PROPUESTA DE IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES PARA EL IMTP

ÁNGELA MARÍA VILLOTA ECHEVERRI

UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
PRÁCTICAS PROFESIONALES
PEREIRA
2010

PROPUESTA DE IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES PARA EL IMTP

ÁNGELA MARÍA VILLOTA ECHEVERRI

Informe de Práctica Profesional

Tutor
JHONATTAN CORDOBA RAMIREZ
Ing. Sistemas y Telecomunicaciones

UNIVERSIDAD CATÓLICA POPULAR DEL RISARALDA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES
PRÁCTICAS PROFESIONALES
PEREIRA
2010

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE APÉNDICES

Pág.

RESUMEN

RESUMEN

Poseer una buena configuración de la red en una empresa, contar con una buena infraestructura de dispositivos de red y una alta protección en cuanto a seguridad informática, garantiza el buen desarrollo de los procedimientos internos que se realizan en el IMTP para el beneficio de la comunidad, por esto, a partir de un análisis previo a la red, se propone un diseño para la misma acorde a las necesidades del Instituto, cumpliendo con los estándares necesarios.

Palabras Claves: Red, Cableado, Telecomunicaciones, Ancho de Banda, Direccionamiento IP, Vlan´s, Seguridad Informática, Servidores.

ABSTRACT

Having a good network configuration in a company, have a good infrastructure network devices and high protection in terms of security, ensuring the smooth running of the internal procedures are performed in the IMTP for the benefit of the benefit of the community, so, from a previous analysis to network design is proposed for the same line with the needs of the Institute, meet the standards required.

Keywords: Network, Wiring, Telecommunications, Bandwidth, IP addressing, VLAN's, Security, Servers

INTRODUCCIÓN

A través del tiempo el hombre ha ido evolucionando conforme sus necesidades se amplían, dentro del ámbito de las comunicaciones la necesidad de comunicarse a grandes distancias condujo a realizar grandes descubrimientos tales como el telégrafo, posteriormente el teléfono y así se fueron desarrollando dispositivos de comunicación; en la actualidad el Internet es el gran descubrimiento ya que a través de él las distancias se acortaron, el intercambio de información en tiempo real es un hecho, vender por Internet es la actualidad y mas que esto, en las organizaciones ya es un medio de comunicación y las aplicaciones se han desarrollado para la simplificación de procesos.

Las redes de Computadoras, han salido a relucir en el importante avance tecnológico que ha caracterizado a las últimas décadas del presente siglo, estas, son herramientas que permiten utilizar el recurso de la información de manera eficiente, rápida y confiable, facilitando al hombre el manejo del recurso informativo, así como el acceso a este.

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 ofimáticos. 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. Es por esto que en el IMTP se quiere realizar una renovación tecnológica, para hacer una reestructuración en la red interna solucionado los problemas que se vienen presentando por la presencia de programas malintencionados, produciendo esto una gran lentitud en la red lo que conlleva en la mayoría de los casos a que los procesos y tramites que se prestan a la comunidad se vean afectados por constantes caídas del sistema. Lo que se pretende es hacer un estudio de la red actual del Instituto y plantear un diseño acorde a las necesidades del mismo, para seguir prestando todos sus servicios de una manera adecuada y eficiente.

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 instalación correcta de switches para intercomunicar equipos de cómputo, routers y demás elementos de comunicación que sean requeridos. Así mismo definir una topología de red implementando todos los estándares del cableado estructurado.

1. PRESENTACIÓN DE LA ORGANIZACIÓN O SITIO DE PRÁCTICA

1.1 CREACIÓN

El honorable Concejo Municipal de Pereira, creó el Instituto Municipal de Tránsito de Pereira, mediante Acuerdo 137 de 1994, iniciando actividades a partir de enero de 1996.

1.2 NATURALEZA

Es un establecimiento público del orden Municipal con Personería Jurídica, autonomía administrativa y patrimonio independiente.

1.3 CLASIFICACIÓN

Somos un organismo de Tránsito de clase “A” código 66001, según Resolución 00765 del 27 de octubre de 1995 del Ministerio de Transporte.

1.4 REPRESENTACIÓN LEGAL

La Dirección y Administración del Instituto está a cargo de un Director General, de libre nombramiento y remoción del Alcalde de Pereira.

1.5 POLÍTICA DE CALIDAD

En el Instituto Municipal de Tránsito de Pereira, nos comprometemos con el mejoramiento continuo, actuando con liderazgo en la prestación de servicios de tránsito, con talento humano competente, respetando la esperanza de vida

1.6 MISIÓN

Ofrecer una eficiente movilidad por las vías públicas de Pereira, teniendo como puntos de partida:

- ✓ La difusión de la cultura vial
- ✓ El establecimiento del compromiso social en la comunidad
- ✓ La minimización del impacto sobre el medio ambiente
- ✓ La generación de procesos de aprendizaje continuo para los funcionarios, comprometiéndolos a garantizar un excelente servicio.

1.7 VISIÓN

Ser una entidad competitiva a nivel nacional en servicios de transito, con el mejor talento humano y una constante innovación, realizando actividades que contribuyan a la cultura ciudadana, vial y a la preservación del medio ambiente, teniendo como principio fundamental la excelencia en el desarrollo de las actividades.

1.8 PRINCIPIOS INSTITUCIONALES

- ✓ Servicio integral con enfoque al cliente
- ✓ Transparencia en el desarrollo de las actividades
- ✓ Difusión de la educación vial
- ✓ Preservación y cuidado del medio ambiente
- ✓ Comunicación institucional
- ✓ Promoción de ciudadanía basado en la “cultura de la legalidad”

1.9 VALORES PERSONALES

- ✓ **Honestidad:** Moderación en la persona, para actuar con rectitud, honradez y decencia.
- ✓ **Respeto:** Reconocimiento de la legitimidad del otro para ser distinto a uno.
- ✓ **Responsabilidad:** Obligación de responder por los propios actos.
- ✓ **Lealtad:** Fidelidad en el trato o en el desempeño de un cargo.
- ✓ **Transparencia:** Calidad del comportamiento evidente.

1.10 VALORES INSTITUCIONALES

- ✓ **Compromiso:** Obligación contraída. Palabra dada, fe empeñada. Palabra que se da uno mismo para hacer algo.
- ✓ **Colaboración:** Acción y efecto de trabajar en común con otra persona.
- ✓ **Eficacia:** Fuerza y capacidad para obrar. Capacidad de acción para hacer efectivo un propósito.
- ✓ **Cumplimiento:** Acción y efecto de llevar a cabo. Hacer lo que se debe o lo que se está obligado en los términos previstos.
- ✓ **Justicia:** Lo que debe hacerse según derecho o razón. Virtud de dar a cada uno lo que le corresponde o le pertenece.

1.11 ESTRUCTURA ORGÁNICA Y SERVICIOS

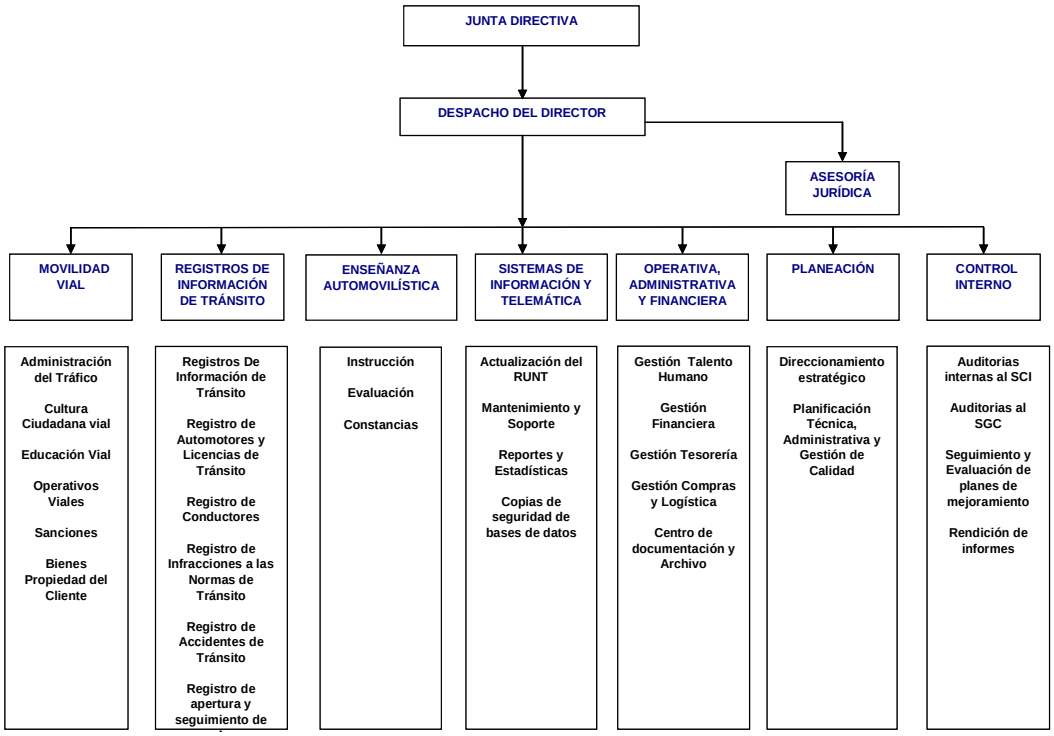


Figura 1. Organigrama de la empresa

1.12 DEPARTAMENTO EN EL QUE SE UBICA LA PRÁCTICA

Subdirección General de Sistemas de Información y Telemática.

1.13 NÚMERO DE EMPLEADOS

180.

1.14 RESEÑA HISTÓRICA

El Concejo Municipal de Pereira Mediante el Acuerdo 137 de diciembre 20 de 1994, acuerda crear el Instituto Municipal de Tránsito y Transporte de Pereira, como un establecimiento público, de orden Municipal, con personería jurídica, autonomía administrativa y patrimonio independiente; cumpliendo con las funciones que le asigne el Código Nacional de Tránsito Terrestre, la Ley, los Decretos Reglamentarios, las Ordenanzas y los Acuerdos Municipales; y aunque su área de jurisdicción sería el Municipio de Pereira, podía ejercer las funciones de Transporte Público en el Área Metropolitana del Centro de Occidente, conformada por los Municipios de Pereira, Dosquebradas y La Virginia.

