositivos finales.

Para determinar si todos los hosts formarán parte de la misma red o si toda la red se dividirá en subredes independientes se debe tomar en cuenta los equipos de capa 3, en este caso el router TP-Link WR340G que posee la empresa no es administrable, lo que significa que no es posible utilizar subredes por cada interfaz del router. Se procederá a utilizar el direccionamiento para la misma subred.

3.3.6 DOCUMENTACIÓN DE LA RED FÍSICA Y LÓGICA.

PLAN DE DISTRIBUCIÓN

CONEXIÓN	ID DEL CABLE	PUERTOS	TIPO DE CABLE	ESTADO
CABLE M-ROUTER	ISP-R1AR	RJ45(ISP)-WAN(ROUTER)	UTP – CAT 5e	UTILIZADO
ROUTER-SWITCH	R1AR-SW	R1-SW1	UTP – CAT 5e	UTILIZADO
ROUTER - SERVIDOR	R1AR-SERV	R2-SERV	UTP – CAT 5e	UTILIZADO
SWITCH - PARGER	SWP2-PCGER	SW2-(PC-GER)	UTP – CAT 5e	UTILIZADO
SWITCH - PARCOB	SWP3-PCCOB	SW3-(PC-COB)	UTP – CAT 5e	UTILIZADO
SWITCH - PARSIS	SWP4-PCSIS	SW4-(PC-SIS)	UTP – CAT 5e	UTILIZADO
SWITCH - PARCON	SWP5-PCCON	SW5-(PC-CON)	UTP – CAT 5e	UTILIZADO
SWITCH - PARCON1	SWP6-PCCON1	SW6-(PC-CON1)	UTP – CAT 5e	UTILIZADO
SWITCH - PARREC	SWP7 - PCREC	SW7-(PC-REC)	UTP – CAT 5e	UTILIZADO
SWITCH - PARCOB1	SWP8 - PCCOB1	SW8-(PC-COB1)	UTP – CAT 5e	UTILIZADO
SWITCH - PARFAC	SWP9 - PCFAC	SW9-(PC-FAC)	UTP – CAT 5e	UTILIZADO
SWITCH - PARCAJ	SWP10 - PCCAJ	SW10-(PC-CAJ)	UTP – CAT 5e	UTILIZADO
SWITCH - PARPV1	SWP11- PCPV1	SW11-(PC-PV1)	UTP – CAT 5e	UTILIZADO
SWITCH - PARPV2	SWP12 - PCPV2	SW12-(PC-PV2)	UTP – CAT 5e	UTILIZADO

Tabla. 3.1: Tabla de identificación de la red.
Fuente: Autor

ESPACIO DE DIRECCIONAMIENTO DISPONIBLE 192.168.1.0/27
Máscara de Subred: 255.255.255.224
Primera dirección válida: 192.168.1.1/27 (ROUTER)

Última dirección válida: 192.168.1.30/27 (SERVIDOR)
Dirección de Broadcast: 192.168.1.31/27
Direcciones válidas: 30

Nombre de Equipo	Dirección IP	Máscara de subred	Dirección de Gateway
parger-2adm	192.168.1.2	255.255.255.224	192.168.1.1
parcob-3adm	192.168.1.3	255.255.255.224	192.168.1.1
parsis-4adm	192.168.1.4	255.255.255.224	192.168.1.1
parcon-5adm	192.168.1.5	255.255.255.224	192.168.1.1
parcon1-6adm	192.168.1.6	255.255.255.224	192.168.1.1
parrec-7adm	192.168.1.7	255.255.255.224	192.168.1.1
parcob1-8adm	192.168.1.8	255.255.255.224	192.168.1.1
parfac-9adm	192.168.1.9	255.255.255.224	192.168.1.1
parcaj-10adm	192.168.1.10	255.255.255.224	192.168.1.1
parpv1-11adm	192.168.1.11	255.255.255.224	192.168.1.1
parpv2-12adm	192.168.1.12	255.255.255.224	192.168.1.1

Tabla. 3.2: Tabla de direccionamiento de la red.
Fuente: Autor

3.4 RECOMENDACIÓN DE EQUIPOS

3.4.1 FACTORES DE SELECCIÓN DE DISPOSITIVOS

Se deben considerar varios factores al seleccionar un dispositivo para una LAN particular. Estos factores incluyen, entre otros:

Costo
Velocidad y tipos de puertos/interfaces
Posibilidad de expansión
Características del sistema operativo

FACTORES A CONSIDERAR EN LA ELECCIÓN DE UN SWITCH

Si bien existen varios factores que deben considerarse al seleccionar un switch, el próximo tema analizará dos de ellos: las características de la interfaz y el costo.

COSTO

El costo de un switch se determina según sus capacidades y características. La capacidad del switch incluye el número y los tipos de puertos disponibles además de la velocidad de conmutación. Otros factores que afectan el costo son las capacidades de administración de red, las tecnologías de seguridad incorporadas y las tecnologías opcionales de conmutación avanzadas.

Al utilizar un simple cálculo de "costo por puerto", en principio puede parecer que la mejor opción es implementar un switch grande en una ubicación central. Sin embargo, este aparente ahorro en los costos puede contrarrestarse por el gasto generado por las longitudes de cable más extensas que se necesitan para conectar cada dispositivo de la LAN a un switch. Esta opción debe compararse con el costo generado al implementar una cantidad de switches más pequeños conectados a un switch central con una cantidad menor de cables largos.

Otra consideración en los costos es cuánto invertir en redundancia. El funcionamiento de toda la red física se ve afectada si existen problemas con un switch central único.

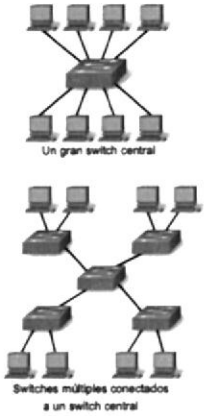


Fig3.12: Factores que determinan la elección de un switch lan.
Fuente: www.cisco.com

VELOCIDAD Y TIPOS DE PUERTOS E INTERFACES

La necesidad de velocidad está siempre presente en un entorno LAN. Se encuentran disponibles computadoras más nuevas con NIC incorporadas de 10/100/1000 Mbps. La selección de dispositivos de Capa 2 que puedan ajustarse a mayores velocidades permite a la red evolucionar sin reemplazar los dispositivos centrales.

FACTORES PARA TENER EN CUENTA AL ELEGIR UN ROUTER

Cuando se selecciona un router, deben coincidir las características del mismo con su propósito. Al igual que el switch, también deben considerarse las velocidades, los tipos de interfaz y el costo. Los factores adicionales para elegir un router incluyen:
Posibilidad de expansión
Características del sistema operativo

POSIBILIDAD DE EXPANSIÓN

Los dispositivos modulares tienen ranuras de expansión que proporcionan la flexibilidad necesaria para agregar nuevos módulos a medida que aumentan los requisitos. La mayoría de estos dispositivos incluyen una cantidad básica de puertos fijos además de ranuras de expansión.

CARACTERÍSTICAS DEL SISTEMA OPERATIVO

Según la versión del sistema operativo, el router puede admitir determinadas características y servicios, como por ejemplo:
Seguridad
Calidad de servicio (QoS)
Voz sobre IP (VoIP)
Enrutamiento de varios protocolos de capa 3
Servicios especiales como Traducción de direcciones de red (NAT) y Protocolo de configuración dinámica de host (DHCP). [1]

Fig3.13: Routers con capacidad de expansión y múltiples tipos de medios.
Fuente: www.cisco.com

Se ha propuesto una lista de equipos para un mejor desempeño y administración de los datos de la empresa, considerando la seguridad, convergencia, confiabilidad y escalabilidad se han seleccionado equipos de red con características robustas para cubrir las necesidades de una empresa competitiva priorizando la seguridad en la información.

