

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**TECNOLOGIAS DE ALTA DISPONIBILIDAD EMPLEADAS EN LAS
CENTRALES DE RIESGOS**

**INFORME DE COMPETENCIA PROFESIONAL
PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO ELECTRÓNICO**

**PRESENTADO POR:
RICARDO OSWALDO CHIOK CORDOVA**

**PROMOCIÓN
1992-II**

**LIMA-PERÚ
2011**

**TECNOLOGIAS DE ALTA DISPONIBILIDAD EMPLEADAS EN LAS
CENTRALES DE RIESGOS**

DEDICATORIA

**Me gustaría dedicar este Informe:
Para mi querida UNI,
Para mis Padres,
Para mi esposa Daisy.
Mis hijas Keisy y Antonella**

SUMARIO

El presente informe trata sobre los inicios de las Centrales de Riesgos y como fue su participación con los Bancos y Centros Comerciales, por lo que se detallará desde los inicios de Certicom hasta su llegada a Infocorp (Equifax Perú).

Para ello, veremos todo lo relacionado a la infraestructura informática y de telecomunicaciones que se tuvo que implementar para brindar la información crediticia a los Bancos y Centros Comerciales.

Se tendrá que ver con los temas relacionados a redes, comunicaciones de datos y telecomunicaciones que se tuvieron que implementar para este objetivo.

Veremos una Introducción al conocimiento de los principales protocolos de redes y de los componentes básicos de una red local, su función y conexión, distintas topologías de red y medios de transmisión. Uso de redes locales e instalación de una red local.

Inicialmente veremos los tipos de conexiones como se inicio por vía Dial-Up y RSDI para brindar servicio. Luego por Internet y la Red Privada Bancared y sus diferentes enlaces a los diversos Bancos y Centros Comerciales, a través de los protocolos TCP/IP y SNA, de acuerdo a los productos que teníamos a través del Telnet o cuando el cliente no tenia habilitado el telnet se cambiaba la aplicación a través del puerto 2001, finalmente se creo el servicio online de la pagina Web el cual funciona actualmente y para concluir los temas de alta disponibilidad.

Para ello, se tenia como socio estratégico a la Empresa IBM del Perú, del cual se adquirió inicialmente un servidor y arreglo de discos en 1999, y luego, con el avance tecnológico, otro Servidor IBM mejorado integrado con discos en RAID y finalmente, se adquirió 4 Servidores IBM Rackeable: primero la compra de un Storage IBM DS4300 y luego se terminó utilizando la Virtualizacion, en la cual se adquirió licencias Vmware y los Servidores IBM se integró con 1 Storage de 1 TB de capacidad con discos SAS unidos con 2 Switches SAN conectados con fibra óptica, con lo cual se consiguió la consolidación de servidores y la reducción del tamaño del Data Center, que finalmente se trasladó al interior del local IBM del Perú ubicado en la Av. Javier Prado, donde está operando actualmente.

INDICE

PROLOGO	1
CAPITULO I	
PLANTEAMIENTO DEL PROBLEMA DE INGENIERIA	2
1.1 Antecedentes	2
1.2 Alcances y Objetivo	4
CAPITULO II	
MARCO TEÓRICO CONCEPTUAL	7
2.1 Origen de la Ethernet	7
2.2 Redes de Computadores	8
2.2.1 Introducción a las tecnologías LAN	8
2.3 Componentes Básicos de una Red	9
2.4 Topologías	9
2.4.1 Topología en estrella	9
2.4.2 Control de acceso al medio	10
2.4.3 Tarjetas de Conexión de Red (NIC)	10
2.4.4 Cableado	11
2.4.5 Par Trenzado	11
2.5 Características de las Redes	14
2.6 Seguridad Informática	14
2.7 Estructura de las Redes	16
2.8 Servicios	18
2.9 Centro de procesamiento de datos (Data Center)	19
2.10 Sistema de Comunicación	19
2.11 Tipos De Ondas	19
2.12 Codificación De La Información	20
2.13 Problemas De La Transmisión	21
2.1.4 Tipos de cables	23
2.1.5 Tipos de Señal	26
2.1.6 Tipos de Transmisión	27
2.1.7 Nivel De Enlace o Datos	30
CAPITULO III	
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA	33
3.1 TIPOS DE CONEXIONES	33
3.1.1 Analógico	33

3.1.2	ISDN (Integrated Services Digital Network	33
3.1.3	Systems Network Architecture (SNA)	33
3.1.4	Conexión ADSL.....	34
3.1.5	Líneas Dedicadas.....	34
3.2	ALTA DISPONIBILIDAD	35
3.2.1	Tiempo de inactividad	35
3.2.2	Disponibilidad	36
3.2.3	Diseño de un sistema de alta disponibilidad	36
3.2.4	Redundancia	37
3.2.5	Evaluación de riesgos	39
3.3	HSRP - Redundancia en la salida a Internet y Bancared	40
3.4	Redundancia en la Red de área de almacenamiento	44
3.5	VIRTUALIZACIÓN.....	48
3.6	BANCARED.....	49
3.6.1	Bancared.....	49
3.6.2	Características	49
3.6.3	Operatividad	50
3.6.4	Entidades Financieras Interconectadas.....	50
3.6.5	Entidades Proveedoras de Información Interconectadas	51
3.7.	MPLS (Multi Protocol Label Switching)	52
3.7.1	Mpls.....	52
3.7.2	Antecedentes.....	52
3.7.3	Cómo funciona MPLS	53
3.7.4	La comparación de IP versus MPLS	55
3.7.5	Virtual Private Network-VPN.....	58
3.7.6	Multiprotocolo.....	58
3.8	MONITORIZACION	60
3.8.1	JController	60
3.8.2	Nagios.....	61
CAPITULO IV		
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS		63
4.1	Análisis del Problema	63
4.2	Esquema del tendido de cables y ubicación de las máquinas	65
4.2.1	Requerimientos Previos	65
4.2.2	Descripción Específica de los equipos.....	66
4.3	Aplicación en las red de datos	67
4.4	Diseño del Sistema	68
4.5	Aplicación en los enlaces.....	70
4.6	Aplicación en la red SAN	72
CONCLUSIONES Y RECOMENDACIONES.....		77

ANEXO A

GLOSARIO DE TÉRMINOS	80
BIBLIOGRAFÍA	82

PRÓLOGO

Central de Riesgos es un sistema de registro que consolida la información de la situación crediticia de los deudores de las empresas del sistema financiero

"Las centrales de riesgos seguirán invirtiendo permanentemente en innovación y desarrollo tecnológico para proporcionar un servicio de excelencia y calidad a su red de más de 2,500 clientes que diariamente evalúan sus operaciones crediticias", señaló una fuente de la compañía.

Servicio que presta la Superintendencia de Banca y Seguros y las centrales de riesgo privadas (Infocorp y Certicom), consistente en el análisis de la información suministrada por las entidades de crédito sobre los riesgos bancarios asumidos por personas o empresas, con objeto de identificar a los prestatarios que puedan originar problemas de reembolso.

Debido a la necesidad de los clientes de tener la información 24X7, se tendría que tener en la mayoría de los sistemas con alta disponibilidad, por lo cual se realizó proyectos para alcanzar este objetivo, así logrando la satisfacción del cliente.

Se dará a conocer las soluciones empleadas como los tipos de conexiones y de la Alta Disponibilidad, dando a conocer las tecnologías empleadas, tanto en las redes de telecomunicaciones y servicios de base datos que requerían urgencia, nombrando aquí solo los principales proyectos realizados por mi persona, lo cual demostraré la eficiencia de éstos.

Para concluir, se hablará de la Red Privada Bancared, dado que en ésta se realizaba la mayor cantidad de conexiones debido a el mayor de numero de clientes usaban esta red, y la tecnología empleada para esta red de comunicaciones como el MPLS.

Para finalizar se concluirá con el análisis y presentación de resultados de cada de las soluciones presentadas dando los logros y objetivos trazados el cual nos dará a conocer la eficiencia de la Central de Riesgos.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA DE INGENIERIA

1.1 Antecedentes

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande d

maquinas que funcionan como servidor de archivo compartido.

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN nos ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticas. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial, ethernet o fibra óptica al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, la Ethernet, utiliza un mecanismo denominado Call Sense Múltiple Access-Collision Detect (CSMA-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos desde 10 Mbits/seg, hasta 10 GB, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Ethernet y CSMA-CD son dos ejemplos de LAN. Hay tipologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios. Los primeros, por lo general máquinas más potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos, por lo general computadoras personales.

La construcción de esta red LAN, que permite el acceso a los nuevos sistemas de comunicación. si bien está orientada a satisfacer necesidades del medio, también se crea como un reto a su diseñador, quien se inicia en este medio y como objetivo basado en un proyecto final específicamente orientado al cableado estructurado, que además de dejar un gran enriquecimiento intelectual, nos ofrece la oportunidad de poner en practica todos estos conocimientos tecnológicos adquiridos durante la trayectoria a través de las clases

vista. La lógica expositiva responde a los diferentes pasos que he seguido para diseñar una red LAN, a saber: análisis de temas centrales y pertinentes a través de consultas bibliográficas, estudios de factibilidad a partir de trabajos de campo y decisiones respecto de aspectos técnicos y físicos que surgieron como resultado de los procesos anteriores.

Para este proyecto de Red, la misma está basada en una topología tipo estrella, por ser ofrecer esta una gran ventaja; su estructura se caracteriza por existir en ella un nodo central encargado de la gestión y el control de la red, al cual se conectan todos los equipos mediante enlaces bi-direccionales; el inconveniente de esta tipología es que la máxima vulnerabilidad se encuentra en el nodo central, ya que si éste falla, toda la red fallará, lo cual es bastante improbable debido a la gran seguridad que posee dicho nodo. Una ventaja de esta configuración, es que cada conexión no tiene que soportar múltiples PC compitiendo por el acceso, de manera que es posible lograr altas frecuencias de transferencias de datos (aunque la máquina central debe ser bastante rápida). Para aumentar el número de estaciones de la red o eliminar estaciones no es necesario interrumpir, ni siquiera parcialmente, la actividad, realizándose la operación con bastante sencillez y sin perjudicar al resto de la red.

1.2 Alcances y Objetivo

En un mundo tan desarrollado como el actual, los recursos de información son tan amplios que van mas allá de lo que podemos imaginar. Son muchas las organizaciones que cuentan con un número considerable de ordenadores en operación y con frecuencia alejados unos de otros. Por Ejemplo, una compañía con varias fábricas puede tener un ordenador en cada una de ellas para mantener un seguimiento de inventarios, observar la productividad y llevar la nómina local.

Inicialmente cada uno de estos ordenadores puede haber estado trabajando en forma aislada de las demás pero, en algún momento, la administración puede decidir interconectarlos para tener así la capacidad de extraer y correlacionar información referente a toda la compañía. Uno de los medios que hace posible esta conexión son la redes, una red es un sistema de comunicaciones, que permite comunicarse valga la redundancia, con otros usuarios, y compartir archivos y periféricos. Es decir, es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información. Es un conjunto interconectado de ordenadores autónomos. La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, acceder a la información de otra computadora y poder tener inclusive, comunicación directa con otros usuarios en otras computadoras, las cuales proporcionan servicios tales como: correo electrónico (E-mail), video Conferencia y una de las más usadas World Wide Web.

Cabe destacar que el diseño se realiza con el objetivo de crear una red en la Central de Riesgos, para el cual se realizó un análisis de temas respecto de la instalación de una Red, La instalación de una red implica la toma de decisiones sobre diferentes aspectos, entre otros: técnicos, económicos, lugar donde se va a realizar la instalación y tipo de cableado más adecuado entre otros, pero que fundamentalmente es un proyecto que propiamente es ideológico, y con la finalidad propiamente de poner en práctica los conocimientos adquiridos. Es a través del diseño de esta red, en el cual se basa en el diseño cableado estructurado, que vamos a poder reflejar los conocimientos adquiridos en este semestre.

Análisis de temas respecto al diseño del cableado estructurado de las redes LAN; para el mismo funcionan una serie de reglas el cableado estructurado es un enfoque sistemático del cableado. Es un método para crear un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, administradores de red y cualquier otro técnico que trabaje con cables. Hay tres reglas que ayudan a garantizar la efectividad y eficiencia en los proyectos de diseño del cableado estructurado. La primera regla es buscar una solución completa de conectividad. Una solución óptima para lograr la conectividad de redes abarca todos los sistemas que han sido diseñados para conectar, tender, administrar e identificar los cables en los sistemas de cableado estructurado. La implementación basada en estándares está diseñada para admitir tecnologías actuales y futuras. El cumplimiento de los estándares servirá para garantizar el rendimiento y confiabilidad del proyecto a largo plazo. La segunda regla es planificar teniendo en cuenta el crecimiento futuro. La cantidad de cables instalados debe satisfacer necesidades futuras. Se deben tener en cuenta las soluciones de Categoría 5e, Categoría 6 y de fibra óptica para garantizar que se satisfagan futuras necesidades. La instalación de la capa física debe poder funcionar durante diez años o más. La regla final es conservar la libertad de elección de proveedores. Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar ser mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones, existen Códigos y estándares de cableado eestructurado. Los estándares son conjuntos de normas o procedimientos de uso generalizado, o que se especifican oficialmente y que sirven como modelo de excelencia. Un proveedor especifica ciertos estándares. Los estándares de la industria admiten la interoperabilidad entre varios proveedores de la siguiente forma:

- Descripciones estandarizadas de medios y configuración del cableado backbone y horizontal.
- Interfaces de conexión estándares para la conexión física del equipo.

- Diseño coherente y uniforme que siga un plan de sistema y principios de diseño básicos.

Hay numerosas organizaciones que regulan y especifican los diferentes tipos de cables. Las agencias locales, estatales, de los condados o provincias y nacionales también emiten códigos, especificaciones y requisitos. Una red que se arma según los estándares debería funcionar bien o ínter operar con otros dispositivos de red estándar. El rendimiento a largo plazo y el valor de la inversión de muchos sistemas de cableado de red se ven reducidos porque los instaladores no cumplen con los estándares obligatorios y recomendados.

Estos estándares se revisan constantemente y se actualizan periódicamente para reflejar las nuevas tecnologías y las exigencias cada vez mayores de las redes de voz y datos. A medida que se incorporan nuevas tecnologías a los estándares, otras son eliminadas. Una red puede incluir tecnologías que ya no forman parte de los estándares actuales o que pronto serán eliminadas. Estas tecnologías por lo general no exigen una renovación inmediata. Con el tiempo, quedan reemplazadas por tecnologías más rápidas y modernas.

Muchas organizaciones internacionales tratan de desarrollar estándares universales. Organizaciones como IEEE, ISO y IEC son ejemplos de organismos internacionales de homologación. Estas organizaciones incluyen miembros de muchas naciones, las cuales tiene sus propios procesos para generar estándares. En muchos países, los códigos nacionales se convierten en modelos para agencias provinciales, estatales, municipios y otros entes gubernamentales que los incorporan en sus leyes y ordenanzas. El cumplimiento de los mismos luego se transfiere a la autoridad local. Siempre verifique con las autoridades locales qué códigos hay que cumplir. La mayoría de los códigos locales tienen prioridad sobre los códigos nacionales, que a su vez tienen prioridad sobre los internacionales.

Como primer objetivo se realiza la implementación de la red Lan consecutivamente se va proporcionando los elementos que mantengan la continuidad del Sistema y así aparecen soluciones que se deben implementar logrando la eficiencia de la Central de Riesgos. Es por ello que es necesario mantener la operabilidad de estos recursos por ende es la necesidad de contar con tecnologías de alta disponibilidad que logren el objetivo de mantener el sistema siempre operativo y esto nos traerá la satisfacción del cliente de usarlo logrando el objetivo final.

CAPITULO II MARCO TEORICO CONCEPTUAL

A continuación se señalan las bases teóricas que se consideran como válidas y confiables a la sustentación de las variables objeto de estudio de la presente investigación.

Mediante la ejecución de teorías referidas a la información, del uso y diseño de redes LAN Ethernet, el usuario tiene la oportunidad diseñar una red.

2.1 Origen de la Ethernet:

La idea original de Ethernet nació del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales interfirieran entre sí. El problema de acceso por varios usuarios a un medio compartido se estudió a principios de los 70 en la Universidad de Hawai. Se desarrolló un sistema llamado Alohanet para permitir que varias estaciones de las Islas de Hawai tuvieran acceso estructurado a la banda de radiofrecuencia compartida en la atmósfera. Más tarde, este trabajo sentó las bases para el método de acceso a Ethernet conocido como CSMA/CD.

La primera LAN del mundo fue la versión original de Ethernet. Robert Metcalfe y sus compañeros de Xerox la diseñaron hace más de treinta años. El primer estándar de Ethernet fue publicado por un consorcio formado por Digital Equipment Company, Intel y Xerox (DIX). Metcalfe quería que Ethernet fuera un estándar compartido, a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto. Los primeros productos que se desarrollaron utilizando el estándar de Ethernet se vendieron a principios de la década de 1980. Ethernet transmitía a una velocidad de hasta 10 Mbps en cable coaxial grueso a una distancia de hasta 2 kilómetros (Km). Este tipo de cable coaxial se conocía como thicknet (red con cable grueso) y tenía el ancho aproximado de un dedo pequeño.

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con el modelo OSI de la Organización Internacional de Estándares (ISO). Por eso, el estándar IEEE

802.3 debía cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

Las diferencias entre los dos estándares fueron tan insignificantes que cualquier tarjeta de interfaz de la red de Ethernet (NIC) puede transmitir y recibir, tanto tramas de Ethernet como de 802.3. Básicamente, Ethernet y IEEE 802.3 son un mismo estándar.

El ancho de banda de 10 Mbps de Ethernet era más que suficiente para los lentos computadores personales (PC) de los años 80. A principios de los 90, los PC se volvieron mucho más rápidos, los tamaños de los archivos aumentaron y se producían cuellos de botella en el flujo de los datos. La mayoría a causa de una baja disponibilidad del ancho de banda. En 1995, el IEEE anunció un estándar para la Ethernet de 100 Mbps. Más tarde siguieron los estándares para Ethernet de un gigabit por segundo (Gbps, mil millones de bits por segundo) en 1998 y 1999.

2.2 Redes de Computadores

La definición más clara de una red es la de un sistema de comunicaciones, ya que permite comunicarse con otros usuarios y compartir archivos y periféricos. Es decir, es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información.

Se entiende por red al conjunto interconectado de ordenadores autónomos. Se dice que dos ordenadores están interconectados, si éstos son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación

2.2.1 Introducción a las tecnologías LAN

Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo, lo que se desea lograr con estas redes es velocidades de transmisión de datos altas en distancias relativamente cortas.

Al implementar una red LAN, varios conceptos claves se presentan por si mismos. Uno es la elección del medio de transmisión, los cuales pueden ser par trenzado, coaxial, fibra óptica o medios inalámbricos.

Otro problema de diseño es cómo realizar el control de acceso, con un medio compartido resulta necesario algún mecanismo para regular el acceso al medio de forma eficiente y rápida. Los dos esquemas más comunes son CSMA/CD tipo Ethernet y anillo con paso de testigo. El control de acceso al medio a su vez está relacionado con la topología que adopte la red, siendo las más usadas el anillo, la estrella y el bus. De esta manera, podemos decir que los aspectos tecnológicos principales que determinan la naturaleza de una red LAN son:

- Topología
- Medio de transmisión
- Técnica de control de acceso al medio

2.3 Componentes Básicos de una Red

Servidor.- Es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones. Puede ser dedicado o no dedicado.

El sistema operativo de la red está cargado en el disco fijo del servidor, junto con las herramientas de administración del sistema y las utilidades del usuario.

La tarea de un servidor dedicado es procesar las peticiones realizadas por la estación de trabajo. Estas peticiones pueden ser de acceso a disco, a colas de impresión o de comunicaciones con otros dispositivos. La recepción, gestión y realización de estas peticiones puede requerir un tiempo considerable, que se incrementa de forma paralela al número de estaciones de trabajo activas en la red. Como el servidor gestiona las peticiones de todas las estaciones de trabajo, su carga puede ser muy pesada.

Se puede entonces llegar a una congestión, el tráfico puede ser tan elevado que podría impedir la recepción de algunas peticiones enviadas.

Cuanto mayor es la red, resulta más importante tener un servidor con elevadas prestaciones. Se necesitan grandes cantidades de memoria RAM para optimizar los accesos a disco y mantener las colas de impresión. El rendimiento de un procesador es una combinación de varios factores, incluyendo el tipo de procesador, la velocidad, el factor de estados de espera, el tamaño del canal, el tamaño del bus, la memoria caché así como de otros factores.

2.4 Topologías

Las topologías usuales en LAN son bus, árbol, anillo y estrella.

2.4.1 Topología en estrella

En redes LAN con topología en estrella, cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción. En general, existen dos alternativas para el funcionamiento del nodo central.

Una es el funcionamiento en modo de difusión, en el que la transmisión de la trama por parte de una estación se transmite sobre todos los enlaces de salida del nodo central.

En este caso, aunque la disposición física es una estrella, lógicamente funciona como un bus; una transmisión desde cualquier estación es recibida por el resto de las estaciones y solo puede transmitir una estación en un instante de tiempo dado. Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de

tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.

2.4.2 Control de acceso al medio

Todas las LAN constan de un conjunto de dispositivos que deben compartir la capacidad de transmisión de la red, de manera que se requiere algún método de control de acceso al medio con objeto de hacer un uso eficiente de esta capacidad. Esta es la función del protocolo de control de acceso al medio (MAC). Los parámetros clave en cualquier técnica de control de acceso al medio son dónde y cómo. Dónde se refiere a si el control se realiza en forma centralizada o distribuida. En un esquema centralizado se diseña un controlador con la autoridad para conceder el acceso a la red. En una red descentralizada, las estaciones realizan conjuntamente la función de control de acceso al medio para determinar dinámicamente el orden en que transmitirán. El segundo parámetro, Cómo viene impuesto por la topología y es un compromiso entre factores, tales como el costo, prestaciones y complejidad. En general, se pueden clasificar a las técnicas de control de acceso como sincronías o asíncronas. Con las técnicas sincronías se dedica una capacidad dada a la conexión, estas técnicas no son óptimas para redes LAN, dado que las necesidades de las estaciones son imprescindibles. Es preferible por lo tanto, tener la posibilidad de reservar capacidad de forma asíncrona (dinámica) más o menos, en respuesta a solicitudes inmediatas. La aproximación asíncrona se puede subdividir en tres categorías: rotación circular, reserva y competición. Con la rotación circular, a cada estación se le da la oportunidad de transmitir, ante lo que la estación puede declinar la proposición o puede transmitir sujeta a un límite. En cualquier caso, cuando termina debe ceder el turno de transmisión a la siguiente estación. Con las técnicas de contención no se realiza un control para determinar de quién es el turno, si no que todas compiten por acceder al medio, ésta es una técnica apropiada para el tráfico a ráfagas.