En el mismo Acuerdo 137, se establece su dirección y administración, los integrantes de la Junta Directiva, del Comité Coordinador y sus respectivas funciones, como también sus fuentes principales del patrimonio. Se autoriza además al Alcalde Municipal para que en un plazo de 6 meses suprima el Departamento de Transporte Público Metropolitano de la estructura del Municipio, que por ese entonces estaba adscrito a él, para fusionarlo con el nuevo Instituto de Tránsito y Transporte del orden Municipal

En octubre de 1995, el Ministerio de Transporte, bajo la resolución No. 007365, clasifica al Instituto Municipal de Tránsito y Transporte de Pereira en categoría “A” y le adjudica el código No. 66001.

El 1 de enero de 1996, inicia labores el nuevo organismo de tránsito del orden municipal, fusionado con el departamento de transporte público metropolitano, denominado INSTITUTO MUNICIPAL DE TRÁNSITO Y TRANSPORTE DE PEREIRA, con jurisdicción Municipal para los asuntos de tránsito y con jurisdicción Metropolitana para los asuntos de transporte. Con un manual de funciones y un reglamento interno de trabajo adoptado mediante el Acuerdo 003 de 1996 y unos estatutos a través del Acuerdo 01-97 del 21 de marzo de 1997. Hacia julio de 1999, la Junta Directiva del IMTTP, en virtud de las afugias económicas por las que estaba pasando la entidad, aprueba una reestructuración administrativa, estableciendo una nueva estructura interna y las funciones por dependencias; una planta global de personal y un manual de funciones y requisitos para los cargos de

la nueva planta; a través de los Acuerdos 003, 004 y 005 respectivamente, la cual no se llevó a cabo en su totalidad.

Hacia el 29 de agosto de 2000, después de ratificarse mediante acuerdo 005 que el servicio de Transporte Público tiene el carácter de Metropolitano en los Municipios de Pereira, Dosquebradas y La Virginia, se constituye como autoridad única de Transporte Metropolitano, al Área Metropolitana del Centro Occidente, mediante el Acuerdo 017 de diciembre 27 de 2001; suprimiéndose el Departamento de Transporte Público Metropolitano de la estructura del Instituto Municipal de Tránsito, para ubicarlo en esa Entidad.

Mediante acta 09 de diciembre 12 de 2002, la Junta Directiva del IMTTP, autoriza adelantar todas las acciones necesarias para asumir la administración de los patios oficiales de tránsito y grúas por parte del IMTTP, anteriormente servicios prestados a través de una empresa privada, iniciando operaciones el 5 de junio de 2003, bajo la Resolución 0833 de 2003.

A finales del año 2004, inicia la Entidad una nueva prestación de servicios derivados del sector tránsito, con el Centro de Enseñanza Automovilística, con la autorización del Ministerio de Transporte a través de la Resolución 002912 de 2004, asignándole el código No. 011-66001000.

En enero 19 de 2006, recibe el concepto positivo para la CERTIFICACIÓN EN CALIDAD ISO 9001:2000 Y NTCGP 1000:2004; adoptándose el mismo día EL PROGRAMA DE MODERNIZACIÓN Y FORTALECIMIENTO INSTITUCIONAL mediante el Acuerdo 001, el cual consta de:

1. Programa de Modernización Institucional
2. Programa de Reestructuración Y Reorganización Administrativa Integral
3. Programa de Fortalecimiento Institucional
4. Programa de Modernización Tecnológica

Así mismo mediante los siguientes Acuerdos, todos del día 19 de enero de 2006 se adopta:

1. Acuerdo 002 de 2006: una nueva estructura orgánica

2. Acuerdo 003 de 2006: las escalas de remuneración, según las categorías de empleos
3. Acuerdo 004 de 2006: la planta de cargos, sistema de nomenclatura, clasificación y categoría de los empleos

Mediante Decreto 662 del 20 de octubre de 2006, expedido por la Alcaldía Municipal de Pereira, se modifica la razón social del Instituto Municipal de Tránsito y Transporte de Pereira y se establece su estatuto básico. Se suprime la función de transporte de su razón social; quedando así: INSTITUTO MUNICIPAL DE TRÁNSITO DE PEREIRA.

El 5 de marzo de 2007, la empresa BBQI, realiza la auditoria de mantenimiento del Sistema de Gestión de Calidad, manteniéndose la certificación otorgada por esta empresa en el año 2006.

El 4 de abril del año 2008 se recibió segunda visita de seguimiento de parte de la firma BVQI, en el cual se evalúo la mejora continua del Sistema de Gestión de Calidad.

2. DEFINICIÓN DE LAS LÍNEAS DE INTERVENCIÓN

La línea de intervención se enmarca en el ámbito de las Telecomunicaciones puesto que el estudio con su respectivo análisis y diseño que se pretende realizar es sobre la red de telecomunicaciones actual del IMTP.

3. DIAGNÓSTICO DEL ÁREA DE INTERVENCIÓN O IDENTIFICACIÓN DE LAS NECESIDADES

El estado actual de la red de de área local de transito se encuentra de la siguiente manera:

En el momento se encuentran 95 computadores personales interconectados a través de 8 switch distribuidos en el edificio, formando una topología en estrella. 3 Switch de estos se encuentran en la Subdirección de Informática en el cuarto de telecomunicaciones, a estos switch llegan aproximadamente 50 PC's puesto que es la red nueva del Instituto, además de estos equipos, llegan a los switch conexiones (cascadas) de los otros switch que se encuentran distribuidos en el Instituto.

Los servidores que proporcionan servicios, información, aplicaciones institucionales e Internet a la institución deben estar disponibles las 24 horas del día, 365 días del año; estos se encuentran en el cuarto de telecomunicaciones, libres de contacto con instalaciones eléctricas en mal estado, pero a su vez el acceso en esta área no esta totalmente restringido, además cuentan con sistema de refrigeración en el día, pero en la noche este es suspendido, interrumpiendo las condiciones de ventilación y refrigeración necesarias, además se encuentran elementos que no deberían estar allí, como computadores e impresoras de reserva y en mal estado, se encuentra también una cafetera e implementos de cafetería.

El instituto cuenta con 7 servidores: Datos (principal), Respaldo, Imágenes, Pantallas de toque, Orión, Dominio (sin funcionamiento), y para superar problemas que se vienen presentando en la red, como la infección a causa de virus de computadores y la red en general, se encuentra instalado un demo de "Fortinet" que implementa servicios como: Firewall, Detección y Prevención de Intrusos, Antivirus y Antispyware, AntiSpam, Filtro Web, Gateway VPN. Además, pone fin a la vulnerabilidad de las redes y proporciona una completa serie de servicios a nivel de aplicación y red en un mismo dispositivo que se sitúa en el extremo de la red, lo que elimina muchas de las limitaciones impuestas por el uso de múltiples dispositivos.

La calidad de la red se puede dividir en dos segmentos, puesto que una parte de las oficinas de la organización se encuentran remodeladas al igual que sus conexiones de red. Mientras que el resto de oficinas son un poco más antiguas por consiguiente su red también. En estas oficinas se puede observar que el cableado estructurado no va por canaletas como esta estandarizado. Los equipos que se encuentran en estas dependencias van conectados a unos switch que están en determinadas oficinas y que llegan en cascada al cuarto de telecomunicaciones.

4. EJE DE INTERVENCIÓN

La necesidad a intervenir en el período de practica de acuerdo con las prioridades del Instituto Municipal de Transito de Pereira, es a través de un estudio previo de la red de telecomunicaciones actual, diseñar una solución para el mejoramiento de la misma, cumpliendo con todos los estándares que están definidos, ya que el instituto contara con una renovación tecnológica, en la que se pretende dar solución en gran medida a los problemas que se tienen en este momento en la red de telecomunicaciones y a su vez contar con tecnología de punta.

5. JUSTIFICACIÓN DEL EJE DE INTERVENCIÓN

Como en toda empresa se tiene una cantidad considerable de equipos que manejan cierta información y aplicativos institucionales en común, es necesaria la comunicación entres todos para mejorar procesos internos, compartir recursos e información, independientemente de la ubicación física del recurso y del usuario. La mejor manera de que esto se lleve a cabo es a través del uso de las redes; pero no basta simplemente con instalar una red de cualquier manera, se debe cumplir con unos estándares establecidos para la implementación de la red en general, pero sobretodo para su buen funcionamiento. Es por ello, que realizar un análisis detallado y aportar conocimientos para lograr esto, puede ser de gran ayuda, ya que se tienen diferentes puntos de vista de lo que le sucede a la red del Instituto de Transito, y darle soluciones eficientes para lograr el mejor desenvolvimiento de las labores de cada dependencia y aun mas brindar la mejor atención al publico, puesto que del buen funcionamiento de las redes depende en gran medida el cumplimiento de los procesos que la empresa realiza.

6. OBJETIVOS

6.1 OBJETIVO GENERAL

Realizar el estudio de la situación actual de la red de telecomunicaciones del IMTP con el fin de detectar falencias, de igual forma analizar y diseñar mejoras en el sistema de telecomunicaciones, brindando soluciones eficientes.

6.2 OBJETIVOS ESPECÍFICOS

- ✓ Realizar un estudio detallado del entorno en el que se ejecuta el proyecto
- ✓ Documentar falencias encontradas en la red de telecomunicaciones del IMTP
- ✓ Diseñar una solución para la red de telecomunicaciones del IMTP
- ✓ Documentar completamente el proceso realizado durante el desarrollo de la solución.

7. MARCO TEÓRICO

Actualmente, el manejo de la información de modo eficiente constituye una de las principales preocupaciones dentro de cualquier organización, sea esta de origen público o privado, por lo que se hace necesario manejarla y emplearla con mucho criterio, ya que de ello podría depender, el éxito o fracaso de las mismas.