3.4.2 PRESUPUESTO DE EQUIPOS RECOMENDADOS

Equipo	Valor unitario	Cantidad	Total
Servidor Dell PowerEdge R210 II	1349,00	1	1349,00
Router Cisco 2911/k9 Integrated Services	2083,64	1	2083,64
Switch Cisco Catalyst WS 2960TCL-24P	1696,00	2	3392,00
Rack de Piso 4 Ft	115,00	1	115,00
		TOTAL	6939,64

SERVIDOR POWEREDGE R210 II

Fig3.14: Servidor Dell Poweredge R210 II.
Fuente: www.dell.com/ec/empresas/p/poweredge-r210-2/pd

ESPECIFICACIONES TÉCNICAS
Procesador Procesador Intel® Xeon® E3-1220 3.10 GHz, 8M Cache, Turbo, Quad Core/4T (80W) **Sistema operativo** Windows Server 2008 R2 Foundation **Memoria** 4GB Memory (2x2GB), 1600Mhz, Single Ranked, Low Volt UDIMM **RAID** No RAID - Onboard SATA, 1-2 Hard Drives connected to onboard SATA Controller **Disco duro** 1TB 7.2K RPM SATA 3Gbps 3.5in Cabled Hard Drive **Garantía** 1 Año de garantía Básica en el sitio con respuesta al siguiente día laborable. **Chasis** PowerEdge R210II Chassis with Cabled 2x3.5 HDs and Quad-Pack LED Diagnostics **Unidad óptica** DVD-ROM, Interno **NIC** Adaptador Gigabit Ethernet Integrado de doble puerto

ROUTER CISCO 2911 (ISR)

Fig3.15: Router Cisco 2911 Integrated Services.
Fuente: www.cisco.com

ESPECIFICACIONES TÉCNICAS
3 puertos Ethernet 10/100/1000 integrados (conector RJ-45 solamente)
Una ranura para el módulo de servicio
4 ranuras mejoradas de alta velocidad para interfaz WAN
2 ranuras para el procesador de señales digitales (DSP)
Energía totalmente integrado de distribución de los módulos de soporte 802.3af Power Over Ethernet (PoE) y Cisco PoE mejorada
Integrado con aceleración por hardware de encriptación VPN para conectividad segura y comunicaciones de colaboración integrada de control de amenazas utilizando Cisco IOS Firewall, Cisco IOS Firewall basada en zonas, IOS de Cisco IPS y Cisco IOS Content Filtering
Gestión de la identidad mediante la autenticación, autorización y contabilidad (AAA) y la infraestructura de clave pública
Alta densidad de paquetes de voz módulo DSP, soporte optimizado para voz y video Normas certificadas por los servicios del navegador VoiceXML
Memoria DRAM 512 MB (instalados) / 2 GB (máx.) Memoria Flash 256 MB (instalados) / 8 GB (máx.)
Protocolo de direccionamiento OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático IPv6
Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet

SWITCH 2960G-24TC

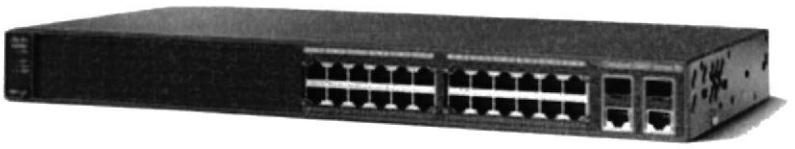


Fig3.16: Switch Cisco 2960G.
Fuente: www.cisco.com

ESPECIFICACIONES TÉCNICAS
Cantidad de puertos 24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Memoria RAM 64 MB / Memoria Flash 32 MB
Velocidad de transferencia de datos 1 Gbps
Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet
Puertos auxiliares de red 4x10/100/1000Base-T/SFP (mini-GBIC)(señal ascendente)
Protocolo de gestión remota SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c
Modo comunicación Semidúplex, dúplex pleno
Auto-sensor por dispositivo, soporte de DHCP, negociación automática, soporte VLAN, snooping IGMP
Cumplimiento de normas IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah
Dimensiones (Ancho x Profundidad x Altura) 44.5 cm x 32.8 cm x 4.4 cm
Peso 4.5 kg
Alimentación CA 120/230 V (50/60 Hz)
Garantía limitada de por vida

CAPITULO 4
IMPLEMENTACIÓN DE LA RED LAN

El principal problema que presentaba la empresa es que no tenía un correcto diseño en su red, por lo que se propuso un nuevo diseño de cableado estructurado en planta baja y primer piso, donde se ubican los dispositivos finales que utilizan los empleados y propietarios de la empresa para el control del sistema contable.

Se implementó una red inalámbrica con la seguridad adecuada para que puedan acceder al sistema las computadoras portátiles y dispositivos móviles los usuarios autorizados.

4.1 DISEÑO DE CAPA 1

El diseño en la capa 1 incluye el tipo de cableado y su estructura general que se ha utilizado en este proyecto.

4.1.1 CONSIDERACIONES DEL CABLEADO ESTRUCTURADO

Encontrar una solución de conectividad completa, una solución óptima para la conectividad de red incluye todos los sistemas que están diseñados para conectarse, administrar e identificar los sistemas de cableado estructurado.

Planeamiento para el crecimiento futuro, el enorme crecimiento en tecnologías de la información y el rápido aumento del número de nuevos dispositivos y servicios hacen que las nuevas instalaciones cumplen o exceden las normas para asegurarse de que la infraestructura esté en su lugar.

Mantener la libertad de elección en los vendedores, un sistema no estándar de un solo proveedor puede hacer más difícil cambiar de dirección en un momento posterior, a pesar de la garantía a corto plazo y los beneficios de certificación que puedan existir.

4.1.2 ESTÁNDARES UTILIZADOS EN EL PROYECTO

TIA/EIA-568-B intenta definir estándares que permitirán el diseño e implementación de sistemas de cableado estructurado para edificios comerciales y entre edificios en campus. El sustrato de los estándares define los tipos de cables, distancias, conectores, arquitecturas, terminaciones de cables y características de rendimiento, requisitos de instalación de cable y métodos de pruebas de los cables instalados.

El estándar principal, el TIA/EIA-568-B.1 define los requisitos generales, mientras que -568-B.2 se centra en componentes de sistemas de cable de pares balanceados.

4.1.3 SUBSISTEMAS DE CABLEADO ESTRUCTURADO

Los subsistemas de cableado estructurado que se mencionarán en el proyecto son:

Cableado de distribución (cableado horizontal)
Área de trabajo

4.1.4 MATERIALES

Para la ejecución del proyecto se requirió de ciertos materiales para una óptima instalación del cableado siguiendo las normas de calidad establecidas. La empresa Aricamerluiz proporcionó varias herramientas además de los materiales que se tuvieron que adquirir para poner en marcha el proyecto, a continuación se detallan los materiales utilizados en el diseño de capa 1, 2 y 3.

DISPOSITIVOS PASIVOS UTILIZADOS

1 ponchadora para plug RJ45
1 herramienta de impacto para Jack de RJ45
1 cortadora
1 juego de destornilladores
1 soporte de pared de 9UR
9 face plates dobles
9 cajas de montaje superficiales
18 jack RJ45 para face plates
50 plug RJ45
1 rollo de 305 m. de cable UTP cat 5e
10 canaletas 40 x 25mm
10 canaletas 20 x 12mm
10 tubos pvc de 1 pulg.