2.4.3 Tarjetas de Conexión de Red (NIC)

Una tarjeta de interfaz de red (NIC), o adaptador LAN, provee capacidades de comunicación en red desde y hacia un PC. En los sistemas computacionales de escritorio, es una tarjeta de circuito impreso que reside en una ranura en la tarjeta madre y provee una interfaz de conexión a los medios de red. En los sistemas computacionales portátiles, está comúnmente integrado en los sistemas o está disponible como una pequeña tarjeta PCMCIA, del tamaño de una tarjeta de crédito. PCMCIA es el acrónimo para Personal Computer Memory Card International Association (Asociación Internacional de Tarjetas de Memoria de Computadores Personales). Las tarjetas PCMCIA también se conocen como tarjetas PC. La NIC se comunica con la red a través de una conexión serial y con el computador a través de una conexión paralela. La NIC utiliza una Petición

de interrupción (IRQ), una dirección de E/S y espacio de memoria superior para funcionar con el sistema operativo. Un valor IRQ (petición de interrupción) es número asignado por medio del cual donde el computador puede esperar que un dispositivo específico lo interrumpa cuando dicho dispositivo envía al computador señales acerca de su operación. Por ejemplo, cuando una impresora ha terminado de imprimir, envía una señal de interrupción al computador. La señal interrumpe momentáneamente al computador, de manera que éste pueda decidir qué procesamiento realizar a continuación. Debido a que múltiples señales al computador en la misma línea de interrupción pueden no ser entendidas por el computador, se debe especificar un valor único para cada dispositivo y su camino al computador. Antes de la existencia de los dispositivos Plug-and-Play (PnP), los usuarios a menudo tenían que configurar manualmente los valores de la IRQ, o estar al tanto de ellas, cuando se añadía un nuevo dispositivo al computador.

2.4.4 Cableado

Una vez que tenemos las estaciones de trabajo, el servidor y las placas de red, requerimos interconectar todo el conjunto. El tipo de cable utilizado depende de muchos factores, que se mencionarán a continuación

Los tipos de cableado de red más populares son: par trenzado, cable coaxial y fibra óptica.

Además se pueden realizar conexiones a través de radio o microondas.

Cada tipo de cable o método tiene sus ventajas. y desventajas. Algunos son propensos a interferencias, mientras otros no pueden usarse por razones de seguridad.

La velocidad y longitud del tendido son otros factores a tener en cuenta el tipo de cable a utilizar.

2.4.5 Par Trenzado.-

El cable de par trenzado no blindado (UTP) es un medio de cuatro pares de hilos que se utiliza en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislante. Además, cada par de hilos está trenzado. Este tipo de cable cuenta sólo con el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aun más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.

El estándar TIA/EIA-568-B.2 especifica los componentes de cableado, transmisión, modelos de sistemas, y los procedimientos de medición necesarios para verificar los cables de par trenzado balanceado. Exige el tendido de dos cables, uno para voz y otro para datos en cada toma. De los dos cables, el cable de voz debe ser UTP de

cuatro pares. El cable Categoría 5 es el que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones. Sin embargo, las predicciones de los analistas y sondeos independientes indican que el cable de Categoría 6 sobrepasará al cable Categoría 5 en instalaciones de red. El hecho que los requerimientos de canal y enlace de la Categoría 6 sean compatibles con la Categoría 5e hace muy fácil para los clientes elegir Categoría 6 y reemplazar la Categoría 5e en sus redes. Las aplicaciones que funcionan sobre Categoría 5e también lo harán sobre Categoría 6.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios para networking. De hecho, el UTP cuesta menos por metro que cualquier otro tipo de cableado para LAN. Sin embargo, la ventaja real es su tamaño. Debido a que su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Esto puede ser un factor sumamente importante a tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se está instalando el cable UTP con un conector RJ-45, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad. El cableado de par trenzado presenta ciertas desventajas. El cable UTP es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios para networking y la distancia que puede abarcar la señal sin el uso de repetidores es menor para UTP que para los cables coaxiales y de fibra óptica.

El cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable de par trenzado es el más rápido entre los medios basados en cobre.

Para que sea posible la comunicación, la señal transmitida por la fuente debe ser entendida por el destino. Esto es cierto, tanto desde una perspectiva física como en el software. La señal transmitida necesita ser correctamente recibida por la conexión del circuito que está diseñada para recibir las señales. El pin de transmisión de la fuente debe conectarse en fin al pin receptor del destino. A continuación se presentan los tipos de conexiones de cable utilizadas entre dispositivos de internetwork.

El cable que se conecta desde el puerto del switch al puerto de la NIC del computador recibe el nombre de cable directo.

El cable que conecta un puerto de un switch al puerto de otro switch recibe el nombre de cable de conexión cruzada.

El cable que conecta el adaptador de RJ-45 del puerto COM del computador al puerto de la consola del router o switch recibe el nombre de cable rollover. A continuación se mostrara los cables:

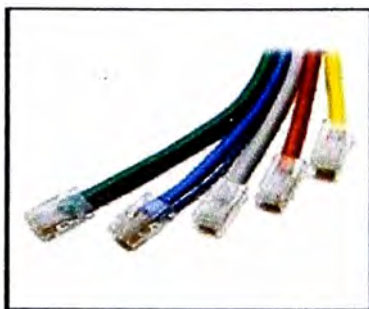


Figura 2.1 Cables , fuente : www.panduit.com

Estaciones de Trabajo:

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los hosts se ven sumamente limitadas. Los dispositivos host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneo de imágenes o acceso a bases de datos PC's conectadas a la red, a través de las cuales podemos acceder a los recursos compartidos en dicha red, como discos, impresoras, módems, etc. Pueden carecer de la mayoría de los periféricos pero siempre tendrán un NIC, un monitor, un teclado y un CPU.

Servidores:

Computadores que proporcionan servicios a las estaciones de trabajo de la red, tales como almacenamiento en discos, acceso a las impresoras, unidades para respaldo de archivos, acceso a otras redes o computadores centrales.

Repetidores:

Un repetidor es un dispositivo de red que se utiliza para regenerar una señal. Los repetidores regeneran señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación. Un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un router o puente.

Puente:

Los puentes convierten los formatos de transmisión de datos de la red, además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.

Routers:

Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden

conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

Switch Ethernet:

Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.

Telnet

Conecta a una computadora remota como si nuestra computadora fuera un terminal en la misma. Esto hace posible que tengamos acceso a todo el Software y recursos de la máquina a la que nos conectamos, incluso que ejecutemos programas en ella

2.5 Características de las Redes:

Los sistemas operativos sofisticados de red local, ofrecen un amplio rango de servicios. Aquí se citarán algunas características principales:

Servicios de archivos.-Las redes y servidores trabajan con archivos. El administrador controla los accesos a archivos y directorios. Se debe tener un buen control sobre la copia, almacenamiento y protección de los archivos.

Compartir recursos.- En los sistemas dedicados, los dispositivos compartidos, como los discos fijos y las impresoras, están ligados al servidor de archivos, o en todo caso, a un servidor especial de impresión.

SFT(Sistema de tolerancia a fallas).- Permite que exista un cierto grado de supervivencia de la red, aunque fallen algunos de los componentes del servidor. Así, si contamos con un segundo disco fijo, todos los datos del primer disco se guardan también en el de reserva, pudiendo usarse el segundo si falla el primero.

Sistema de Control de Transacciones.- Es un método de protección de las bases de datos frente a la falta de integridad. Así, si una operación falla cuando se escribe en una base de datos, el sistema deshace la transacción y la base de datos vuelve a su estado correcto original.

Seguridad.- El administrador de la red es la persona encargada de asignar los derechos de acceso adecuados a la red y las claves de acceso a los usuarios. El sistema operativo con servidor dedicado de Novell es uno de los sistemas más seguros disponibles en el mercado.

2.6 Seguridad Informática.- Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la

información contenida). Para ello, existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Técnicas para asegurar el sistema:

- Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red. Zona desmilitarizada
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.
- Sistema de Respaldo Remoto. Servicio de backup remoto.

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

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

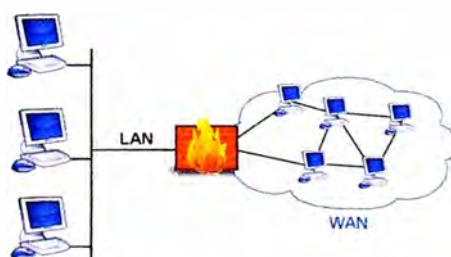


Figura 2.2 Firewall, Fuente: www.cisco.com

Acceso Remoto.- Gracias al uso de líneas telefónicas, Ud. podrá conectarse a lugares alejados con otros usuarios.

Conectividad entre Redes.- Permite que una red se conecta a otra. La conexión habrá de ser transparente para el usuario.

Comunicaciones entre usuarios.- Los usuarios pueden comunicarse entre sí fácilmente y enviarse archivos a través de la red.

Servidores de impresoras.- Es una computadora dedicada a la tarea de controlar las impresoras de la red. A esta computadora se le puede conectar un cierto número de impresoras, utilizando toda su memoria para gestionar las colas de impresión que almacenará los trabajos de la red. En algunos casos se utiliza un software para compartir las impresoras.

Colas de impresión.- Permiten que los usuarios sigan trabajando después de pedir la impresión de un documento.

Sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Scrip Kiddies que usan herramientas automáticas.

Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos

2.7 Estructura de las Redes

Las redes de computadores personales son de distintos tipos, y pueden agruparse de la siguiente forma:

Sistemas punto a punto.- En una red punto a punto, donde cualquiera de sus estaciones puede funcionar como servidor, puesto que puede ofrecer sus recursos a las restantes estaciones de trabajo. Así mismo, pueden ser receptores que pueden acceder a los recursos de otras estaciones sin compartir la suyas propias. Es decir, el concepto básico es la compartición de recursos. Sin embargo, poseen algunas desventajas: falta de seguridad y velocidad.

Sistemas con servidor dedicado.- Un sistema operativo de red local ejecutándose en modo dedicado utilizará todos los recursos de su procesador, memoria y disco fijo a su uso por parte de la red. En estos sistemas, los discos fijos reciben un formato especial. Fundamentalmente, ofrecen la mejor respuesta en tiempo, seguridad y administración.

El Netware de Novell se puede usar en modo dedicado.

Sistemas con servidor no dedicado.- Ofrece las mismas posibilidades que un sistema dedicado, añadiendo la posibilidad de utilizar el servidor como estación de trabajo. El servidor se convierte en dos máquinas. No obstante, disminuye su eficiencia.

Razones para instalar redes

Desde sus inicios, una de las razones para instalar redes era compartir recursos, como discos, impresoras y trazadores. Ahora existen además otras razones:

Disponibilidad del software de redes.- El disponer de un software multiusuario de calidad que se ajuste a las necesidades de la empresa. Por ejemplo: Se puede diseñar un sistema de puntos de venta ligado a una red local concreta. El software de redes puede bajar los costos si se necesitan muchas copias del software.

Trabajo en común.- Conectar un conjunto de computadoras personales formando una red que permita que un grupo o equipo de personas involucrados en proyectos similares puedan comunicarse fácilmente y compartir programas o archivos de un mismo proyecto.

Actualización del software.- Si el software se almacena de forma centralizada en un servidor es mucho más fácil actualizarlo. En lugar de tener que actualizarlo individualmente en cada uno de los PC de los usuarios, pues el administrador tendrá que actualizar la única copia almacenada en el servidor.

Copia de seguridad de los datos.- Las copias de seguridad son más simples, ya que los datos están centralizados.

Ventajas en el control de los datos.- Como los datos se encuentran centralizados en el servidor, resulta mucho más fácil controlarlos y recuperarlos. Los usuarios pueden transferir sus archivos vía red antes que usar los disquetes.

Uso compartido de las impresoras de calidad.- Algunos periféricos de calidad de alto costo pueden ser compartidos por los integrantes de la red. Entre éstos: impresoras láser de alta calidad, etc.

Correo electrónico y difusión de mensajes.- El correo electrónico permite que los usuarios se comuniquen más fácilmente entre sí. A cada usuario se le puede asignar un buzón de correo en el servidor. Los otros usuarios dejan sus mensajes en el buzón y el usuario los lee cuando los ve en la red. Se pueden convenir reuniones y establecer calendarios.

Ampliación del uso con terminales tontos.- Una vez montada la red local, pasa a ser más barato el automatizar el trabajo de más empleados por medio del uso de terminales tontos a la red.

Seguridad.- La seguridad de los datos puede conseguirse por medio de los servidores que posean métodos de control, tanto software como hardware. Los terminales tontos impiden que los usuarios puedan extraer copias de datos para llevárselos fuera del edificio.

2.8 Servicios:

Correo Electrónico (e-mail).- Servicios que permite conectar ordenadores mediante un sistema de correo personal. Cada usuario tiene asignada una dirección en la que recibe todos los mensajes que se le envíen en cuestión de minutos.

Usenet News.- Sistemas de conferencias que permite agrupar a personas interesadas en diversas áreas. Una conferencia es un foro multimedia a través del que se intercambia información de muy diversa naturaleza.

Chat.- Sistema de conferencia que se establece entre los usuarios de las terminales que se encuentra disponibles en la empresa y que permite el intercambio de información en tiempo real.

Telnet.- Protocolo que permite conectarse con otro ordenador de la red de Internet.

Ftp.- Protocolo que permite la transferencia de ficheros de un ordenador a otro.

Proveedor

Son entidades o empresas que dan acceso a Internet a otras empresas o a particulares con un costo determinado, tienen la capacidad de crear e introducir contenidos dentro de la red.

Usuario

Personas que a través de un proveedor acceden a Internet y toda la información y servicio.

Rack: (soporte metálico) es una estructura de metal muy resistente, generalmente de forma cuadrada de aproximadamente 3mt de alto por uno de ancho, en donde se colocan los equipos, que son ajustados al rack sobre sus orificios laterales mediante tornillos

Pach Panel's: son estructuras de metal con placas de circuitos que permiten interconexión entre equipos. Un Pach Panel's posee una determinada cantidad de puertos (RJ45 End Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas o dientes. En estos conectores es donde se colocan las cerdas de los cables provenientes de las cajas de distribución u otros Pach Panel's.

La idea de los Pach Panel's, además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan los equipos de una red de una mejor manera.

Dato: Técnicamente un dato es un hecho o una cifra en bruto, sin procesar.

Información: Conjunto de datos procesados expresados con un sentido lógico.

Mensaje: Información que se pretende llegue del emisor al receptor por medio de un sistema de comunicación.

Sistema: Conjunto de elementos interrelacionados armónicamente para alcanzar un objetivo común.

Sistema Operativo: Programa de control maestro que administra el funcionamiento del sistema informático interactuando con los programas de aplicación.

Trama de Red: es una unidad de envío de datos. Viene a ser el equivalente de paquete de datos o Paquete de red, en el Nivel de enlace de datos del modelo OSI.

Normalmente una trama constará de cabecera, datos y cola. En la cola suele estar algún chequeo de errores. En la cabecera habrá campos de control de protocolo. La parte de datos es la que quiera transmitir en nivel de comunicación superior, típicamente el Nivel de red.

En la capa de enlace la facilidad de área extensa por la que se pueden comunicar los sistemas mediante un protocolo de la capa de enlace de datos.

2.9 Centro de procesamiento de datos (Data Center) : aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Una vez acondicionado el habitáculo, se procede a la instalación de las computadoras, las redes de área local, etc. Esta tarea requiere un diseño lógico de redes y entornos, sobre todo en aras a la seguridad. Algunas actuaciones son:

- Creación de zonas desmilitarizadas (DMZ).
- Segmentación de redes locales y creación de redes virtuales (VLAN).
- Despliegue y configuración de la electrónica de red: pasarelas, encaminadores, conmutadores, etc.
- Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
- Creación de la red de almacenamiento.
- Instalación y configuración de los servidores y periféricos.
- Etc

2.10 SISTEMA DE COMUNICACIÓN

Sistema que transmite información desde un lugar (emisor) a otro (receptor)

Origen: Quien posee la información.

Destino: Quien espera recibir la información

Emisor: Punto de origen que emplea un sistema de comunicación para transmitir un mensaje.

Receptor: Punto de destino del mensaje que se ha transmitido por un medio de un sistema de comunicación

Canal : Es el medio de transmisión de los mensajes

2.11 TIPOS DE ONDAS

Onda: Una onda es una perturbación que se propaga, las ondas materiales (todas menos las electromagnéticas) requieren un medio elástico para propagarse.

El medio elástico se deforma y se recupera vibrando al paso de la onda.

Longitud de onda, frecuencia y período

Ciclo (Oscilación): Serie completa de sucesos

Longitud de onda: como la distancia que recorre el pulso mientras un punto realiza una oscilación completa.

Período (T): El tiempo que tarda en realizar una oscilación

Frecuencia (F): Es el número de oscilaciones (vibraciones) que efectúa cualquier punto de la onda en un segundo.

Tipos de Ondas: Ondas transversales y Ondas longitudinales

En función del soporte que requieren para su propagación las ondas se clasifican en mecánicas y electromagnéticas. Las mecánicas requieren un medio elástico para propagarse y las electromagnéticas se pueden propagar en el vacío.

Si las clasificamos en función de cómo vibran respecto a la dirección de propagación, tenemos las ondas transversales y las longitudinales.

Si las partículas del medio en el que se propaga la perturbación vibran perpendicularmente a la dirección de propagación, las ondas se llaman transversales. Si vibran en la misma dirección se llaman longitudinales.

2.12 CODIFICACIÓN DE LA INFORMACIÓN

Definición: La información para ser transmitida, necesita ser adaptada al medio de transmisión . Para ello, será preciso codificarla, de tal forma que pueda asegurarse una recepción clara y segura.

Si tenemos la información en un determinado alfabeto fuente y queremos transformarla en otro alfabeto destino, podemos definir codificación como la realización de dicha transformación, siendo el código la correspondencia existente entre cada símbolo del alfabeto fuente y cada conjunto de símbolos (palabras) del alfabeto destino.

Código Morse: Primer código utilizado para la transmisión a distancia a través de señales eléctricas, inventado por el físico norte americano Samuel F. B. Morse en 1820 lo que dio origen al telégrafo electromagnético. Este en 1896 se convirtió en el telégrafo sin hilos o radio telégrafo.

El código Morse esta conformado por puntos y rayas que se diferencian en el tiempo de duración de la señal activa o 1. Un 1 corto corresponde al punto y un largo (aproximadamente de duración de tres veces el punto) corresponde a la raya. Entre cada dos símbolos (punto o raya) existe un 0 separador o ausencia de señal, cuya duración es aproximadamente la del punto. La separación entre caracteres es tres veces mayor que la del punto, y para la separación de palabras transmitidas el tiempo es de 7 veces el del punto. Todas estas referencias y la propia duración del punto en unidades de tiempo dependerán de la velocidad de transmisión que se utilice.

Código Baudot: Inventado por Emile Baudot en 1874. Se trata de un código de 5 bits capaz de representar hasta 32 caracteres distintos, pero tiene además 2 de ellos que permiten conmutar entre dos grupos denominados letras y figuras. El grupo de letras contiene el abecedario completo de mayúsculas de la A a la Z, mientras que el grupo de figuras contiene las cifras del 0 al 9, los signos de puntuación y caracteres especiales hasta un total de 26.

Código Binario: El proceso de asignar a cada objeto perteneciente a un conjunto una secuencia de bits, o especificar las reglas que lo relacionan, es crear un código binario.

Las señales que maneja un ordenador son señales biestado a las que se asignan los valores 0 y 1, es decir, el ordenador sólo puede trabajar con información binaria. El problema es que la información que maneja el usuario y que le envía al ordenador no tiene por qué ser información binaria. El usuario trabaja con números en base diez y con las letras del abecedario, por ejemplo, y no con ceros y unos. Cualquier objeto se representa en un ordenador mediante una secuencia de bits y, por tanto, es necesario un sistema de codificación que establezca una correspondencia entre la información que se le da a un ordenador y esas secuencias de bit.

objeto1 >> secuencia1

objeto2 >> secuencia2

objeto3 >> secuencia3

Un ejemplo de código binario para las cuatro primeras letras del abecedario podría ser:

A >> 00

B >> 01

C >> 10

D >> 11

El número de objetos diferentes que se pueden codificar con n bits son 2^n (2 elevado a n). Así, con 2 bits podemos codificar como mucho, 4 objetos, y con 8 bits (un byte) podemos codificar hasta 256 objetos.

Existen varios criterios genéricos para establecer esta correspondencia que dan lugar a tipos diferentes de códigos. Dichos criterios se denominan sistemas de codificación

Utilidad del Código: Un código se dice que es útil cuando existe una correspondencia biunívoca y recíproca entre los símbolos del alfabeto fuente y las palabras del alfabeto destino.

Código Redundante: Cuando existen palabras del alfabeto destino no utilizadas o sin significado o parte de los símbolos podrían no ser necesarios, aunque en general, estos símbolos se utilizan para controlar posibles errores.

2.13 PROBLEMAS DE LA TRANSMISIÓN

Contaminaciones de la señal

Capacidad del canal: Es la cantidad máxima de unidades de información que pueden transferirse por unidad de tiempo a través de un canal, la capacidad de Bits por segundo depende de:

- El ancho de banda (W)
- La potencia de la señal (S)
- La potencia del ruido (N)

$$C = W \cdot \text{Log}_2 (1 + S / N) \quad (2.1)$$

C está medido en bits por segundo. Si el logaritmo está tomado en base 2, W se medirá en hercios; la señal y el poder del ruido S y N se miden en vatios o voltios.

Ancho de Banda: Es el rango de frecuencias a las cuales es permitido transitar por un canal de comunicación, aquellas frecuencias por fuera de este rango se eliminan. Se encuentra relacionado con la cantidad de datos que una línea puede transportar.

Velocidad de Modulación (Vm): Es el número máximo de veces que puede cambiar (conmutar) la señal en el canal, su unidad de medida es el **baudio**.

Velocidad de Transmisión (Vt) : Es el número de elementos binarios (bits) enviados por el canal por unidad de tiempo, su unidad de medida son los bits por segundo.

Relación Señal Ruido (Signal to Noise Ratio): Es la relación entre la cantidad de señal deseada y el ruido no deseado en un punto del cable. (Potencia de la señal sobre la potencia del ruido)

2.14 Tipos de cables

El funcionamiento del sistema cableado deberá ser considerado, no sólo cuando se están apoyando necesidades actuales, sino también cuando se anticipan necesidades futuras. Hacer esto permitirá la migración a aplicaciones de redes más rápidas, sin necesidad de incurrir en costosas actualizaciones de sistema de cableado. Los cables son el componente básico de todo sistema de cableado existen diferentes tipos de cables. La elección de uno respecto a otro depende del ancho de banda necesario, las distancias existentes y el coste del medio.

Cada tipo de cable tiene sus ventajas e inconvenientes; no existe un tipo ideal. Las principales diferencias entre los distintos tipos de cables radican en la anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la amortiguación de la señal y la distancia recorrida.

En la actualidad existen básicamente tres tipos de cables factibles de ser utilizados para el cableado en el interior de edificios o entre edificios:

- Coaxial
- Par Trenzado (2 pares)
- Par Trenzado (4 pares)
- Fibra Óptica

(De los cuales el cable Par Trenzado(2 y 4 pares) y la Fibra Óptica son reconocidos por la norma **ANSI/TIA/EIA-568-A** y el Coaxial se acepta pero no se recomienda en instalaciones nuevas).

A continuación se describen las principales características de cada tipo de cable, con especial atención al par trenzado y a la fibra óptica, por la importancia que tienen en las instalaciones actuales, así como su implícita recomendación por los distintos estándares asociados a los sistemas de cableado.

Cable Coaxial

El cable coaxial para banda base y el cable coaxial para banda ancha son muy parecidos en su construcción, pero sus principales diferencias son: la cubierta del cable, los diámetros y la impedancia.

