UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

DEPARTAMENTO ARQUITECTURA Y REDES DE COMPUTADORA

LICENCIATURA EN REDES INFORMÁTICAS

ASIGNATURA:

ANÁLISIS Y DISEÑO DE REDES

DR. VLADIMIR VILLARREAL

2020

CONTENIDO

Las redes de computadoras, como la imprenta hace 500 años, permiten que el ciudadano común distribuya sus puntos de vista en diversos modos y a audiencias diferentes, lo cual antes no era posible. Este nuevo fondo de libertad ofrece consigo muchos temas sociales, políticos y morales sin resolver.

Andrew Tanenbaum

I. ELEMENTOS BÁSICOS DEL DISEÑO DE REDES

OBJETIVOS:

- Identificar y organizar los componentes físicos y lógicos que conforman el análisis y diseño de una red de transmisión de datos ajustándolos a los requerimientos específicos de cada proyecto.
- Aplicar criterios y metodologías en la presentación de propuestas para el diseño de redes de transmisión de datos, con el fin de lograr un enfoque sistémico en la elaboración del proyecto.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Esta sección de aprendizaje, detalla los principales elementos, criterios y metodologías a tomar en cuenta en el análisis y diseño de un proyecto de red de transmisión de datos, desarrollándolo con un enfoque sistémico para que de manera integral permita identificar y comprender con mayor claridad y profundidad los requerimientos organizacionales.

I. Elementos básicos de diseño de redes

Introducción

Diseñar una red de manera adecuada es un reto que involucra algo más que realizar una interconexión física entre dos o más computadores, una red requiere realmente cumplir muchas características para sea escalable y administrable.

Para diseñar una red confiable que cumpla con los requisitos de escalabilidad, confiabilidad y proyección a futuro, se debe tener en cuenta que no existe un diseño estándar del que se pueda tomar referencia, si no que existen lineamientos básicos para cada red, se busca entonces crear una metodología para estandarizar los requisitos mínimos en la implementación y auditoria de una red.

1.1 Enfoque Sistémico

El enfoque sistémico es, sobre todo, una combinación de filosofía y de metodología general, engranada a una función de planeación y diseño. Se basa en la metodología interdisciplinaria que integra técnicas y conocimientos de diversos campos fundamentalmente a la hora de planificar y diseñar sistemas complejos y voluminosos que realizan funciones específicas.

Un diseño basado en un enfoque sistémico debe cumplir con los siguientes puntos:

- Interdisciplinario
- Cualitativo y Cuantitativo a la vez
- Organizado
- Creativo
- Teórico
- Empírico
- Pragmático

El enfoque sistémico debe centrarse constantemente en sus objetivos totales. Por tal razón es importante definir primeros los objetivos del sistema y examinarlos continuamente y, quizás, redefinirlos a medida que se avanza en el diseño.

Utilidad y Alcance de diseñar la red bajo un enfoque sistémico:

Ayudará a analizar y desarrollar el diseño de manera integral permitiendo identificar y comprender con mayor claridad y profundidad los problemas organizacionales, sus múltiples causas y consecuencias. Así mismo, viendo a la organización como un ente integrado, conformada por partes que se interrelacionan entre sí a través de una estructura que se desenvuelve en un entorno determinado, se estará en capacidad de poder detectar con la amplitud requerida tanto la problemática, como los procesos de cambio que de manera integral, es decir a nivel humano, de recursos y procesos, serían necesarios de implantar en la misma, para tener un crecimiento y desarrollo sostenibles y en términos viables en un tiempo determinado.

1.2 Metodología para el Diseño

Seguir una metodología nos permite dividir un problema grande (instalar una red) en varios más pequeños y manejables (etapas del diseño de una red). Es importante preparar un plan para realizar el trabajo de la forma más profesional y ordenada posible.

Para que una red sea efectiva y sirva para las necesidades de los usuarios, debe diseñarse e implementarse de acuerdo con una serie de eventos sistemáticos planificados, que incluyen lo siguiente:

- Reunión de los requisitos y las expectativas de los usuarios
- Análisis de los requisitos.
- Diseño de la estructura (es decir, la topología).
- Documentación de la implementación física y lógica

Primeramente, al diseñar una red, debe de reunirse datos acerca de la estructura de la organización. Esta información incluye el historial de la organización y su estado actual, el crecimiento proyectado, las políticas operativas y los procedimientos de administración, los sistemas y procedimientos de oficina y los puntos de vista de las personas que utilizarán red. Necesita contestar las siguientes preguntas: ¿Quiénes son las personas que utilizarán la red? ¿Cuál es su nivel de capacidad y cuáles son sus actitudes acerca de los computadores y de las aplicaciones informáticas? Si contesta estas preguntas y otras preguntas similares, esto lo ayudará a determinar cuánta capacitación será necesaria y cuántas personas se necesitan para soportar la red.

Lo ideal es que el proceso de reunión de información ayude a clarificar e identificar los problemas. También debe determinar si hay políticas documentadas en vigencia. ¿Algunos de los datos han sido declarados críticos para el trabajo? ¿Algunas operaciones han sido declaradas críticas para el trabajo? (Los datos y las operaciones críticos para el trabajo son aquellos que se consideran fundamentales para la empresa, y el acceso a ellos es crucial para las actividades que se ejecutan diariamente). ¿Cuáles son los protocolos que están permitidos en la red? ¿Sólo se soportan determinados hosts de escritorio?

A continuación, debe determinar cuál es la persona dentro de la organización que tiene autoridad sobre el direccionamiento, la denominación, el diseño de topología y la configuración. Algunas empresas cuentan con un departamento central de sistemas de Información de administración (MIS) que controla todo. Algunas empresas cuentan con varios departamentos MIS pequeños y, por lo tanto, deben delegar la autoridad a los departamentos. El enfoque se debe centrar en la identificación de recursos y limitaciones de la organización. Los recursos de la organización que pueden afectar la implementación de un nuevo sistema de red, se clasifican en dos categorías generales: hardware/software informático y recursos humanos. El hardware y el software informático existente de una organización se debe documentar y se deben identificar las necesidades de hardware y software proyectadas. ¿Cómo se vinculan y comparten estos recursos actualmente? ¿Cuáles son los recursos financieros de los que dispone la organización? La documentación de esta clase de cosas lo ayuda a estimar los costos y desarrollar un presupuesto para la red. Debe asegurarse de que comprende las cuestiones relacionadas con el rendimiento de cualquier red existente.

1.2.1 Pasos para el diseño de una red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) **Recolección de datos organizacionales:** puede incluir la historia de la empresa, las políticas administrativasa y operativas con las que cuentan, etc.
b) **Preparar el plan de diseño de una red**

Establezca los objetivos *primarios* (exigencias obligatorias), ***secundarios*** (servicios recomendables) y ***terciarios***(exigencias a futuro).