DISPOSITIVOS ACTIVOS UTILIZADOS

1 Cable modem Motorola 5121
1 Router TP-Link WR340G
1 Switch D-Link DES1024D
1 kit probador de puntos de red RJ45

4.2 TENDIDO DE CABLES

Como primer paso se realizaron las medidas respectivas de las canaletas por donde se instalaría el cableado, las canaletas que no poseían adhesivos se las aseguró en la pared con tornillos, las cajas sobrepuestas se procedieron a instalar a una altura de 30 cm del piso, y asegurándolas con tornillos en la pared.

El tendido de cable UTP categoría 5e se lo realizó por medio de canaletas plásticas pegadas en la pared de cada estación de trabajo en planta baja y los departamentos del primer piso. En ambos lugares se utilizó tubería pvc y canaletas, sin embargo en el primer piso se utilizó mayor cantidad de canaletas para una mejor presentación, en el cableado desde el primer piso hacia planta baja se utilizó tubos pvc y en varios sectores de planta baja se utilizó tubería por la incomodidad y dificultad de instalar canaletas.

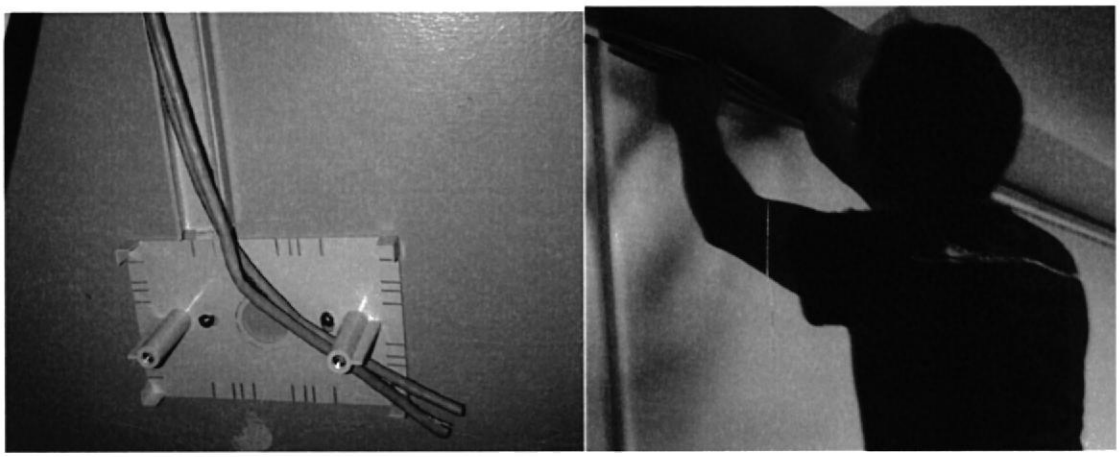


Fig4.1: Tendido de cables.
Fuente: Autor

Para instalar el cableado desde los equipos principales hacia el área de trabajo, se midió la distancia que existe entre ellos con un pequeño excedente de 50cm. para los cortes respectivos del cable para instalar los conectores en los puntos de red, y en el otro extremo la instalación del Jack para RJ45, además que como norma debe quedar una cantidad adicional de cable en la parte del punto de red para posibles cambios del Jack y realizar un nuevo ponchado.

Una vez medidos y cortados los cables se introdujeron en las canaletas respectivas, para introducir los cables por las canaletas donde hay ángulos de 90° se destapó la canaleta para evitar que existan dobleces del cableado involuntario y disminuir la dificultad del trabajo, para realizar el tendido hacia planta baja, se utilizó un cable resistente a tensión para jalar el grupo de cables que irían hacia el otro extremo, algo similar a instalar cableado de fibra óptica por tuberías subterráneas.

Entre las normas que se tomó para la instalación del cableado horizontal, es que la distancia total no deberá ser mayor a 90 metros, considerando que se debe dejar 5 metros de cable para un patch cord de la salida de telecomunicaciones (puntos de red) hacia el PC de usuario, 5 metros para un patch cord del patch panel del cuarto de equipos hacia el switch o router, en este caso no hay un patch panel instalado pero aún así la distancia del cableado no sobrepasa los 80 metros desde el switch hasta planta baja que es el cableado mas extenso. Se evitó en lo posible doblar el cableado de forma innecesaria puesto que esto relativamente daña el trenzado de los pares de cables y así se pierde calidad en la comunicación.

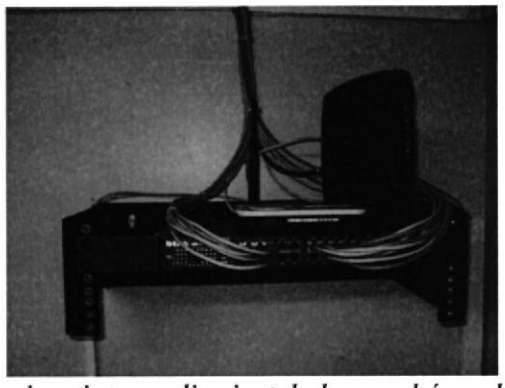


Fig4.2: Equipos intermedios instalados en el área de sistemas.
Fuente: Autor

4.3 INSTALACIÓN DE LOS PUNTOS DE RED

Para la instalación de los puntos de red o salidas de telecomunicaciones se utilizó las cajas sobrepuestas, face plates, jacks RJ45, y la herramienta de impacto (*impact tool*).
El ponchado de los jacks con el cableado correspondiente a cada departamento se lo realizó con la configuración *T568B* en ambos extremos (punto de red y conexión al switch) para que de esta forma la conexión del cable horizontal sea lineal.

La identificación de los colores en los costados del Jack permiten establecer la configuración *T568A / T568B*.

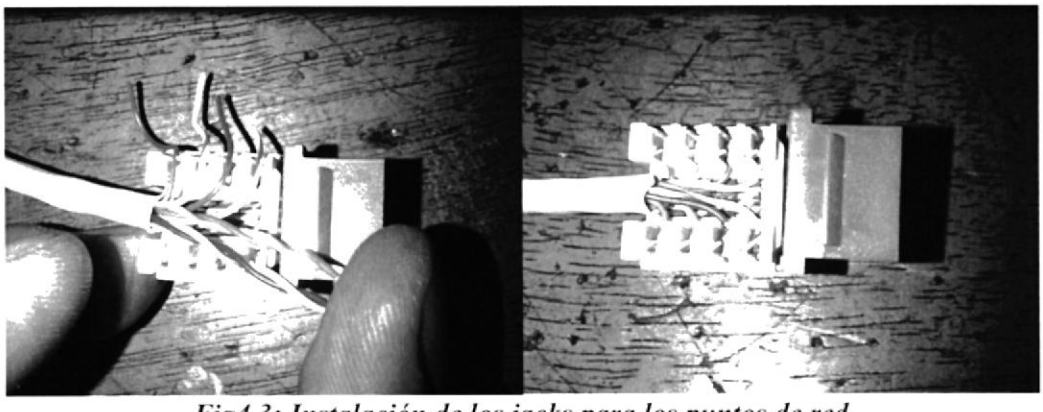


Fig4.3: Instalación de los jacks para los puntos de red.
Fuente: Autor

Tanto planta baja como el primer piso son los que poseen los equipos de acceso y administración del sistema, se instaló un punto de red por cada departamento, haciendo un total de 11 puntos de red para los pisos mencionados.

1. Planta Baja consta de varias dependencias de servicio al cliente, bodega, caja, en divisiones respectivas en el mismo espacio físico, ahí se instalaron 3 puntos de red, uno para caja y dos para los puntos de venta.