El cable coaxial para banda base es de 3/8 de pulgada y utiliza una cubierta de plástico, mientras que el cable coaxial para banda ancha es de 1/2 pulgada y está cubierto de una malla o tela de aluminio y funda protectora de plástico.

Coaxial Grueso (IEEE 802.3 10Base5)

Opera en la transferencia de datos a 10 Mbps en una sola banda (banda ancha) y alcanza distancias máximas de 500m. Transmisión análoga.

Banda Ancha= Frecuencia superior a 4Khz

10= velocidad en Mbps

5= 5 multiplicado por 100

Impedancia 75 !

Frecuencia 300 Mhz

El tipo de conector utilizado es el tipo N

Coaxial Delgado (IEEE 802.3 10Base2)

Opera en la transferencia de datos a 10 Mbps en banda base y alcanza distancias máximas de 185m. Transmisión digital.

10= velocidad en Mbps

Impedancia 50 !

El tipo de conector utilizado es el tipo BNC

Par Trenzado (Twisted Pair) IEEE 10BaseT

Son dos hilos de cobre aislados, generalmente de 1mm de espesor entrelazados en forma helicoidal. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran alrededor (Dos cables paralelos se constituyen en una antena simple, en tanto un par trenzado no). El ancho de banda depende del grosor y la longitud. Se usan tanto para transmisión analógica como digital y es recomendado por la normativa EIA/TIA 568 se divide en:

UTP (Unshielded Twisted Pair)

Utilizado generalmente en el sistema telefónico, por lo general vienen 4 pares de hilos cubiertos por una funda plástica, y algunas veces tienen cubiertas de aluminio para ayudar a incrementar la velocidad de transmisión de datos y protegerlos del ruido

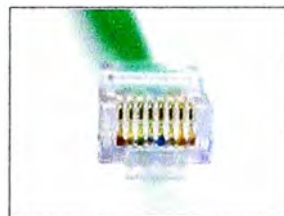


Figura 2.3 Jack RJ-45 y Conectores RJ-45, Fuente: www.panduit.com

STP (Shielded Twisted Pair)

Cada par se cubre con una malla metálica, de la misma forma que los cables coaxiales, y el conjunto de pares se recubre con una lámina blindada. Se referencia frecuentemente con sus siglas en inglés STP (Shield Twisted Pair, Par Trenzado blindado).

El empleo de una malla blindada reduce la tasa de error, pero incrementa el coste, al requerirse un proceso de fabricación más costoso.

Existen varios niveles en este tipo de cable y depende de la velocidad a la que queramos transmitir

Nivel 3.

Este nivel se usa para soportar hasta 10 Mbps y distancias de 90 metros. Generalmente se usa en redes Ethernet que no pretenden utilizar altos volúmenes de transferencia, como pudieran ser imágenes, video etcétera.

Nivel 4.

Este nivel se utiliza para garantizar hasta 20 Mbps y distancias de 100mts. Este tipo de cable puede utilizarse para las tecnologías Ethernet y/o Token Ring 4/16 Mbps. Al igual que la anterior, no soporta grandes transferencias de información.

Nivel 5.

Este es el nivel más usado en la actualidad, debido a que garantiza hasta 100 Mbps y 100 metros de estación a estación . Es el recomendado para la transferencia de imágenes, video, videoconferencias, etcétera.

Entre mayor sea el nivel, mayor son los costos. La diferencia entre ellos es la cantidad de trenzas por pulgada con que cuenta el cable, además de el recubrimiento que se le da a cada uno de ellos.

Especificaciones:

- Distancia máxima 100 metros
- Impedancia 100 !
- Mínimo 2 pares
- Máxima velocidad de transferencia entre 10 y 100 Mbps.

Emplea conectores RJ45

Fibra Óptica

Los cables de fibra óptica se usan para transmitir señales digitales de datos en forma de pulsos modulados de luz. La fibra óptica consiste en un cilindro de vidrio extremadamente delgado, llamado centro (Core) y recubierto de vidrio conocido como Cladding. Se usa tanto en banda base como en banda ancha. Existen dos fibras por cable, una de transmisión y otra de recepción.

La fibra puede transmitir a 100Mbps y no tiene interferencias de ningún tipo, la distancia máxima recomendada es de 1000m.

Tipos: Puede ser unimodo (Single Mode) y multimodo (multimode).

La unimodo se utiliza para grandes distancias y requiere de un láser

La multimodo se usa en distancia más pequeñas, es más barata y emplea un diodo emisor de luz (Led). Usa conectores ST y SMA

2.15 Tipos de Señal

Señal análoga: Usa variaciones (modulaciones) en una señal, para enviar información. Es especialmente útil para datos en forma de ondas como las ondas del sonido. Las señales análogas son las que usan normalmente su línea de teléfono y sus parlantes.

Las señales análogas toman un conjunto infinito de valores en un intervalo de interés.

-El equipo usado para efectuar esta transformación se le denomina genéricamente Digitalizador.

- Si la red es análoga y las señales que se desean transmitir son digitales deben ser previamente moduladas.

- Al equipo usado para efectuar esta transformación se le denomina genéricamente Modem.
- Debido a la Atenuación propia del medio, las señales análogas deben ser Amplificadas por consiguiente, el ruido que acompaña a la señal también es amplificado.
- La información esta contenida en la forma de onda que se transmite.

Las señales análogas se pueden modular en:

Amplitud Modulada: Se emplean dos niveles diferentes de voltajes para representar el 0 y el 1 respectivamente.

Frecuencia Modulada: Se utilizan dos o más tonos diferentes.

Modulación por Fase: La portadora se desplaza en forma sistemática 45,135,225 ó 315 grados, en intervalos espaciados de manera uniforme, y para cada uno de estos desplazamientos de fase transmite 2 bits de información.

Señal Digital: Es una corriente de 0 y 1 toman un conjunto finito de valores en un intervalo de interés.

- La información esta contenida en los pulsos codificados que se transmiten.
- Cuando la red es digital y las señales que se desean transmitir son análogas, estas deben ser previamente digitalizadas.
- Debido a la Distorsión provocada por el medio, las señales digitales deben ser regeneradas, por consiguiente la señal transmitida mantiene su forma original hasta llegar al destino.

La señal digital se puede modular por Pulse Coded Modulation (PCM)

Cuando se habla por teléfono sale una señal análoga normal que después se digitaliza mediante un Codec produciendo un numero de 7 u 8 bits. El Codec efectúa 8000 muestras por segundo ($125 \mu s$ /muestra) con este número de muestras es suficiente para capturar toda la información de un ancho de banda de 4Khz.

2.16 Tipos de Transmisión.

Serie: Transmisión sobre un canal de una sola línea, la mayoría de las redes de comunicaciones utilizan la transmisión en serie entre terminales y computadoras. En la transmisión serie los bits van uno detrás de otro a través de un cable. Se requiere de una sincronización.

Paralelo: Los datos pueden transmitirse entre ordenadores y terminales mediante cambios de corriente o tensión en un cable, salen un grupo de bits a la vez por varias líneas (Se puede decir que el paralelo es la unión de varias series), o sea cada bit de un carácter se traslada por su propio cable.

Hay una señal llamada Strobe o reloj que va sobre un cable adicional e indica al receptor cuando están presentes todos los bits sobre sus respectivos cables para que se pueda tomar una muestra de valores.

La comunicación en paralelo es útil a corta distancia, siendo más rápida.

Direccionabilidad del canal

Simplex: Transmisión en un sentido, o sea la comunicación se hace de un emisor a un receptor, el cual recibe el mensaje y no puede contestar inmediatamente debido a que solo puede leer el mensaje.

Half Duplex: Transmisión de datos en ambas direcciones, pero una sola dirección a la vez. En cada instante la dirección es en un solo sentido.

Full Duplex: Transmisión y recepción simultánea de señales

Tipos de Comunicación.

Sincronización: Cuando transmitimos en serie en un canal debemos tener en cuenta lo siguiente:

- ¿Cuándo debo interpretar la señal?
- ¿Cómo debo interpretar la señal?

El ponerse de acuerdo en estos puntos es lo que llamamos Sincronismo (el emisor informa al receptor sobre los instantes en que se va a transmitir las señales), las comunicaciones pueden ser de tipo Sincrónica o Asincrónica.

Asincrónica: Esta orientada a transmisión de caracteres, la unidad de información (cada carácter) va acompañada de un bit de arranque o cabecera (start) y uno o dos bits de parada o terminación (stop). El bit de arranque tiene funciones de sincronización de los relojes del transmisor y del receptor activando los mecanismos de muestreo, cuenta y recepción de las señales que seguirán. El bit o bits de parada se usan para separar un carácter del siguiente.

Se acostumbra agregar un bit de paridad (par o impar) a continuación de los bits de información. El intervalo de tiempo para transmisión de datos es diferente para cada información, como quien dice NO existe relación temporal entre el envío de un carácter y el envío del siguiente.

Una ventaja del asincrónico es la poca pérdida de información en una falla pues transmite de uno a uno, pero esto lo hace lento y no aprovecha toda la línea de transmisión.

Sincrónica: Surge ante la necesidad de obtener un mayor rendimiento en la relación entre los bits útiles y los bits transmitidos. Existen dos relojes, uno en el emisor y otro en el receptor. Esta orientada a la transmisión de bloques de caracteres. La información útil es transmitida entre dos grupos denominados genéricamente delimitadores, siendo el delimitador de encabezado el que se encarga de sincronizar los relojes. Los paquetes viajan en el mismo intervalo de tiempo. La línea de transmisión siempre está en actividad, si no se envía información se transfieren caracteres especiales de sincronización y relleno, está orientada a transmitir bloques de caracteres. La señal de sincronismo en el extremo fuente será común para ambos equipos y en ambos extremos de la línea.

Presenta una mayor velocidad, dando un alto rendimiento en la transmisión, aprovechando mejor la línea, pero en caso de falla debe retransmitir mayor cantidad de bytes.

Multiplexar: Es colocar simultáneamente dos o más transmisiones separadas en un mismo canal. Se puede hacer por frecuencia y tiempo.

Multiplexión por División de Frecuencia (FDM): Consiste en poner a viajar en un canal de comunicaciones señales a diferentes frecuencias. Se aprovecha el ancho de banda disponible del circuito y se le subdivide en subcanales, donde cada uno tiene una frecuencia para transmitir los binarios 1 y 0. Para separarlos se utilizan guarda bandas

Guarda Banda: Porciones No usadas del ancho de banda que separan cada par de frecuencias de las otras, busca eliminar la interferencia entre subcanales.

Una ventaja es que en un instante de tiempo (t), todos los canales transmiten simultáneamente, pero una vez definidos los subcanales es difícil adicionar más.

Multiplexión por División de Tiempo (TDM): Comparte el uso del circuito de comunicaciones entre varias terminales, donde cada una tiene su tiempo asignado para el uso del canal. En el instante en que una terminal transmite en un tiempo (t) utiliza todo el ancho de banda del medio. El tiempo asignado es igual para todos.

Conmutación

Relacionado con la selección de la(s) mejor(es) rutas (trayectorias) que permiten que la información viaje de fuente a destino. La conmutación puede ser:

Conmutación de Circuitos: Establece el camino o ruta antes de transmitir (Quien realiza la llamada determina el destino enviando un mensaje especial a la red con la dirección del receptor de la llamada). Se establece una línea de comunicación directa entre las estaciones a través de la conmutación adecuada de todos los nodos intermedios.

El mensaje solo puede ser enviado cuando quien efectúa la llamada se da cuenta que esta ha sido establecida (ejemplo la telefonía). No es ideal para la transmisión de datos.

Conmutación de Mensajes: En este tipo de conmutación no hay un establecimiento anticipado de ruta entre el que envía y el que recibe. En su lugar cuando el que envía tiene listos un bloque de datos, éste se almacena en la primera central de conmutación (IMP) para expedirse después dándose un solo salto a la vez. Cada bloque se recibe íntegramente, se revisa en busca de errores y se transmite con posterioridad.

Conmutación de Paquetes: Es la más utilizada en la transmisión de datos, en este método los mensajes son divididos en submensajes de igual longitud llamados Paquetes. Cada paquete se enruta de manera independiente de fuente a destino. El desensamble del mensaje se realiza en el nodo fuente antes de proceder a realizar la entrada a la red y cada paquete es colocado dentro de una trama de bits que contiene la información necesaria acerca del paquete:

- Dirección de destino
- Número de secuencia de paquete
- Información para detectar errores

Los paquetes pueden alcanzar el destino por diferentes caminos y orden.

2.17 NIVEL DE ENLACE O DATOS (Data Link Layer)

El nivel de datos es donde los bits tienen algún significado en la red, recibe los paquetes del nivel de red (Network Layer), los prepara en forma correcta (tramas) para poder enviarlos (transmitirlos) a el nivel físico.

De igual forma sucede cuando recibe bits del nivel físico y tiene que ponerlos correctamente (tramas) para verificar si la información que esta recibiendo está libre de errores, si vienen en orden, si no faltan algunos de ellos, etcétera, para poder entregarlos al nivel de red sin ningún error.

Dentro de sus funciones se incluyen la de notificar al emisor (computadora remota) si alguna trama se recibió en el mal estado (basura), o si se omitieron algunas de las tramas y se requiere que sean enviadas nuevamente (retransmisión); de igual manera, se debe notificar si una trama esta duplicada o llego sin problemas. Es responsable en saber donde comienza la transmisión de la trama y donde termina, así como garantizar hasta qué punto las computadoras se encuentran sincronizadas y si emplean el mismo sistema de codificación y decodificación.

El nivel de datos o enlace tiene a su cargo la integridad de la recepción y envío de la información. Los datos se transmiten en forma de Tramas.

La IEEE en febrero de 1980 normalizó la capa física y de enlace (de datos) y la denominó 802. Aunque estaban de acuerdo con el modelo OSI pensaban que era necesario tratar con mayor detalle esta capa, por lo cual la dividieron en dos subniveles: el Control de Acceso al Medio MAC (IEEE 802.1) y el Control de Enlace Lógico LLC (IEEE 802.2).

Estudiaremos:

Sub Capa MAC` (IEEE 802.1)

- CsmA/Cd (IEEE 802.3)

Método No Persistente

Método P Persistente

Método 1 Persistente

- Token Bus (IEEE 802.4)

- Token Ring (IEEE 802.5)

Control de Enlace Lógico (Logical Link Control-LLC) IEEE 802.2

Sub Capa MAC (IEEE 802.1)

La sub capa MAC es especialmente importante en las LAN (Red de Área Local), dado que casi todas ellas utilizan un canal de acceso múltiple como base para sus

comunicaciones (El problema es determinar quien tiene el derecho de utilizar el canal cuando existe una competición por este). A diferencia de esto, una WAN (Red de Área Extendida) utiliza enlaces punto a punto, con excepción de las redes satélite.

El subnivel MAC es el nivel inferior y proporciona a la tarjeta de red de la computadora un acceso compartido hacia el nivel físico. El nivel MAC se comunica directamente con la tarjeta de red y es responsable de la entrega de los datos sin errores entre dos computadores en la red.

Para evitar posibles colisiones, los terminales escuchan el medio antes de poder transmitir, esto es lo que denominamos CSMA/CD (Acceso Múltiple por Detección de Portadora con detección de Colisión).

CSMA/CD (IEEE 802.3) Carrier Sense Acces/Colision Detect.

Método de acceso con análisis de portadora y detección de colisión. Cuando una estación desea transmitir, escucha la información que fluye a través del cable. Si el cable se encuentra ocupado, la estación espera hasta que esté en estado inactivo, en caso contrario, transmite de inmediato. Si dos o más estaciones en forma simultánea comienzan a transmitir en un cable inactivo, generara una colisión. Estas estaciones terminarán su transmisión, esperarán un tiempo aleatorio y repetirán de nuevo todo el proceso completo. El método de acceso al medio es Probabilístico.

CD (Colisión Detect)

Cuando se ha generado una colisión, existen algunos protocolos para reiniciar la transmisión como son:

- Método No Persistente
- Método P Persistente
- Método 1 Persistente.

NO PERSISTENTE

Antes de empezar a transmitir la estación escucha el canal, si nadie está transmitiendo, la estación empieza a hacerlo sola. Sin embargo, si el canal ya se encuentra en uso, la estación no está escuchando el canal continuamente, con el propósito de utilizarlo en el momento en que detecte la terminación de la transmisión anterior, si no mas bien, espera un intervalo aleatorio de tiempo para después transmitir el algoritmo.

P PERSISTENTE

Cuando una estación esta lista para empezar a transmitir, escucha el canal; si éste se encuentra desocupado, la estación transmite con una probabilidad p .

P = Probabilidad que la estación transmita

$P = 0.25$, se genera un número aleatorio K

Si $K \geq P$

No transmito

Sino

Transmito

Probabilidad = $\frac{1}{4} = 0.25 = 25\%$

N Estaciones 4

Se genera $K = 0.30$ No transmite

Se genera $K = 0.20$ Si transmite

Si N aumenta , P disminuye.

UNO PERSISTENTE

Cuando una estación desea enviar alguna información, primero escucha el canal para saber si alguien está transmitiendo; si el canal está efectivamente ocupado, la estación espera hasta que quede libre. Cuando la estación detecta un canal libre, empieza a transmitir la trama. Si llega a ocurrir una colisión, la estación espera durante un intervalo de tiempo aleatorio, para después empezar todo de nuevo. A este protocolo se le llama 1 persistente, porque la estación transmite con probabilidad 1, cada vez que encuentre el canal desocupado.

$P = 1$

Generar $K < 1$ (Menor que P)

Si $K \geq P$

No transmito

Sino

Transmito

Siempre intenta retransmitir

CAPITULO III METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

3.1 TIPOS DE CONEXIONES EMPLEADAS

A continuación listamos las tecnologías que se han utilizado o se utilizan para acceder a las Centrales de Riesgos:

3.1.1 Analógico (hasta 56k)

También llamado acceso dial-up, es económico pero lento. Se utiliza un módem interno o externo en donde se conecta la línea telefónica. La computadora se conecta a través de un número telefónico (que provee el ISP) para conectarse a la red Lan. El módem convierte la señal analógica (el sonido) en señal digital para recibir datos, y el proceso inverso para enviar datos. Se tuvieron que utilizar un router Acces Server con una pila de modems y además contar con el servicio Inavía instalando un servidor Radius.

Al utilizar línea telefónica, la calidad de conexión no es siempre buena y está sujeta a pérdida de datos y limitaciones de todo tipo. Por ejemplo, durante la conexión, no es posible usar la misma línea telefónica para hablar, es por ello que se contrató líneas telefónicas para este uso. Una conexión dial-up posee velocidades que van desde los 2400 bps hasta los 56 kbps.

3.1.2 ISDN (Integrated Services Digital Network).

Es un estándar de comunicación internacional para el envío de voz, datos y video a través de una línea digital de teléfono llamada también RSDI. La velocidad típica en un ISDN va desde los 64 kbps a los 128 kbps. Lo cuales teníamos conexión con la Empresa BellSouth.

3.1,3 Systems Network Architecture (SNA)

Es una arquitectura de red diseñada y utilizada por IBM para la conectividad con sus hosts o mainframe —grandes ordenadores y servidores muy robustos que soportan millones de transacciones que por lo general son utilizados en bancos— así como los servidores IBM AS/400, considerados como servidores middlerange. Por otro lado, existe el servidor SNA Server o el Host Integration Server, que corriendo en Microsoft Windows Server, funciona como gateway entre la red de mainframes en SNA y una red TCP/IP con Windows (Donde el que realiza la consulta es por lo general un host IBM que aprovecha la infraestructura de servidores Windows NT/2000/2003).

Originalmente fue diseñado para permitir la comunicación con un host. Cada red o subred eran controladas por este host. Los ordenadores se podían comunicar con dicho host, sin embargo, no podían establecer comunicación directa con otros ordenadores. Este estilo de red recibe el nombre de subárea SNA. El nuevo diseño de red que sí que permite, sin necesidad de host, la comunicación peer-to-peer implementando SNA, es el APPN (Advanced Peer-to-Peer Networking).

SNA define los estándares, protocolos y funciones usadas por los dispositivos para permitirles la comunicación entre ellos en las redes SNA. Define varios protocolos, incluidos el SDLC (Synchronous Data Link Control) que se configuró en los routers (es controlador de enlace de datos síncrono), se utiliza para nombrar el protocolo diseñado por IBM para enlaces síncronos a través de una línea para la capa 2 del modelo OSI de comunicaciones. Como su nombre implica, es un protocolo síncrono, lo que supone la transmisión de la señal de reloj con los datos.

3.1.4 Conexión ADSL : Asymmetric Digital Subscriber Line ("Línea de Abonado Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, []siempre y cuando la longitud de línea no supere los 5,5 km, medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

CARACTERISTICAS:

La conexión está siempre activa, contrario al Dial-Up donde el abonado necesita un nombre de usuario y contraseña para "marcar" su conexión.

Las direcciones IP pueden ser dinámicas o estáticas, dependiendo del ISP.

Tuvimos mejores conexiones con los clientes y aumento del Ancho de Banda.

3.1,5 Líneas Dedicadas

Una línea arrendada (leased line), también llamada comúnmente línea privada o dedicada, se obtiene de una compañía de comunicaciones para proveer un medio de comunicación entre dos instalaciones, que pueden estar en edificios separados en una misma ciudad o en ciudades distantes. Aparte de un cobro por la instalación o contratación [pago único], la compañía proveedora de servicios (carrier) le cobrará al usuario un pago mensual por uso de la línea, el cual se basará en la distancia entre las localidades conectadas.

Este tipo de líneas tienen gran uso cuando se requiere cursar:

- Una cantidad enorme de tráfico y
- Cuando este tráfico es continuo.

Las ventajas de la líneas arrendadas son:

- Existe un gran ancho de banda disponible (desde 64 Kbps hasta decenas de Mbps)

- Ofrecen mucha privacidad a la información
- La cuota mensual es fija, aun cuando ésta se use en exceso.
- La línea es dedicada las 24 hrs.
- No se requiere marcar ningún número telefónico para lograr el acceso.

Las desventajas:

- El costo mensual es relativamente costoso.
- No todas las áreas están cableadas con este tipo de líneas.
- Se necesita una línea privada para cada punto que se requiera interconectar.
- El costo mensual dependerá de la distancia entre cada punto a interconectar.

Este tipo de líneas son proporcionadas por cualquier compañía de comunicaciones; los costos involucrados incluyen un contrato inicial, el costo de los equipos terminales (DTU, Data Terminal Unit) y de una mensualidad fija.

3.2 . ALTA DISPONIBILIDAD

Alta disponibilidad (High availability) es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado. Disponibilidad se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible.

3.2.1 Tiempo de inactividad

Típicamente, tiempo de inactividad planificado es un resultado del mantenimiento que es perjudicial para la operación del sistema y usualmente no puede ser evitado con la configuración del sistema actualmente instalada. Eventos que generan tiempos de inactividad planificados quizás incluyen parches al software del sistema que requieran un rearranque o cambios en la configuración del sistema que toman efecto después de un rearranque. En general, el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o de gestión iniciado.

Tiempos de inactividad no planificado surgen de algún evento físico, tales como fallos en el hardware o anomalías ambientales. Ejemplos de eventos con tiempos de inactividad no planificados incluyen fallos de potencia, fallos en los componentes de CPU o RAM, una caída por recalentamiento, una ruptura lógica o física en las conexiones de red, rupturas de seguridad catastróficas o fallos en el sistema operativo, aplicaciones y middleware.