Establezca los criterios de evaluación. Qué puntos le indican que su diseño e implantación es el correcto. Esos puntos pueden ser algunos de los siguientes:

- Tiempos
- Costos
- Capacidad de expansión
- Eficacia
- Mejora de la productividad
- Integridad y confiabilidad (menor número de errores)
- Seguridad

c) **Análisis de la red en el sitio.**

Si ya existe una red se deberá evaluar su estado actual: tiempos de respuesta, tráfico, número de fallas, aplicaciones que actualmente utiliza, tipo de red, dispositivos con los que cuentan (servidores, pc, routers, etc), quiénes la utilizan, cuáles son funciones, etc.

d) **Definición de nuevas exigencias**

¿Desarrollará la empresa nuevos productos o servicios en el futuro? ¿Abrirá otras oficinas? ¿Requerirá de nuevos servicios como transmisión de video, etc? ¿Existe una tendencia tecnológica que deberá implementar en lo inmediato?

e) **Estudios de viabilidad.** Pueden ser los siguientes:

- Viabilidad técnica. Hardware y software necesarios
- Viabilidad operacional. Efecto de la red en la estructura organizacional de la empresa.
- Viabilidad económica. Costos y ventajas.
- Viabilidad financiera. Financiamiento y rentabilidad.

f) **Determinar el tamaño y la arquitectura de la red.** Indique los lugares donde se extenderá la red. Pueden ser varios edificios o pisos. Evaluar el tipo de topología a utilizar según los requerimientos

g) **Cálculo del tráfico de la red.** Estime cuántos MB (megabytes) utilizará cada usuario por día. Calcule el total de tráfico en un día. Si es un ambiente laboral de 8 horas,

divida el tráfico por día / 8 para obtener el tráfico por hora. Divida entre 3600 para obtener tráfico por segundo.

h) Configuración. Se refiere a la descripción formal y diseño físico y lógico de los elementos de hardware (servidores, routers, etc) y software (protocolos de enrutamiento, etc) de la red, incluyendo su arquitectura y modo de operación

i) Elaboración de un sistema de seguridad y control. Se establecen medidas de control a tres niveles: Prevención, Detección y Corrección. Para prevención se crea un modelo de amenazas que describa las amenazas y los recursos en riesgo. Otros controles comunes son: tener un plan de recuperación, contar con extintores, buena ubicación de los servidores, fuentes de poder ininterrumpibles, contratos con los proveedores de servicios, uso de fibra óptica, programas antivirus, capacitación, software para contraseñas, etc.

j) Evaluación del costo. Consiste en establecer los costos directos e indirectos.

- **Directos** pueden ser: costos de computadoras, dispositivos de comunicación, software, personal técnico, mantenimiento, copias de seguridad, redacción de la documentación, personal, seguridad, otros costos (aire acondicionado, corriente eléctrica, etc).
- **Costos indirectos** puden ser: Capacitación, aumento de fallas o interrupcines durante las primeras actividades.

  En esta etapa se deben dejar claras las ventajas:

  - **Reducción de costos**, pues disminuye el personal, las actividades manuales, el costo en inventarios o en operación.
  - **Incrementa la rentabilidad**, ya que mejora el servicio al cliente o las operaciones son más rápidas.
  - **Ventajas intangibles**. Se reduce el consumo de papel, las decisiones se toman más rápido, se mejora la ventaja competitiva de la empresa, los empleados están más a gusto, etc.

k) Implantación. Se debe realizar un plan de instalación de todos los equipos y dispositivos, desde el cableado hasta servidores y estaciones de trabajo. ¿El antiguo sistema y el nuevo funcionarán en paralelo un tiempo? ¿o se tiene que desinstalar la antigua red o sistema para implantar el nuevo? ¿se realizará primero un piloto?

l) **Administración**. En esta etapa se analizan y diseñan todas las medidas para la administración de la red, incluyendo todos los mecanismos tanto hardware como software, además de establecer las funciones del personal encargado de dicha administración.

m) **Pruebas y Documentación del diseño.**

Se utilizan los criterios de rendimiento que se establecieron en la etapa b.

Hay varias formas de probar el diseño de una red, pero en el siglo XXI nadie monta una red si antes no la ha modelado y simulado previamente. Estas herramientas permiten analizar el comportamiento o desempeño de la red diseñada, a partir de los patrones de tráfico actuales y futuros, ante la cantidad prevista de usuarios y su futuro crecimiento, los servicios, nuevas aplicaciones. etc. La documentación debe ser tanto de todas las conexiones físicas, como de las conexiones lógicas, software instalado, políticas de seguridad (incluidas medidas de contingencia), etc. Este paso es muy importante, pues del mismo dependerán las acciones futuras de mantenimiento y operación.

1.3 Criterios para construir una red

Para adherirse a las buenas prácticas de diseño hay que procurar que los principios del diseño de redes tengan las características siguientes:

- ✓ **Modularidad:** Los diseños de las redes modulares soportan crecimiento y cambios mediante el empleo de bloques constructivos, también denominados módulos, lo que permite escalar la red de forma fácil en vez de rediseñar la misma.
- ✓ **Elasticidad:** Los diseños de las redes tienen que tener características de alta disponibilidad y su tiempo de funcionamiento tiene que ser de un 100%. Imaginen una red corporativa de un banco que podría perder millones por solo interrumpirse un segundo. De ahí que se hable de la capacidad de recuperación de una red en milisegundos.
- ✓ **Flexibilidad:** Los cambios en los negocios es una garantía para cualquier empresa, de ahí que se requiera una rápida adaptabilidad y por ende los diseños de las redes corporativas tienen que procurar y facilitar esos cambios.

- ✓ **Funcionalidad:** una red debe ser funcional, debe permitir que los usuarios de red cumplan con los requisitos de trabajo, debe proveer conectividad entre los usuarios y aplicaciones a tiempos de respuesta razonables.
- ✓ **Escalabilidad:** "Todas las redes deben ser capaces de crecer continuamente y abordar las nuevas tecnologías minimizando los costes de implementación" , esto es uno de los requerimientos que más fácil se deja de tener en cuenta en el análisis de la red, en la mayoría de los casos no se prevé el crecimiento estructura.
- ✓ **Adaptabilidad:** Se debe realizar el diseño de redes teniendo en cuenta tecnologías futuras y no se debe limitar la red para la implementación de estas nuevas tecnologías mientras se puedan adquirir.
- ✓ **Administración:** El diseño de la red debe resultar de fácil manejo para el monitoreo, administración y control de incidencias
- ✓ **Seguridad:** Este es un aspecto de alta prioridad, lo que requiere definir las políticas y herramientas de seguridad informática a implementar en la red.
- ✓ **Afordabilidad (Costo-Efectividad):** Muchos usuarios toman en muchas ocasiones este objetivo por encima del desempeño y de la disponibilidad. Para que un diseño de red sea costeable o accesible, el mismo debe transportar la mayor cantidad de tráfico para un determinado costo. Este costo financiero incluye el costo de los equipos y además los costos de instalación, operación y mantenimiento de la red.

  En muchas ocasiones los usuarios quieren conmutadores (Switch) que tengan muchos puertos y que sea bajo el costo por puertos. Por otro lado buscan que el costo del cableado sea mínimo y que el proveedor de servicios los ofrezca baratos.

  Por otro lado quieren que las tarjetas de interfaz (NIC) y los servidores sean baratos. En dependencia de las aplicaciones que estén corriendo sobre los sistemas finales, el bajo costo es más importante para los usuarios que la disponibilidad y el desempeño en el diseño de una red de campo. Y esto tiene sus peligros, por lo que hay que tener mucho cuidado.