2. Primer piso posee los siguientes departamentos:

Gerencia:
Se instalará 1 punto de red a pesar de que el gerente utiliza siempre una computadora portátil a la cual solamente él tiene acceso, se le recomendó utilizar el punto de red con un patch cord por seguridad de su información a pesar de que también tiene acceso por la red inalámbrica instalada.

Contabilidad:
Constará de 2 puntos de red, uno para Contabilidad y otro para la Asistente Contable.

Cobranzas:
Aquí se instalará 2 puntos de red, uno para cobranzas y otro para su Asistente.

Sistemas:
Se instalarán 2 puntos de red, uno para el Encargado de Sistemas y otro punto de red para conectar el servidor con un patch cord al router.

Facturación:
Se instalará 1 punto de red, porque hay solamente una persona encargada.

Recursos Humanos:
En este departamento no se instalará puntos de red porque su ubicación hace difícil instalar el cableado hasta la computadora portátil, sin embargo el usuario tendrá acceso al sistema por medio de la red inalámbrica.

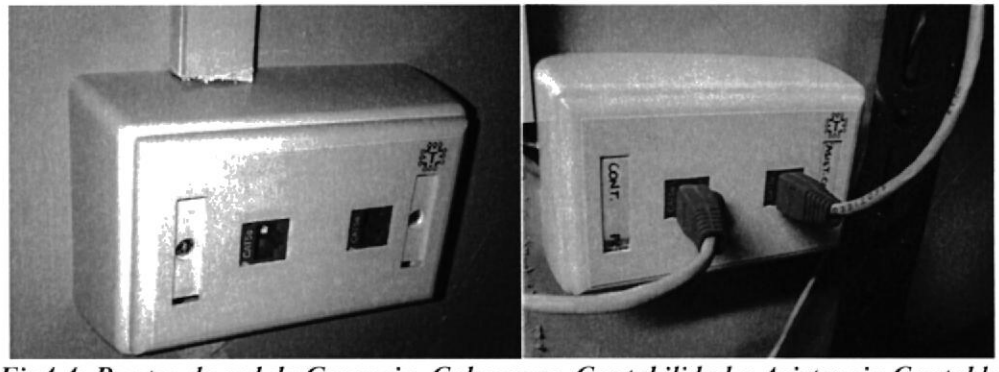


Fig4.4: Puntos de red de Gerencia, Cobranzas, Contabilidad y Asistencia Contable.
Fuente: Autor

4.3.1 PRUEBAS DE CONECTIVIDAD

Para verificar el correcto cableado y que exista la conectividad necesaria entre las estaciones de trabajo - router - servidor, se realizaron varias pruebas para tener acceso al sistema contable.

Prueba de capa 1, se utilizó el tester LAN de cables UTP para comprobar que se haya realizado un correcto ponchado en los terminales de cada conector RJ45, sea lineal o cruzada, esto se observa en los indicadores led del tester.

Fig4.5: Prueba de conectividad con el tester (comprobador).
Fuente: Autor

Prueba de capas 1-2-3, se ejecutó el comando ping desde la pc de un usuario hacia el router, al servidor y desde el servidor hacia un usuario y hacia el router, para determinar: tamaño de paquete en bytes, tiempo de vida.

ping 192.168.1.1 */l* 64
ping 192.168.1.30 */l* 64
ping 192.168.1.4 */l* 32

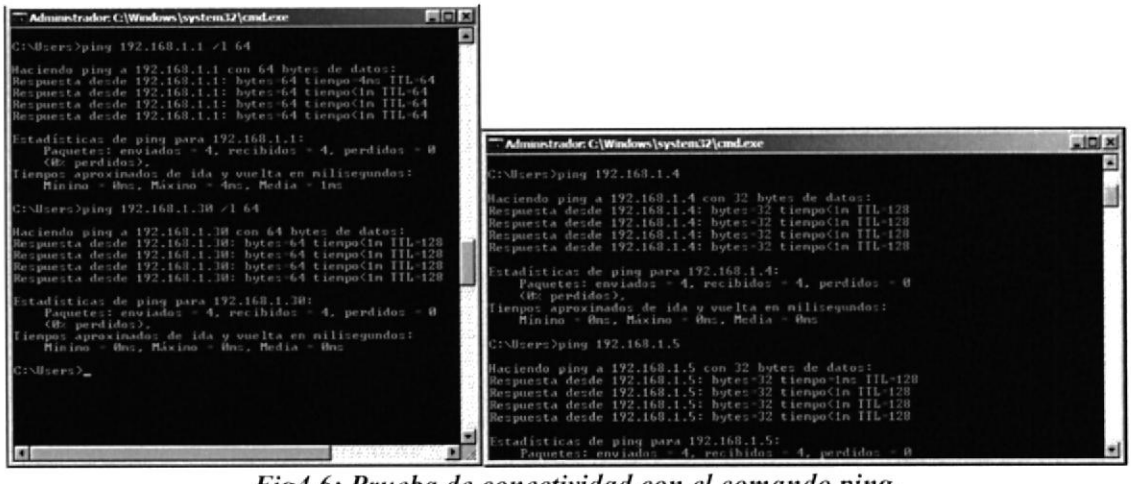


Fig4.6: Prueba de conectividad con el comando ping.
Fuente: Autor

4.4 MANTENIMIENTO PREVENTIVO DEL SERVIDOR

El servidor en óptimas condiciones implica un buen desempeño del sistema contable sin interrupciones ni problemas de acceso al mismo, la frecuencia que se debe dar mantenimiento al servidor depende de ciertas características que se relacionan con el uso, servicios que presta en una empresa, la exposición al polvo y otros medios que físicos y ambientales que corroen sus componentes internos. Como recomendación se sugiere dar mantenimiento de 2 a 4 veces al año, dependiendo de su uso, el servidor de la empresa Aricamerluiz no había recibido ningún tipo de mantenimiento desde que fue adquirido, lo que hacía aproximadamente 5 años.

Es importante recordar que el mantenimiento se debe realizar en horarios planificados para no causar molestias en la interrupción de servicios que otorga el equipo, en este caso el sistema contable, además del mantenimiento físico se debe realizar mantenimiento en el software o limpieza de archivos innecesarios.

Fig4.7: Mantenimiento preventivo del Servidor
Fuente: Autor

Una vez comunicada la inhabilitación del sistema se procedió al mantenimiento con la limpieza del polvo desmontando todas las partes del servidor, se utilizó brochas, contact cleaner, anteriormente se había comunicado el mantenimiento por lo que ya se había realizado el respaldo de las bases de datos y archivos del sistema contable.

El servidor de la empresa tenía instalado Windows Server 2003, se procedió luego de la limpieza a instalar el sistema Operativo Windows Server 2008 para obtener mayores beneficios.

4.5 INSTALACIÓN DE WINDOWS SERVER 2008

Las actualizaciones del sistema operativo además de corregir errores de programación dan soporte a nuevas tecnologías, evitan vulnerabilidades de seguridad.

Windows Server 2008 Enterprise Edition proporciona altos niveles de disponibilidad del sistema y la escalabilidad para soportar el crecimiento de las aplicaciones, otorga de una forma rentable beneficios de la virtualización. Prestaciones de servicios sin interrupciones de negocios para los empleados, además de acceso a usuarios remotos.