Muchos puestos computacionales excluyen tiempo de inactividad planificado de los cálculos de disponibilidad, asumiendo, correcta o incorrectamente, que el tiempo de actividad no planificado tiene poco o ningún impacto sobre la comunidad de usuarios

computacionales. Excluyendo tiempo de inactividad planificado, muchos sistemas pueden reclamar tener alta disponibilidad fenomenal, la cual da la ilusión de disponibilidad continua. Sistemas que exhiben verdadera disponibilidad continua son comparativamente raros y caros, y ellos tienen diseños cuidadosamente implementados que eliminan cualquier punto de fallo y permiten que el hardware, la red, el sistema operativo, middleware y actualización de aplicaciones, parches y reemplazos se hagan en línea.

3.2.2 Disponibilidad es usualmente expresada como un porcentaje del tiempo de funcionamiento en un año dado. En un año dado, el número de minutos de tiempo de inactividad no planeado es registrado para un sistema, el tiempo de inactividad no planeado agregado es dividido por el número total de minutos en un año (aproximadamente 525.600), produciendo un porcentaje de tiempo de inactividad; el complemento es el porcentaje de tiempo de funcionamiento, el cual es lo que denominamos como disponibilidad del sistema. Valores comunes de disponibilidad, típicamente enunciado como número de "nueves" para sistemas altamente disponibles son:

99,9% = 43.8 minutos/mes u 8,76 horas/año ("tres nueves")

99,99% = 4.38 minutos/mes o 52.6 minutos/año ("cuatro nueves")

99,999% = 0.44 minutos/mes o 5.26 minutos/año ("cinco nueves")

Es de hacer notar que tiempo de funcionamiento y disponibilidad no son sinónimos. Un sistema puede estar en funcionamiento y no disponible como en el caso de un fallo de red. Se puede apreciar que estos valores de disponibilidad son visibles mayormente en documentos de ventas o marketing, en lugar de ser una especificación técnica completamente medible y cuantificable.

3.2.3 Diseño de un sistema de alta disponibilidad

Paradójicamente, añadiendo más componentes al sistema total, puede socavar esfuerzos para lograr alta disponibilidad. Esto es debido a que sistemas complejos tienen inherentemente más puntos de fallos potenciales y son más difíciles de implementar correctamente. La mayoría de los sistemas altamente disponibles extraen a un patrón de diseño simple: un sistema físico multipropósito simple de alta calidad con redundancia interna comprensible ejecutando todas las funciones independientes emparejadas con un segundo sistema en una localización física separada.

Este clásico patrón de diseño es común entre instituciones financieras, por ejemplo. La industria de la informática y las comunicaciones acogerán la creación de productos de infraestructura de red, servicios y sistemas de alta disponibilidad. El mismo principio de diseño básico se aplica, más allá de la informática, en diversos campos, como potencia nuclear, aeronáutica y cuidados médicos. Las soluciones clásicas propuestas en las últimas décadas proponen el uso de mecanismos de redundancia física

y monitorización para implementar alta disponibilidad. Concretamente, la idea consiste en desplegar el mismo servicio sobre distintas replicas y un protocolo de consenso garantiza que, en cualquier instante de tiempo, al menos una de ellas esta procesando las peticiones proveniente de los clientes. Si por cualquier razón la replica activa sufre un fallo, una nueva replica que estaba actuando como respaldo se selecciona para continuar proporcionando el servicio.

3.2.4 Redundancia

La redundancia es una técnica, mediante la cual un componente del sistema es duplicado y cualquiera de sus instancias puede ser utilizada en caso de falla. Ya que dos componentes idénticos están en línea, el sistema puede continuar su funcionamiento: no debe existir impacto alguno en la operación si es que esto llegara a ocurrir.

Los sistemas de redundancia en redes, comunicaciones de voz y datos y en servidores de red existen desde hace mucho tiempo, pero antes sólo estaban al alcance de empresas muy grandes. Con la caída del precio del hardware y el software en los últimos años, estas tecnologías son asequibles y están disponibles, incluso para empresas pequeñas. Por un coste un poco superior, su red puede instalarse y configurarse con sistemas redundantes en sus puntos críticos, de tal manera que el fallo de un equipo de red no implique la parada de su negocio.

Hoy en día se pueden redundar todos los equipos críticos de red, implantando network teaming para redundar las conexiones de red, alta disponibilidad en switches de red, alta disponibilidad en firewalls, líneas de Internet redundantes con varios routers, etc. Usted mismo puede definir los servicios de red que considera críticos y redundar aquellos equipos de red que no puedan fallar.

Los servicios que realizamos en redundancia y alta disponibilidad de sistemas y redes son:

- Configuración de network teaming o network bonding en tarjetas de red.
 - Instalación y configuración de electrónica de red redundante (trunking, spanning tree...)
 - Instalación y configuración de firewalls en alta disponibilidad.
 - Configuración de conexiones a Internet redundantes (routers, balanceo de carga, etc.)
 - Instalación y configuración de sistemas RAID en servidores y cabinas de discos.
 - Instalación y configuración de servidores web y FTP redundantes con Microsoft NLB.
 - Implantación de servidores virtuales en alta disponibilidad con VMWARE.
 - Alta disponibilidad de Exchange Server con Microsoft Cluster o con CCR.
 - Alta disponibilidad de SQL Server con Microsoft Cluster o replicación de BBDD.
 - Backups y restauración con Acronis True Image, Symantec Backup Exec o Arcserve.
- Más allá del servicio que ofrezca un sistema informático, este sistema debe ser fiable

para que los usuarios puedan utilizarlo en condiciones óptimas. El término "fiabilidad" indica cuán fiable es un sistema informático.

Una falla se produce cuando un servicio no funciona correctamente, es decir que se genera un estado de funcionamiento anormal o que no se adecúa a las especificaciones.

Desde el punto de vista del usuario, un servicio tiene dos estados:

servicio apropiado: cuando satisface las expectativas.

servicio inapropiado: cuando no satisface las expectativas.

Una falla es atribuible a un error, es decir, a un funcionamiento incorrecto local. Pero no todos los errores conducen a una falla en el servicio.

Existen varias maneras de limitar las fallas en el servicio:

La prevención de errores, que consiste en evitar errores anticipándolos.

La tolerancia a errores, cuyo propósito es proporcionar un servicio de acuerdo con las especificaciones, a pesar de los errores, presentando redundancias.

La eliminación de errores, destinada a reducir la cantidad de errores por medio de acciones correctivas.

La predicción de errores, anticipando errores y su posible impacto en el servicio.

El término "fiabilidad", que se utiliza en algunos casos, se refiere a la probabilidad de que un sistema funcione normalmente durante un período de tiempo dado. Esto se denomina "continuidad del servicio".

La disponibilidad se expresa con mayor frecuencia a través del índice de disponibilidad (un porcentaje) que se mide dividiendo el tiempo durante el cual el servicio está disponible por el tiempo total. La disponibilidad se expresa con mayor frecuencia a través del índice de disponibilidad (un porcentaje) que se mide dividiendo el tiempo durante el cual el servicio está disponible por el tiempo total.

Tabla 3.1 Disponibilidad, Fuente: www.renovetec.com

Nombre	Acrónimo	Cálculo	Definición
Tiempo medio entre errores	MTBF	Horas / número de errores	Duración media de funcionamiento de la aplicación antes de que produzca errores.
Tiempo medio de recuperación	MTTR	Horas de reparación / número de errores	Tiempo medio necesario para reparar y restaurar el servicio después de que se produzca un error.

La fórmula de disponibilidad tiene esta forma:

$$\text{Disponibilidad} = (\text{MTBF} / (\text{MTBF} + \text{MTTR})) \times 100 \quad (3.1)$$

Considere, por ejemplo, una aplicación concebida para que funcione continuamente. Pongamos un punto de control de 1.000 horas consecutivas, dos errores de una hora durante ese período darían lugar a una disponibilidad de $((1.000/2) / ((1.000/2) + 1)) \times 100 = (500 / 501) \times 100 = 0,998 \times 100 = 99,8 \%$.

Tabla 3.2 Índice de Disponibilidad, Fuente: <http://technet.microsoft.com>

Índice de disponibilidad	Duración del tiempo de inactividad
97%	11 días
98%	7 días
99%	3 días y 15 horas
99,9%	8 horas y 48 minutos
99,99%	53 minutos
99,999%	5 minutos
99,9999%	32 segundos

3.2.5 Evaluación de riesgos

En efecto, la falla de un sistema informático puede producir pérdidas en la productividad y de dinero, y en algunos casos críticos, hasta pérdidas materiales y humanas. Por esta razón, es necesario evaluar los riesgos ligados al funcionamiento incorrecto (falla) de uno de los componentes de un sistema informático y anticipar los medios y medidas para evitar incidentes o para restablecer el servicio en un tiempo aceptable.

Como es sabido, un sistema informático de redes puede fallar de muchas formas. Las causas de las fallas pueden clasificarse de la siguiente manera:

Causas físicas (de origen natural o delictivo)

Desastres naturales (inundaciones, terremotos, incendios)

Ambiente (condiciones climáticas adversas, humedad, temperatura)

Fallas materiales

Fallas de la red

Cortes de energía

Causas humanas (intencionales o accidentales):

Error de diseño (errores de software, aprovisionamiento de red insuficiente)

Causas humanas (intencionales o accidentales):

Error de diseño (errores de software, aprovisionamiento de red insuficiente)

Causas operativas (vinculadas al estado del sistema en un momento dado):

Errores de software

Falla del software

Todos estos riesgos pueden tener diferentes causas, entre las que se cuentan:

Daños intencionales

Tolerancia a errores

Dado que las fallas no se pueden evitar por completo, existe una solución que consiste en configurar mecanismos de redundancia duplicando los recursos críticos.

La capacidad de un sistema para funcionar a pesar de que alguno de sus componentes falle se conoce como tolerancia a errores.

Cuando uno de los recursos falla, los otros recursos siguen funcionando, mientras los administradores del sistema buscan una solución al problema. Esto se llama "Servicio de protección contra fallas" (FOS).

Idealmente, si se produce una falla material, los elementos del material defectuoso deben ser intercambiables en caliente, es decir, capaces ser extraídos y reemplazados sin que se interrumpa el servicio.

3.3 HSRP - Redundancia en la salida a Internet y Bancared

El **Hot Standby Router Protocol**, es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Es un protocolo muy similar a VRRP, que no es propietario. Es por ello que CISCO reclama que VRRP viola una serie de patentes que le pertenecen.

El funcionamiento del protocolo HSRP es el siguiente: Se crea un grupo (también conocido por el término inglés Clúster) de routers, en el que uno de ellos actúa como maestro, enrutando el tráfico, y los demás actúan como respaldo a la espera de que se produzca un fallo en el maestro. HSRP es un protocolo que actúa en la capa 3 del modelo OSI, administrando las direcciones virtuales que identifican al router que actúa como maestro en un momento dado.

Supongamos que disponemos de una red que cuenta con dos routers redundantes, Router1 y Router2. Dichos routers pueden estar en dos posibles estados diferentes: maestro (Router 1) y respaldo (Router 2). Ambos routers intercambian mensajes, concretamente del tipo HSRP hello, que le permiten a cada uno conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985. Si el router maestro no envía mensajes de tipo hello al router de respaldo dentro de un

determinado período, el router respaldo asume que el maestro está fuera de servicio (ya sea por razones administrativas o imprevistas, tales como un fallo en dicho router) y se convierte en el router maestro. La conversión a router activo consiste en que uno de los router que actuaba como respaldo obtiene la dirección virtual que identifica al grupo de routers.

HSRP se encuentra disponible desde CISCO IOS 10.0, pero se han incorporado nuevas funcionalidades en las versiones 11 y 12.

Para determinar cuál es el router maestro, se establece una prioridad en cada router. La prioridad por defecto es 100. El router de mayor prioridad es el que se establecerá como activo. Hay que tener presente que HSRP no se limita a 2 routers, sino que soporta grupos de routers que trabajen en conjunto, de modo que se dispondría de múltiples routers actuando como respaldo en situación de espera.

Paso de estado "respaldo" a estado "maestro"

El router en espera toma el lugar del router maestro, una vez que el temporizador holdtime expira (un equivalente a tres paquetes hello que no vienen desde el router activo, timer hello por defecto definido a 3 y holdtime por defecto definido a 10).

Los tiempos de convergencia dependerán de la configuración de los temporizadores para el grupo y del tiempo de convergencia del protocolo de enrutamiento empleado.

Por otra parte, si el estado del router maestro pasa a down, el router decrementa su prioridad. Así, el router respaldo lee ese decremento en forma de un valor presente en el campo de prioridad del paquete hello, y se convertirá en el router maestro si ese valor decrementado es inferior a su propia prioridad. Este proceso decremental puede ser configurado de antemano estableciendo un valor por defecto del decremento (normalmente, de 10 en 10).

Ejemplo de configuración

Para el Router 1, que vamos a establecer como maestro o primario:

Configuración de la dirección IP de la interfaz Ethernet.

Configuración de la dirección IP virtual.

Configuración de la prioridad HSRP con un valor igual a 100.

Para el Router 2:

Configuración de la dirección IP de la interfaz Ethernet.

Configuración de la dirección IP virtual.

Configuración de la prioridad HSRP con un valor menor a 100.

En los terminales conectados a los routers se configura la dirección IP virtual como default gateway, no la dirección real de la interfaz de los dispositivos. De este modo, si uno de los dispositivos queda fuera de servicio, el otro toma su lugar automáticamente y

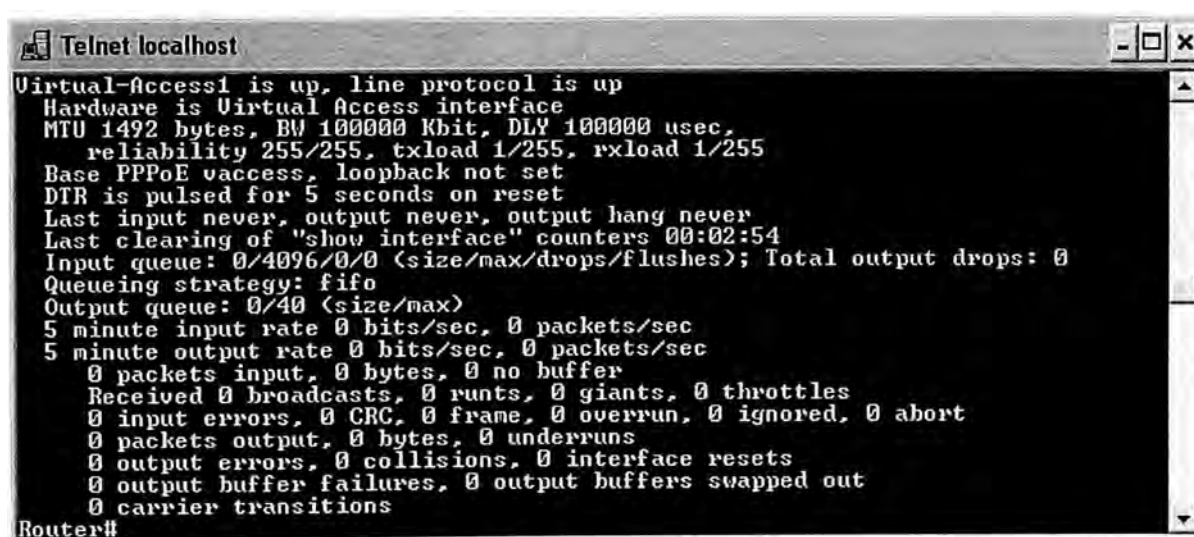
de modo transparente para los nodos. El tiempo requerido para este cambio es menor a los 10 segundos.

HSRP-Comandos CISCO

- standby [grupo] ip [IP virtual] Poner la IP virtual en el grupo HSRP que queramos.
- enable preempt El router pasa de pasivo a activo cuando se da cuenta de que el router activo ha caído o él mismo tiene la prioridad más alta.
- standby [grupo] priority [prioridad] Asignamos la prioridad al router. La prioridad por defecto es 100, si ponemos 110 el router será el activo en el grupo.
- standby [grupo] authentication [string] Cadena de 8 caracteres opcionales que pueden ser usados en los paquetes "hello" multicast para autenticar el grupo HSRP.
- standby [grupo] timers [hello] [holdtime] Poner el período de tiempo entre los paquetes "hello" y el "holdtime" antes de asumir que un router activo ha caído. Por defecto es 3 10 respectivamente.
- show standby Muestra la información de HSRP, que incluye el estado de los reenvíos, la prioridad HSRP y las interfaces a las que realizan seguimientos del router al que se realizan consultas. También muestra información acerca de la dirección IP de reserva configurada y las direcciones IP de los posibles routers de reserva de cada grupo HSRP

HSRP-Comando show

- Haciendo un show interfaces en los routers configurados, podemos comprobar el estado de nuestro punto de acceso virtual, solo necesitamos que uno de los dos routers lo mantenga activo.
- Pero se puede observar que mientras este en este estado los dos routers lo mostraran en sus respectivos shows.
- También podemos observar que nos muestran las estadísticas del punto de acceso virtual como si fuera cualquier otra interface del router.



```

Telnet localhost
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
MTU 1492 bytes, BW 1000000 Kbit, DLY 1000000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Base PPPoE vaccess, loopback not set
DTR is pulsed for 5 seconds on reset
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:02:54
Input queue: 0/4096/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
Router#

```

Figura 3.2 Interface Virtual, Fuente: Router Cisco

HSRP-Comando show standby

- Con show standby pasamos a comprobar el estado del punto de acceso con más detalle. Podemos comprobar que la MAC virtual es la misma, aunque configuremos el punto de acceso con más de una interficie.
- También se observa como es el router con más prioridad el que está activo.
- Se observa también como el router activo va enviando señales cada cierto tiempo para indicar que está activo.

```

Telnet localhost
Router#show standby
FastEthernet0/0 - Group 1
  State is Active
  2 state changes, last state change 00:03:39
  Virtual IP address is 192.168.1.4
  Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.000 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3, priority 110 (expires in 9.428 sec)
  Priority 120 (configured 120)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
FastEthernet0/1 - Group 1
  State is Active
  2 state changes, last state change 00:03:37
  Virtual IP address is 192.168.2.4
  Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.028 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.2.3, priority 110 (expires in 8.028 sec)
  Priority 120 (configured 120)
  IP redundancy name is "hsrp-Fa0/1-1" (default)
Router#
  
```

Figura 3.3 Comando Show Standby, Fuente: Router Cisco

```

Telnet localhost
Router#show standby
FastEthernet0/0 - Group 1
  State is Standby
  1 state change, last state change 00:03:26
  Virtual IP address is 192.168.1.4
  Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.180 secs
  Preemption enabled
  Active router is 192.168.1.2, priority 120 (expires in 7.988 sec)
  Standby router is local
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
FastEthernet0/1 - Group 1
  State is Standby
  1 state change, last state change 00:03:25
  Virtual IP address is 192.168.2.4
  Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.188 secs
  Preemption enabled
  Active router is 192.168.2.2, priority 120 (expires in 8.856 sec)
  Standby router is local
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Fa0/1-1" (default)
Router#
  
```

Figura 3.4 Muestra estado Standby, Fuente: Router Cisco

- Con R1 caído, se puede ver como R2 pasa a ser el activo, como en este caso solo tenemos 2 routers, ya no hay ningún otro conocido en espera, como se puede observar, la información del punto de acceso virtual no varía.
- En cuanto R1 vuelva a iniciarse, se pondrá en espera con menos prioridad de la que tenía antes, y R2 estará activo hasta que tenga algún problema.

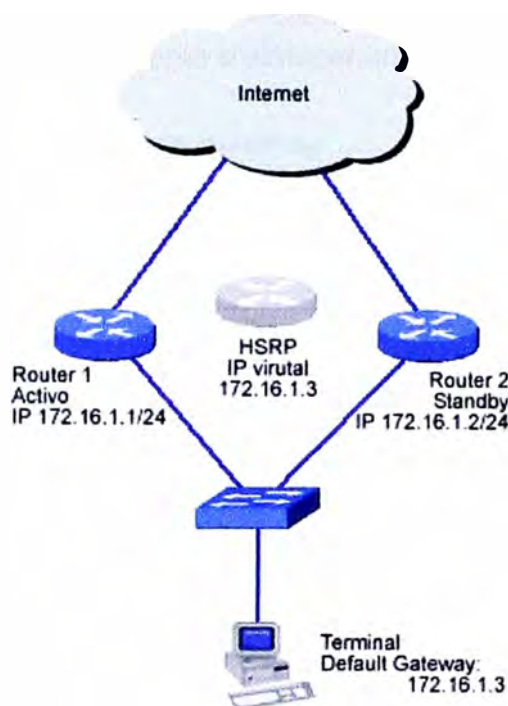


Figura 3.5 Configuración HSRP, Fuente: learningnetwork.cisco.com

3.4 Redundancia en la Red de área de almacenamiento

Una red de área de almacenamiento, en inglés SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Las SAN se componen de tres capas:

Capa Host. Esta capa consiste principalmente en Servidores, dispositivos o componentes (HBA, GBIC, GLM) y software (sistemas operativos).

Capa Fibra. Esta capa la conforman los cables (Fibra óptica) así como los SAN Hubs y los SAN switches como punto central de conexión para la SAN.

Capa Almacenamiento. Esta capa la componen las formaciones de discos (Disk Arrays, Memoria Caché, RAIDs) y cintas empleados para almacenar datos.

La red de almacenamiento puede ser de dos tipos:

Red Fibre Channel. La red Fibre Channel es la red física de dispositivos Fibre Channel que emplea Fibre Channel Switches y Directores y el protocolo Fibre Channel Protocol (FCP) para transporte (SCSI-3 serial sobre Fibre Channel) Red IP. Emplea la infraestructura del estándar LAN con hubs y/o switches Ethernet interconectados. Una SAN IP emplea iSCSI para transporte (SCSI-3 serial sobre IP) .

Una red SAN es utilizada para transportar datos entre servidores y recursos de almacenamiento. La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor.

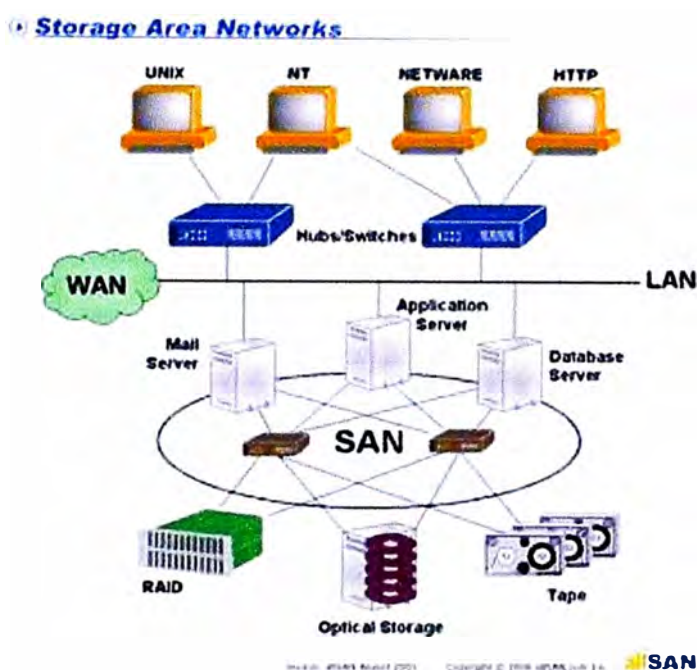


Figura 3.6 SAN , Fuente : files.wordpress.com/

Las SAN poseen las siguientes características:

- Rendimiento: Permiten acceso concurrente por dos o más servidores lo que proporciona un mejor rendimiento.
- Disponibilidad: Se puede hacer una copia exacta de los datos a una distancia de 10Km lo que las hace más seguras.
- Escalabilidad: Como las LAN/WAN puede usar muchas tecnologías. Lo que permite fácil reubicación, seguridad migración y duplicación de datos.
- Seguridad: La seguridad en las SAN ha sido desde el principio un factor fundamental, desde su creación se notó la posibilidad de que un sistema accediera a un dispositivo que no le correspondiera o interfiriera con el flujo de información, es por ello que se ha implementado la tecnología de zonificación, la cual consiste en que un grupo de elementos se aislen del resto para evitar estos problemas, la zonificación puede llevarse a cabo por hardware, software o ambas, siendo capaz de agrupar por puerto o por WWN (World Wide Name), una técnica adicional se implementa a nivel del dispositivo de

almacenamiento, que es la Presentación, consiste en hacer que una LUN (Logical Unit Number) sea accesible sólo por una lista predefinida de servidores o nodos.