1.4 Documentos de Diseño de una red.

La documentación de la red es muy importante para la administración de la red, esta debe ser algo parecido a un diario de ingeniería en el cual se lleva un registro detallado de todo el proceso de instalación y problemas que se presentaron cuando fueron instaladas, incluido en este mismo la solución que se ejecutó para el problema, es necesario recordar que se deben tener en cuenta los siguientes aspectos a la hora de generar este registro:

- ✓ Diagramas físicos de red
- ✓ Tipos de cables empleados
- ✓ La longitud de cada cable
- ✓ El tipo de terminación de cada cable
- ✓ La localización geográfica en la estructura física
- ✓ Esquema de etiquetado para fácil identificación

También, deben contemplarse los siguientes aspectos:

- ✓ **Disposición de centros de distribución principal e intermedio:** se debe realizar un diagrama físico y lógico de la estructura de red de los centros de distribución principal, así mismo especificar la ubicación exacta de los equipos de distribución como servidores racks y equipos auxiliares y etiquetas de patch panel.
- ✓ **Auditorias de inventario:** las auditorias de inventario permite llevar una inventario completo de todos los dispositivos de red, lo ideal de este es que se realice un inventario de los equipos cuando son adquiridos recientemente, un ejemplo claro para la organización de fichas de inventario deberían tener la siguiente información:
    - Número de serie del dispositivo
    - Localización física
    - Descripción completa de memoria
    - Tipo de memoria
    - Periféricos en general (Marca, modelo, tipo)
    - Comentarios generales del dispositivo
    - Software instalado
    - Licencia de software

- ✓ **Records de mantenimiento:** es importante llevar un registro de todos los mantenimientos realizados de los equipos que conforman la red, esto aminora el tiempo de respuesta para corregir futuros problemas en el mismo dispositivo o en otros dispositivos similares.
- ✓ **Políticas de usuario:** en este deben estar depositados todos los permisos de usuarios y como estos interactúan con la red, este documento de políticas debe ser documentado al lado del administrador de red para que se cumplan con las políticas de red y no entren en conflicto con los alcances de la empresa.

En términos generales la documentación consta de:

- ✓ Plano físico de cada una de las instalaciones que abarca la red LAN (planta, edificios, campo, etc.)
- ✓ Planos de conexiones lógicas de cada subred y la Red completa.
  Los planos lógicos de la red que dan una visión de toda la Red, sirviendo además en caso de detección de problemas como para la implementación de futuras expansiones.
- ✓ Plano de la Interconexión de los puertos de los Conmutadores y Enrutadores en los armarios y cuartos de control
- ✓ Tablas de direccionamiento empleado a cada nivel.
- ✓ Tablas de Rutas
- ✓ Tablas NAT
- ✓ Tablas con las Redes VLAN.
- ✓ Programas de configuración de cada Conmutador y cada Enrutador
- ✓ Tablas y Gráficos de los principales parámetros que miden el desempeño de la red. Los resultados de las pruebas ejecutadas con los principales resultados alcanzados en los diferentes escenarios. Recuerde que no basta con una sóla prueba para considerar resultados fiables.

Actividad 1.: Caso de Estudio

Seguros Del Istmo es una Compañía de Seguros con sucursales distribuidas en diferentes puntos del país.

Su organización empresaria es de tipo piramidal, con su cima en la Casa Central ubicada en la ciudad de Panamá y 4 sucursales distribuidas en las ciudades de Santiago, Colón, David y Chitré. La mayor autoridad de la Casa Central es el Gerente General, quien tiene a su cargo un Gerente de Sucursales. Este gerente es el encargado de coordinar las actividades de las distintas sucursales, quien se relaciona directamente con cada gerente de sucursal, ubicado en las diferentes ciudades.

Seguros S.A. está elaborando un proyecto de instalación de un sistema de red que permita desarrollar procesos de consulta de cotizaciones y presupuestos, realizar contrataciones de seguro, brindar asistencia a los clientes y mantener un sistema centralizado de todas sus operaciones. Con esta finalidad contrató el desarrollo de una base de datos on-line, un sistema de seguros y un sistema de consultas internas on-line que operarán sobre servidores instalados en la Casa Central. La salida a Internet de todas las sucursales será a través de Casa Central.

Se le pide elaborar los siguientes puntos:

- Levantamiento de las necesidades funcionales y no funcionales de la empresa
- Planteamiento de Objetivos de diseño
- Análisis de requisitos.
- Estudio de factibilidad tecnológica y económica de implementación de una red.
- Presentación de herramientas que permitan la recolección de información a los usuarios (modelo de entrevistas, cuestionarios, etc).
- Evalaución de estado actual de red.

II. ANÁLISIS DE LOS REQUERIMIENTOS

OBJETIVOS:

- Interpretar los requerimientos funcionales y no funcionales que son vitales para definir un diseño de red que se encuentre dentro del poder adquisitivo de la empresa tanto económico, humano y tecnológico.
- Identificar los elementos funcionales de un sistema de cableado estructurado, sus características y cómo la aplicación de normas y estándares relacionados con el cableado estructurado facilitan el buen desempeño de la red.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Esta sección de aprendizaje, trata sobre el estudio profundo de una necesidad tecnológica que tiene una empresa, organización o negocio. El análisis de requerimientos especifica las características operacionales que tendrá la red de transmisión de datos a desarrollar. Estos requerimientos deben obtenerse a través de entrevistas, observación, indagación y demás técnicas específicas, con el fin de recabar toda la información posible desde los distintos clases de usuarios de la red.

II. Análisis de los requerimientos

Introducción

Es en este punto, en que el analista encargado del diseño de red, debe acoplar los requerimientos de usuario con la disponibilidad física de la red y definir un diseño que se encuentre dentro del poder adquisitivo de la empresa tanto económico como tecnológico, es posible que en algunos casos el analista se vea en la obligación de eliminar o unificar requerimientos.

Es viable que de la anterior identificación se genere una gran cantidad de requerimientos, por esta razón se deben enumerar y asignar una prioridad a cada una de las necesidades de la empresa. Por cada una de estas se debe evaluar la factibilidad económica, factibilidad tecnológica y viabilidad, apuntando siempre a los objetivos estratégicos empresariales.

Toda esta información se obtendrá del personal de la empresa, podrán proporcionar información acerca del crecimiento de los últimos meses, incluso de los últimos tres años, tanto de personal como en las áreas de trabajo, así como del presupuesto y de los tiempos planeados para ejercerlo. Algunas recomendaciones para la obtención de información:

- Solicite la información siempre en formato escrito o electrónico
- Nunca crea o asuma, siempre verifique.
- Siempre tenga a mano documentos como estándares de cableado o de seguridad.
- En los casos que no se tenga la información, solicite que la generen en el momento
- Verifique que la información recibida sea lo más actualizada posible.

Para finalizar esta etapa y poder continuar, será necesario ordenar la información de acuerdo a ciertos criterios lógicos; por información financiera, de recursos humanos, documentación técnica, etcétera. Todo esto permitirá contrastar la información y tener un control absoluto sobre la misma y de esta manera poder observar que se tiene y que hace falta.

2.1 Identificación del uso de la red

Es esencial indagar en las aplicaciones que se implementarán en el sistema de comunicaciones, tales como telefonía, datos y video, sus requerimientos serán de vital importancia, ya que permitirá seleccionar características técnicas, de diseño y localización de los equipos y materiales a utilizar.

El modelo de negocio de la organización, es también un aspecto importante, ya que este dará al diseñador de la red una perspectiva general de la estrategia de la empresa y su implementación, sus clientes, definición y diferenciación de sus productos y/o servicios, definición de los procesos que se lleván a cabo, cómo conseguirá el beneficio y cómo lo distribuirá. Por tanto el modelo de negocio de una empresa determina la forma por la cual un negocio crea, proporciona y captura valor. Estos puntos proporcionarán de una idea clara y detallada para la identificación del uso de la red, y permitirá diseñar la red tomando en cuenta los aspectos de escalabilidad, funcionalidad, flexibilidad, etc.

2.2 Especificación de tareas del Computador

Los profesionales se han vuelto más independientes y, a medida que han surgido nuevas dinámicas de trabajo, requieren en sus tareas mayor movilidad, trabajar en archivos en la nube, analizar datos, programar, navegar por internet, realizar videollamadas, trasladarse de un lugar a otro y trabajar a cualquier hora. Muchas tareas también requieren un buen poder de procesamiento y una gran pantalla, así como, la comodidad de varios periféricos, trabajar con software diferentes como pueden ser de diseño, cálculo, presupuestos, modelado, documentos, etc. En el área comercial, los sistemas de punto de venta son ideales para automatizar los procesos del negocio, mejorar el seguimiento del inventario y permitir una administración más efectiva de la información para aumentar las ganancias y disminuir las ineficiencias.