Son muchas las herramientas que, en la actualidad, facilitan al hombre el manejo del recurso informativo, así como el acceso a este. Una de estas herramientas, que permite utilizar el recurso de la información de manera más eficiente, rápida y confiable, la constituyen las redes de Computadoras, las cuales aparecen enmarcadas dentro del vertiginoso avance tecnológico que ha caracterizado a las últimas décadas del presente siglo.[1]

Cada uno de los tres últimos siglos fue dominado por una tecnología. El siglo XVIII fue la era de los grandes sistemas mecánicos que acompañaron la Revolución Industrial. EL siglo XIX fue la edad de la máquina de vapor. Durante el siglo XX la tecnología clave fue la obtención, el procesamiento y la distribución de la información. Entre otros acontecimientos, vimos la instalación de redes mundiales de telefonía, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedentes de la industria de la computación, acompañada de las redes de computadoras, sin dejar a un lado el lanzamiento de satélites de comunicaciones.

Una red es un conjunto de computadoras o dispositivos de procesamiento conectados entre sí en forma lógica y física con la finalidad de optimizar sus recursos y emular el proceso de un sistema de cómputo único. [2]

Las Instituciones públicas, deben garantizar a sus usuarios el acceso a la información con fines eminentemente colaborativos, por lo que no podían permanecer ajenas al uso de esta herramienta.

Con la implementación de las redes y la forma como se depende en este momento de ellas, es fundamental para toda organización contar con su propia red LAN que al igual que una red WAN, es una red de comunicaciones que interconecta varios

[1] http://www.monografias.com/trabajos7/rela/rela.shtml
[2] Tanenbaum Andrew S. Redes de Computadoras

dispositivos y proporciona un medio para el intercambio de información entre ellos. Su cobertura es pequeña, generalmente un edifico,[3] pero gracias a estas, se eliminan los limites que se tenían en el espacio para la comunicación de los computadores, puesto que ya sin importar la localización geográfica de estos siempre estarán disponibles para cualquiera en la red. Es habitual que la LAN sea propiedad de la misma entidad propietaria de los dispositivos conectados a la red.

La existencia de una red LAN en una organización implica el cumplimiento de varios estándares para su implementación, igualmente la definición de una topología de red, que la más usada es la topología en estrella**,** en esta configuración todos los equipos están conectados directamente al conmutador y las comunicaciones se han de hacer necesariamente a través de él. Permite incrementar y disminuir fácilmente el número de estaciones. Si se produce un fallo en una de ellas no repercutirá en el funcionamiento general de la red; pero, si se produce un fallo en el conmutador, la red completa se vendrá abajo. [4]

De igual manera el cableado estructurado forma parte de estas redes y debe cumplir ciertas normas para su utilización; Un sistema de cableado según el Curso Cisco Networking Academy V2.1.2, debe ser capaz de integrar tanto a los servicios de voz, datos y vídeo, como los sistemas de control y automatización de un edificio bajo una plataforma estandarizada y abierta. El cableado estructurado tiende a estandarizar los sistemas de transmisión de información al integrar diferentes medios para soportar toda clase de tráfico, controlar los procesos y sistemas de administración de un edificio.

Aplicar un estándar de cableado estructurado ofrece muchas ventajas, entre las que destacamos:

- Facilita las tareas de mantenimiento y supervisión, ya que resulta más sencillo identificar las estructuras de cableado.
- Asegura un funcionamiento optimo si se cumplen todos los requisitos del estándar
- Posibilita la inclusión de una alta densidad de cableado
- Permite la integración de diferentes tecnologías de redes.
- Resulta fácilmente ampliable.

[3] Stallings William. Comunicaciones y redes de Computadores.

4 Raya José Luis, Raya Laura, Martínez Miguel A. Redes locales. Instalación y configuraciones básicas

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

- Área de trabajo.
- Cuarto de telecomunicaciones, también denominado servicio de distribución.
- Cableado backbone, también denominado cableado vertical.
- Cableado de distribución, también denominado cableado horizontal.

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

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

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

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

Cuarto de telecomunicaciones: El cuarto de telecomunicaciones es el lugar donde se realizan las conexiones a los dispositivos intermediarios. Estos cuartos

contienen dispositivos intermediarios (hubs, switches, routers y unidades de servicio de datos [DSU]) que conectan la red. Estos dispositivos proporcionan transiciones entre el cableado backbone y el cableado horizontal.

Dentro del cuarto de telecomunicaciones, los patch cords realizan conexiones entre los patch panels, donde terminan los cables horizontales, y los dispositivos intermediarios. Los patch cables también interconectan estos dispositivos intermediarios.

Los estándares de la Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) establecen dos tipos diferentes de patch cables de UTP. Uno de los tipos es el patch cord, con una longitud de hasta 5 metros y se utiliza para interconectar el equipo y los patch panels en el cuarto de telecomunicaciones. Otro tipo de patch cable puede ser de hasta 5 metros de longitud y se utiliza para conectar dispositivos a un punto de terminación en la pared.

Estos cuartos a menudo tienen una doble finalidad. En muchas organizaciones, el cuarto de telecomunicaciones también incluye los servidores utilizados por la red.

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

Cableado backbone: El cableado backbone se refiere al cableado utilizado para conectar los cuartos de telecomunicaciones a las salas de equipamiento donde suelen ubicarse los servidores. El cableado backbone también interconecta múltiples cuartos de telecomunicaciones en toda la instalación. A menudo, estos cables se enrutan fuera del edificio a la conexión WAN o ISP.

Los backbones, o cableado vertical, se utilizan para el tráfico agregado, como el tráfico de entrada o de salida de Internet, y para el acceso a los recursos

corporativos en una ubicación remota. Gran parte del tráfico desde varias áreas de trabajo utilizará el cableado backbone para acceder a los recursos externos del área o la instalación. Por lo tanto, los backbones generalmente requieren de medios de ancho de banda superiores como el cableado de fibra óptica.[5]

Para realizar las conexiones anteriormente descritas existen diferentes tipos de medios que deben considerarse para implementar una red LAN exitosa en el IMTP.

Tipos de medios
UTP (Categorías 5, 5e, 6 y 7).
Fibra óptica.
Inalámbrico.

Cada tipo de medios tiene ventajas y desventajas. Algunos de los factores que se deben considerar son los siguientes:

Longitud del cable: ¿El cable debe atravesar una habitación o extenderse desde un edificio hasta otro? La longitud total del cable que se requiere para conectar un dispositivo incluye todos los cables desde los dispositivos finales del área de trabajo hasta el dispositivo intermediario en el cuarto de telecomunicaciones (generalmente un switch). Esto incluye el cable desde los dispositivos hasta el enchufe de pared, el cable a través del edificio desde el enchufe de pared hasta el punto de conexión cruzada, o patch panel, y el cable desde el patch panel hasta el switch. Si el switch se ubica en los cuartos de telecomunicaciones en diferentes pisos de un edificio o en diferentes edificios, el cable entre estos puntos debe incluirse en la longitud total.

Se debe tener en cuenta la atenuación que es la reducción de la potencia de una señal a medida que se transmite a través de un medio. Cuanto más extensos sean los medios, más la atenuación afectará la señal. En algún punto, la señal no será detectable. La distancia del cableado es un factor esencial en el rendimiento de la señal de datos. La atenuación de la señal y la exposición a una posible interferencia aumenta con la longitud del cable.

[5] Curso Cisco Networking Academy V4.0

Por ejemplo, cuando se utiliza un cableado UTP para Ethernet, la longitud del cableado horizontal (o fijo) necesita mantenerse a una distancia máxima recomendada de 90 metros para evitar la atenuación de la señal. Los cables de fibra óptica pueden proporcionar una distancia de cableado mayor de hasta 500 metros o algunos kilómetros, según el tipo de tecnología. Sin embargo, el cable de fibra óptica también puede sufrir una atenuación cuando se alcanzan estos límites.

Costo: ¿El presupuesto permite que se utilice un tipo de medios más costoso? El costo asociado con el cableado de una LAN puede variar según el tipo de medio y es posible que el personal no pueda darse cuenta del impacto sobre el presupuesto. En un entorno ideal, el presupuesto permitiría instalar un cableado de fibra óptica para cada dispositivo de la LAN. Si bien la fibra proporciona un ancho de banda superior que el UTP, los costos de la instalación y el material son considerablemente mayores. Se debe lograr que coincidan las necesidades de rendimiento por parte de los usuarios con el costo de equipo y cableado para obtener la mejor relación costo/rendimiento.

Ancho de banda: ¿La tecnología utilizada con los medios ofrece un ancho de banda apropiado? Los dispositivos de una red presentan requisitos de ancho de banda diferentes. Al seleccionar los medios para las conexiones individuales, se debe considerar cuidadosamente los requisitos de ancho de banda.

Por ejemplo, un servidor generalmente necesita mayor ancho de banda que una computadora dedicada a un único usuario. Para la conexión del servidor, se debe utilizar aquellos medios que proporcionarán un ancho de banda superior y que podrán desarrollarse para cumplir con mayores requisitos de ancho de banda y utilizar las tecnologías más nuevas. Un cable de fibra puede ser una elección lógica para la conexión de un servidor.

Actualmente, la tecnología utilizada en los medios de fibra óptica ofrece el mayor ancho de banda disponible entre las opciones para los medios LAN. Teniendo en cuenta el ancho de banda aparentemente ilimitado disponible en los cables de fibra, se esperan velocidades mayores para las LAN. El medio inalámbrico también admite aumentos considerables en el ancho de banda, pero tiene limitaciones en cuanto al consumo de la potencia y la distancia.

Facilidad de instalación: ¿Tiene el equipo de implementación la capacidad de instalar el cable o es necesario contratar a un proveedor? La facilidad al instalar un cableado varía según los tipos de cables y la estructura del edificio. El acceso al

piso y a sus espacios, además de las propiedades y el tamaño físico del cable, influyen en la facilidad de instalación de un cable en distintos edificios. Los cables de los edificios generalmente se instalan en canales para conductores eléctricos.

El cable UTP es relativamente liviano, flexible y tiene un diámetro pequeño, lo que permite introducirlo en espacios pequeños. Los conectores, enchufes RJ-45, son relativamente fáciles de instalar y representan un estándar para todos los dispositivos Ethernet.