Compartir el almacenamiento simplifica la administración y añade flexibilidad, puesto que los cables y dispositivos de almacenamiento no necesitan moverse de un servidor a otro. Cada dispositivo de la SAN es "propiedad" de un solo ordenador o servidor. Como ejemplo contrario, NAS permite a varios servidores compartir el mismo conjunto de ficheros en la red. Una SAN tiende a maximizar el aprovechamiento del almacenamiento, puesto que varios servidores pueden utilizar el mismo espacio reservado para crecimiento.

El mundo antes de SAN

- Bus or Channel attached storage

Altas tasas de transferencia

25 metros de cable como máximo

Configuraciones estáticas

- Network attached storage

Bajas tasas de transferencia

Congestión en la red

Configuraciones escalables

SAN toma lo mejor de ambos mundos

- Channels

Alta velocidad

Bajo retardo

Alta confiabilidad

Tecnología probada

- Networks

Muchas direcciones

Distancias extendidas

Servicios compartidos

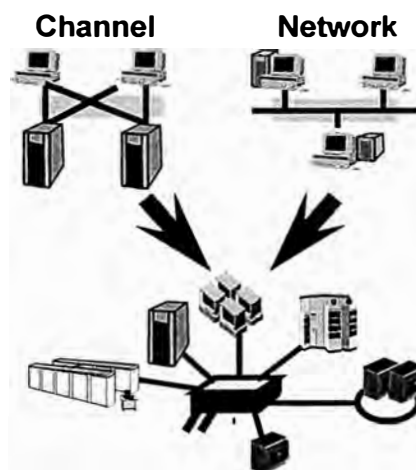
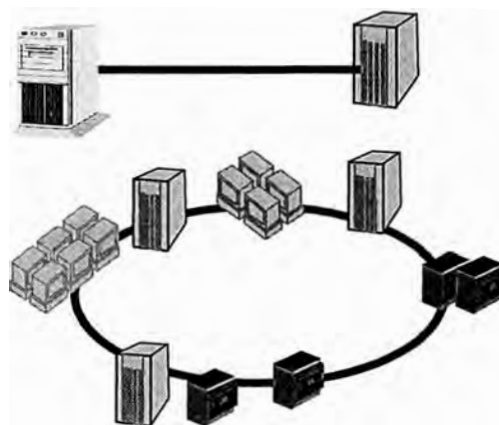
Altamente escalable

Componentes de una SAN

- Fabric Switch
- Small Form Factor Hot-Pluggable (SFP)
- Host Bus Adapter (HBA)
- Fibre Channel Cable

Fabric Switch

- Componente indispensable en la mayoría de redes SAN actuales.



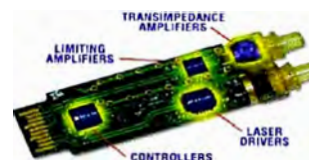
- Permite interconectar varios dispositivos en forma simultanea dentro de una SAN de tal manera que cada conexión disponga de todo el ancho de banda soportado por los puertos del switch
- El SFP es el componente del switch encargado de convertir las señales ópticas (laser) provenientes de algún dispositivo (HBA, Storage, etc.) en señales eléctricas que interpreta el procesador interno del switch.
- El SFP puede soportar múltiples velocidades.
- Se puede conectar/desconectar en caliente.

Existen dos tipos de SFP:

- Shortwave.- Para distancias cortas (hasta 500m)
- Longwave.- Para distancias mayores (hasta 10 Km)

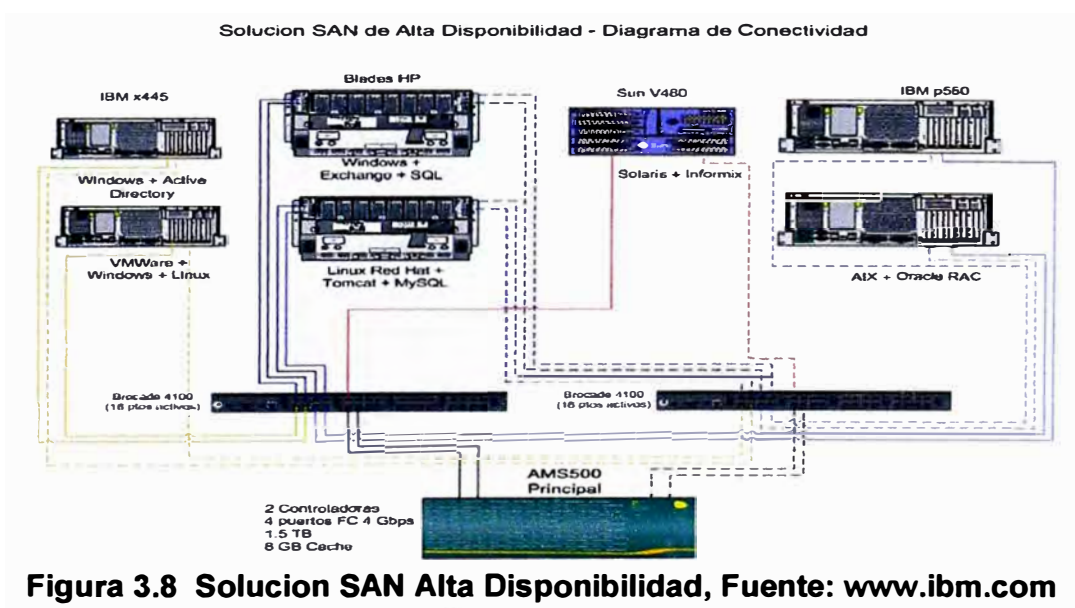
Host Bus Adapter (HBA)

- El HBA se conecta a los hosts a través de un bus I/O (generalmente PCI para Open Systems) y realiza la interfaz para el intercambio de datos entre la SAN y el Sistema Operativo.
- Existen HBAs de uno o dos puertos.



Cable Fibre Channel

- Se utiliza para conectar los distintos elementos de una red SAN (p.e. un HBA a un switch).
- Existen distintos tipos de cables y se utilizan dependiendo de la distancia.
- En ambos extremos se ubican los conectores que pueden ser del tipo LC o SC.



3.5 VIRTUALIZACIÓN:

- Beneficios

Mejor utilización de los recursos de HW.

Reducción de consumo de energía

Reducción de consumo de Aire Acondicionado

Facilidad en el provisionamiento .

Reducción en el costo de HW

Mejor administración y monitoreo de recursos.

Reducción de costos operativos

- Ahorros

Capacidad de consolidación en relación de 10:1 por lo menos.

Aumento en la utilización de hardware de hasta un 70 %.

Disminución en el costo de nuevo HW de hasta un 50 %.

Disminución en el consumo de energía y Aire Acondicionado de hasta un 50 %.

Disminución en el espacio físico de hasta un 50 %.

VMware High Availability (HA).- Es una solución asequible y fácil de utilizar, que garantiza la alta disponibilidad de las aplicaciones que se ejecutan en las máquinas virtuales. En caso de fallo de un servidor físico, las máquinas virtuales afectadas se reinician automáticamente en otros servidores de producción con capacidad adicional. En caso de fallo del sistema operativo, VMware HA reinicia la máquina virtual afectada en el mismo servidor físico. La combinación de VMware HA y las funciones de disponibilidad de la plataforma VMware vSphere™ permite a las organizaciones seleccionar y obtener fácilmente el nivel de disponibilidad requerido para todas las aplicaciones críticas.

VMware HA permite a los departamentos de IT:

- Minimizar las paradas no planificadas y las interrupciones del servicio de IT, además de eliminar la necesidad de hardware dedicado en espera y la instalación de software adicional.
- Proporcionar alta disponibilidad, uniforme y asequible en todo el entorno de IT virtualizado, sin el coste ni la complejidad de las soluciones de failover específicas de sistemas operativos o aplicaciones.

A continuación veremos a 2 Servidores ESX_1 y ESX_2 los cuales tiene maquinas virtuales conectados a traves de un cable directo para lograr disponibilidad en el sistema. Cada servidor cuenta con servidores Web y servidores de base de datos. Los servidores Web son consultados por Internet y Bancared, en casos de fallas se habilita los adicionales para proseguir con el sistema , aparecieron nuevas necesidades en las cuales se requieren mas servidores para se requerirá mas espacio. asi se lograría alta disponibilidad de servidores conjuntamente con bases de datos en casos de fallas.

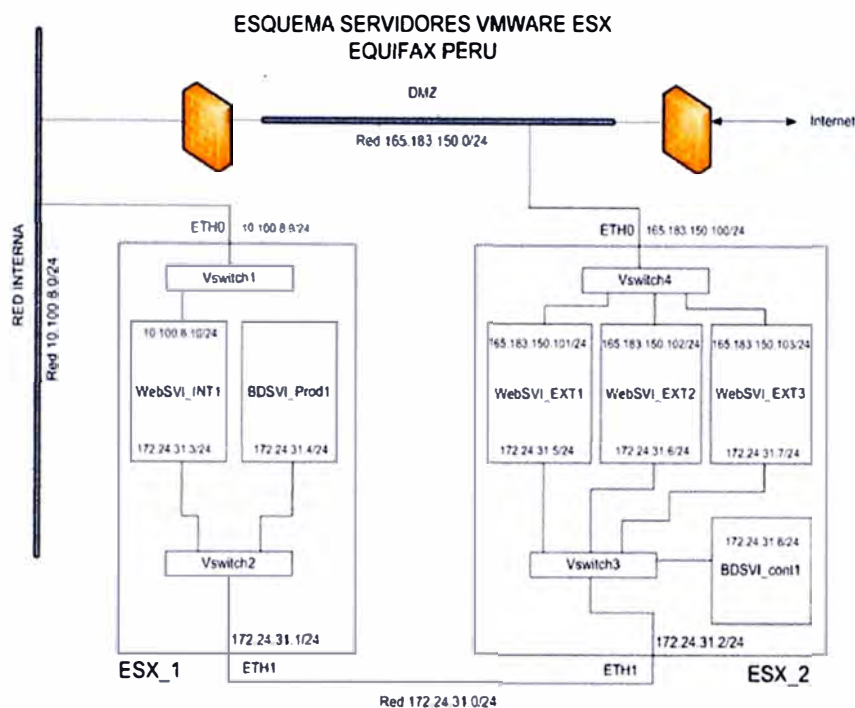


Figura 3.8 Virtualización 2 Servidores, Fuente: Equifax Peru

3.6. BANCARED

3.6.1 Bancared .- Red Privada de Comunicaciones de ASBANC, es el medio de transporte para el intercambio de información y ejecución de transacciones entre las entidades financieras y las instituciones públicas y privadas con las que mantiene comunicación (proveedores de información).

Bancared cuenta con tecnología de punta y exigentes mecanismos de contingencia y seguridad.

Bancared ha sido diseñada e implementada por los expertos de comunicaciones de la banca y es administrada por ASBANC, a través de un contrato de outsourcing con TELMEX (hoy Claro) con nivel de servicio, que asegura la eficiencia y calidad de las comunicaciones.

3.6.2 Características:

- Utiliza tecnología MPLS de Telmex (hoy Claro)
- Enlaces de fibra óptica
- Ancho de banda escalable
- Alta disponibilidad (el enlace principal supera 99.98% anual)
- Altos niveles de seguridad
- Certificación contra vulnerabilidad
- Nivel de servicio contratado:
 - Soporte 7x24 / 365 días
 - Personal especializado
 - Renovación tecnológica permanente

NETWORK EQUIFAX PERU

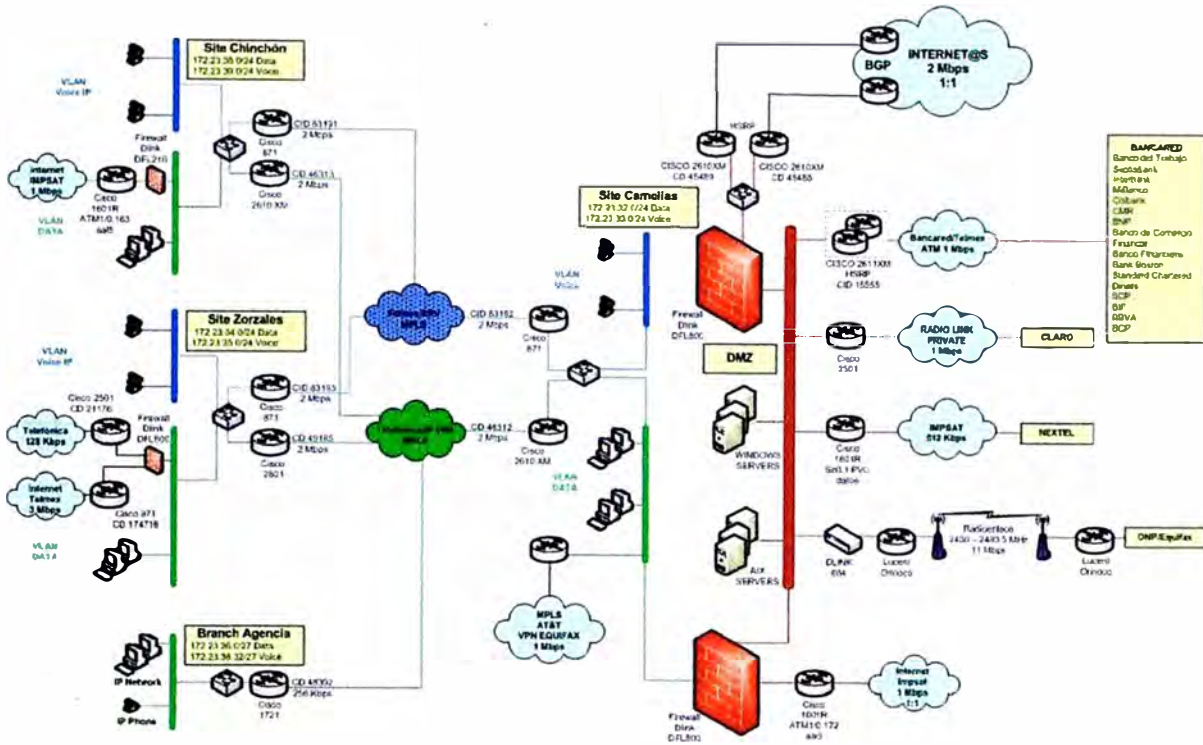


Figura 3.9 Red Equifax Peru (2009), Fuente: Equifax Perú

3.6.3 Operatividad

Bancared inició operaciones en abril del 2000, con 17 bancos y 3 proveedores de información interconectados.

Paulatinamente, se han incorporado nuevas entidades como resultado de la excelente calidad de servicio que ofrece, así como por los múltiples beneficios y ahorros que genera.

Al mes de Marzo del 2010, están interconectados en Bancared, 23 entidades financieras, así como, 29 entidades proveedoras de servicios e información.

Durante los diez primeros años de operatividad, la Red ha superado el 99.98% de disponibilidad del servicio.

3.6.4 Entidades Financieras Interconectadas

- Banco de Crédito del Perú
- Interbank
- Citibank
- Scotiabank Perú
- BBVA Banco Continental
- Banco de Comercio
- Banco Financiero
- Banco Interamericano de Finanzas
- Crediscotia

- Mibanco
- HSBC Bank Perú
- Banco Santander
- Banco de la Nación
- Banco Ripley
- Banco Falabella
- Banco Azteca Perú S.A.
- Deutsche Bank (Perú) S.A.
- Caja Metropolitana de Lima
- Caja Nuestra Gente
- COFIDE
- Financiera TFC
- Financiera Edyficar
- BCRP (Red independiente LBTR - Bancos)

3.6.5 Entidades Proveedoras de Información Interconectadas

- Acelor S.A.C (Certicom S.A.)
- Programa Integral de Seguridad Bancaria - PISB - ASBANC
- Datatec
- Unibanca
- Registro Nacional de Identificación y Estado Civil - RENIEC
- Infocorp
- Superintendencia de Banca y Seguros - SBS
- Telmex
- Sedapal
- Procesos MC (Master Card)
- América Móviles
- Western Union
- Sunat / Aduanas
- Cavali
- Edelnor
- Diners Club
- E.Wong
- SAT
- Universidad de Lima
- Petroperú
- Nextel
- Univ. Tecnológica del Perú

- Municipalidad de Miraflores
- Perurail (en proceso)
- Hermes
- Unique
- Globokas
- Municipalidad de Surco

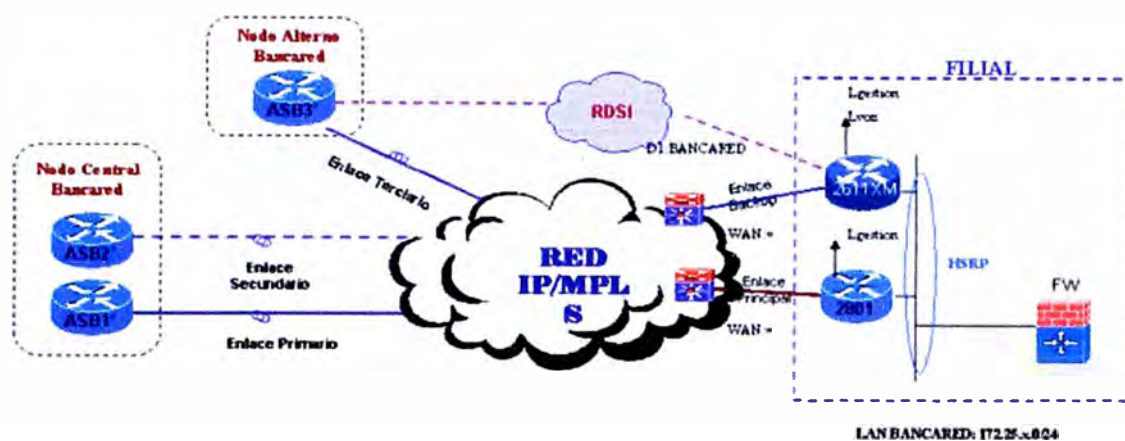


Figura 3.10 Empleo de MPLS en Bancared, Fuente: ASBANC

3.7 MPLS (Multi Protocol Label Switching)

3.7.1 Mpls es una repleto de reenvío de tecnología avanzada que soporta los servicios IP. MPLS ofrece ninguna a ninguna conectividad, permitiendo múltiples ubicaciones para comunicarse entre sí y compartir ancho de banda de otros. MPLS también permite al cliente para ejecutar múltiples tipos de tráfico, tales como voz, datos y vídeo a través de una única red con calidad de servicio (QoS).

3.7.2 Antecedentes.- Un número de diferentes tecnologías se desplegaron previamente con objetivos esencialmente idénticos, tales como Frame Relay y ATM. MPLS es ahora sustituir estas tecnologías en el mercado, sobre todo porque es más acorde con las actuales y futuras necesidades tecnológicas.

En particular, MPLS omite la conmutación y señalización de protocolo equipaje de células de la ATM. MPLS reconoce que las pequeñas células de la atmósfera no son necesarios en el núcleo de las redes modernas, ya que las redes modernas de óptica (de 2001) es tan rápido (a 10 Gbit/s, y más allá también), que incluso de larga duración en 1.500 paquetes de bytes no incurre en importantes tiempos de espera reales de retrasos (la necesidad de reducir estos retrasos - por ejemplo, para soportar tráfico de voz - fue la motivación de la naturaleza celular de cajeros automáticos). Las ventajas de MPLS, principalmente giran en torno a la capacidad de soporte de servicio múltiples modelos y

realizar la gestión del tráfico. MPLS también ofrece un marco de recuperación robusta: Marco de Multi-Protocol Label Switching (MPLS), basados en la recuperación que va más allá de la simple protección de los anillos de fibra óptica síncrona (SONET / SDH).

3.7.3 ¿Cómo funciona MPLS?

Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers).

Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los routers IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias. Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento.

Los LER están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR. Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias.

Las etiquetas son distribuidas entre LERs y LSRs a través del "Protocolo de distribución de etiquetas (LDP) Label Switch Routers en una red MPLS con regularidad etiqueta de intercambio y accesibilidad de información entre ellos, utilizando procedimientos estandarizados; con el fin de construir una imagen completa de la red se

puede utilizar para paquetes hacia adelante. Label Switch Caminos (LSP) son establecidos por el operador de red para una variedad de propósitos, como para crear una red basada en IP de redes privadas virtuales o para enrutar el tráfico a lo largo de las rutas especificadas a través de la red. En muchos aspectos, LSP no son diferentes de PVC en el cajero automático o retransmisión redes Frame, salvo que no dependen de una determinada tecnología de Capa 2.

MPLS/IP-ATM Red de acceso

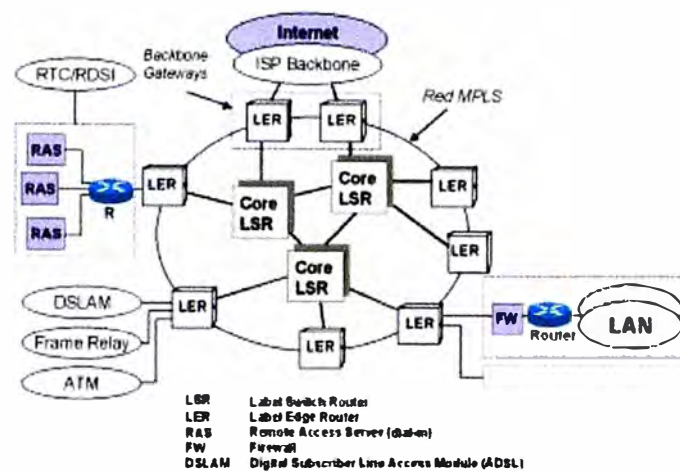


Figura 3.11 UNA RED MPLS, Fuente: www.cisco.com

En el contexto específico basado en MPLS de red privada virtual (VPN), LSRs que funcionan como entrada y salida de routers a menudo son llamados PE (Provider Edge) routers. Los dispositivos que funcionan sólo como enrutadores de tránsito son igualmente llamada P (Provider) routers. El trabajo de un router P es mucho más fácil que la de un router PE, por lo que puede ser menos complejos y pueden ser más confiables debido a esto.