Una vez definidas las tareas que estarán desempeñando los computadores y demás equipo de la red, es esencial verificar que el equipo cumpla con ello, desde el sistema operativo hasta el hardware. Así, se podrá ahorrar dinero y optimizar los tiempos. Elegir equipos que ofrezcan mayor funcionalidad, escalabilidad y garantía a largo plazo.

2.3 Determinación del grado de Centralización

La empresa debe valorar algunos aspectos en el momento de organizar su red de información en cuanto al nivel de centralización o descentralización que esta tendrá. Para esto, se debe tomar en cuenta los siguientes puntos:

- Una compañía que mantenga una estructura organizativa descentralizada debe tener los recursos de información descentralizados también y viceversa.

- Existe una gama muy amplia de posibilidades de centralización y descentralización de las redes, desde un único ordenador mainframe con pantallas en el mismo local del centro de procesamiento de datos (máxima centralización) hasta un sistema formado por varios ordenadores no conectados (máxima descentralización). Hoy, las empresas optan por una situación mixta o intermedia: un servidor y los demás ordenadores conectados en red a este servidor. Cada ordenador es autónomo pero ofrece la posibilidad de conexión entre los distintos ordenadores de la empresa para compartir datos .
- La centralización tiene la cualidad de permitir un control más sencillo, ya que es la mejor forma de captar, manipular y usar la información cuando es necesario que un gran número de usuarios puedan acceder a ella. Otra de sus ventajas es que evita la inconsistencia de las aplicaciones y de los programas de los departamentos. Su máximo inconveniente radica en que genera retrasos y pérdidas de tiempo al establecer prioridades entre usuarios, a la vez que anula la iniciativa individual.
- En cambio, la descentralización permite adaptar las necesidades del usuario, por lo tanto, motiva al usuario, facilita el reparto de las tareas y multiplica la eficacia de las funciones directivas. El centro de información pasa a tener una función consultora. El gran inconveniente es que la tecnología no satisface siempre en coste y calidad a los requerimientos de cada usuario.

En un principio, la descentralización era obligada ya que los ordenadores apenas podían manipular la carga de trabajo de un único departamento. Con el desarrollo de los mainframes y de las redes terminales provocaron la centralización de las aplicaciones y de las bases de datos. Después se volvió a la descentralización con los miniordenadores, ya que con la tecnología de los sistemas abiertos la informática departamental, de grupo y de usuario final se hizo una realidad. Como consecuencia de ello, se trasladó las bases de datos y especialistas de la información a algunos departamentos, así como la creación de centros de información para apoyar a la informática de usuario final. La última tendencia es la de controlar más los recursos de información de una empresa. El resultado ha sido volver a la centralización, y en otras ocasiones, un desarrollo de estructuras híbridas con componentes centralizados y descentralizados.

El hardware ofrece alternativas para la descentralización en diversas áreas:

- Capacidad de procesamiento. Con la instalación de varios procesadores es posible que cada usuario tenga el suyo. El ordenador central queda liberado, sobre todo en ocasiones donde el usuario demanda por mucho tiempo el ordenador, y también en las ocasiones que requiere liberar líneas de comunicación al tratarse de ordenadores situados en distintos locales.
- Con la descentralización de los programas y datos, el funcionamiento de los usuarios gana en independencia, dependiendo menos del equipo central. Pero surge el problema de redundancia cuando los datos deben ser compartidos por varios usuarios. Por tanto, esta descentralización sólo es recomendable cuando sean datos que no vayan a ser compartidos o cuando el alto volumen de la base de datos y su distribución geográfica lo requiera.
- En cuanto a los usuarios, este problema está casi resuelto ya que hoy cada usuario trabaja en su propio ordenador.
- La descentralización física planteada de modo distinto según el escenario. Por un lado en locales separados por vías públicas, y por otro, dentro de un mismo local donde prevalecen los factores como el tipo de perfil del trabajo de los usuarios (demanda de tiempo de procesador, rapidez de tiempo de respuesta, necesidad de compartir información con otros usuarios) o aspectos económicos.

Según García Bravo, el equilibrio entre el equipo multiusuario y la red local, conforma las características de cada empresa. Lo ideal sería mantener una centralización en el terreno técnico y una descentralización en los usuarios. Las ventajas de la descentralización de usuarios estriban en que éstos interactúan con el ordenador satisfaciendo sus necesidades de manera más eficaz, mientras decrecen los costes de hardware y software. Tampoco hay que olvidar la existencia de varios procesadores independientes, así como la independencia de análisis y diseño de cada unidad, y por último, la gestión de las bases de datos y aplicaciones en cada departamento. Como desventaja hay que señalar la posible incompatibilidad entre hardware, software y sistemas, y que los precios de los costes de comunicación se disparen.

Al dilema de la centralización o descentralización, Monforte propone la llamada informática distribuida. Esta tecnología es posible gracias a las posibilidades de interconexión de las telecomunicaciones. Mantiene un equilibrio entre la centralización y la descentralización. Se desarrollan aplicaciones específicas para determinados puestos de trabajo que mediante su

interconexión, facilita el intercambio de información siempre que se necesite. Se trata de una arquitectura mixta donde sólo se descentraliza la dependencia funcional, mientras que las demás unidades siguen unidas al departamento central. Pero hoy ya no sólo es descentralización funcional sino geográfica también, aun manteniendo la dependencia de las personas y el control centralizado en el departamento de informática.

Centralizar o no, es una solución a medida de cada empresa. Es decir, cualquier actuación debe tener en cuenta la naturaleza de la empresa, su tamaño, su tecnología y complejidad. Lo ideal es adoptar lo mejor de cada solución y evitar aquellas acciones que nos conduzcan a caminos sin retorno y a la vuelta a una organización jerárquica donde la información fluye en un único sentido (de arriba a abajo), y donde el usuario pierde su papel activo.

2.4 Requerimientos

La especificación de requerimientos es un documento con los requerimientos de la red, pero con alto detalle, incluyendo todos los servicios y los niveles mínimos de rendimiento que deben cumplirse. La especificación de requerimientos no especifica exactamente cómo será implementada la funcionalidad requerida, sino simplemente, provee un conjunto de criterios para que la red cumpla con sus objetivos principales, describiendo las limitaciones de costo y restricciones de tiempo, este documento es la salida de la etapa de análisis de requerimientos y representa un hito significativo en el proyecto. la especificación de requisitos debe incluir las siguientes secciones:

- ✓ El papel que desempeña la red dentro de la empresa.
- ✓ Las características operacionales y restricciones de la red.
- ✓ La información que la red necesita y la que provee.
- ✓ La velocidad de respuesta que se necesita mediante el uso de la red
- ✓ El número promedio y máximo en un mismo momento de usuarios en el sistema.
- ✓ Numero de localidades que se van a comunicar y distancia entre si.
- ✓ Tipo de servicio que el usuario requiere.
- ✓ La necesidad de un tipo de transacción especifica.
- ✓ La información completa que debe manejar el sistema durante una transacción determinada.
- ✓ El volumen de datos que la red manejará.