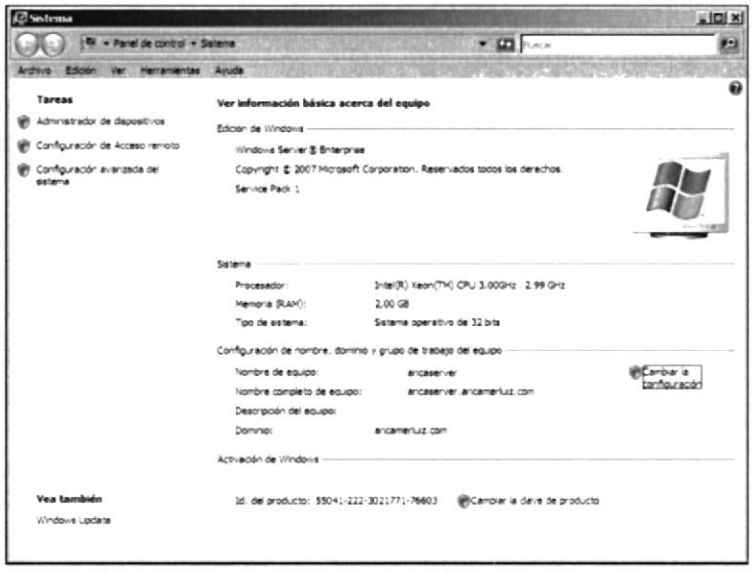


Fig4.8: Instalación de Windows Server 2008 y características del equipo
Fuente: Autor

Una vez finalizado el proceso de instalación, se estableció un controlador de dominio mediante el comando *dcpromo*, se ingresó una contraseña segura, se creó el dominio *aricamerluiz.com* para obtener una estructura de equipos conectados en red con prestaciones de servicios según las necesidades de cada departamento.

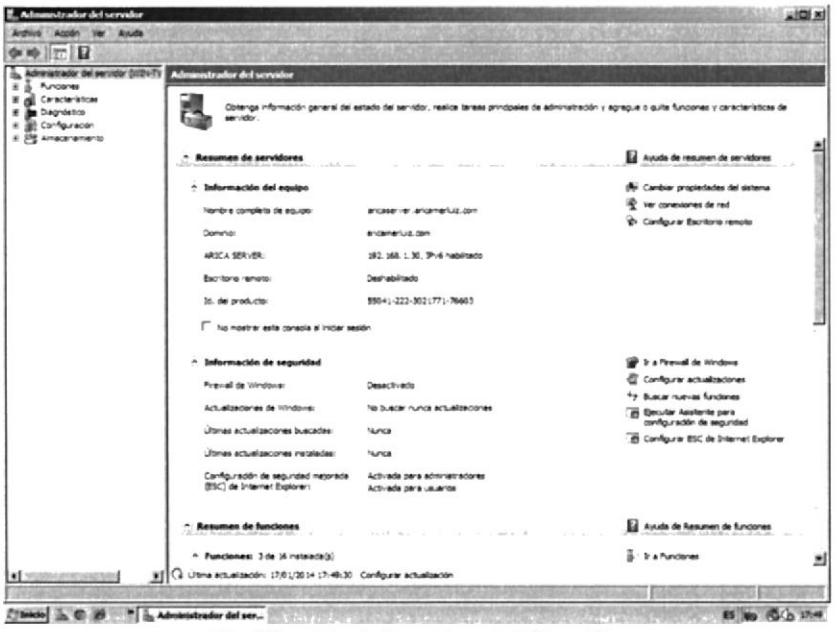


Fig4.9: Administrador del Servidor
Fuente: Autor

MANTENIMIENTO DE LOS COMPUTADORES DE USUARIOS

El mantenimiento preventivo de los computadores de escritorio de los empleados se efectuó con la debida anticipación, se realizó la limpieza de sus partes con contact cleaner y se actualizó el Sistema Operativo de Windows XP a Windows 7.

Fig4.10: Mantenimiento de los computadores de usuarios.
Fuente: Autor

4.6 SEGURIDAD Y CONTROL DE LOS DATOS DE LA EMPRESA

LINEAMIENTOS DE SEGURIDAD INFORMÁTICA.

A pesar de que se tenga un diseño y una administración excelente de una red LAN deben de existir lineamientos y normas que los usuarios deben seguir para proteger y mantener los recursos de la red funcionando de manera correcta en cada una de sus terminales. Dichas normas y lineamientos no deben ser un pesar para los usuarios de la red sino una recomendación que les permitirá desarrollar sus actividades sin ningún problema durante un largo período de tiempo.

Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a los usuarios autorizados para hacerlo. Los objetivos son:

- ✓ Restringir el acceso de las personas de la organización y de aquellas que no lo son, a la información y recursos de la red.
- ✓ Asegurar que los usuarios puedan trabajar pero que no puedan modificar los programas ni la información de la red.
- ✓ Asegurar que se utilicen los datos, archivos y programas correctos.
- ✓ Asegurar que la información transmitida sea la misma que reciba el destinatario y que no llegue a otro usuario.
- ✓ Asegurar que existan sistemas y procedimientos de emergencia alternativos de transmisión entre diferentes puntos.

Organizar a cada uno de los usuarios por jerarquía informática, con claves distintas y permisos establecidos en todos y cada uno de los sistemas empleados en la red.

AMENAZAS.

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento o de transmisión de la información se consideran seguras, se debe de tener en cuenta las circunstancias "no informáticas" que pudieran afectar a la información o recursos de la

red, estas circunstancias son imprevisibles o inevitables, de modo que la única protección posible es la redundancia en el caso de los datos y la descentralización en el caso de las comunicaciones.

Este tipo de circunstancias pueden ser causados por:

Un operador: causa del mayor problema ligado a la seguridad de un sistema informático debido a que no es conciente de lo que hace debido a su falta de conocimiento o simplemente actúa con dolo.

Software malicioso: este tipo de software esta destinado a perjudicar o a hacer un uso ilícito de los recursos del sistema, es instalado en las terminales de la red por lo general las PC, su función es abrir una puerta a intrusos o bien modificar los datos de la red. Los tipos de software malicioso son; virus, worms, trojans, bombs, spyware, etc.

Un Intruso: es un usuario informático que consigue acceder a los datos o programas sin autorización este tipo de usuarios son: hacker, cracker, defacer, script boy, viruxer, etc.

Personal interno de sistemas: se refiere a la mala administración de los sistemas de red dentro de una organización por parte de los responsables de sistemas, puede ser por falta de conocimiento o por mala intención.

4.6.1 POLÍTICAS DE SEGURIDAD.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a los usuarios para mejorar sus actividades productivas, educativas, tecnológicas, entre otras, esto ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los usuarios de una organización sobre la importancia y sensibilidad de la información y los servicios críticos que permiten crecer y mantenerse en competencia.

Una política se seguridad tiene como finalidad asegurar los derechos de acceso a los datos y recursos con herramientas de control y mecanismos de identificación y autenticación. Dichos mecanismos permiten saber que tipo de permisos y privilegios se les dará a los usuarios La seguridad informática no debe impedir el trabajo de los operadores además debe asegurar que puedan utilizar el sistema informático con toda confianza.

Las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, finalmente las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, tales como: el aumento de personal, cambios en la infraestructura de la red, alta rotación de personal, desarrollo de nuevos servicios y aplicaciones, crecimiento de la empresa, cambio o diversificación del área de negocios, etc.

4.6.2 BENEFICIOS DE UN SISTEMA DE SEGURIDAD

Los beneficios de un sistema de seguridad son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales.

4.6.3 PRIVACIDAD EN LA RED.

Las redes de datos son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión como cables, enlaces inalámbricos, satélites, routers, conmutadores, etc. También incluyen servicios de apoyo como DNS incluidos en los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.

Conectadas a las redes existen diversas aplicaciones como sistemas de correo electrónico, exploradores web, etc. También existen equipos terminales como; servidores, teléfonos, PCs, etc.