Cuando un paquete sin etiquetar entra en el router de entrada y debe ser transmitida a un túnel MPLS, el primer router determina la equivalencia de clases de la expedición (FEC), el paquete debe ser y, a continuación se inserta o más etiquetas de una en-creado MPLS paquete nuevamente el cabecera.. El paquete se transmite luego al router del siguiente salto para este túnel. Cuando un paquete etiquetado es recibido por un router MPLS, la etiqueta superior se examina. Con base en el contenido de la etiqueta de un intercambio, empuje (imponer) o el pop (eliminar), la operación se puede realizar en paquete de la etiqueta de la pila. Los routers pueden tener pre-compilados tablas de búsqueda que les dicen qué tipo de operación que se basa en la etiqueta superior del paquete entrante, para que puedan procesar el paquete muy rápidamente. En una operación de swap de la etiqueta, se intercambia con una nueva etiqueta, y el paquete se remite a lo largo de la ruta de acceso asociadas a la nueva etiqueta. En una operación de empujar una nueva

etiqueta, se inserta en la parte superior de la etiqueta existente, efectivamente "encapsular" el paquete en otra capa de MPLS. Esto permite enrutamiento jerárquico de paquetes MPLS. . En particular, esto es utilizado por las VPN MPLS.

En una operación emergente de la etiqueta se quita el paquete, que puede revelar un interior por debajo de la etiqueta. Si la etiqueta apareció fue el último en la etiqueta de la pila, el paquete "hojas" del túnel MPLS.. Esto se hace generalmente por el router de salida.

MPLS puede hacer uso de las infraestructuras de red ATM, ya que sus flujos de etiqueta se pueden asignar a identificadores de circuitos virtuales ATM, y viceversa.

3.7.4 La comparación de IP versus MPLS

MPLS no se puede comparar a la propiedad intelectual como una entidad separada, ya que trabaja en conjunto con IGP y el período de los protocolos de enrutamiento IP. MPLS permite a las redes IP una simple ingeniería de tráfico.

MPLS se basa en los protocolos de enrutamiento IGP para construir su tabla de reenvío de la etiqueta, y el alcance de cualquier IGP suele estar restringida a una única compañía y razones de estabilidad política. Como todavía no existe un estándar en MPLS para las compañías no es posible tener el mismo servicio MPLS (Layer 2 o Layer 3) VPN que cubren más de un operador.

MPLS local de protección

En el caso de un fallo de los elementos de red cuando se emplean los mecanismos de recuperación en la capa IP, la restauración puede tardar varios segundos en lo que es inaceptable para aplicaciones en tiempo real (como VoIP En cambio, los locales de protección MPLS cumple con los requisitos de aplicaciones en tiempo real con recuperación) los tiempos comparables a los de los anillos SONET (hasta 50 ms.

Comparación de MPLS frente a Frame Relay

Frame Relay destinado a hacer un uso más eficiente de los recursos físicos, que permiten la underprovisioning de servicios de datos por las compañías de telecomunicaciones (telcos) a sus clientes, ya que los clientes probablemente no se utiliza un servicio de datos de 100 por ciento del tiempo. En los últimos años, Frame Relay ha adquirido una mala reputación en algunos mercados a causa de exceso de reserva de ancho de banda de estas empresas de telecomunicaciones.

Las empresas de telecomunicaciones suelen vender frame relay a las empresas que buscan una alternativa más barata a las líneas dedicadas en diferentes áreas geográficas dependía en gran medida de las empresas de telecomunicaciones y las políticas gubernamentales. Muchos clientes tienden a migrar de Frame Relay a MPLS sobre IP o Ethernet en los próximos años, que en muchos casos, reducir costos y mejorar la administración y el rendimiento de sus redes de área amplia.

Comparación de MPLS frente a ATM

Si bien los protocolos y tecnologías subyacentes son diferentes, tanto MPLS y ATM proporcionar un servicio orientado al transporte de datos a través de redes informáticas. En ambas tecnologías las conexiones son señaladas entre los extremos, el estado de la conexión se mantiene en cada nodo de la ruta de acceso y las técnicas de encapsulación se utilizan para transportar datos a través de la conexión.

MPLS es capaz de trabajar con paquetes de longitud variable, mientras que el transporte ATM de longitud fija (53 bytes) células. Los paquetes deben ser segmentadas, se transportan de nuevo montados a través de una red de cajeros automáticos utilizando una capa de adaptación, lo que añade complejidad considerable y los gastos generales de la secuencia de datos. MPLS, por el contrario, simplemente añade una etiqueta a la cabecera de cada paquete y lo transmite en la red.

Una conexión MPLS es unidireccional - permitiendo el flujo de datos en una sola dirección entre dos puntos finales.. Establecer vías de comunicación entre dos extremos requiere un par de proveedores de servicios lingüísticos que se establezcan. Debido a que dos proveedores de servicios lingüísticos son necesarios para la conectividad, los datos que fluyen en la dirección de avance puede utilizar una ruta diferente de los datos que fluyen en la dirección contraria. punto a punto de conexiones ATM (circuitos virtuales), por el contrario, son, lo que permite el flujo de datos en ambas direcciones sobre el mismo camino (bi-direccional sólo svc conexiones ATM; pvc conexiones ATM son unidireccionales).

La mayor ventaja única que ha MPLS sobre ATM es que fue diseñado desde el principio para ser complementarios a la propiedad intelectual.. routers modernos son capaces de soportar tanto MPLS e IP de forma nativa a través de una interfaz común permite a los operadores de red una gran flexibilidad en el diseño de redes y operación. Cajeros automáticos incompatibilidades con la propiedad intelectual que requieren una adaptación compleja por lo que es en gran medida inadecuados en las redes IP de hoy su mayor parte.

Los competidores de MPLS

El uso principal de MPLS es aplicar la ingeniería de tráfico limitado y Capa 3/Layer 2 "tipo de proveedor de servicios" VPN sobre redes IPv4. Los únicos competidores que son tecnologías como MPLS, que también ofrecen servicios como proveedor de servicios de Capa 2 y Capa 3 VPN.

Acceso a las redes MPLS

MPLS soporta una amplia gama de tecnologías de acceso, incluyendo ATM y Frame Relay T1 Mientras que menos conexiones ADSL caro también se puede utilizar,

no permiten a los usuarios de la red para cosechar los beneficios de MPLS importantes del servicio de aplicación priorización de clase.

Beneficios de MPLS

MPLS ofrece a las redes con una forma más eficiente para administrar las aplicaciones y la información se mueven de un lugar. Con la convergencia de voz, video y aplicaciones de datos, redes de empresas se enfrentan a crecientes demandas de tráfico. MPLS permite a la clase de servicio (CoS) de marcado y priorización de tráfico de la red, para que los administradores pueden especificar qué aplicaciones deben moverse a través de la red por delante de los demás. Esta función hace que una red MPLS especialmente importante para las empresas que necesitan garantizar el rendimiento de las aplicaciones de baja latencia, como VoIP y sus funciones críticas del negocio, otros.

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces.

Los beneficios que MPLS proporciona a las redes IP son: realizar ingeniería del tráfico o TE (Traffic Engineering), cursar tráfico con diferentes calidades de clases de servicio o CoS (Class of Service) o grados de calidad de servicio o QoS (Quality of Service), y crear redes privadas virtuales o VPN (Virtual Private Networks) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado.

Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes. Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (Wide Area Network) privada sobre la

Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec.

3.7.5 Virtual Private Network-VPN

Tráfico originados en una empresa o grupos de empresas pasan por la Internet de manera transparente, agregada, eficiente y segura.

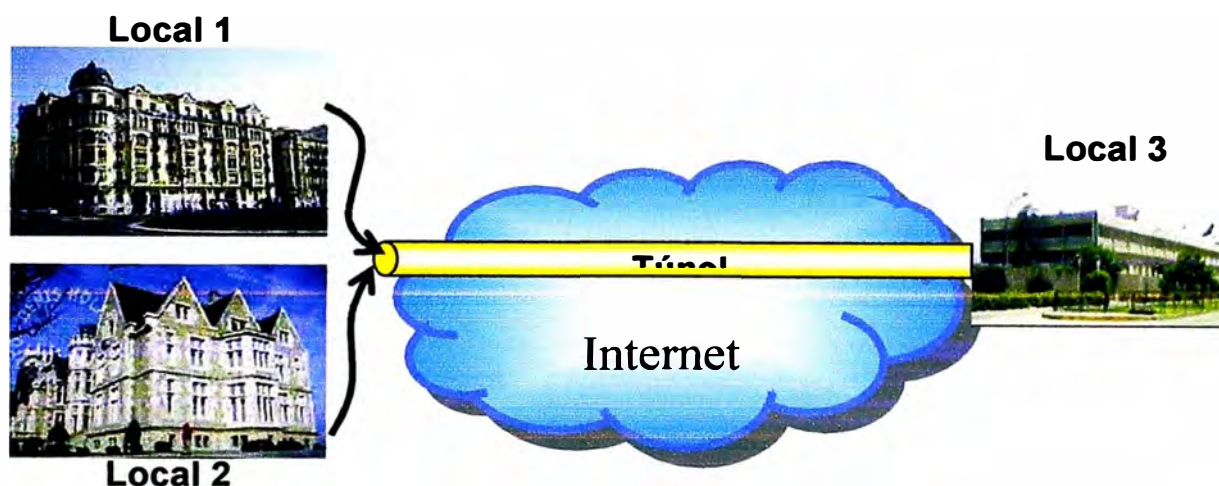


Figura 3.12 VPN entre 3 Locales, Fuente: www.cisco.com

3.7.6 Multiprotocolo

MPLS es usado sobre múltiples tecnologías

Routers IP deben ser actualizados para soportar MPLS.

Switches ATM deben ser actualizados para soportar MPLS.

Switches Frame Relay deben ser actualizados para soportar MPLS.

MPLS en Internet basada en IP es independiente del tipo de protocolo IP: IPv4/IPv6.

El router IP MPLS coloca una etiqueta delante del protocolo de capa 3, que es la base de la conmutación.

Se conoce como túnel al efecto de la utilización de ciertos protocolos de red que encapsulan a otro protocolo. Así, el protocolo A es encapsulado dentro del protocolo B, de forma que el primero considera al segundo como si estuviera en el nivel de enlace de

datos. La técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

Ejemplos de protocolos tunelizados

Protocolos orientados a datagramas:

- L2TP (Layer 2 Tunneling Protocol)
- MPLS (Multiprotocol Label Switching)
- GRE (Generic Routing Encapsulation)
- PPTP (Point-to-Point Tunneling Protocol)
- PPPoE (point-to-point protocol over Ethernet)
- PPPoA (point-to-point protocol over ATM)
- IPSec (Internet Protocol security)
- IEEE 802.1Q (Ethernet VLANs)
- DLSw (SNA over IP)
- XOT (X.25 datagrams over TCP)
- 6to4 (IPv6 over IPv4 as protocol 41)

Protocolos orientados a flujo:

- TLS (Transport Layer Security)
- SSH (Secure Shell)

Tunelizar para evitar un Cortafuegos

La técnica de tunelizar puede ser usada también para evitar o circunvalar en cortafuegos. Para ello, se encapsula el protocolo bloqueado en el cortafuegos dentro de otro permitido, habitualmente HTTP.

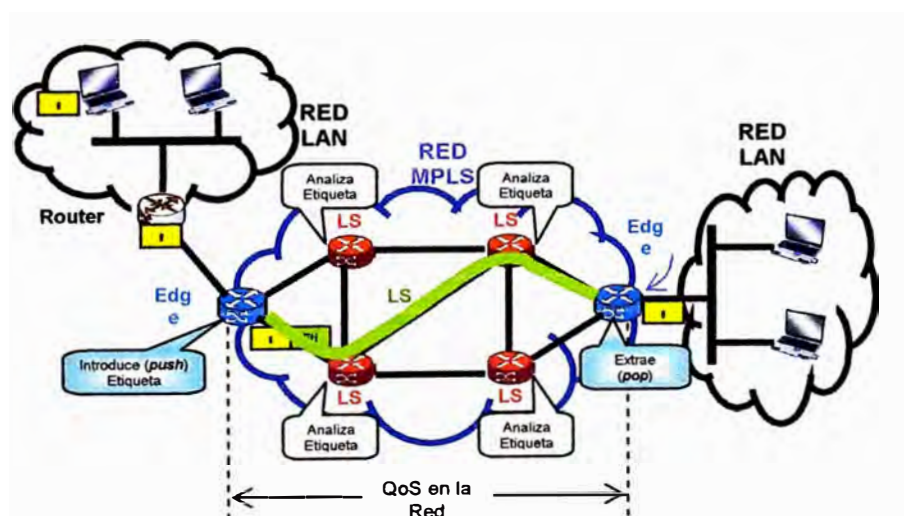


Figura 3.13 ESCENARIO DE UNA RED MPLS, Fuente: uam.es

3.8. MONITORIZACION

Se cuentan con Operadores de Centro de Computo los cuales tiene turnos rotativos de 24X7 y dan solucion a la alta disponibilidad mediante los procedimientos respectivos. Consiste en una monitorización de aplicaciones de negocio e infraestructura IT a través de la implantación de una serie de soluciones opensource que nos proporcionan.

Alertas en caso de caída de servicio

Representaciones topológicas de la red

Informes por servicio

Informes por host

Informes por grupos de servicios

Gracias a la flexibilización de estas soluciones podemos realizar monitorizaciones de negocio a medida con una gran facilidad de implantación.

3.8.1 JCONTROLLER

Se desarrollo una herramienta Web en la cual muestra las transacciones que ejecutan en las Bases de Datos durante todo el dia, contaba con reportes de días anteriores. Cuando no se ejecutaban ninguna transacción se ponía en rojo dando alertas en pantalla, mientras funcionaba estaba en verde.

Aquí muestro la página Web de Jcontroller:

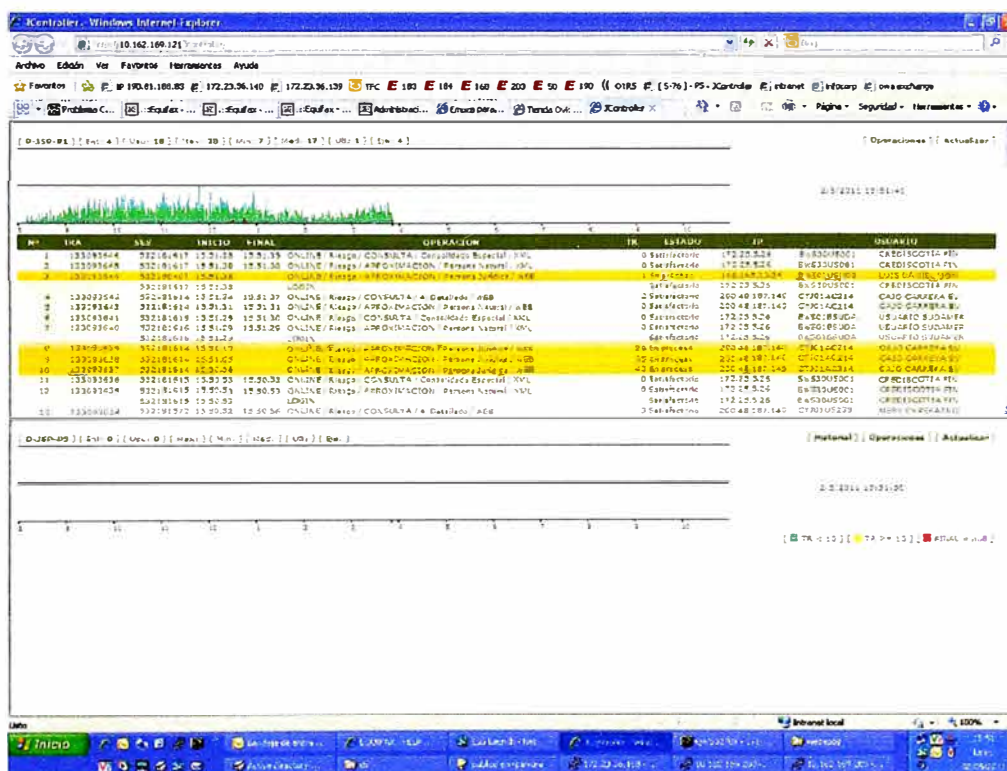


Figura 3.14 JController, Fuente: Web Acelor SAC

3.8.2 NAGIOS

– Sistema de monitorización de las aplicaciones y servicios proporcionados por el SI, que informa automática e instantáneamente 24 horas al día, 365 días al año, en caso de que se produzca un fallo en los mismos.

– Software Libre. S.O. Linux.

– Altamente configurable mediante plugins

– Disponible interfaz web para consulta del estado de los recursos y servidores

– Sistema de notificaciones muy flexible.

Monitorización de servicios de red

– Carga de CPU

– Chequeo de puertos (TCP, UDP)

– Tráfico de red (carga de las interfaces)

Un servicio o recurso puede tener 4 estados

• OK, CRITICAL, WARNING, UNKNOWN

– Cuando se produce un cambio de estado se dispara una alerta que puede producir una notificación al responsable de la máquina/servicio.

– Tipos de notificación.

• Interfaz web (sonora, visual)

• Mensaje Correo electrónico.

• Mensaje SMS.

Host	Service	Status	Last Check	Duration	Attempts	Status Information
Host1	DNS	OK	03-14-2008 10:13:08	7d 22h 11m 7s	1/3	DNS OK - 0.108 second response time
	IMAP	OK	03-14-2008 10:13:26	4d 2h 25m 11s	1/3	IMAP OK - 0.065 second response time
	IMAPS	OK	03-14-2008 10:13:26	4d 2h 25m 11s	1/3	IMAPS OK - 0.093 second response time
	POP	OK	03-14-2008 10:14:54	4d 2h 23m 20s	1/3	POP OK - 0.045 second response time
	POPS	OK	03-14-2008 10:13:26	4d 2h 25m 11s	1/3	POPS OK - 0.058 second response time
	SMTP	OK	03-14-2008 10:14:54	4d 2h 23m 20s	1/3	SMTP OK - 0.021 sec. response time
Host2	Nagios	OK	03-14-2008 10:13:26	0d 0h 9m 49s	1/3	Nagios ok: localised 6 processes, status log updated 235 seconds ago
	Nagios_Web	OK	03-14-2008 10:17:53	34d 22h 3m 14s	1/3	OK - HTTP/1.1 301 Moved Permanently - 0.064 second response time
Host2	CPU Load	OK	03-14-2008 10:17:54	7d 22h 11m 8s	1/3	SNMP OK - 24
	U1	OK	03-14-2008 10:14:02	35d 18h 30m 5s	1/3	SNMP OK - 8281741 609
	U2	OK	03-14-2008 10:17:54	7d 22h 11m 8s	1/3	SNMP OK - 0.0
	U3	OK	03-14-2008 10:14:02	35d 18h 37m 59s	1/3	SNMP OK - 1155854672 1383741 868
	U4	OK	03-14-2008 10:17:54	7d 22h 11m 9s	1/3	SNMP OK - 903.0
Host4	ArchivoDemocracia	OK	03-14-2008 10:15:02	2d 12h 33m 12s	1/3	HTTP OK: HTTP/1.1 200 OK - 6380 bytes in 0.058 seconds
Host6	CG	OK	03-14-2008 10:17:54	7d 22h 11m 9s	1/3	HTTP OK: HTTP/1.1 200 OK - 43872 bytes in 0.157 seconds
Host6	FTP	OK	03-14-2008 10:14:55	4d 2h 23m 19s	1/3	FTP OK - 3.806 second response time on port 21 (220 FTP server ready)
Host7	Unobora	OK	03-14-2008 10:17:54	7d 22h 11m 9s	1/3	HTTP OK: HTTP/1.1 200 OK - 8555 bytes in 0.038 seconds

Figura 3.15 Nagios, Fuente: Web Nagios

– Permiten resolver el problema más rápidamente y en ocasiones de forma automática mediante “handlers”o pequeños programas que se ejecutan cuando ocurre un fallo en el sistema (ej. levantar servidor web si se detecta estado critical).

- Tiene en cuenta las dependencias entre servicios (ej. Base de datos -aplicación web – servidor web)
- Se producen en función de la hora y/o día (ej. backups, mantenimientos, etc)
- Se elige el método en función del estado del servicio (ej. email para warning, SMS para critical y ok)

CAPITULO IV

ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Análisis del Problema

Teniendo en cuenta las definiciones teóricas y después de someterlas a un análisis contextualizado, considero conveniente:

La construcción de una red de área local especificada en el estándar de la IEEE número 802.3, llamada comúnmente Ethernet, la misma no es una tecnología sino una familia de tecnologías LAN, que se pueden entender mejor utilizando el modelo de referencia OSI. Todas las LAN deben afrontar el tema básico de cómo denominar a las estaciones individuales (nodos) y Ethernet no es la excepción. Las especificaciones de Ethernet admiten diferentes medios, anchos de banda y demás variaciones de la Capa 1 y 2. (Mas precisamente, la especificación 802.3u) 100Base-TX, que se refiere a una transmisión sobre UTP "Categoría 5e" a una velocidad de 100 Mhz con topología en estrella.

La ubicación en un local de ocho (08) metros de frente por doce (12) de fondo con una instalación eléctrica independiente para las computadoras con sus correspondientes descarga a tierra, considero conveniente contar con los artefactos eléctricos indispensables colocados en líneas de alimentación separadas del equipamiento, en virtud de ser éstos posibles generadores de campos magnéticos que producirían un grave deterioro a la red.

La disposición de las máquinas responderá a un esquema de "puesto individual de trabajo" o cubículo destinado al efecto, ubicada en forma longitudinal al salón, una al lado de otra guardando una cierta distancia, divididas convenientemente para guardar la privacidad del usuario.

La conexión al modem (DTE) de la empresa que brindará el servicio, lo haremos a través de un cable ethernet ubicado en el local por el proveedor, a uno de los puertos del switch (DCE) donde comienza nuestra conexión; esta conexión es el principal "cuello de botella", porque estará limitando físicamente el ancho de banda posible de utilizar.

La conexión de toda la red Lan se realizará mediante cableado horizontal. El tendido comienza en las cajas de servicio de cada estación y finaliza en el Switch que se encuentra dentro del rack, el cableado es sobre UTP Categoría 5e norma EIA/TIA 568B, es el que mejor se corresponde con el local y el tipo de instalación a realizar, lo que para

evitar daños físicos a los conductores, se colocarán dentro de unos conductos o canaletas, que serán, de material conductor debidamente aterrizado, evitando así la posibilidad de interferencias electromagnéticas; este tendido va ubicado suspendidos en la parte superior del salón, para estar lo más lejos posible del tendido eléctrico que se encuentra empotrado en la pared, favoreciendo el ordenamiento del local.