- ✓ Requerimientos de confiabilidad, las consecuencias aceptables de una avería, (disponibilidad, tiempo de reparación, etc.)
- ✓ Estimaciones sobre los servicios y tráfico de red.
- ✓ Equipo que se utilizará.
- ✓ Indicar donde estarán los dispositivos en que cantidad y que función estarán desarrollando (terminales, computadoras personales (tamaño y velocidad del CPU, memoria principal), monitores, dispositivos de almacenamiento, fuentes de datos análogos (teléfonos, cámaras de video y equipos sensores), dispositivos de impresión, (tipos de impresoras), otros dispositivos como scanner, mouses, tabletas graficas, plumas ópticas, cajas registradoras, lectores de códigos de barras)).
- ✓ Despliegue de equipos y software de usuarios finales.
- ✓ Aplicaciones de red.
- ✓ Capacidad de almacenamiento de datos en la red.
- ✓ Seguridad de la red.
- ✓ Procedimientos de recuperación y respaldo de datos.
- ✓ Apoyo de soporte y mantenimiento.
- ✓ Programación para entrenamiento de usuario
- ✓ Limitaciones de presupuesto.

La especificación de requerimientos de cualquier servicio o producto no es una ciencia exacta, pero un análisis formal del proceso incrementará las probabilidades de acierto en las siguientes etapas de diseño e implementación.

Debemos tener presente, que no será suficiente preguntar al cliente que es lo que quiere, ya que podrían estar dudosos de lo que su red en el futuro requerirá, y podrían tener solo una vaga idea de lo que puede o no lograrse desde un punto de vista tecnológico. Conversar con el personal de todos los niveles en la organización ayudará a ver todo el panorama completo y asegurar que los requerimientos sean especificados.

Los servicios requeridos de seguro incluirán una red básica de servicios tal como compartir archivos, autenticación para el uso de impresoras en red, correo electrónico y acceso a internet son los primeros en la lista y tendrán implicaciones en el tráfico y seguridad de la red. Otros servicios podrían ser requeridos, como aplicaciones de trabajo en red, video

conferencias, etc. Estos requerimientos inevitablemente tienen gran impacto en los requerimientos de ancho de banda.

Una vez que la lista de servicios requeridos ha sido creada, será necesario determinar cuántos usuarios normalmente usarán estos servicios en cualquier momento dado y que tanta será la demanda, Esta información puede ser obtenida con una estimación del tráfico que fluye en diferentes partes de la red a diferentes horas del día, el número y tipos de transacciones de negocio que son realizadas cada día, por ejemplo que tan seguido los datos existentes son modificados o leídos.

El modelo del negocio es de fundamental importancia para la verificación de los requerimientos, ya que provee un punto de vista del negocio independiente de la tecnología, de tal forma que las decisiones de los sistemas y procedimientos, puedan ser hechas para cubrir necesidades del negocio.

En cuánto al requerimeinto de rendimiento de la red, es usualmente especificado en base al promedio de velocidad que un servicio de red responde a una petición de usuario y el nivel general de disponibilidad de la red, es decir, cuando tiempo la red funciona de modo normal.

Finalmente, hay que tener presente que el rendimiento puede tener un significado diferente para cada persona en particular. Los usuarios tienen expectativas de acerca de los resultados finales y el tipo de tecnología, cualquiera que sea ésta, puede afectar las expectativas, sobre todo en momentos de gran demanda, donde podrían darse circunstancias adversas que son inevitables y vienen de tiempo en tiempo. Es una buena política educar a los usuarios que tengan una expectativa razonable y realista en vez de hacer promesas que no podamos mantener o llevar a cabo sin el equipo y capacidad necesaria.

2.4.1 Hardware y software: En el análisis de requerimientos para el hardware y software se deben tomar los siguientes aspectos:

- ✓ **Determinación de las necesidades de hardware y software**

  Es posible que la inversión que se dispone exija la selección y compra de un sistema con la configuración mínima necesaria para satisfacer las necesidades inmediatas. No obstante, es probable que se requiera mayor poder de cómputo en el futuro, si es así, conviene adquirir un sistema que se pueda ampliar para satisfacer requerimientos futuros.

- ✓ **Existencia de equipo y software en la organización**

  Es recomendable realizar un inventario de hardware y software en el caso de que la empresa ya cuente con equipos y software disponibles. El tipo de equipo, modelo, fabricante etc. Edad estimada de equipo. Vida proyectada del equipo. Ubicación del equipo.

- ✓ **Proceso de estimación de las cargas de trabajo presentes y futuras.**

  Primero se debe estimar las cargas de trabajo, tanto actuales, como las proyectadas para el futuro en la red.

  Identificar los requerimientos generales del hardaware y software, como las características que deben tener para mantener el tráfico de paquetes primordiales ya identificados y elegidos. Ya que en un sistema de red, los equipos realizan diversas tareas y requieren diferentes permisos de acceso, etc., podemos encontrar, que no todos pueden ejecutar las mismas aplicaciones, será preciso coordinar cuidadosamente los programas elegidos con el equipo necesario. Por ejemplo, es preciso determinar cuanto almacenamiento primario y secundario en línea se requiere para trabajar con los programas de aplicación y sistemas elegidos. Se debe analizar cual será la impresora apropiada, si será la adecuada para la cantidad de impresiones que se manejan. También es preciso tomar en cuenta otros tipos de cargas que circularán por la red, como pueden ser los sistemas de videovigilancia, telefonía IP,etc.

- ✓ **Equipos y sistemas compatibles:** el problema de la compatibilidad es algo que puede ocurrir, existe compatibilidad si los programas, datos o dispositivos electrónicos de un sistema se pueden usar sin modificación en otro. Si todos los componentes de la red provienen del mismo fabricante, es probable que no se presenten problemas con las conexiones compartidas o interfaces entre los diferentes dispositivos. Pero si se requiere conectar un equipo marca X con uno marca Y, pueden surgir problemas. La compatibilidad implica que se puedan conectar varios sistemas entre sí y lograr que funcionen de manera aceptable.

- ✓ **Evaluación del software:** para evaluar el software es importante puntualizar las siguientes características: efectividad de desempeño, eficiencia, facilidad de uso, flexibilidad, calidad de la documentación y soporte del fabricante.

También se debe evaluar los requerimientos de los sistemas operativos, manejadores de base de datos, tipos de aplicaciones, utilerías, software de control, seguridad y administración de la red, lenguajes que serán utilizados para el desarrollo de aplicaciones.

- ✓ **Equipo que se Utilizará:** indicar donde estarán los dispositivos en que cantidad y que función estarán desarrollando.

2.4.2 Interconexión: Algunos aspectos a tener en cuenta en el análisis de requerimientos de interconexción son:

- ✓ Los acuerdos de interconexión entre los equipos, deben incluir la especificación clara de los elementos a utilizar, y deben considerar las normas establecidas por los entes de regulación y estandarización, tales como la ITU y el ETSI.
- ✓ También se requiere señalización de control de transporte, para garantizar la transmisión de los requerimientos de QoS; por lo que es necesario el uso de perfiles de protocolos comunes entre los dominios interconectantes, para soportar servicios tradicionales y nuevos.
- ✓ La seguridad a través de diferentes puntos de interconexión en la red, depende de la implementación de los mecanismos que se decidan emplear para la protección de la red. Se debe prevenir el uso indebido de los recursos e información por parte de otras redes, y además garantizar el cumplimiento de los objetivos de seguridad, tales como: privacidad, autenticación, control de acceso, entre otros.
- ✓ El Enrutamiento es un aspecto crucial para la interconexión, y para permitir las comunicaciones entre todos los usuarios de las redes interconectadas, es necesario planificar el enrutamiento estableciendo las comunicaciones de manera eficiente, y con una calidad de servicio predefinida.
- ✓ Proporcionar calidad de servicio de la interconexión para garantizar un nivel de desempeño óptimo. El tráfico proveniente de la interconexión no debe ser discriminado teniendo en cuenta parámetros como: clases de QoS, métricas de QoS, acuerdos de QoS, etc.
- ✓ Líneas de comunicación: Punto a punto, multipunto, half dúplex, full dúplex, análogas, digitales, 2 o 4 cables, modos de transmisión (Banda base o banda ancha),

métodos de Acceso (Token bus, token ring, bus CSMA/CD), protocolos (HDLC, SDLC, X.25, etc.), anchos de banda, tipo de redes locales (Ethernet, Decnet, etc.), utilización de redes publicas, nacionales y/o internacionales, o líneas privadas.