Muchos cables de fibra óptica contienen una fibra de vidrio delgada. Esta característica genera problemas para el radio de curvatura del cable. La fibra puede romperse al enroscarla o doblarla fuertemente. La terminación de los conectores del cable (ST, SC, MT-RJ) son mucho más difíciles de instalar y requieren de un equipo especial.

En algún punto, las redes inalámbricas requieren de cableado para conectar dispositivos, como puntos de acceso, a la LAN instalada. Los medios inalámbricos a menudo son más fáciles de instalar que un cable de fibra o UTP, ya que se necesitan menos cables en una red inalámbrica.

Susceptibilidad a EMI/RFI: ¿Interferirá con la señal el entorno en el que estamos instalando el cable? La Interferencia electromagnética (EMI) y la Interferencia de radiofrecuencia (RFI) deben tenerse en cuenta al elegir un tipo de medios para una LAN. La EMI/RFI en un entorno industrial puede producir un impacto significativo sobre las comunicaciones de datos si se utiliza un cable incorrecto.

La interferencia puede provenir de máquinas eléctricas, rayos y otros dispositivos de comunicación, incluyendo computadoras y equipos de radio.

Los medios inalámbricos son los más susceptibles a la RFI. Antes de utilizar una tecnología inalámbrica, se deben identificar las posibles fuentes de interferencia y reducirlas en lo posible.[6]

Anteriormente se nombraban los dispositivos finales e intermedios que intervienen en una red, a continuación se detallaran sus características.

[6] Curso Cisco Networking Academy V4.0

Dispositivos finales y su rol en la red: Los dispositivos de red con los que la gente está más familiarizada se denominan dispositivos finales. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente.

Algunos ejemplos de dispositivos finales son:

Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores Web), Impresoras de red, Teléfonos VoIP, Cámaras de seguridad, Dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA).

En el contexto de una red, los dispositivos finales se denominan host. Un dispositivo host puede ser el origen o el destino de un mensaje transmitido a través de la red. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia una comunicación, utiliza la dirección del host de destino para especificar dónde debe ser enviado el mensaje.

En las redes modernas, un host puede funcionar como un cliente, como un servidor o como ambos. El software instalado en el host determina qué rol representa en la red. Los servidores son hosts que tienen software instalado que les permite proporcionar información y servicios, como e-mail o páginas Web, a otros hosts en la red. Los clientes son hosts que tienen software instalado que les permite solicitar y mostrar la información obtenida del servidor.

Dispositivos intermedios y su rol en la red: Además de los dispositivos finales con los cuales la gente está familiarizada, las redes dependen de dispositivos intermediarios para proporcionar conectividad y para trabajar detrás de escena y garantizar que los datos fluyan a través de la red. Estos dispositivos conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork.

Algunos dispositivos de red intermediarios:

Dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos), dispositivos de internetworking (routers), servidores de comunicación y módems, y dispositivos de seguridad (firewalls).

Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

Regenerar y retransmitir señales de datos, mantener información sobre qué rutas existen a través de la red y de la internetwork, notificar a otros dispositivos los errores y las fallas de comunicación, direccionar datos por rutas alternativas cuando existen fallas en un enlace.

Cuando se conectan diferentes tipos de dispositivos, se utiliza un cable de conexión directa. Cuando se conectan el mismo tipo de dispositivos, se utiliza un cable de conexión directa.

Cables UTP de conexión directa

Un cable de conexión directa tiene conectores en cada extremo y su terminación es idéntica conforme a los estándares T568A o T568B.

La identificación del estándar del cable utilizado le permite determinar si cuenta con el cable correcto para un determinado trabajo. Más importante aún, es normal utilizar los mismos códigos de color en toda la LAN para lograr consistencia en la documentación.

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

Cables UTP de conexión cruzada

Los cables de conexión cruzada conectan directamente los siguientes dispositivos en una LAN:
Switch a switch
Switch a hub
Hub a hub
Router a conexión del puerto Ethernet del router
Equipo a equipo
Equipo a puerto Ethernet del router [7]

[7] Curso Cisco Networking Academy V4.0

Contar con una buena tecnología en dispositivos que conforman la red LAN es fundamental puesto que mejora considerablemente la confiabilidad y el buen desempeño de las actividades que se realizan, por esta razón la utilización de servidores como Proxy y Firewall en la red previenen y mejoran la seguridad de todos los dispositivos pero principalmente lo mas valioso que tiene una empresa que es su información, un Proxy y un firewall en sus definiciones más simples respectivamente son: Servidor que actúa como "representante" de una aplicación efectuando solicitudes en Internet en su lugar. De esta manera, cuando un usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un servidor proxy, la aplicación primero se conectará con el servidor proxy y le dará la solicitud. El servidor proxy se conecta entonces al servidor al que la aplicación del cliente desea conectarse y le envía la solicitud. Después, el servidor le envía la respuesta al proxy, el cual a su vez la envía a la aplicación del cliente.[8] Un firewall, filtra los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre ellos. Puede ser configurado para permitir que solo determinadas direcciones, origen y destino, puedan acceder a su red (o desde ella).[9]

Como se nombro anteriormente los switch son dispositivos intermedios que hacen parte fundamental en una red, a continuación se explicara en detalle sus características, su importancia y los factores que se deben tener en el momento de seleccionarlos.

Un **switch** o **conmutador** es un dispositivo de interconexión de redes informáticas. Es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro. Su empleo es muy común cuando existe el propósito de conectar múltiples redes entre sí para que funcionen como una sola. Un conmutador suele mejorar el rendimiento y seguridad de una red de área local.

El funcionamiento de un conmutador o switch tiene lugar porque el mismo tiene la capacidad de aprender y almacenar direcciones de red de dispositivos alcanzables a través de sus puertos. A diferencia de lo que ocurre con un hub o concentrador, el switch hace que la información dirigida a un dispositivo vaya desde un puerto origen a otro puerto destino. Cuando se conectan dos switches, cada uno almacena las direcciones MAC de los dispositivos accesibles desde sus puertos.

[8] Curso Cisco Networking Academy V2.1.2

[9] Raya José Luis, Raya Laura, Martínez Miguel A. Redes locales. Instalación y configuraciones básicas

Esto quiere decir que, en el puerto de interconexión, se alojan las direcciones MAC de los dispositivos del otro switch. Los conmutadores o switches son ampliamente utilizados en todo tipo redes, a pequeña y gran escala.[10]

Existen varios factores que deben considerarse al seleccionar un switch: las características de la interfaz y el costo.

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

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

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

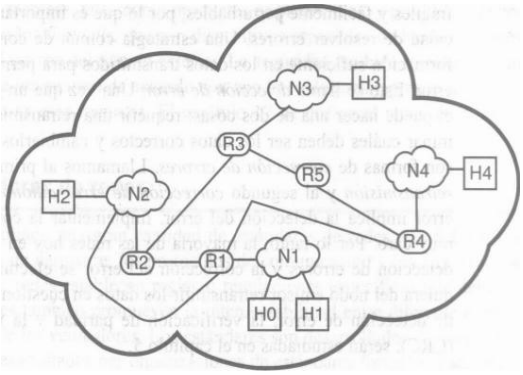
Existen varias formas de proporcionar redundancia.

Velocidad y tipos de puertos e interfaces: La necesidad de velocidad está siempre presente en un entorno LAN. Se encuentran disponibles computadoras más nuevas con NIC incorporadas de 10/100/1000 Mbps. La selección de dispositivos de Capa 2 que puedan ajustarse a mayores velocidades permite a la red evolucionar sin reemplazar los dispositivos centrales. [11]

[10] http://www.definicionabc.com/tecnologia/switch.php

[11] Curso Cisco Networking Academy V4.0

Es importante conocer cuál es la ruta que un paquete de datos toma al viajar entre los nodos fuente y destino. Para ello se habla del enrutamiento, que es usualmente efectuado por unidades especiales dedicadas de hardware llamadas enrutadores. Una ilustración de enrutamiento se muestra en la figura, que representa una red y sus segmentos relacionados, llamados subredes. Observe que, las redes se representan como nubes. Como se muestran aquí, se tienen cuatro subredes interconectadas (N1-N4), cinco anfitriones (HO-H4), y cinco enrutadores (R1-R5). Como ejemplo de enrutamiento, note que los paquetes de datos que se originan en H1 y con destino a H2 pueden tomar varias rutas a través de la red. Una ruta es a través de R1 solamente. Una segunda ruta es R1-R2. Una tercera es la ruta R1-R4-R5-R3-R2. La "mejor" ruta que los paquetes pueden tomar está en una función de un criterio (o criterios) específico llamado métrica. Las métricas de un enrutamiento común incluyen distancia, número de saltos de ruta y ancho de banda, que especifica la capacidad del enlace. Por ejemplo, si la métrica usada es el número de saltos, entonces la mejor ruta para la figura es a través de R1, ya que ésta implica un solo salto. Sin embargo, si la métrica es la distancia y, de las tres rutas posibles, la distancia más corta es a través de R1-R2, entonces ésta resulta ser la mejor ruta. [12]



Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red. Este dispositivo opera en capa tres del modelo OSI. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.

Figura 2. Métricas de enrutamiento

Un router se vale de un protocolo de enrutamiento, que le permite comunicarse con otros enrutadores o encaminadores y compartir información entre sí para saber cuál es la ruta más rápida y adecuada para enviar datos. Siempre buscará la ruta más corta o la que tenga menos tráfico para lograr su objetivo y, por otra parte, que si no funciona una ruta, tiene la capacidad de buscar una alternativa.

Un típico enrutador funciona en un plano de control (en este plano el aparato obtiene información acerca de la salida más efectiva para un paquete específico

[12] Gallo A. Michael, Hancock M. William. Comunicación entre computadores y tecnologías de redes. Mexico 2002; p. 17

de datos) y en un plano de reenvío (en este plano el dispositivo se encarga de enviar el paquete de datos recibidos a otra interfaz).