Por lo tanto una red de datos ofrece los medios que permiten la comunicación de diversos equipos y usuarios, pero también están propensas a ser controladas por personas no autorizadas. Cuando nos referimos a la privacidad de la red, se evoca al cuidado o medidas establecidas para que la información de los sistemas como datos de clientes, servicios contratados, reportes financieros y administrativos, estrategias de mercado, etc., no puedan ser consultados por intrusos.

REQUISITOS PARA MANTENER LA PRIVACIDAD EN LAS REDES DE DATOS.

Las redes deben cumplir los siguientes requisitos para mantener su privacidad ante las posibilidades de intrusión.

Disponibilidad: significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones de los usuarios.

Autenticación: confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación para los servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos, la autenticación de los sitios web, etc.

Integridad: confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente

importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica.

Confidencialidad: protección de las comunicaciones o los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que pueden amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

4.6.4 RIESGOS EN LA PRIVACIDAD DE LAS REDES

Interceptación de las Comunicaciones: la comunicación puede ser interceptada y los datos copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes, por ejemplo, pinchando la línea, o controlando las transmisiones.

Acceso no autorizado a ordenadores y redes de ordenadores: el acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma mal intencionada para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques aprovechando la tendencia de la gente a utilizar contraseñas previsibles, aprovechar la tendencia de la gente a desvelar información a personas en apariencia fiables e interceptación de contraseñas.

Perturbación de las redes: actualmente las redes se encuentran ampliamente digitalizadas y controladas por ordenadores, pero en el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos ordenadores. En la actualidad, los ataques más peligrosos se concretan a los puntos débiles y más vulnerables de los componentes de las redes como son sistemas operativos, routers, conmutadores, servidores de nombres de dominio, etc.

Ejecución de programas que modifican y destruyen los datos: los ordenadores funcionan con programas informáticos, pero lamentablemente, los programas pueden usarse también para desactivar un ordenador y para borrar o modificar los datos. Cuando esto ocurre en un ordenador que forma parte de una red, los efectos de estas alteraciones pueden tener un alcance considerable. Por ejemplo, un virus es un programa informático mal intencionado que reproduce su propio código que se adhiere, de modo que cuando se ejecuta el programa informático infectado se activa el código del virus.

Declaración Falsa: a la hora de efectuar una conexión a la red o de recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función del contexto de la comunicación. Para la red, el mayor riesgo de ataque procede de la gente que conoce el contexto. Por tal razón, las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos, como pueden ser transmitir datos confidenciales a personas no autorizadas, rechazo de un contrato, etc.

Accidentes no Provocados: numerosos problemas de seguridad se deben a accidentes imprevistos o no provocados como: son tormentas, inundaciones, incendios, terremotos, interrupción del servicio por obras de construcción, defectos de programas y errores humanos o deficiencias de la gestión del operador, el proveedor de servicio o el usuario. [5]

4.6.5 INSTALACIÓN DE CÁMARAS IP

La instalación de las cámaras IP tiene consideración en el diseño de la red Lan de la empresa, la razón porque son tomadas en cuenta es por la dirección IP que se les ha asignado por ser fija y no dinámica (*DHCP*), de manera que se asignó una ip a cada cámara. El total de cámaras instaladas es de 9.

5 cámaras en planta baja
2 cámaras en primer piso
2 cámaras en bodegas del segundo piso.

Para garantizar un constante acceso y control de las cámaras se procedió a utilizar cableado UTP por cada una y se desactivó el wifi. Las cámaras se conectan directamente al switch, para configurarlas se las conectó individualmente donde se leas asignó los siguientes parámetros:

Usuario: admin
Password: *******
Puerto: 81-89
Ip: 192.168.1.20 – 192.168.1.28
Máscara de red: 255.255.255.224
Gateway: 192.168.1.1

TRENDNET TV-IP551W

Fig4.11: Cámara IP Trendnet.
Fuente: www.trendnet.com

CARACTERÍSTICAS
Sensor: Sensor CMOS de 1/5 de pulgada
Distancia focal: 4mm
Iluminación mínima: 1 lux
Profundidad de enfoque: 20 cm ~ infinito
Visión: Horizontal: 38.0° Vertical: 28.7° / Diagonal: 46.5°
Zoom Digital: 4x
Micrófono omni-direccional integrado
Sensibilidad: -38dB +/- 3dB (máx 5 metros) S/N: >60dB
Formato: PCM
IEEE 802.3u 10/100Mbps Auto-MDIX Fast Ethernet
Power (Encendido), Link/Act (Enlace/Actividad)
Permite conexión WPS
Consumo eléctrico Máx 5 vatios
Potencia de entrada: 120~240V AC, 50~60Hz, 0.2A

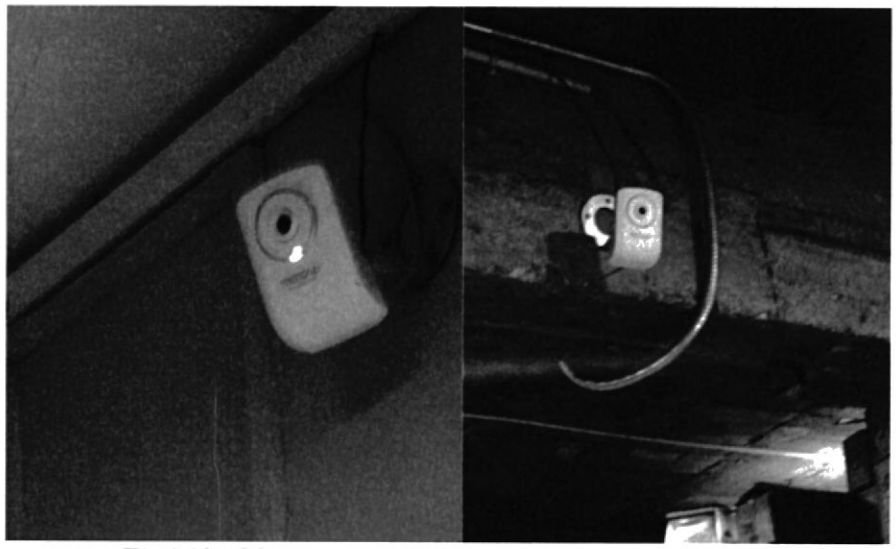


Fig4.12: Cámaras instaladas en primer y segundo piso
Fuente: Autor

4.6.6 INSTALACIÓN DE BIOMÉTRICO

El biométrico dactilar representa un sistema de control que todas las empresas deberían implementar para obtener beneficios tanto trabajadores como empleadores, de esta manera se registrarían en bases de datos los cumplimientos de horarios establecidos y se obtendría un registro de horas extra.

Fig4.13: Registro de ingreso en biométrico.
Fuente: Autor

Fig4.14: Biométrico instalado en la empresa.
Fuente: http://www.dinodirect.com

ESPECIFICACIONES TÉCNICAS

Platform	CPU : ARM9; SDRAM : 64Mb; FLASH : 32Mb
Fp amount	15000pcs / 3000pcs
Record amount	60000/160000
Administrator amount	1000
Registration method	Fingerprint or password
Safety level	1-4 optional
ID range	In the range of 1-99999999 , 3pcs fingerprints and 1 password for each ID
Times for fp registration	3
Communication method	USB-Slave. RS485. TCP/IP. U disk
Serial communication baud rate (BPS)	9600,19200,38400,57600,115200
language	Simplified Chinese, traditional Chinese and English
Hint	Voice and buzzer optional
displayer	128*64 pixels LCD
Name to be displayed	5 words or 10 ASIIC characters
Working temperature	0%-45℃
Working relative humidity	20%-80%

La instalación del biométrico se efectuó en planta baja, se conectó al puerto USB y al computador del departamento de Cobranzas donde se configuró e ingresó la información de la empresa, empleados y los detalles necesarios o convenientes para el empleador. La conexión permanente puede ser por medio de un cable serial-RS485 o conexión USB, se optó por la primera opción.