2.4.3 Tráfico

Estas especificaciones son medidas en términos de tipo (datos, voz o video) y volúmen de datos (bits por segundo, erlangs o número de canales). Una solución es incorporar todos estos requerimientos distintos y de esta manera obtener el total de tráfico en la red. El tráfico de la red se establece cuando un usuario envía mensajes a otro, por lo cual es necesario identificar a cada emisor y receptor y estimar cuanto tráfico enviará a los demás. La estimación del tráfico puede complementarse por un análisis de las aplicaciones que serán usadas en la red. Estimar el volumen de tráfico que será generado por cada aplicación incorporarla a la de los usuarios. Cuando se tienen distintos tipos de tráfico, las estimaciones deber ser expresadas en bits por segundo.

2.4.4 Seguridad

En el análisis de requerimientos de seguridad debe tomar en cuenta el conjunto de bienes informáticos y de datos, a partir de su importancia y el papel que representan para el cumplimiento de las actividades de la organización. Por lo que debe prestarse especial atención a aquellos que son críticos en virtud de la función que realizan o lo servicios que proporcionan, su importancia y el riesgo a que están sometidos.

Este análisis implica:

- ✓ Determinar qué se trata de proteger
- ✓ Determinar de qué es necesario protegerse
- ✓ Determinar cuán probables son las amenazas.
- ✓ Determinar si han ocurrido incidentes de violación a la seguridad.
- ✓ Condiciones de las edificaciones, su ubicación, estructura, disposión de recintos y condiciones contructivas.

2.5 Planificación Estructurada del Cableado

Una vez recopilada toda la información, ésta se procesará para contar con todos los detalles para el diseño. Se analizará el diseño de manera modular, cada módulo corresponderá a cada uno de los subsistemas especificados por el estándar que sea elegido, se considerará: el cuarto de equipos, los cuartos de telecomunicaciones, las rutas del backbone, las rutas del cableado horizontal, la entrada de servicios, las áreas de trabajo, además de los sistemas de tierras físicas.

En este punto, también se debe considerar el tipo de clableado que será instalado en cada una de las áreas, ya sea par trenzado, fibra óptica. Puede que sea necesario que el cableado vertical sea de fibra óptica, debido a sus ventajas en velocidad de transferencia y soporte de distintos tipos de tráfico, con esta elección será necesario tomar en cuenta los materiales y las dictancias entre los puntos de acceso; los mismas especifcaciones deben considerarse en el caso de utilizar par trenzado.

Se comenzará por el cuarto de equipos, se tomará en cuenta que en estas áreas se encuentran los servidores y las principales aplicaciones, se seguirá por los cuartos de telecomunicaciones, lugares de donde partirán los cableados horizontales y donde llegarán los de backbone. Después de seleccionar las mejores ubicaciones de los cuartos, se trazarán las rutas del backbone para interconectarlos, posteriormente los puntos de servicios de las áreas de trabajo y finalmente las rutas entre éstos y los cuartos de comunicaciones que darán como resultado los cableados horizontales.

De esta forma, se creará un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, administradores de red y cualquier otro técnico que trabaje con cables.

La siguiente figura muestra un ejemplo de cableado estructurado con sus principales componentes:

1: Área de trabajo, 2: Toma de equipos, 3: Cableado horizontal, 4: Armario de telecomunicaciones, 5: Cableado vertical.

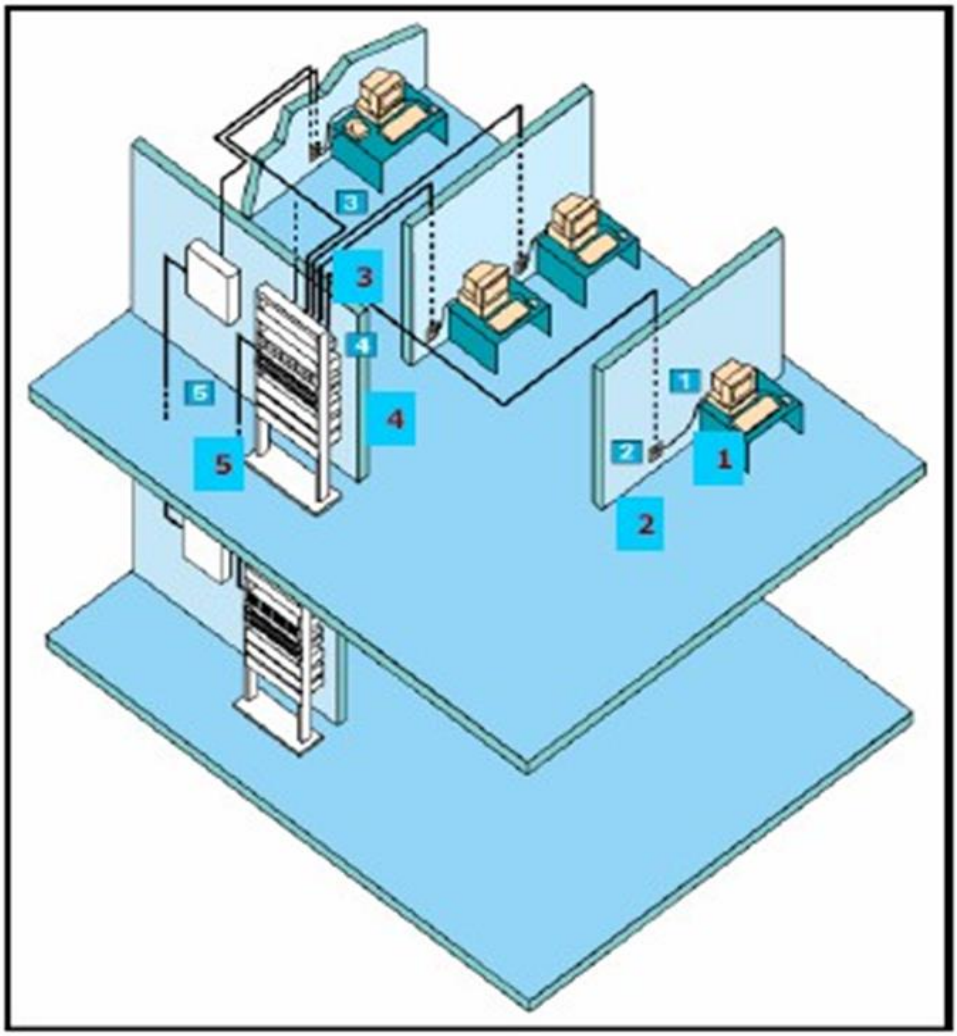

Figura 1.: Principales componentes del cableado estructurado

Hay tres reglas que ayudan a garantizar la efectividad y eficiencia en los proyectos de diseño del cableado estructurado.

- ✓ **La primera regla** es buscar una solución completa de conectividad. Una solución óptima para lograr la conectividad de redes, abarca todos los sistemas que han sido diseñados para conectar, tender, administrar e identificar los cables en los sistemas de cableado estructurado. La implementación basada en estándares está diseñada para

admitir tecnologías actuales y futuras. El cumplimiento de los estándares servirá para garantizar el rendimiento y confiabilidad del proyecto a largo plazo.