En su uso más común, un enrutador permite que en una casa u oficina pequeña varias computadoras aprovechen la misma conexión a Internet. En este sentido, el router opera como receptor de la conexión de red para encargarse de distribuirlo a todos los equipos conectados al mismo. Así, se conecta una red o Internet con otra de área local.[13]

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

- Posibilidad de expansión
- Medios
- Características del sistema operativo

Posibilidad de expansión: Los dispositivos de red, como los routers y switches, forman parte tanto de las configuraciones físicas modulares como de las fijas. Las configuraciones fijas tienen un tipo y una cantidad específica de puertos o interfaces. Los dispositivos modulares tienen ranuras de expansión que proporcionan la flexibilidad necesaria para agregar nuevos módulos a medida que aumentan los requisitos. La mayoría de estos dispositivos incluyen una cantidad básica de puertos fijos además de ranuras de expansión. Se debe tener precaución al seleccionar las interfaces y los módulos adecuados para los medios específicos ya que los routers pueden utilizarse para conectar diferentes cantidades y tipos de red.

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

[13] http://www.definicionabc.com/tecnologia/router.php

Medios de red: La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

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

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

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

Para la selección de dispositivos, el presupuesto es un detalle importante a tener en cuenta. Los routers pueden ser costosos según las interfaces y las características necesarias. Los módulos adicionales, como la fibra óptica, pueden aumentar los costos. Los medios utilizados para conectar el router deben admitirse sin necesidad de comprar módulos adicionales. Esto puede mantener los costos en un nivel mínimo.

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. El concepto de direccionamiento implica asignar a un nodo de red una dirección única que permita a otros sistemas o dispositivos localizarlo. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Una dirección IP debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por un conjunto de cuatro números, cada uno de los cuales puede oscilar entre 0 y 255.

Para desarrollar un esquema de direccionamiento para una red, se comienza por definir la cantidad total de hosts. Además, se considera cada dispositivo que requerirá una dirección IP, ahora y en el futuro.

Algunos dispositivos finales que requieren una dirección IP son:

- Equipos de usuarios.
- Equipos de administradores.
- Servidores.
- Otros dispositivos finales, como impresoras, teléfonos IP y cámaras IP.

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

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

Entre los dispositivos de red que requieren una dirección IP para la administración se incluyen:

- Switches.
- Puntos de acceso inalámbrico.

Es posible que existan otros dispositivos en una red que requieran una dirección IP. Se agregan a la lista para calcular cuántas direcciones se necesitará tener en cuenta para el crecimiento de la red a medida que se agregan más dispositivos.
Una vez que se ha establecido la cantidad total de hosts (actuales y a futuro), se considera el rango de direcciones disponibles y dónde encajan en la dirección de red determinada.

Luego, se determina si todos los hosts formarán parte de la misma red o si toda la red se dividirá en subredes independientes.

Existen muchas razones para dividir una red en subredes:

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

Diferentes requisitos de red: Si los diferentes grupos de usuarios requieren servicios informáticos o de red específicos, resulta más sencillo administrar estos requisitos si aquellos usuarios que comparten requisitos se encuentran todos juntos en una subred.

Seguridad: Se pueden implementar diferentes niveles de seguridad en la red basándose en las direcciones de red. Esto permite la administración del acceso a diferentes servicios de red y de datos.

La asignación de direcciones IP dentro de las redes debería ser planificada y documentada a fin de:

Evitar duplicación de direcciones: Como se sabe, cada host en una interwork debe tener una dirección única. Sin la planificación y documentación adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

Proveer y controlar el acceso: Algunos hosts ofrecen recursos tanto para la red interna como para la red externa. Un ejemplo de estos dispositivos son los servidores. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos.

Monitorear seguridad y rendimiento: De igual manera, es necesario monitorear la seguridad y el rendimiento de los hosts de la red y de la red en general. Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red que tiene una dirección problemática.

Unos de los posibles problemas que presenta una red a raíz de una mala configuración en los equipos pueden ser:

Perdida de datos: La pérdida de datos es producida por algún virus o por otro tipo de incidencia, los más comunes son: mal manejo por parte del usuario o personas inescrupulosas que acceden al sistema o mediante Internet, estos incidentes pueden evitarse instalando códigos en las estaciones de trabajo para que así tengan acceso solo personal autorizado, en cuanto a Internet existe diferente tipo de hardware o software en el mercado conocidos como Muros de fuego (Firewall), que evita intrusiones no deseadas.

Caídas Continuas de la Red: La caída continua en una red se debe en la mayoría de los casos a una mala conexión Servidor-Concentrador/switch, o la conexión existente con el proveedor de Internet.[14]

El lenguaje usado por los miembros de una red se llama protocolo de red de comunicación. Los protocolos facilitan el establecimiento de una comunicación proporcionando a los miembros un lenguaje común. Desde una perspectiva general, un **protocolo** de red de comunicación es un conjunto aceptado o establecido de procedimientos, reglas o especificaciones formales que gobiernan un comportamiento o lenguaje específico.

Un protocolo de red es una especificación formal que define cómo habrán de "comportarse" los nodos o comunicarse entre sí. Entre otras cosas, los protocolos de red definen el formateado de datos, la integridad y transmisión de éstos. En síntesis, un protocolo de red especifica el vocabulario y reglas de la comunicación de los datos.

Sin un enlace, no puede compartirse la información entre los miembros y sin un lenguaje específico, la comunicación, no puede ser establecida. Así, el enlace físico proporciona un ambiente para la comunicación, mientras que un lenguaje común garantiza que ésta se establezca.

Las redes actuales emplean una gran cantidad de protocolos que varían de muy simples a bastante complejos. Los protocolos son el pegamento que unen entre sí

[14] http://www.monografias.com/trabajos28/manual-redes/manual-redes.shtml

las redes de computadoras y definen cómo deben ser efectuadas operaciones específicas.

La comunicación exitosa entre los hosts de una red requiere la interacción de Gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Estos protocolos se implementan en el software y hardware que está cargado en cada host y dispositivo de red.[15]

Algo que no puede mejorar ni el switch, ni el hub o concentrador, es el envío de mensajes de broadcast dentro de una red LAN.

En una LAN estos mensajes de broadcast son enviados a través de todos los puertos de un hub o de un switch. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta, además todas las computadoras escucharán el mensaje pero sólo podrá contestarlo la que se está buscando, no importando si se encuentra o no conectada dentro del switch o concentrador.

Estos mensajes de broadcast son, en muchas ocasiones, tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro del "dominio de broadcast" o LAN.

Para solventar dicha situación se crea el concepto de **Redes de Área Local Virtuales (VLANs)**, configuradas dentro de los switches, que dividen en diferentes "dominios de broadcast" a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.

Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

[15] Curso Cisco Networking Academy V4.0

Con los switches, el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los “dominios de colisión” por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los “dominios de broadcast”, en lugar de uno solo, se puede configurar el switch para que existan más “dominios”.
- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.
- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.

El funcionamiento e implementación de las VLANs está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q. En este se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente

Las VLAN deben ser rápidas, basadas en switches para que sean interoperables totalmente –porque los routers no dan la velocidad requerida- , su información deberá viajar a través del backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la maquina cada vez que se cambie de lugar.[16]

DIRECCIONAMIENTO IP: Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que se aplicará cuando se proporcionen direcciones IP a los equipos y otros hosts la nuestra red. La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Una dirección IP debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por

[16] http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf

un conjunto de cuatro números, cada uno de los cuales puede oscilar entre 0 y 255.

Una dirección IP también está formada por dos partes: el ID de host y el ID de red. La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado el equipo. Todos los equipos del mismo segmento deben tener el mismo ID de red.

La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento.

Las clases de direcciones se utilizan para asignar IDs de red a organizaciones para que los equipos de sus redes puedan comunicarse en Internet. Las clases de direcciones también se utilizan para definir el punto de división entre el ID de red y el ID de host.

Se asigna a una organización un bloque de direcciones IP, que tienen como referencia el ID de red de las direcciones y que dependen del tamaño de la organización.

Clase A: Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.

Clase B: Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

Clase C: Las direcciones de clase C se utilizan para redes de área local pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.[17]

[17] http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

Para realizar el direccionamiento IP del IMTP se utilizaran máscaras de subred de tamaño variable (variable length subnet mask, VLSM) que no es más que un proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según se adaptan a las necesidades de hosts por subred,[18] para evitar así el desperdicio de direcciones IP y optimizar la red.

De acuerdo a lo anterior se utilizara una dirección clase C puesto que es una organización relativamente pequeña.

La dirección de red será: 192.168.0.0

Las subredes se plantean de la siguiente manera, con sus respectivos números de host:

Subred 1: 20 Host.
Dirección, Jurídica, Planeación

Subred 2: 15 Host.
Control Interno, Movilidad

Subred 3: 30 Host.
Financiera, Escuela

Subred 4: 10 Host.
Sistemas

Subred 5: 35 Host.
Registros de Información

Subred 6: 10 Host.
Externos

[18] http://www.garciagaston.com.ar/verpost.php?id_noticia=189

Las direcciones de subred quedarían asignadas así:

Subred 1: 192.168.0.0/27
Rango para direccionar host: 192.168.0.1/27 - 192.168.0.30/27

Subred 2: 192.168.0.32/2
Rango para direccionar host: 192.168.0.33/28 - 192.168.0.46/28

Subred 3: 192.168.0.64/27
Rango para direccionar host: 192.168.0.65/27 - 192.168.0.94/27

Subred 4: 192.168.0.96/28
Rango para direccionar host: 192.168.0.97/28 - 192.168.0.110/28

Subred 5: 192.168.0.128/26
Rango para direccionar host: 192.168.0.129/26 - 192.168.0.190/26

Subred 6: 192.168.0.208/28
Rango para direccionar host: 192.168.0.209/28 - 192.168.0.30/28

SEGURIDAD INFORMÁTICA

La seguridad se ha convertido en un aspecto primordial de la implementación y la administración de red. El desafío general de la seguridad es encontrar un equilibrio entre dos requisitos importantes: la necesidad de abrir redes para respaldar las oportunidades comerciales en evolución y la necesidad de proteger la información comercial privada, personal y estratégica.