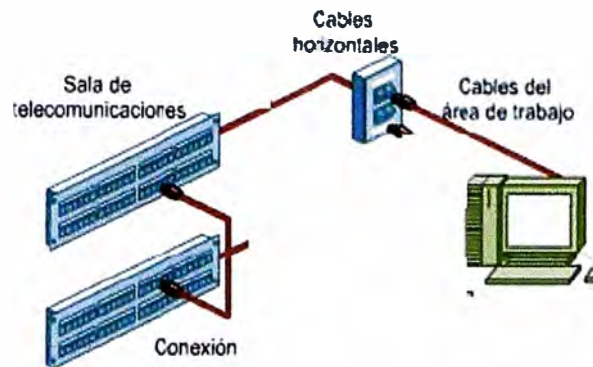


Figura 4.1 Instalaciones, Fuente: www.tecnicasprofesionales.com

Las máquinas se conectarán con cualquier otra a través del Switch, las conexiones se realizarán un patch core (cable directo) con conectores RJ 45 End-Plug (EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. Las letras RJ significan "registered jack" (jack registrado), y el número 45 se refiere a una secuencia específica de cableado). Desde la tarjeta de interfaz de red (NIC)

Para instalar los cables en los conectores correspondientes debemos seguir el estándar establecido para lograr el correcto funcionamiento de nuestra red; el cable UTP Cat. 5e posee 4 pares bien trenzados entre sí:

Blanco/Azul-----Azul Contactos 5 y 4
 Blanco/ Naranja---Naranja Contactos 3 y 6
 Blanco/ Verde-----Verde Contactos 1 y 2
 Blanco/ Marrón----Marrón Contactos 7 y 8

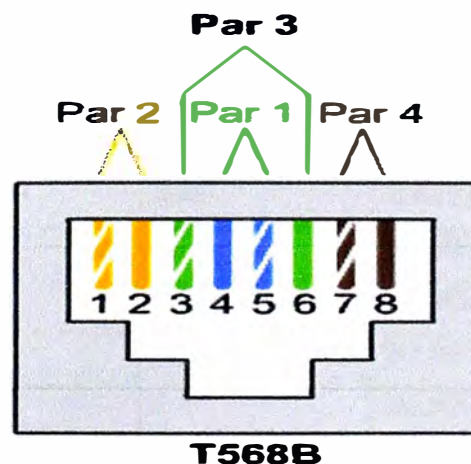


Figura 4.2 Norma EIA/TIA 568B, Fuente: www.utm.edu

4.2 Esquema del tendido de cables y ubicación de las maquinas:

Para la comunicación de todas las estaciones y la conexión a Internet, el protocolo TCP/IP, el cual es un protocolo utilizado por todos los ordenadores conectados a Internet, hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión; aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.



Figura 4.3 Patch Panel, Fuente: www.panduit.com

4.2.1 Requerimientos Previos:

El Hardware requerido que se inicio la red es el siguiente:

Descripción General:

Tabla 4.1 Primer Equipamiento de Hardware, Fuente: Proveedor IBM

N°	DESCRIPCIÓN GENERAL	CANTIDAD	COSTO (\$)
1	Computador Personal Pentium 4 de 2.8 Ghz	20	20,000.00
2	Switch 3Com SuperStack 3 Switch 4226T de 26 puertos, proporciona 24 puertos 10/100 con auto detección y dos puertos 10/100/1000 fijos.	1	800.00
3	Rack Panel 4 puestos	1	1,200.00
4	Pach Panel de 48 puertos categoría 5e marca hubble	1	500.00
5	Bobina de cable utp cat 5e 305 mts	2	200.00
6	Conectores RJ-45	300	100.00
7	Jack RJ-45	50	50.00
8	Canaletas porta cables	100 Mts	30.00
9	Cajetin Externo RJ45 CAT.5e	20	20.00
10	Servidor IBM SP2	1	30,000.00
11	Arreglo de discos	1	5000.00
Los precios en dólares e incluyen el IGV(18%)			\$ 57,900.00

El Software con el que cuenta el equipo es el siguiente

- Microsoft Windows Server 2000 para el servidor y Windows XP. Professional. Para las estaciones de trabajo
- Microsoft Office XP Professional
- Internet Explorer.

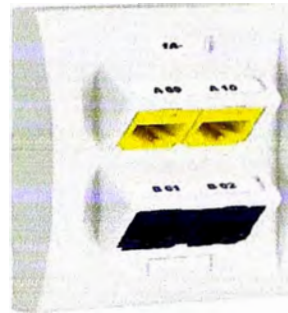


Figura 4.4 Canaletas y Accesorios usados, Fuente: www.panduit.com

4.2.2 Descripción Específica de los equipos:

- Computador Pentium 4 de 2.8 ghz:
- Procesador Pentium 4 de 2.8 ghz system bus 800 mhz, Intel. inside original
- Súper fan cooler original (ventilador) para el procesador
- Mother board o tarjeta madre Intel o pc-chips original
- Bus 533
- Socket 478
- 4 bancos para memoria ddr 333 / 266 / 200 mhz
- Puertos usb 2.0
- Puertos ps/2
- Puerto serial
- Puerto paralelo
- Red 10/100 bps
- Sonido 3d
- Video hasta 128 mb acelerado
- Memoria de 256 mb ddr pc-2700
- Disco duro 40 gb o más
- Cd-rom negro
- Floppy 3 1/2 de 1.44 mb
- Super case atx tower

- Teclado ps/2 de 101 teclas español
- Mouse 3 botones ps/2 con netscroll

4.3 APLICACIÓN EN LA RED DE DATOS

3Com SuperStack 3 Switch 4226T de 26 puertos, proporciona 24 puertos 10/100 con autodetección y dos puertos 10/100/1000 fijos.

Ports: 24 autosensing 10BASE-T/100BASE-TX, two 10BASE-T/100BASE-TX/1000BASE-T

- Media Interfaces: RJ-45
- Ethernet switching features: Full-rate nonblocking on all Ethernet ports, full/half-duplex auto-negotiation and flow control, multicast Layer 2 filtering, 802.1Q VLAN support, 802.1p traffic prioritization, IGMP snooping
- Height: 4.36 cm (1.7 in)
- Width: 44.0 cm (17.3 in)
- Depth: 27.4 cm (10.8 in)
- Weight: 3.0 Kg (6.5 lb)

El 3Com SuperStack 3 Switch 4226T completa la creciente oferta de conmutadores avanzados para backbone de red de 3Com. Este dispositivo de gama Ethernet y Fast Ethernet de Capa 2 gestionado para grupos de trabajo proporciona 24 puertos 10/100 con autodetección y 2 puertos 10/100/1000 fijos.

- La configuración del switch es totalmente automática y no requiere ningún hardware adicional. La riqueza en funcionalidades del switch proporciona una conmutación para grupos de trabajo extremadamente eficaz frente a su coste.
- Las funciones de robusta disponibilidad incluyen agregación de enlaces, soporte para Rapid Spanning Tree, opción de fuente de poder redundante, que aseguran el máximo en periodos de actividad para las aplicaciones críticas.
- Características: Control de flujo, capacidad duplex, conmutador MDI/MDI-X, negociación automática, soporte VLAN, manejable, apilable. Con una tecnología de conectividad por cable, una velocidad de transferencia de 100 Mbs y modo de comunicación semidúplex, dúplex pleno.

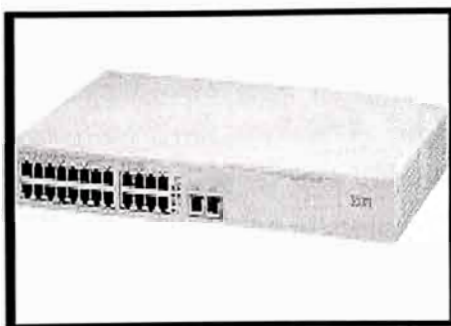


Figura 4.5 Switch, Fuente: www.3com.com

4.4 Diseño del Sistema

Se comenzó a desarrollar el prototipo de red, que permitiera una la comunicación entre los hots de la misma.

Aqui observamos el primer equipamiento de hardware que se diseño logrando lo que veremos a continuación:

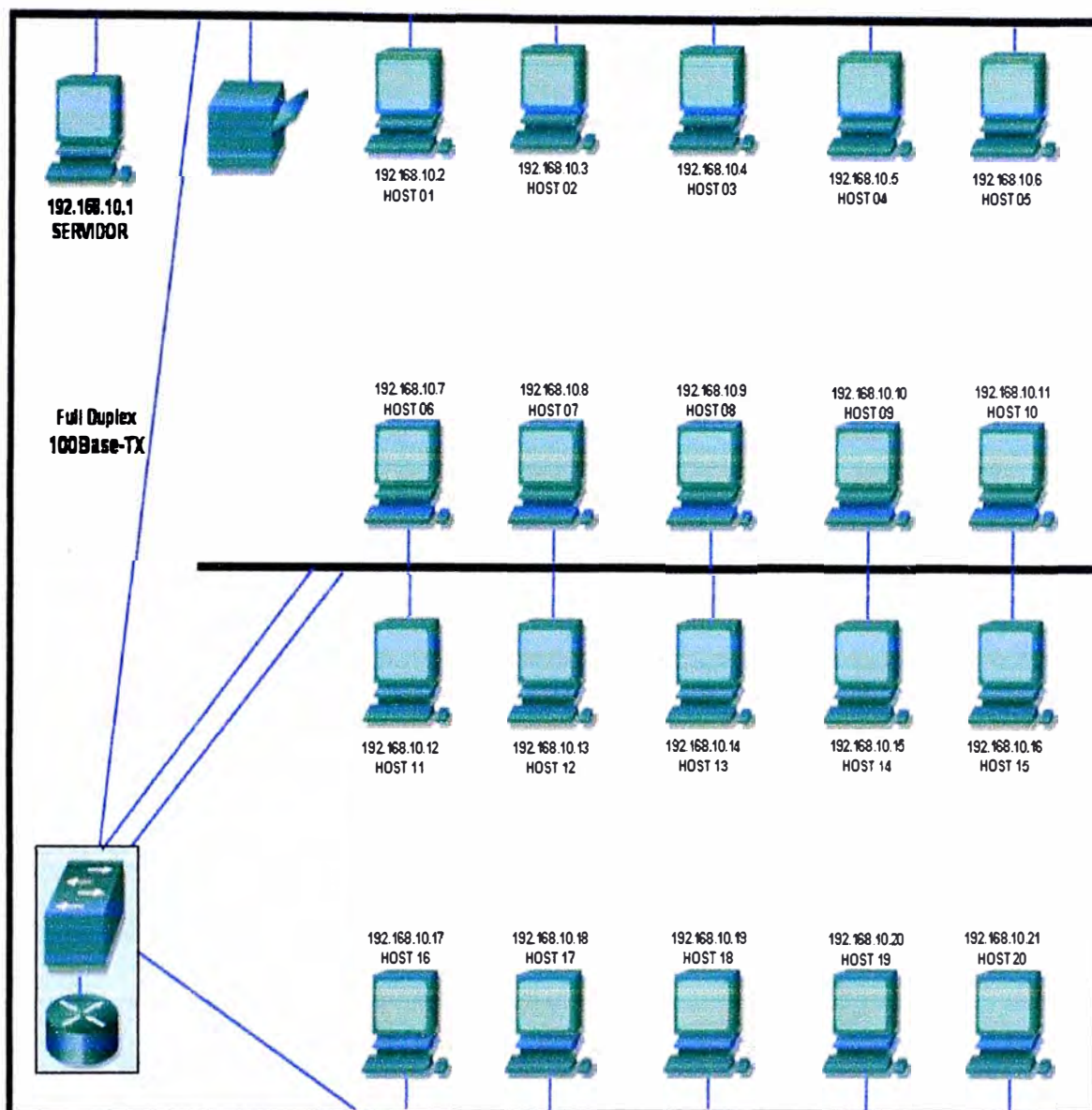


Figura 4.6 Diagrama de Red LAN, Fuente: Elaboración Propia

Pero la red creció ya que se requería aparte de mas computadoras para el personal se solicitaron mas servicios y por ende mas servidores. Se empezó a desarrollar la pagina Web Online de consultas para ello se tuvieron que cambiar el Servidor Principal por dos servidores con características modernas según el mercado.

Se instalaron las bases de datos en sus discos internos pero la información era demasiada por lo se requirió solicitar la compra de un Storage que se unieron con estos servidores con cable de fibra óptica, lo que se llamo el Proyecto SAN.

Adicionalmente el número de clientes creció también, se tuvieron que adquirir mas estaciones y servidores, ante este aumento se opto por la virtualización. El numero de personal aumento por lo que se tuvieron que originar nuevas sedes creándose VPNs. A continuación veremos el diagrama de tiempo de ejecución del inicio de la Central de Riesgos:

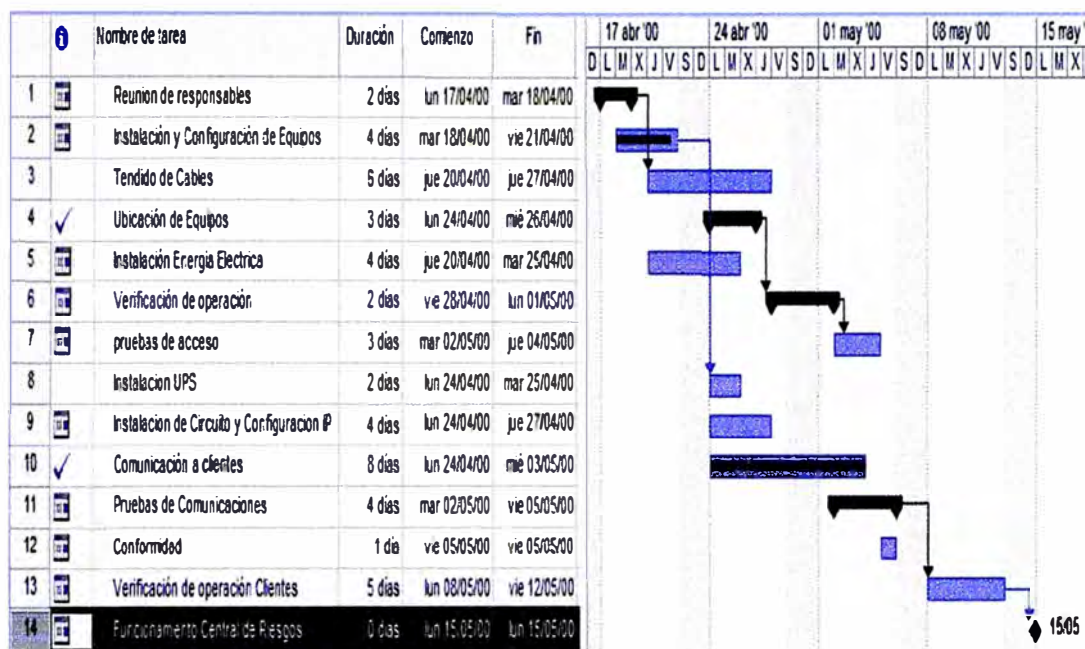


Figura 4.7 Diagrama de Tiempo, Fuente: Elaboración Propia

Es así en la fusión de Certicom e Infocorp tenemos a Equifax Perú la cual a continuación mostrare el diagrama de Red:

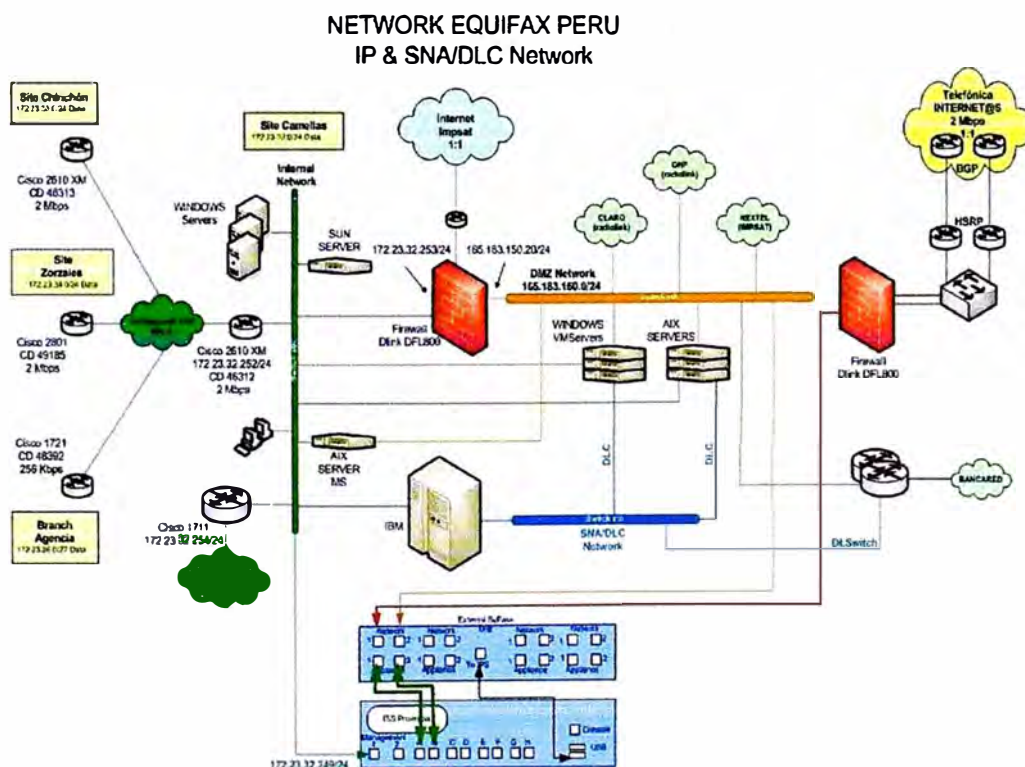


Figura 4.8 Red IP y SNA Equifax Perú, Fuente: Equifax Peru

4.5 APLICACIÓN EN LOS ENLACES

Se necesitaba tener un enlace como respaldo mediante un enlace de Fibra adicional de otro POP de acceso y que se conecte a R2, esto con la finalidad de que funcione en estado STAND BY.

Se reutilizará el enlace de fibra del CID 185444, cuyo circuito el cliente dará de baja antes de implementar el requerimiento.

DIAGRAMA DE RED ACTUAL

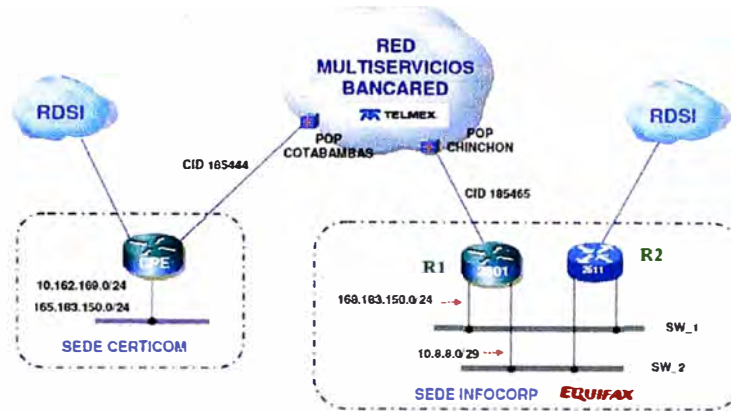


Figura 4.9 Diagrama la Red Privada Bancared, Fuente: Telmex Perú

SOLUCION PROPUESTA

- _ Un enlace de respaldo conectado al router R2
 - _ Protocolo de respaldo HSRP (ya existe), para redundancia de gateway IP.
 - _ Ambos circuitos deben de emplear la misma configuración de enrutamiento y/o bridge.
 - _ Se usará la red 172.25.29.0 / 24 y la nueva red 172.25.34.0 / 24
 - _ Se conectará la línea ISDN hacia el equipo router R2
 - _ Si, estando caído el enlace Principal (fibra) ó router (R1) se cae también el enlace de Contingencia (fibra), entonces de forma automática se activa la línea ISDN BRI.
- No se considera en los routers configuración de comandos de DLSW.

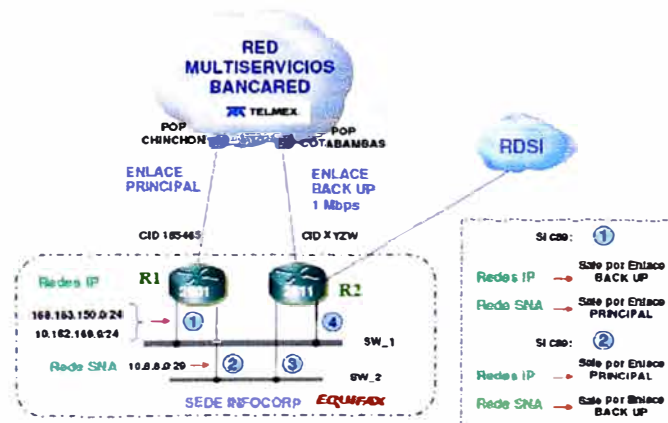


Figura 4.10 HSRP en la Red Privada Bancared, Fuente: Telmex Peru

Un enlace de respaldo conectado al router R2

- _ Protocolo de respaldo HSRP para redundancia de gateway IP.
- _ Ambos circuitos deben de emplear la misma configuración de enrutamiento y/o bridge.
- _ Los enlaces están en diferentes POP de acceso ya que es el mismo proveedor.
- _ Se conectará la línea ISDN hacia el equipo router R2
- _ Si, estando caído el enlace Principal (fibra) o router (R1) se cae también el enlace de Contingencia (fibra), entonces de forma automática se activa la línea ISDN BRI.
- _ Con esto se tiene un enlace como respaldo mediante un enlace de Fibra adicional de otro POP de acceso y que se conecte a R2, esto con la finalidad de que funcione en estado STAND BY.
- _ Ambos routers manejarán el mismo rango del pool de direcciones IP para las traslaciones de direccionamiento IP (172.25.29.0 / 24 y 172.25.34.0 / 24).
- _ En los routers de ASBANC se modificarán los distribute-list, accesslist, etc., requeridos para habilitar el enlace de respaldo.

Ya que los routers son alquilados se pagaban una mensualidad de Linea Dedicada Telmex 1024/1024 (Fibra Optica) por linea.

* Instalación \$ 612.00

* Mensualidad \$ 250.00 por enlace

Los precios en dólares e incluyen el IGV(18%)

La instalación incluye router e instalación en situ. Aproximadamente demoran una semana en hacer las instalaciones pues tienen que pedir permiso al municipio, al edificio, etc.

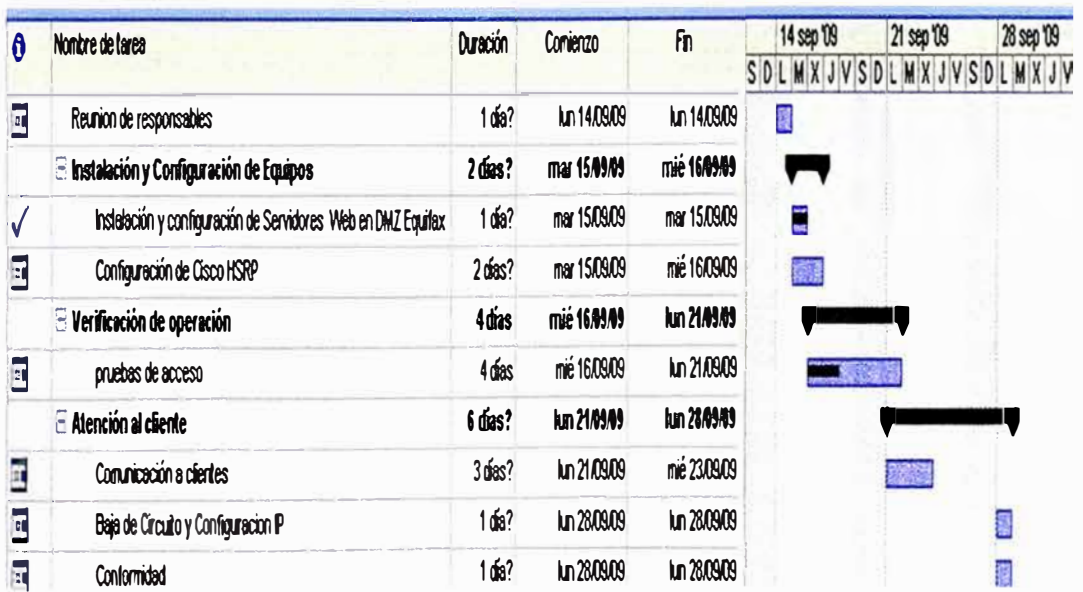


Figura 4.11 Diagrama de Tiempo, Fuente: Elaboración Propia

También el mismo criterio se aplicó para las líneas dedicadas de Internet, teniendo alta disponibilidad para los servicios WWW, ftp, correo electrónico.