- ✓ **La segunda regla** es planificar teniendo en cuenta el crecimiento futuro. La cantidad de cables instalados debe satisfacer necesidades futuras. Se deben tener en cuenta las soluciones de Categoría 5e, Categoría 6 y de fibra óptica para garantizar que se satisfagan futuras necesidades. La instalación de la capa física debe poder funcionar durante diez años o más.
- ✓ **La tercera regla** es conservar la libertad de elección de proveedores. Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar ser mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones.

2.5.1 Cableado de área (recinto)

El cableado del recinto se identificará sobre un plano de las posibilidades de ubicación y los aspectos estructurales; algo muy importante es el tamaño que tendrá, porque de esto dependerá cuanto espacio de suelo se utilizará para la colocación de los equipos, asimismo de la medida en las paredes para los paneles de parcheo u otros equipos. La localización de las tomas de corriente será vital, ya que si no existen suficientes, no están cerca de los equipos o no cumplen con las especificaciones técnicas, se deberá considerar la instalación de estas. El tipo de equipos que se instalarán influye en la selección de estas áreas, ya que se debe tener presente si serán equipos que serán montados sobre mesas, en el piso, o si serán instalados en racks, gabinetes o montados sobre la pared. A estos, también se suma los requerimientos de los sistemas de aire acondicionado o climas artificiales, control de polvo y humedad, iluminación, instalaciones eléctricas reguladas, polarizadas y debidamente aterrizadas (cumpliendo también con las especificaciones del estándar EIA/TIA606), control de incendios con extintores, aspersores de agua o gas halón, protecciones para evitar la propagación de los incendios, así como las posibles fuentes de emisiones de interferencias magnéticas. Todo deberá estar marcado en un plano para su fácil localización.

La facilidad de acceso con puertas que abren hacia fuera del cuarto de equipos, al igual que el paso a los servicios, son una responsabilidad de acuerdo con el estándar EIA/TIA569.

Además, hay que observar la suficiencia de servicios de red en el cuarto de equipos, por lo general este sitio se encuentran los servidores y requerirán estar conectados a la red, de tal manera que se estimará por lo menos una salida por cada equipo que se instale en esta área. Como resultado se obtendrá la ubicación de el o los cuartos de equipos, se indicará que áreas servirá y los servicios que contendrá, así como una lista de los materiales requeridos para su instalación y funcionamiento. Los más comunes a considerar serán racks o gabinetes para montar los servidores y computadoras, paneles de parcheo, y equipos de suministro de corriente ininterrumpida (no breaks) o alimentación eléctrica redundante en caso de fallas.

Para las salidas de los servicios se tomarán en cuenta detalles de ubicación en el área de trabajo, que deben adaptarse a la distribución del mobiliario, la cual se proyectará o en el caso de que ya esté instalada, observada y analizada, ya que la colocación de las salidas y de los ductos, ya sean canaletas o tubería perimetral dependerá de dónde estén ubicados los escritorios, divisiones modulares y otros muebles.

Éstas salidas deberán instalarse a una altura de no más de 30 cm. del piso y con suficiente accesibilidad a los usuarios. En los casos de que sean necesarios los MUTOs (*multi-user telecommunications outlet*, salida de telecomunicaciones multiusuarios) se podrán colocar a una altura mayor para evitar daño en los cables; asimismo se dispondrán en un área accesible a todos los usuarios que se conectarán a él para evitar que los cables pasen por encima de otros muebles, accesos o zonas transitadas. Es necesario considerar servicios para dispositivos tales como impresoras de red, fax automáticos, equipos de videoconferencia, entre otros, que no son propiamente un usuario pero requieren un servicio de red.

El resultado será un plano con la ubicación e identificación de cada una de las salidas de las áreas de trabajo, así como los tipos de servicio que tendrá cada uno (telefonía, datos, video, etcétera.)

- ✓ **Cableado de cuarto de telecomunicaciones**

  Las consideraciones para el cuarto de comunicaciones serán las mismas que para el cuarto de equipos, en cuanto a los espacios, servicios, instalaciones, medidas, etcétera, y se tomará en cuenta los accesos a las rutas de los conjuntos de ductos del

backbone. Además se valorará el montaje de los equipos de terminación del cableado (paneles de parcheo), el equipo activo y las terminaciones de algunos otros servicios como telefonía y video. Cabe destacar, que el cuarto de telecomunicaciones deberá ser de uso exclusivo para estos equipos, por lo que otros controles como centros de carga, encendido de aire acondicionado, bombas de agua deberán ser reubicados; muchos menos utilizar el lugar como oficina o área de trabajo. El punto más importante será la longitud máxima que cubre el cableado horizontal, ya que éste inicia en el cuarto de telecomunicaciones y deberá ser ubicado estratégicamente para cubrir la mayor área posible. Una recomendación es seleccionar varios lugares como posibles ubicaciones, para que cuando se tome la decisión se pueda colocar en el mejor lugar, y en caso de que sean necesarios dos o más cuartos de telecomunicaciones seleccionarlos de las áreas previstas.

Una vez elegido se marcará como un IDF (intermediate distribution facility, distribución intermedia del sistema de cableado) y se continuará con el mismo procedimiento para cada una de las plantas de cada edificio. Después de esto, se decidirá cuál de los cuartos de comunicaciones será el principal, que se marcará como MDF (main distribution facility, distribución principal del cableado). Al analizar la situación se tomarán en cuenta dos cosas: si es un sólo edificio el que se cableará, se buscará la mejor ubicación. En el caso de que sea un ambiente de campus, se estudiará primero en qué edificio será conveniente que se coloque el MDF y posteriormente en qué piso se instalará. En un ambiente de un solo edificio, la ubicación óptima será en el piso de en medio, ya que las distancias de los enlaces serán menores. Esto es: si el cuarto principal se encuentra en el primer piso, las distancias a los primeros pisos será muy corta, pero para llegar al último se deberá recorrer todo el edificio. En cambio al estar en un piso intermedio, las distancias para llegar al primero y al último serán más cortas. La figura 2. Muestra un ejemplo de la posible ubicación de los IDF y del MDF.

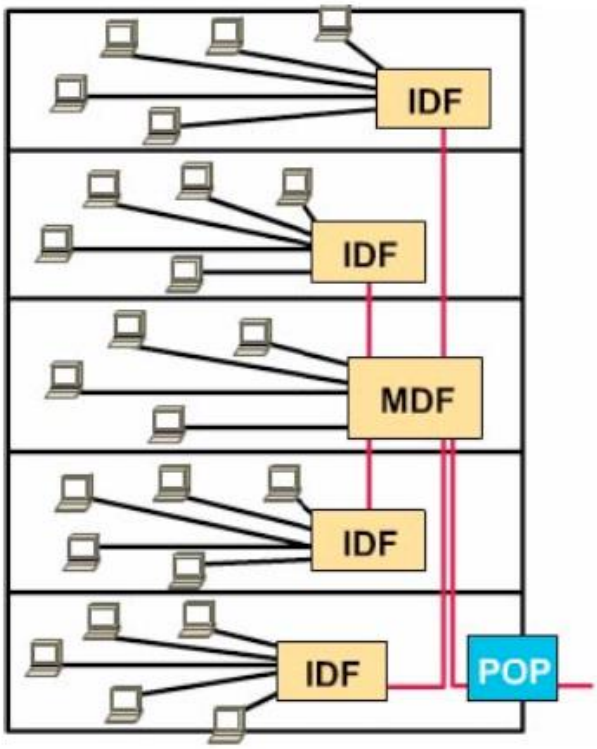

Figura 2.: Ubicación tentativa del MDF en un ambiente de un sólo edificio de múltiples pisos.