La aplicación de una política de seguridad eficaz es el paso más importante que puede dar una organización para proteger su red. Brinda pautas acerca de las actividades que deben llevarse a cabo y los recursos que deben utilizarse para proporcionar seguridad a la red de una organización.

¿Por qué es importante la seguridad de la red? En muy poco tiempo, las redes informáticas crecieron en tamaño y en importancia. Si la seguridad de la red se encuentra afectada, podría tener consecuencias graves, como la pérdida de privacidad, el robo de información e, incluso, responsabilidad legal. Para que esta situación constituya un desafío aun mayor, los tipos de amenazas potenciales a la seguridad de la red se encuentran siempre en evolución.

La creciente amenaza a la seguridad: Con los años, las herramientas y los métodos de ataque a las redes han evolucionado. En 1985 los agresores debían tener conocimientos avanzados de informática, programación y networking para utilizar herramientas rudimentarias y realizar ataques básicos. Con el correr del tiempo, y a medida que los métodos y las herramientas de los agresores mejoraban, ya no necesitaban el mismo nivel avanzado de conocimientos. Esto, efectivamente, disminuyó los requisitos de nivel inicial para los agresores. Quienes antes no hubieran cometido delitos informáticos, ahora pueden hacerlo.

Tipos de delitos informáticos: Con la mejora de las medidas de seguridad en el transcurso de los años, algunos de los tipos de ataques más comunes disminuyeron en frecuencia, y surgieron nuevos tipos. La concepción de soluciones de seguridad de red comienza con una evaluación del alcance completo de los delitos informáticos. Estos son los actos de delitos informáticos denunciados con más frecuencia que tienen implicancias en la seguridad de la red:

- Abuso del acceso a la red por parte de personas que pertenecen a la organización
- Virus
- Suplantación de identidad en los casos en los que una organización está representada de manera fraudulenta como el emisor
- Uso indebido de la mensajería instantánea
- Denegación de servicio
- Acceso no autorizado a la información
- Robo de información de los clientes o de los empleados
- Abuso de la red inalámbrica
- Penetración en el sistema
- Fraude financiero
- Detección de contraseñas
- Registro de claves
- Alteración de sitios Web
- Robo de información patentada

- Fraude en las telecomunicaciones
- Sabotaje

Redes abiertas vs redes cerradas: Los modelos de seguridad de la red siguen una escala progresiva, desde "abierto": se otorga permiso a cualquier servicio, a menos que esté expresamente denegado, hasta "restrictivo": se deniega permiso a servicios de forma predeterminada, a menos que sean considerados necesarios. En el caso de redes abiertas, los riesgos de seguridad son evidentes. En el caso de las redes cerradas, las reglas de lo que está permitido son definidas en forma de política por una persona o un grupo dentro de la organización.

Realizar un cambio en la política de acceso puede ser tan simple como pedirle a un administrador de red que active un servicio. Según la empresa, un cambio podría exigir modificar la política de seguridad de la empresa para permitirle al administrador activar el servicio.

Una alternativa extrema para administrar la seguridad es cerrar por completo una red al mundo exterior. Una red cerrada proporciona conectividad solamente a las personas y sitios conocidos de confianza. Una red cerrada no permite conectarse a las redes públicas. Como no hay conectividad con el exterior, las redes diseñadas de esta manera se consideran seguras contra los ataques externos. Sin embargo, todavía hay amenazas internas. Una red cerrada no es de mucha ayuda para impedir ataques desde el interior de la empresa.

Desarrollo de una política de seguridad: El primer paso que debe dar una organización para proteger sus datos y a sí misma del resto de la responsabilidad es desarrollar una política de seguridad. Una política es un conjunto de principios que guían los procesos de toma de decisiones y permiten que los líderes de una organización distribuyan la autoridad con confianza. RFC2196 establece que "una política de seguridad es una declaración formal de las normas por las que se deben regir las personas que obtienen acceso a los bienes de tecnología e información de una organización." Una política de seguridad puede ser tan simple como una breve Política de uso aceptable para recursos de red, o puede contener varios cientos de páginas y detallar cada aspecto de conectividad y las políticas asociadas.

Una política de seguridad debe cumplir los siguientes objetivos:

- Informar a los usuarios, al personal y a los gerentes acerca de los requisitos obligatorios para proteger los bienes de tecnología e información
- Especificar los mecanismos a través de los cuales se pueden cumplir estos requisitos
- Proporcionar una línea de base a partir de la que se pueda adquirir, configurar y auditar redes y sistemas informáticos para que cumplan la política.

Amenazas a la infraestructura física: Cuando se piensa en la seguridad de la red, o incluso en la seguridad informática, uno imagina agresores que explotan las vulnerabilidades del software. Una clase de amenaza menos glamorosa, pero no menos importante, es la seguridad física de los dispositivos. Un agresor puede denegar el uso de los recursos de la red si dichos recursos pueden ser comprometidos físicamente.

Las cuatro clases de amenazas físicas son:

Amenazas al hardware: Daño físico a los servidores, routers, switches, planta de cableado y estaciones de trabajo

Amenazas ambientales: Temperaturas extremas (calor o frío extremos) o condiciones extremas de humedad (humedad o sequedad extremas)

Amenazas eléctricas: Picos de voltaje, voltaje suministrado insuficiente (apagones), alimentación ilimitada (ruido) y pérdida total de alimentación

Amenazas al mantenimiento: Manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos fundamentales, cableado insuficiente y rotulado incorrecto

Algunos de estos problemas deben ser abordados dentro de una política de la organización. Algunos están sujetos a un buen liderazgo y administración dentro de la organización.

A continuación, se presentan algunas formas de mitigar las amenazas físicas:

Mitigación de amenazas al hardware: Cierre el armario del cableado y permita el acceso sólo al personal autorizado. Bloquee el acceso a través de techos falsos, pisos falsos, ventanas, conductos o puntos de entrada que no sean el punto de acceso seguro. Use el control de acceso electrónico y registre todas las tentativas de entrada. Controle las instalaciones con cámaras de seguridad. Bloquee el equipo y evite el acceso no autorizado desde las puertas, el cielorraso, el piso, las ventanas, los conductos y los respiraderos. Monitoree y controle las entradas de los armarios con registros electrónicos. Utilice cámaras de seguridad.

Mitigación de amenazas ambientales: Cree un entorno operativo propicio, a través del control de la temperatura, de la humedad, el flujo de aire positivo, las alarmas ambientales remotas, y la grabación y vigilancia.

Mitigación de amenazas eléctricas: Disminuya los problemas de alimentación eléctrica instalando sistemas UPS y conjuntos de generadores, mediante un plan de mantenimiento preventivo, la instalación de suministros de energía redundante y alarmas y vigilancia remotas.

Mitigación de amenazas al mantenimiento: Mitigación de amenazas relacionadas con el mantenimiento: use tendidos de cables limpios, rotule los cables y componentes críticos, use procedimientos de descarga electrostática, tenga una provisión de repuestos fundamentales y controle el acceso a los puertos de la consola.

AMENAZAS A LAS REDES

Amenazas no estructuradas: Consisten principalmente en personas sin experiencia que usan herramientas de piratería informática de fácil acceso, como secuencias de comandos de shell y crackers de contraseñas. Hasta las amenazas no estructuradas, que se ejecutan con el único propósito de probar las habilidades de un agresor, pueden provocar daños graves a una red.

Amenazas estructuradas: Provienen de personas o grupos que tienen una mayor motivación y son más competentes técnicamente. Estas personas conocen

las vulnerabilidades del sistema y utilizan técnicas de piratería informática sofisticadas para introducirse en las empresas confiadas. Ingresan en computadoras de empresas y del gobierno para cometer fraude, destruir o alterar registros o, simplemente, para crear confusión. Utilizan tácticas de piratería informática tan complejas y sofisticadas que sólo los investigadores especialmente capacitados entienden lo que está ocurriendo.

Amenazas externas: Pueden provenir de personas u organizaciones que trabajan fuera de una empresa y que no tienen acceso autorizado a los sistemas informáticos ni a la red. Ingresan a una red principalmente desde Internet o desde servidores de acceso telefónico.

Amenazas internas: Provocadas por una persona que tiene acceso autorizado a la red, ya sea mediante una cuenta o acceso físico.

Política de Seguridad

"Una política de seguridad es una declaración formal de las reglas a las cuales se debe adherir el personal que tiene acceso a los bienes tecnológicos y de información de una organización". (RFC 2196, Manual de seguridad de sitio)

¿Qué es una política de seguridad?

Una política de seguridad es un conjunto de pautas establecidas para proteger a la red de los ataques, ya sean desde el interior o desde el exterior de una empresa. Una política de seguridad favorece a una organización de las siguientes maneras:

- Proporciona un medio para auditar la seguridad actual de la red y compara los requisitos con lo que se encuentra instalado.
- Planifica mejoras de seguridad, incluidos equipos, software y procedimientos.
- Define las funciones y las responsabilidades de los ejecutivos, administradores y usuarios de la empresa.
- Define qué comportamientos están permitidos y cuáles no.
- Define un proceso para manejar los incidentes de seguridad de la red.

- Permite la implementación y el cumplimiento de la seguridad global al funcionar como norma entre los sitios.
- Crea una base para fundar acciones legales, en caso de ser necesario.
- Una política de seguridad es un documento dinámico, en el sentido de que se trata de un documento que nunca está terminado y que se actualiza constantemente con los cambios operados en los requisitos de la tecnología y de los empleados. Actúa como puente entre los objetivos de administración y los requisitos específicos de la seguridad.

Funciones de una política de seguridad

Una política de seguridad integral cumple las siguientes funciones esenciales:

- Protege a las personas y a la información
- Establece las normas de comportamiento esperado de los usuarios, de los administradores de sistemas, de la dirección y del personal de seguridad
- Autoriza al personal de seguridad a realizar controles, sondeos e investigaciones
- Define y autoriza las consecuencias de las violaciones
- La política de seguridad es para todos, incluso para los empleados, contratistas, proveedores y clientes que tienen acceso a la red. Sin embargo, debe tratar a cada uno de estos grupos de manera diferente.