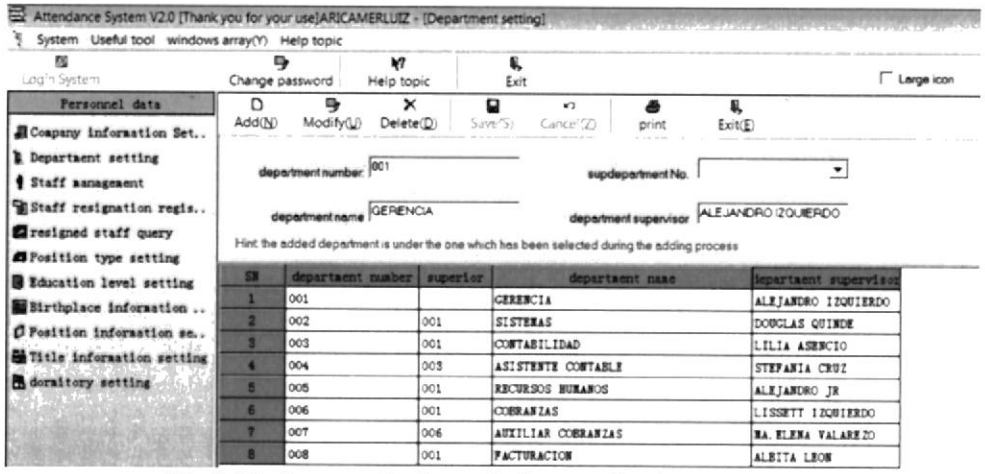


Fig4.15: Ingreso de datos de los empleados y empresa.
Fuente: Autor

4.7 ACCESO REMOTO

En el acceso remoto se ven implicados protocolos para la comunicación entre ordenadores, dispositivos móviles, y aplicaciones en ambos dispositivos que permitan recibir/enviar los datos necesarios. Además deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y las aplicaciones).

Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras. Se pueden acceder a archivos, dispositivos periféricos (como impresoras), configuraciones, cámaras, equipos de red, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

Existen múltiples programas que permiten controlar una computadora remotamente, también existen aplicaciones web que permiten el acceso remoto a determinados recursos utilizando sólo un navegador web, ya sea a través de internet o cualquier otra red.

Siempre que se aplique suficiente seguridad serán mayores los beneficios de poder acceder remotamente a determinados dispositivos.

En la empresa Aricamerluiz se han habilitado las configuraciones remotas del router para obtener ventajas de acceso a las cámaras IP, al sistema contable y desde luego al router.

4.7.1 ACCESO REMOTO AL ROUTER

El router es el dispositivo que direcciona los paquetes de datos que se envían y reciben dentro y fuera de la red local, es muy importante considerar las funciones que tiene habilitadas para obtener un desempeño favorable y que facilite el tráfico de los dispositivos conectados a él. Es imporante tener acceso remoto para monitorear, diagnosticar y habilitar o desabilitar funciones que sean necesarias según el caso lo requiera.

Para habilitar el acceso remoto se ingresa por la ip del router 192.168.1.1 se digita el usuario y password, en el menú Remote Management se llenan los dos campos donde se establece un puerto en este caso 3388 y la dirección ip pública desde donde se desea tener acceso, en este caso se ingresó 255.255.255.255 para ingresar al router desde cualquier dirección ip pública.

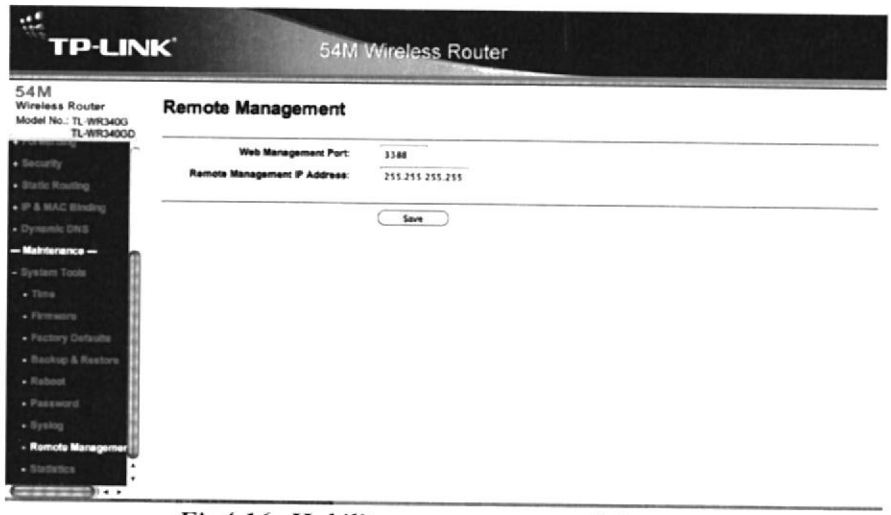


Fig4.16: Habilitar acceso remoto del router.
Fuente: Autor

Se comprobó su acceso al router fuera de la red de la empresa mediante la dirección ip pública y el puerto asignado, luego se debe ingresar el usuario y password establecido.

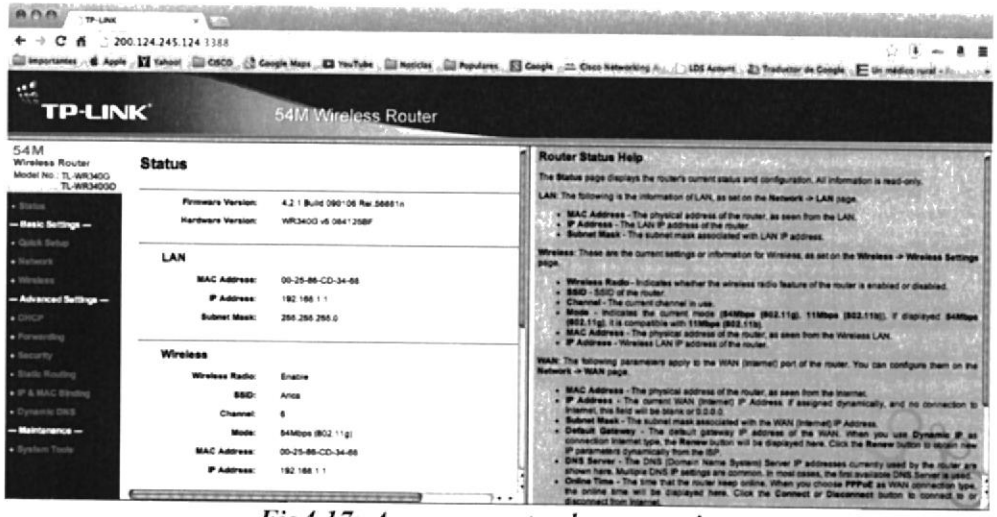


Fig4.17: Acceso remoto al router arica.
Fuente: Autor

4.7.2 ACCESO REMOTO AL SISTEMA CONTABLE.

La importancia de tener acceso al sistema fuera de la red local, fue consultada y propuesta por los administradores y dueños de la empresa, por considerar que al viajar constantemente fuera del país no podían realizar consultas importantes que se ven reflejadas solamente en la base de datos del servidor.

Se indicó que es posible acceder al sistema fuera de la empresa con el router que poseen, sin embargo se planteó que con un router administrable y con características que proporcionen más seguridad, tendrían mayor protección de sus datos.
Para configurar el router, se dirige a la opción forwarding, luego Virtual Servers y se agrega un nuevo servidor virtual. En este caso el puerto que será utilizado para establecer la comunicación, dirección ip del servidor 192.168.1.30, protocolo TCP (orientado a conexión), habilitar y guardar.