4.6 APLICACIÓN EN RED SAN

- Implementar una solución de almacenamiento SAN para los equipos de Producción (línea de negocio).
- Implementar un esquema de contingencia y alta disponibilidad (a nivel de máquina virtual), haciendo uso de las herramientas HA y Vmotion de VMWare.
- Redistribución de servidores y consolidar todos los equipos de DMZ y/o con conexión con Host IBM.
- Optimizar el uso de los recursos de CPU y memoria de los equipos ESX.

Inicialmente contábamos con 2 Servidores unidos al Storage con dos tarjetas de Fibra Óptica cada uno como alta disponibilidad, pero estaba limitado por solo a utilizar 2 Servidores por lo que se requería ingresar más Servidores a la SAN. Para ello se requiere la virtualización debido a que los Servidores tenían instalado AIX que es un sistema parecido al UNIX. Estos servidores compartían el Storage en la cual solo tenía instalado la base de datos. Como cada Servidor tiene 2 tarjetas si tuviera problemas una de ellas seguiría conectado con el storage así manteniendo la conexión.

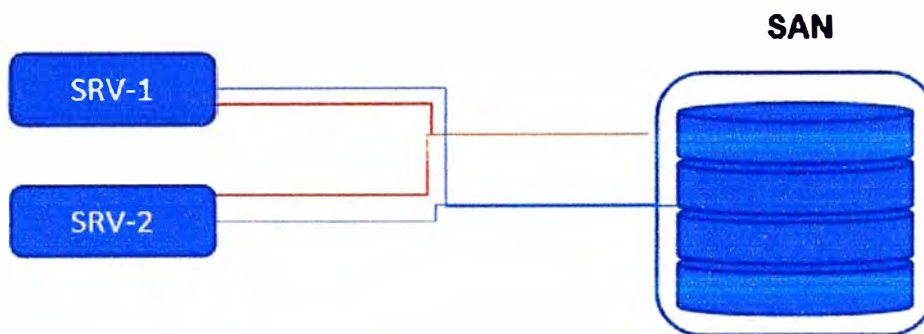


Figura 4.12 Esquema Anterior SAN, Fuente: Elaboración Propia

Se tuvo que consolidar los Servidores en Nuevos Servidores lo cuales le denominamos ESX debido a que contaba con la Virtualización VMware lo cual se hablara en el siguiente capítulo primero usando un solo switch de fibra óptica.

Relación de equipos empleados:

Los equipos para una SAN existen en diferentes marcas pero se utilizó IBM, aquí el detalle:

Equipo SAN

IBM DS 4700 Express Modelo 70

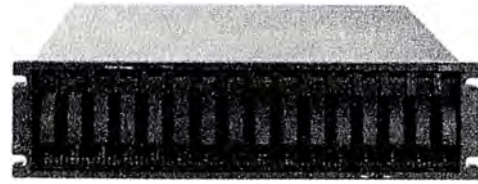
Soporte hasta 33.6 TB

Hasta 2 GB de memoria cache física

Conexión Fibra Canal 4 Gbps

06 HD FC 330 GB/15000 RPM

Precio: \$74,000



Switch IBM TotalStorage SAN 16B-2

16 Puertos de 4 Gbps

Precio: \$ 2,500 dólares



IBM System x3650 M2

Processor/Speed: Quad-Core Intel® Xeon™ Processor X5560

2.80GHz

Number of Processors:

1/2

Memory (Standard/Max/Type)

8GB/128GB/DDR3 RDIMM

Internal Hard Disk (Std/Max) (GB)

0/3.6TB

Form Factor:

2U Rack

Optical device:

CD-RW/DVD Combo V Ultrabay Enhanced

IBM Web price

\$5,200.00 Los precios en dólares e incluyen el IGV(18%)

Figura 4.13 Equipos IBM, Fuente: www.ibm.com

Tabla 4.2 Equipamiento de SAN con 2 Servidores, Fuente: IBM

N°	DESCRIPCIÓN GENERAL	CANTIDAD	COSTO \$
1	Storage IBM DS 4700 Express Modelo 70	1	74,,000.00

2	Switch IBM TotalStorage SAN 16B-2	1	2,500.00
3	Servidor IBM System 3650 M2	2	10,400.00
4	Monitor 17"	2	300.00
Los precios en dólares e incluyen el IGV(18%)			\$ 87,200.00

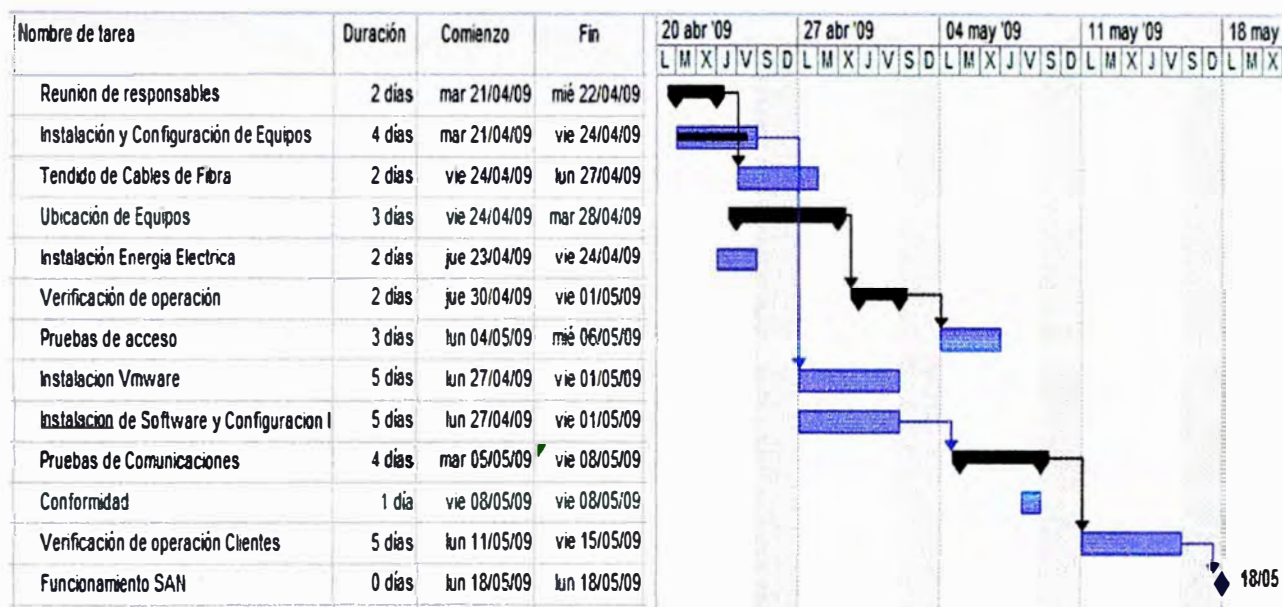


Figura 4.13 Diagrama de Tiempo, Fuente: Elaboración Propia

Configuración SAN

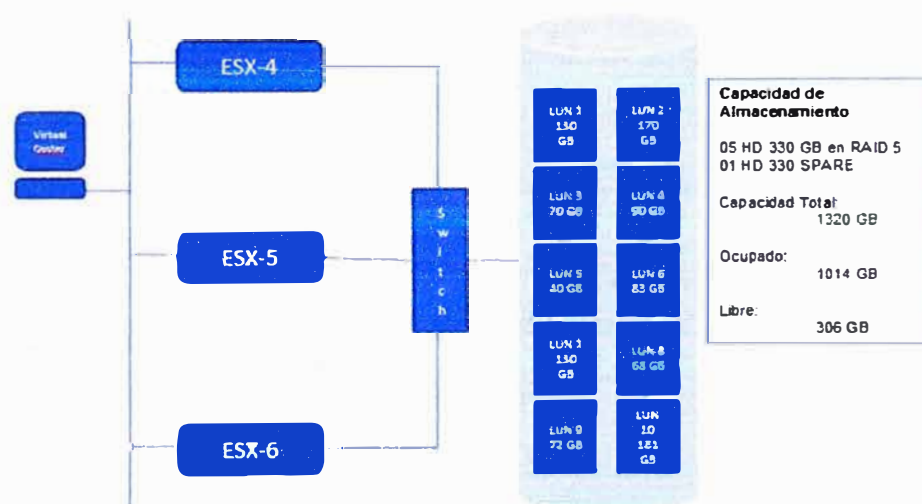


Figura 4.14 Esquema con Switch SAN, Fuente: Elaboración Propia

Ya que es una solución escalable se proyecta tener todo en 5 servidores conectados en 2 switches SAN y estos unidos al Storage, conectando cada servidores que contaban con

dos tarjetas HBA a cada uno de los switches, a continuación veremos como fue la solución final:

En este caso se contó con una PC adicional la cual se llamo Virtual Center que la consola donde se realiza la distribución de los servidores virtuales en los 5 Servidores, si un servidor se para otro asume su función automáticamente, teniendo así una alta disponibilidad de servidores y por ende los servicios continúan, para esta solución se tuvo como elementos:

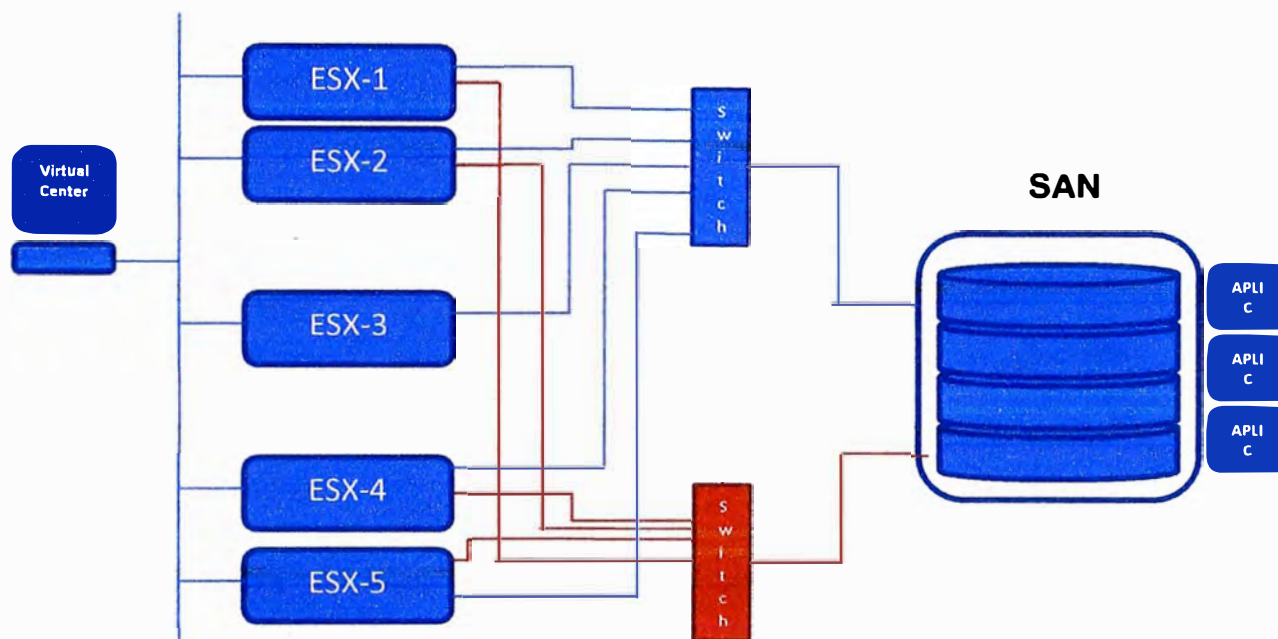


Figura 4.15 Empleo de 2 switches de Fibra Óptica, Fuente: Elaboración Propia

Tabla 4.1 Equipamiento SAN de 5 Servidores, Fuente: IBM del Perú

N°	DESCRIPCIÓN GENERAL	CANTIDAD	COSTO \$
1	Storage IBM DS 4700 Express Modelo 70	1	74,000.00
2	Switch IBM TotalStorage SAN 16B-2	2	5,000.00
3	Servidor IBM System 3650 M2	5	26,000.00
4	Monitor 17"	2	300.00
5	PC IBM Core Duo	1	1,500.00
Los precios en dólares e incluyen el IGV(18%)			\$ 106,800.00

Ya que los servicios a los clientes aumentaron se tuvieron que adquirir dos servidores mas para que sean conectados al storage, creándose entonces la red SAN. Al contar con 5 servidores se tuvo una alta disponibilidad en los sistemas de Central de Riesgos activandose automáticamente las redundancias en caso de fallas.

Por temas de negocio y economía se opto por contratar un housing para el Data Center que estaría alojado en IBM del Peru como ultima etapa aprovechando esto se realizo las soluciones de alta disponibilidad antes del traslado, llegando a tener el siguiente cronograma que a continuación veremos:

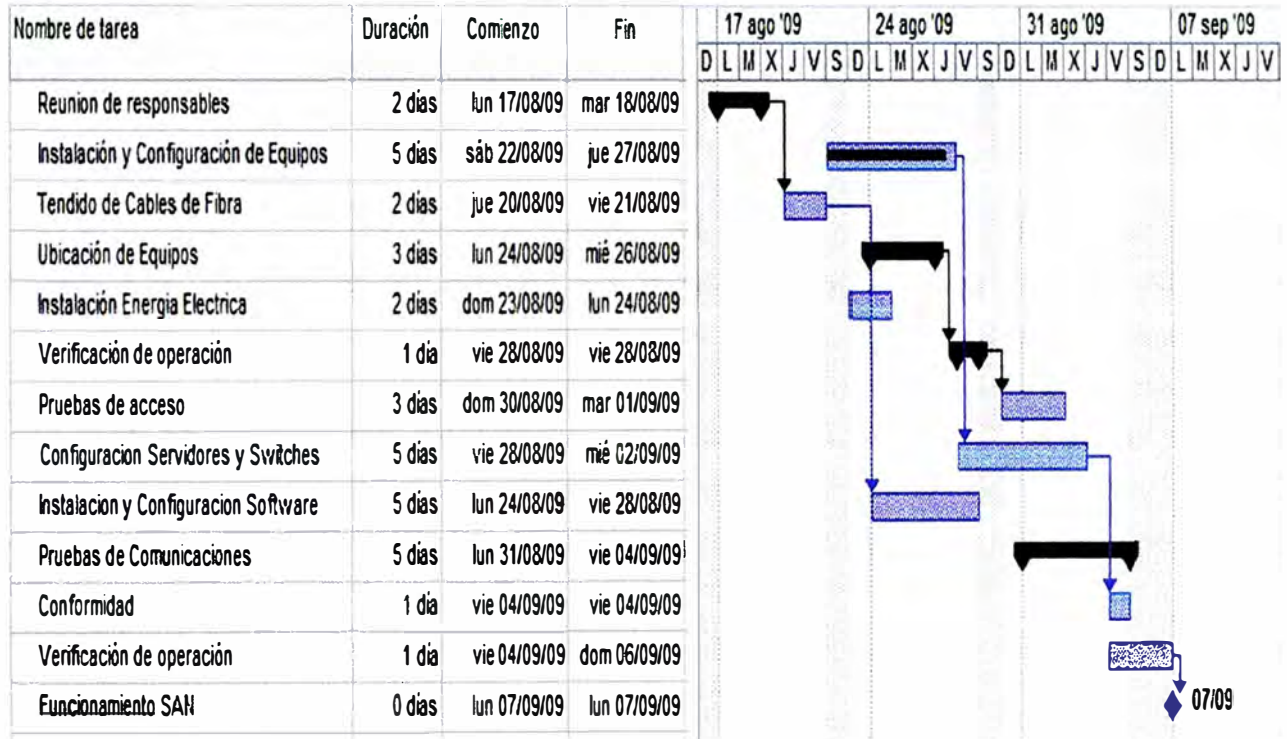


Figura 4.16 Diagrama de Tiempo, Fuente: Elaboración Propia

CONCLUSIONES Y RECOMENDACIONES

1.- El diseño cumplió con las expectativas para el cual se formuló el proyecto, de esta manera logrando el objetivo principal el cual era el diseño e implantación y explotación, en forma rápida, fácil y económica de una Central de Riesgos, atendiendo a los estándares internacionales vigentes en cuanto a requerimientos en la interconexión de equipos en un ambiente de trabajo reducido y de esta manera obtener todas las potencialidades de una red Lan, sin dejar de lado los costos de los materiales ya que si estos no son comprendidos y llevados a la práctica; nuestra red quedara rápidamente fuera de uso; en síntesis, lo básico es saber escoger un tipo de red según las características del lugar a instalar, elegir los protocolos a utilizar y elegir correctamente el sistema operativo de red.

2.- La solución propuesta mantiene en mente rendimiento y disponibilidad como principales preocupaciones: se garantiza que las respuestas a clientes son rápidas y los tiempos de recuperación desde fallo son bajos.

3.- Actualmente estamos trabajando para evaluar las optimizaciones propuestas, así como para mejorar la arquitectura y los protocolos de replicación detallados en este trabajo. Queda pendiente el estudio a fondo de una solución de replicación basada en la detección y diagnóstico de errores que permita la migración de los estados cuando se produzca un fallo, evitando de esta forma la señalización inherentemente asociada a la replicación. De cara a la evaluación, planeamos completar la evaluación de todos los protocolos propuestos así como implementar escenarios avanzados de balanceo y comparación de carga entre las diferentes replicas.

4.- En la medida de lo posible nunca poner juntas en un mismo ducto líneas de datos con líneas de 220V, o si fueran separadas respetar una distancia mínima de 15 a 20 centímetros. Sin embargo en canaletas especiales del tipo cable canal se especifican separaciones físicas de 2 a 3 centímetros entre cables de datos, de 220V (siempre que sean de un sistema UPS) y telefónicas en una misma canaleta.

El aspecto más importante lo constituye la calidad de los materiales empleados para la instalación de la red además es de vital importancia el correcto aterramiento de la red para evitar inconvenientes futuros.

Recuerde también, que la categoría 5e del cable de red es menos susceptible al ruido y a las interferencias. Igualmente si se tratase de líneas telefónicas tratar de colocarlas en conductos separados, o de lo contrario que sean categoría 5e (trenzados), para que no produzcan en efecto de atenuación sobre la red que podría alterar su eficiencia.

Hay que tener el cuidado de seleccionar una marca de materiales reconocida a escala mundial para asegurarse aún más el éxito del diseño.

Usar en cielorrasos o cielos falsos tubería metálica, no Cable canal (PVC)

Conectar correctamente el cableado de la red según los estándares establecidos, en este caso específicamente el T568B para cable UTP y conectores RJ-45. Pues de lo contrario el cable funciona como una antena y capta todo tipo de interferencia.

No exceder la distancia máxima de los cables recomendada por el fabricante, vale aclarar que el límite para el cableado fijo es de 90m y no esta permitido excederse, así como el límite para los patch cord es de 6m en la patchera y 3m en la conexión del terminal, siendo esto nada mas que una aclaración ya que en nuestro caso no se dan tales distancias

Tener en cuenta testear la continuidad del cable UTP mediante la conexión apropiada de los dos extremos terminales del mismo conectados al Switch.

ANEXO A
GLOSARIO

RDSI	RED DIGITAL DE SERVICIOS INTEGRADOS
DIAL-UP	CONEXIÓN POR LÍNEA CONMUTADA
TCP	TRANSPORT CONTROL PROTOCOL
IP	INTERNET PROTOCOL
SNA	SYSTEMS NETWORK ARCHITECTURE
RAID	REDUNDANT ARRAY OF INDEPENDENT/INEXPENSIVE DISKS
SAN	STORAGE AREA NETWORK
LAN	LOCAL AREA NETWORK
NIC	NETWORK INTERFACE CONTROLLER
ISDN	INGLES DE RDSI
ADSL	ASYMMETRIC DIGITAL SUBSCRIBER LINE
MPLS	MULTIPROTOCOL LABEL SWITCHING)
VPN	VIRTUAL PRIVATE NETWORK
CPU	CENTRAL PROCESSING UNIT
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
ISO	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IEC	INTERNATIONAL ELECTROTECHNICAL COMMISSION
OSI	OPEN SYSTEM INTERCONNECTION
UTP	UNSHIELDED TWISTED PAIR
DTE	EQUIPO TERMINAL DE DATOS
DCE	EQUIPO DE TERMINACIÓN DEL CIRCUITO DE DATOS
EIA	ELECTRONIC INDUSTRIES ALLIANCE
TIA	TELECOMMUNICATIONS INDUSTRY ASSOCIATION
VLAN	RED DE ÁREA LOCAL VIRTUAL
MDI/MDI-X	MEDIUM DEPENDENT INTERFACE/ MDI CROSSOVER
CSMA/CD	ACCESO MÚLTIPLE POR DETECCIÓN DE PORTADORA CON DETECCIÓN DE COLISIONES
RAM	MEMORIA DE ACCESO ALEATORIO
MAC	CONTROL DE ACCESO AL MEDIO
PCMCIA	PERSONAL COMPUTER MEMORY CARD INTERNATIONAL ASSOCIATION
IRQ	PETICIÓN DE INTERRUPCIÓN

SFT	SISTEMA TOLERANCIA A FALLOS
CORE	CENTRO
ST	SET AND TWIST)
SMA	SUBMINIATURE VERSION A
SONET	RED ÓPTICA SÍNCRONA
DMZ	ZONA DESMILITARIZADA
ANSI	AMERICAN NATIONAL STANDARDS INSTITUTE
STP	SHIELDED TWISTED PAIR
CODEC	CODIFICADOR-DECODIFICADOR
LAYER	CAPA
LLC	CONTROL DE ENLACE LOGICO
ISP	PROVEEDOR DE SERVICIOS DE INTERNET
HA	HIGH AVAILABILITY
NLB	NETWORK LOAD BALANCING
UDP	USER DATAGRAM PROTOCOL
IOS	INTERNETWORK OPERATING SYSTEM
STANDBY	CONSUMO EN ESPERA
HSRP	HOT STANDBY ROUTER PROTOCOL
VRRP	VIRTUAL ROUTER REDUNDANCY PROTOCOL
ASBANC	ASOCIACIÓN DE BANCOS DEL PERÚ
ATM	MODO DE TRANSFERENCIA ASÍNCRONA
VOIP	VOICE OVER IP
UNI	UNIVERSIDAD NACIONAL DE INGENIERIA

BIBLIOGRAFÍA

- [1] www.cisco.com
- [2] www.ibm.com
- [3] www.hopeisd.com/products/cables/eia568a.html
- [4] www.inictel.edu.pe
- [5] www.iso.org
- [6] www.microsoft.com
- [7] www.renovetec.com
- [8] www.host.ots.utexas.edu
- [9] www.larevistainformatica.com
- [10] www.panduit.com
- [11] www.utm.edu
- [12] www.tecnicasprofesionales.com
- [13] <http://linux-ha.org/>
- [14] http://www.itlp.edu.mx/publica/tutoriales/telepro/t4_4.htm#Estrella
- [15] http://www.itlp.edu.mx/publica/tutoriales/telepro/t4_4.htm#Arbol
- [16] <http://www.gilat.com/Home.asp>
- [17] <http://technet.microsoft.com/en-us/library/cc748824.aspx>
- [18] <http://www.ietf.org/html.charters/vrrpcharter.html>.