Componentes de una política de seguridad

Declaración de autoridad y alcance: define qué persona dentro de la organización propone la política de seguridad, quién es responsable de implementarla y qué áreas están contempladas por la política.

Política de uso aceptable (AUP): define el uso aceptable de los equipos y servicios informáticos y las medidas de seguridad de los empleados adecuadas para proteger los recursos corporativos y la información confidencial de la organización.

Política de identificación y autenticación: define qué tecnologías usa la empresa para garantizar que sólo el personal autorizado obtenga acceso a sus datos.

Política de acceso a Internet: define qué es lo que la empresa tolera y lo que no tolera con respecto al uso de su conectividad a Internet por parte de empleados e invitados.

Política de acceso al campus: define el uso aceptable de los recursos tecnológicos del campus por parte de los empleados y de los invitados.

Política de acceso remoto: define la forma en la que los usuarios remotos pueden utilizar la infraestructura de acceso remoto de la empresa.

Procedimiento para el manejo de incidentes: especifica quién responde ante incidentes de seguridad y cómo se deben manejar.

Además de estas secciones clave de políticas de seguridad, otras que pueden ser necesarias en determinadas organizaciones incluyen:

Política de solicitud de acceso a las cuentas: formaliza el proceso de solicitud de cuentas y de acceso dentro de la organización. Los usuarios y los administradores de sistemas que no cumplen los procesos estándar de solicitudes de cuentas y de acceso pueden dar lugar al inicio de acciones legales contra la organización.

Política de evaluación de adquisiciones: define las responsabilidades respecto de las adquisiciones de la empresa y los requisitos mínimos de las evaluaciones de adquisiciones que el grupo de seguridad de la información debe llevar a cabo.

Política de auditoría: define las políticas de auditoría para garantizar la integridad de la información y de los recursos. Incluye un proceso para investigar incidentes, garantizar el cumplimiento de las políticas de seguridad y controlar la actividad de los usuarios y del sistema donde corresponda.

Política de confidencialidad de la información: define los requisitos necesarios para clasificar y asegurar la información de la manera correspondiente en cuanto a su nivel de confidencialidad.

Política de contraseñas: define las normas para crear, proteger y modificar contraseñas sólidas.

Política de evaluación de riesgos: define los requisitos y otorga la facultad al equipo de seguridad de la información a identificar, evaluar y subsanar riesgos de la infraestructura de la información asociados con la conducción de los negocios.

Debe observarse que los usuarios que desafían o infringen las reglas de una política de seguridad pueden ser sometidos a medidas disciplinarias, que incluyen la rescisión del contrato de trabajo.

BLADE CENTER (SERVIDORES)

Grandes y pequeñas empresas dependen de sus sistemas de información para proporcionar alto rendimiento, disponibilidad y facilidad que los clientes y los socios demandan. Para seguir siendo competitivos las organizaciones deben encontrar la forma económica de simplificar y manejar eficientemente las exigencias de las nuevas tecnologías. Es por eso que estas empresas requieren el mayor rendimiento con el mínimo espacio, recursos tecnológicos y de información simplificados y un bajo presupuesto.

Teniendo en cuenta que una compañía está en constante crecimiento, es importante la Consolidación y actualización de la infraestructura tecnológica; IBM ofrece productos que permiten lograr que una empresa mejore en estos aspectos, dichos productos son los que se describirán a continuación con sus respectivas características y ventajas que imponen sobre la infraestructura tecnología con que cuenta en este momento el IMTP.

La implementación de estos equipos presenta ciertas ventajas sobre los que se encuentran en este momento en el IMTP los cuales se encuentran cumpliendo a cabalidad con todas las funciones para las que están destinados, puesto que son servidores que se encuentran distribuidos y requieren de una administración independiente, ocupando un mayor espacio; a la infraestructura que entra a

reemplazar estos equipos se les asignarán las mismas funciones y se le instalarán los mismos aplicativos que se vienen manejando en el Instituto, además de contar con su propio servidor de correo. Una vez migrada toda la información a las nuevas plataformas los equipos que cumplían la función de servidores se ubicaran en “Torre Central” a manera de respaldo como un plan de contingencia donde se garantice la continuidad y disponibilidad de la información del IMTP ante cualquier tipo de siniestro que pueda presentarse en las oficinas.

CHASSIS BLADE CENTER S

Figura 3. Chassis Blade Center S

El chasis Blade Center S ofrece una de las mejores formas de consolidar y brinda enormes ventajas en redundancia, alta disponibilidad y aprovechamiento de recursos

Integra servidores, almacenamiento, redes, I/O y aplicaciones en un único chasis. Usa conexiones estándares de energía de oficina con 100-240V, (de modo que no se necesitan hacen conversiones o modificaciones en la parte eléctrica). Una tecnología modular flexible integra servidores de blade basados en el procesador Intel® y AMD Opteron™ dando soporte a una amplia gama de sistemas operativos. Incluye herramientas de administración que se integran de una manera abierta y fácil, lo que permite concentrarse en las labores de la empresa, no en las labores de tecnología de información (IT). Ayuda a construir infraestructuras de IT más verdes con la poderosa tecnología de IBM Cool Blue (tecnología que permite aliviar la carga en las unidades de aire acondicionado existentes y reducir potencialmente los costos de energía en hasta un 15%) y un portafolio de productos y herramientas para ayudar a los clientes a planificar, administrar y controlar la energía y el enfriamiento, Optimización de arquitectura tecnológica,

Ahorro en Consumo de energía, Incremento en la productividad orientado en un ambiente de procesadores de última tecnología y crecimiento escalable de acuerdo a las necesidades de la organización

BladeCenter S ofrece una amplia gama de opciones de almacenamiento y de conexión de redes integradas en el chasis para simplificar la complejidad y administrabilidad de la infraestructura, ayudando al mismo tiempo a disminuir el costo total de la propiedad

Dispositivos del producto

- El primer chasis BladeCenter construido específicamente para el entorno empresarial de oficina.
- Las herramientas de administración abierta y fácil brindan una administración avanzada y proactiva.
- Calibrated Vectored Cooling™ ayuda a mantener la salud de su sistema al mantener refrigerados los componentes internos.

Especificaciones técnicas generales

Factor de formato: Rack/7U
6 blade server
Disk bays: Hasta 12 SAS o 12 SATA, o una intercombinación de los dos.
Medio estándar: CD-RW/DVD-ROM accesible desde cada servidor de blade.
Módulos de conmutador: Módulos de conmutador SAS, Gigabit Ethernet, Fibre Channel disponibles.
Módulo de suministro de energía: Hasta cuatro (hot swap, autosensor y redundante 950W/1450W con capacidades de equilibrio de carga y recuperación de fallas).
Módulos de refrigeración: 4 aireadores hot swap y redundantes estándares.
Hardware de administración de sistemas: 1 módulo de administración estándar.
I/O puertos: Teclado, video, mouse, Ethernet, USB.
Diagnóstico de vías luminosas: Servidor de blade, procesador, memoria, suministros de energía, aireadores, modulo de conmutador, módulo de administración, unidades de disco duro y tarjeta de expansión
Garantía Limitada: 3 años.
Almacenamiento externo: SAN

En este chasis Blade S estarán alojados los servidores tipo blade serie H, en los cuales será consolidada toda la infraestructura tecnológica, las aplicaciones Web, correo, SQL, ISA y demás de todas la redes existentes en la actualidad incluyendo sedes regionales.

Servidor de Producción para aplicativos SISTRAFF y SINFAD, basado en Sistema Operativo Windows Server 2003 y Base de datos Oracle 9i. Vale la pena anotar que el proveedor de dichas aplicaciones certificó que las citadas aplicaciones corren en Oracle 10G con Sistema Operativo Windows Server 2003 a 64 bits. La importancia de lo anterior se sustenta en el hecho de que al trabajar a 64 bits se hace un mejor aprovechamiento de la plataforma de Hardware, ya que se pueden direccionar más de 4GB de memoria RAM, así como optimizar el uso del procesador.

Servidor para Directorio Activo de Windows Server 2003, el cual cumplirá adicionalmente las funciones de File Server y Servidor de Imágenes.

Servidor para gestión Documental, basado en Sistema Operativo Windows Server 2003.

Servidor para Aplicaciones WEB, basado en Sistema Operativo Linux Red Hat Enterprise Edition

SERVER BLADE HS22

Figura 4. Blade Server HS22

Aspectos destacados

- Servidor blade modular de alta densidad diseñado para admitir toda la familia de chasis BladeCenter®.
- Diseñado para reducir el tiempo de instalación y el número de personas necesario para realizar el mantenimiento, lo que contribuye a reducir los costos de infraestructura de TI.
- Gracias a la compatibilidad con procesadores de doble núcleo o cuádruple núcleo se consigue el rendimiento necesario incluso para las aplicaciones más exigentes.
- Incluye nuevas redes de alta velocidad con BladeCenter® H para proporcionar un mayor ancho de banda y rendimiento.
- Contribuye a reducir los costos de energía y refrigeración al tiempo que proporciona significativas ventajas de rendimiento en comparación con tecnología más antigua

Características del producto

El diseño revolucionario del blade proporciona flexibilidad y sencillez al centro de datos. IBM Director permite administración remota desde una única consola gráfica, ayudando de este modo a simplificar y automatizar las tareas de TI y redes. Permite agregar o cambiar fácilmente blades sin interrumpir el funcionamiento del resto de los blades instalados en el chasis. Más rendimiento, más eficiencia energética y menores costes para ejecutar las aplicaciones más exigentes. El hypervisor integrado opcional permite la virtualización instantánea. Equipado con Light Path Diagnostics y Predictive Failure Analysis para detectar los fallos de componentes antes de que se produzcan, lo que le ayuda a maximizar la disponibilidad

Especificaciones técnicas generales

Procesador: Procesador Intel® Xeon® de doble núcleo de hasta 3.00GHz o Procesador Quad
Intel® Xeon® de hasta 2.66GHz y de hasta 1333MHz
Memoria (estd./máx.): Hasta 16GB DIMMs con buffer total (interna) y hasta 32GB con Memoria y Unidad de Expansión I/O.
Unidades de disco duro internas: Hasta dos unidades de disco duro (HDD) SAS de 10.000 rpm y diseño pequeño (6.35cm) instaladas en cada blade (además, se

puede añadir tres unidades SAS de intercambio dinámico (hot-swap) con el blade opcional de E/S y Storage).
Capacidad máxima de almacenamiento interno: 734GB (con blade SIO opcional)
Compatibilidad con RAID: RAID-0 o -1 integrado de serie en el servidor blade, RAID- 1E o RAID-5 integrado opcional con blade SIO.
Red: Gigabit Ethernet dual (funciona con TOE), opcional hasta 8 puertos.
Actualización de E/S: 1 conexión de tarjeta de expansión PCI-X (tradicional) y 1 PCI-Express (alta velocidad).
Garantía limitada Garantía limitada in situ durante tres años en piezas y mano de obra.