Fig4.18: Agregar un Servidor Virtual.
Fuente: Autor

Una vez agregado el servidor virtual se realizaron pruebas fuera de la red local y se digitó: ip pública del ISP, puerto asignado al servidor, ruta de acceso de página principal. *(Sistema contable en base a páginas web).*

Fig4.19: Acceso remoto al Sistema Zetalibra.
Fuente: Autor

4.7.3 ACCESO REMOTO A LAS CAMARAS IP

Al configurar las cámaras IP se activó la opción UPNP *(Universal Plug and Play)* que permite agregar un puerto remoto y protocolo de conexión.
Se asignó un puerto a cada cámara como se mencionó anteriormente y se eligió el protocolo de comunicación TCP.

En el router se activó la opción UPNP en el menú forwarding, y luego de unos minutos se podían observar las conexiones disponibles de las cámaras y usuarios que utilizaban Skype con protocolo UDP *(no orientado a conexión)*.

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	Skype UDP at 192.168.1.7:37480	37480	UDP	37480	192.168.1.7	Enabled
2	Skype TCP at 192.168.1.7:37480	37480	TCP	37480	192.168.1.7	Enabled
3	BodegaPA(d8:eb:97:d0:44:40)	88	TCP	88	192.168.1.27	Enabled
4	Ingreso Mezzanine(d8:eb:97:d0:4	81	TCP	81	192.168.1.20	Enabled
5	Mezzanine(d8:eb:97:d0:45:14)	82	TCP	82	192.168.1.21	Enabled
6	BodegaPA1(d8:eb:97:d0:43:6e)	89	TCP	89	192.168.1.28	Enabled
7	Skype UDP at 192.168.1.113:5536	55360	UDP	55360	192.168.1.113	Enabled
8	Skype TCP at 192.168.1.113:5536	55360	TCP	55360	192.168.1.113	Enabled
9	Bodega PB(d8:eb:97:d0:45:19)	90	TCP	90	192.168.1.26	Enabled
10	CAJA(d8:eb:97:d0:44:4c)	86	TCP	86	192.168.1.25	Enabled
11	Planta Baja2(d8:eb:97:d0:44:56)	85	TCP	85	192.168.1.24	Enabled
12	INGRESO(d8:eb:97:d0:45:11)	83	TCP	83	192.168.1.22	Enabled
13	Planta Baja1(d8:eb:97:d0:43:64)	84	TCP	84	192.168.1.23	Enabled

Fig4.20: Habilitar opción UPNP.
Fuente: Autor

Como observación se recomienda utilizar otro medio de conexión por DNS, ya que a pesar de que la conexión está asociada a TCP, y al ingresar usuario y clave, parece ser seguro el acceso por usuarios autorizados, actualmente existen muchos ataques al activar esta opción en el router, con la recomendación de equipos se propuso utilizar VPN (Virtual Private Network) para establecer conexiones encriptadas y mas seguras.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

El diseño de la red lan en la empresa está basado a las normas y protocolos de cableado estructurado para prestar un óptimo desempeño en la interconexión interna y externa. Los estándares se cumplieron y se comprobó los resultados mediante pruebas de calidad

Los puntos de red para cada departamento se instalaron de tal forma que cada usuario conozca el puerto del switch que se le asignó mediante etiquetas. Los patch cords de conexión del router al cable modem y del router al switch se diseñaron para que el cableado esté lo mas organizado posible y sea fácil identificar las conexiones. Las cámaras IP se conectan al switch en un rango de puertos establecidos para reconocerlas correctamente. La concentración del cableado en el área de equipos se organizó de tal forma que su aspecto permite rconocer claramente los dispositivos conectados.

Las pruebas de calidad se realizaron mediante un tester para verificar que exista conectividad y que los 4 pares de cable estén correctamente enlazados sea la norma T568A / T568B, además se realizaron pruebas de ping desde ambos extremos de los puntos instalados. La velocidad de la red es considerada dentro de los rangos de los equipos, cableado y tarjetas de red instaladas que es de 100Mbps.

Los recursos compartidos son designados por el departamento de sistemas y se administran de una forma más segura con la instalación de Windows 2008 Server.

La consideración de implementar nuevos equipos robustos para la red se basó en arquitectura y escalabilidad que toda empresa debe tener presente para estar preparados a los cambios que se generan constantemente. Estos equipos representan actualización de hardware, software, y proporcionan seguridad mediante redes privadas virtuales (VPN) evitando riesgos y ataques por estar conectados a la gran nube de información.

El presupuesto de los equipos se basa en la inversión que la empresa puede realizar a corto plazo ya que representa una continuidad en sus funciones laborales incrementando su desempeño. Los equipos son de marcas mundialmente reconocidas y comercializadas en nuestro país.

Los beneficios deben ser equitativos tanto para los empleados como los empleadores, es por esto que al instalarse sistemas de biométricos y cámaras IP se puede llevar un correcto control de horas laboradas y verificaciones de asistencia laboral, otorgando seguridad para los empleados accediendo física y remotamente.

GLOSARIO

QoS	Calidad de servicio
LAN	Red de área local
WAN	Red de área amplia
Patch cord	Cable para conectar dos dispositivos de red
RJ45	Conector utilizado en tarjetas de red Ethernet
OSI	Modelo de referencia para la resolución de problemas
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IP	Protocolo de internet
UTP	Cable de par trenzado no blindado
Gateway	Puerta de enlace
TCP	Protocolo de control de transferencia
VoIP	Voz sobre protocolo de internet
MDI	Interfaz dependiente del medio
MDIX	Interfaz cruzada dependiente del medio
Tx	Transmisión
Rx	Recepción
Mac	Control de acceso al medio
Nic	Tarjeta de interfaz de red
PC	Computador Personal
DSP	Procesador de señal digital
Mbps	Mega bits por segundo
Kbps	Kilo bits por segundo
Gbps	Giga bits por segundo
Broadcast	Transmisión de datos que será recibida por todos los dispositivos de una red
ADSL	Línea de abonado digital asimétrica
Wifi	Tecnología de comunicación inalámbrica
DNS	Sistema de nombres de dominio
DHCP	Protocolo de configuración dinámica de host
Face plate	Placa frontal que soporta los Jack (conector RJ45 sobrepuesto)
Ping	Comando utilizado para comprobar conectividad en una red
Tester	Equipo comprobador de conexión MDI/MDIX del cableado de red
RS485	Estándar de comunicación serial

BIBLIOGRAFÍA

[1] Cisco
http://www.cisco.com

[2] Microsoft
http://technet.microsoft.com/es-es/library/dd349801%28v=ws.10%29.aspx

[3] Trendnet
http://www.trendnet.com/store/products/products.asp?cat=100

[4] Sisbiocol
www.sistemasbiometricos.co

[5] Icicm
www.icicm.com/files/Seguridad_Redes_Lan.doc

[6] Dell
http://www.dell.com/ec/empresas/p/poweredge-r210-2/pd

[7] Panduit
http://www.panduit.com/wcs/Satellite?pagename=PG_Wrapper&friendlyurl=/en/products-and-services/products/identification

[8] D-Link
http://www.dlink.com/us/en/business-solutions/switching/unmanaged-switches/rackmount/dgs-1024d-24-port-copper-gigabit-switch

[9] TP-Link
http://www.tp-link.com/mx/products/details/?model=TL-WR340G

[10] Intel
http://www.intel.com/p/es_XL/support/highlights/server/sc5275-e