8. DEFINICIÓN OPERACIONAL DE TÉRMINOS

Red: Sistema de interconexión entre equipos que permite compartir recursos e información. Para ello, es necesario contar, además de los ordenadores correspondientes, con las tarjetas de red, los cables de conexión, los dispositivos de interconexión y el software conveniente.

Cable de par trenzado: Este cable consiste en pares de hilos trenzados y recubiertos de una capa externa. Es de fácil instalación y ofrece cierta protección contra las interferencias externas. Los conectores que se utilizan son los denominados **RJ45.**

En función de sus categorías se pueden clasificar en cuatro categorías:

Categoría 5: Se utiliza para transmitir datos con una velocidad de transmisión de hasta 100 Mbps

Categoría 6: Se utiliza para transmitir datos con una velocidad de transmisión de hasta 1000 Mbps

Categoría 7. Es una mejora de la categoría 6, puede transmitir datos hasta 10 Gbps.

Switch: Dispositivo de red que filtra, reenvía o inunda frames basándose en la dirección destino de cada frame.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta más optima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

Firewall: Dispositivo de hardware o aplicación de software diseñado para proteger los dispositivos de red de los usuarios externos de la red y/o de aplicaciones y archivos maliciosos.

Las funciones de cortafuegos se pueden realizar por:

- Ordenadores dedicados exclusivamente al filtrado de paquetes (servidor proxy)
- Encaminadores de red (routers) configurados para esta área.
- Programas de software para distintos sistemas operativos
- Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.

Topologías de las redes locales: Es la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que las conectan.

Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de la topología es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, permitir un mejor control de la red y permitir de forma eficiente el aumento de las estaciones de trabajo. La forma más utilizada actualmente es la configuración en estrella.

Topología en estrella: En esta configuración todos los equipos están conectados directamente al conmutador y las comunicaciones se han de hacer necesariamente a través de él. Permite incrementar y disminuir fácilmente el número de estaciones. Si se produce un fallo en una de ellas no repercutirá en el funcionamiento general de la red; pero, si se produce un fallo en el conmutador, la red completa se vendrá abajo.

Atenuación: Disminución en la potencia de una señal a lo largo de un cable óptico o eléctrico.

Broadcast: Forma de transmisión por la cual un dispositivo transmite a todos los dispositivos dentro de la red o de otra red.

Dirección IP: Numero único que utilizan los dispositivos a fin de identificarse y comunicarse entre ellos en una red de computadoras utilizando el estándar de Protocolo de Internet (IP).

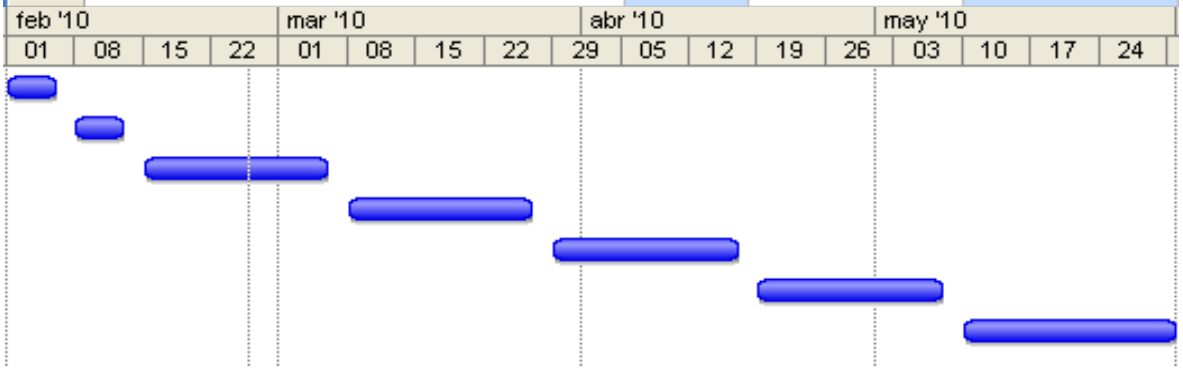
Enrutamiento: Proceso de encontrar una ruta hacia un host destino.

Protocolos de enrutamiento: Protocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento especifico.

Internetwork: Interconexión de dos o más redes diferentes.

9. CRONOGRAMA

	Nombre de tarea	Duración	Comienzo	Fin
1	Levantamiento de inventarios	5 días	lun 01/02/10	vie 05/02/10
2	Observacion Directa de la red	5 días	lun 08/02/10	vie 12/02/10
3	Analisis y estudio del entorno	15 días	lun 15/02/10	vie 05/03/10
4	Documentacion falencias	15 días	lun 08/03/10	vie 26/03/10
5	Diseño de las soluciones	15 días	lun 29/03/10	vie 16/04/10
6	Documentacion del proceso de la solucion	15 días	lun 19/04/10	vie 07/05/10
7	Administracion y verificacion de la instalacion	16 días	lun 10/05/10	lun 31/05/10



10. PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

El prototipo de red que se propone para el IMTP está definido en los planos anteriores, según los estándares de cableado estructurado de La Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA) donde se define que la longitud máxima de cable desde el punto de terminación en el cuarto de telecomunicaciones hasta la terminación en la toma del área de trabajo no puede superar los 90 metros, por lo tanto en el cuarto de Telecomunicaciones ubicado en la Subdirección de Sistemas se ubicaran: 5 Switches 3com 4200G 24-Port donde llegaran todas las conexiones de los equipos de todas las oficinas del Instituto, no se ubicaran switches en otros lugares ya que esto disminuye y afecta la calidad de la red, además se supone que la distancia entre dicho cuarto y los equipos de computo no supera los 90 metros que definen los estándares y las distancias para interconectar los patch panels y el punto de terminación del cableado en la pared hasta el teléfono o la computadora no superan los 5 metros. De igual manera y según los estándares las UPS deben estar alojadas en el mismo cuarto de telecomunicaciones, por esto se encuentran ubicadas en las unidades de rack.

Se configurará una impresora en red por cada oficina del Instituto, esto para ahorrar costos en mantenimientos y cooperar con el medio ambiente.

En el tema de seguridad informática se contemplará la instalación y configuración de los equipos que ofrece Fortinet, el FortiGate que cumpla las funciones de Firewall y Proxy entre otras.

Los servidores serán reemplazados y se consolidará la infraestructura e información en el Chasis Blade Center de IBM y en los Blade Server HS22

Plano de red del Primer Piso
Ver apéndice A

Plano de red del Segundo Piso
Ver apéndice B

CONCLUSIONES

- Por medio del estudio previo a las redes de telecomunicaciones es posible detectar las falencias que esta presenta.

- Cuando se tienen identificadas plenamente las fallas o problemas que presenta la red de telecomunicaciones en una empresa es más viable que las soluciones propuestas mejoren dichos problemas.

- Para realizar el diagnostico de una red se debe enmarcar el entorno que se va a estudiar para simplificar procesos

- En el análisis a la red, cada una de las dificultades encontradas al interior de esta deben quedar documentadas para su posterior solución.

- Al momento de proponer el diseño de la red de telecomunicaciones se deben tener en cuenta y cumplir a cabalidad con todos los estándares establecidos para la implementación de todos los dispositivos.

RECOMENDACIONES

- Para la existencia de una red LAN dentro de una organización se deben cumplir varios estándares además definir e implementar una topología de red

- El cableado estructurado que compone toda la red debe cumplir ciertas normas para su utilización, de igual manera debe integrar tanto los servicios de voz, datos y video.

- En la longitud del cableado estructurado se debe tener en cuenta la atenuación de la señal, pues entre más extensos los medios más se afectara la señal.

- El cableado horizontal de se instala y deben ser conducidos en canaletas.

- Cada equipo o dispositivo que forme parte de la red debe tener una dirección IP exclusiva, que permita a otros sistemas o dispositivos localizarlo.

- Si todos los hosts no forman parte de la misma red, esta se debe dividir en subredes independientes.

- Planificar y documentar la asignación de direcciones IP a fin de evitar duplicación de direcciones, controlar la seguridad y accesibilidad de los dispositivos y además monitorear la seguridad y el rendimiento de los hosts de la red y de la red en general.

- Utilizar un protocolo de red de comunicación para facilitar el establecimiento de la misma.

- Para la protección de la red el paso más importante es la aplicación de una política de seguridad eficaz.

- La creación de VLANs, configuradas dentro de los switches, dividen en diferentes “dominios de broadcast” a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast.

BIBLIOGRAFÍA

Raya José Luis, Raya Laura, Martínez Miguel A. Redes locales. Instalación y configuraciones básicas Alfaomega. Primera Edición

Stallings William. Comunicaciones y redes de Computadores. Pearson Prentice Hall. Séptima Edición 2004

Tanenbaum Andrew S. Redes de Computadoras. Pearson Prentice Hall. Cuarta Edición 2003

Gallo A. Michael, Hancock M. William. Comunicación entre computadores y tecnologías de redes. México 2002.

Curso Cisco Networking Academy V4.0

Curso Cisco Networking Academy V2.1.2

http://www.ecomiltechnologies.com/index.php?option=com_content&task=view&id=13&Itemid=36

http://www.monografias.com/trabajos7/rela/rela.shtml

APÉNDICES

Apéndice A

Apéndice B