Si se trabaja en un ambiente de campus, primero se decidirá el edificio donde se colocará el MDF; se tomará en cuenta en cuál llegará el POP (point of presence, punto de presencia), la entrada de servicios del exterior, tales como las troncales de telefonía, los enlaces inalámbricos, los servicios de conexión a internet o servicios de video. Los materiales más comunes son los mismos que para los cuartos de equipos, y agregando equipo activo de red, tales como hubs, switches, routers, conmutadores, etc.

2.5.2 Cableado Horizontal

Un cable horizontal es el que va del cuarto de telecomunicaciones a la toma del área de trabajo. El cable puede ir en sentido horizontal o vertical. Durante la instalación del cableado horizontal, es importante seguir las siguientes pautas:

- ✓ Los cables siempre deben ser tendidos de forma paralela a la pared.
- ✓ Los cables nunca deben tenderse cruzando el techo en sentido diagonal.
- ✓ El trayecto del cableado debe ser el más directo con la menor cantidad de curvas posibles.

- ✓ Los cables no deben colocarse directamente sobre tejas en el techo.

Una vez instalado el cableado backbone, se debe instalar el cableado horizontal de distribución de la red. El cableado de distribución de la red brinda conectividad a la red desde el cableado backbone. El cableado de distribución de la red, por lo general va desde las estaciones de trabajo de vuelta hasta el cuarto de telecomunicaciones, donde se interconecta al cableado backbone.

- ✓ **Rutas de cableado horizontal:** en este punto se analizarán muchos detalles; el primero es la densidad de los usuarios en cada área y la movilidad de los mismos en el edificio. Esto determinará que tipo de rutas se diseñarán; si la movilidad de los usuarios es poca, entonces se trazarán rutas directas del cuarto de comunicaciones hasta la salida del área de trabajo (rutas *"home-run"*), en cambio, si la movilidad en cierta área es mucha y constantemente se hacen cambios en la distribución del mobiliario y en el número de personas que labora en esa área, se optará por rutas de cableado por zona (que utilizan MUTOs y/o puntos de consolidación intermedios).

  A partir de estas líneas de diseño se pondrá en consideración si el edificio es nuevo o es un edificio ya construido, ya que esto determinará si las rutas se hacen internas (ahogadas en las paredes o en los pisos y/o sobre techos falsos) o perimetrales (encima de las paredes o sobre techos falsos) respectivamente.

  Cuando existe una situación en la que el edificio está en construcción se facilita el diseño de las rutas y éstas quedarán ocultas, pero implica tener una gran visión a futuro. Las rutas de este tipo son permanentes y las salidas de servicios deberán estar muy bien planeadas de acuerdo al crecimiento y la movilidad esperada.

  Para este tipo de rutas se pueden utilizar tubos *Conduit* o tubos de PVC de 1" a 2" y siempre se colocarán registros para facilitar la instalación del cableado. Aunque los estándares internacionales tienen sus recomendaciones.

  Cuando el edificio ya está en funcionamiento se trazarán las rutas perimetrales, hay que valorar que sean funcionales y estéticas. Para las áreas que se utilizarán como oficinas, se dará prioridad a la estética, por lo que la mejor opción para colocar en ductos los cables será la instalación de canaletas. Estos ductos plásticos se pueden encontrar en una gran variedad de colores y estilos, tienen una gran variedad de accesorios para detallar las rutas y darles una mejor vista. En los casos en que las

áreas sean laboratorios, talleres, etc. se instalarán ductos con tubería *Conduit* de .” o de 1”, fijos a las paredes o techos con abrazaderas “omega” o sobre tramos de unicanal.

En este punto se decidirá también que medio se utilizará, ya sea cables de par trenzado o fibra óptica. Al hacer un análisis costo – beneficio, se determinará si el cableado será de cobre, que es más barato pero su limitante es la distancia y la susceptibilidad a interferencias electromagnéticas, o si será de fibra óptica, que no tiene problemas por distancias o interferencias, pero el costo es mucho más elevado así como la dificultad para instalarla.

Es necesario determinar qué tipo de equipo de terminación se utilizará, y esto dependerá del espacio o de la disposición del cuarto de telecomunicaciones. Si el equipo de terminación se montará en racks o en wallbrackets (segmentos de rack montados en la pared). Una vez decidido, se tomará en cuenta las aplicaciones y los tipos de medios utilizados, de tal manera que se podrá elegir entre paneles tipo 110 y LSA (*de Krone*) para telefonía, paneles 110 o paneles de parcheo para datos. En el caso de ser un panel de parcheo, se decidirá el esquema de cableado, si será el 568A o 568B, mismo que será utilizado en los conectores de las salidas en las áreas de trabajo.

Como resultado del análisis, se agregará al plano de cada planta donde se marcarón las posiciones de cada una de las salidas de datos, indicando la cantidad y tipo de servicios, se trazarán también, los puntos de consolidación o MUTOs en caso de que existan, así como al cuarto de comunicaciones al que pertenecen en caso de que existan mas de uno. Sobre el mismo plano se señalarán las rutas, donde se indicarán por medio de líneas de diferentes colores, de qué tipo serán. Es necesario recalcar que es indispensable acotar las distancias y ubicaciones en todos los planos que se trabajen.

Asi mismo, se obtendrá la lista de los materiales a utilizar, que pueden incluir canaletas, tubos, cualquier material para fijar los ductos a la pared, tales como, abrazaderas, unicanal, etc., y al hacer un cálculo de cuantos cables se recibirán se obtendrá el número de paneles de parcheo, racks para montarlo, conectores (plugs y jacks), las cajas para las salidas (en caso de que sean ductos ocultos, sólo los faceplates o carátulas) y dependerá del número de estaciones de trabajo y dispositivos conectados para obtener el número de switches, hubs y demás equipo activo.

Todas las acciones que se deben realizar hasta este momento, se pueden lograr con la ayuda de programas tales como Autocad, Corel Draw o MyHouse que facilitarán el dibujo, la ubicación de las áreas de trabajo, acotar y dibujar a escala y tener una perspectiva general del proyecto; también permitirán, manipular datos de distancias, cantidades, etc., para obtener actualizaciones automáticas de todos los datos.

2.5.3 Cableado Vertical

Cualquier cableado instalado entre la MC (TR primaria, se llama conexión cruzada principal MC, es el centro de la red, allí se origina todo el cableado y se encuentra la mayor parte del equipamiento) y otra TR (Sala de telecomunicaciones) se conoce como cableado backbone. Los estándares establecen con claridad la diferencia entre el cableado horizontal y backbone. El cableado backbone también se denomina cableado vertical. Está formado por cables backbone, conexiones cruzadas principales e intermedias, terminaciones mecánicas y cables de conexión o jumpers usados para conexiones cruzadas de backbone a backbone. El cableado de backbone incluye lo siguiente:

- ✓ TR en el mismo piso, MC a ICC (intermediate cross-connect) e IC a HCC (horizontal cross-connect)
- ✓ Conexiones verticales o conductos verticales entre TR en distintos pisos, tales como cableados MC a IC
- ✓ Cables entre las TR y los puntos de demarcación
- ✓ Cables entre edificios, o cables dentro del mismo edificio, en un campus compuesto por varios edificios.

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

- ✓ **Rutas de cableado vertical o *backbone***

  Las rutas del cableado de backbone se deberán considerar de dos maneras: entre edificios, que se conectarán entre sí en el campus y dentro del edificio, que conectará todas las plantas del mismo con la distribución principal.

  Cuando se analiza la situación de las rutas del *backbone* que conectará los edificios se determinará en cual de ellos se ubicará la distribución principal, ya que el elegido concentrará las conexiones de todos los demás, recibirá la entrada principal de servicios (los servicios de telefonía, conexión a internet, video, etc., del proveedor).

  Se debe especificar cuantos edificios se conectarán por medio de una ruta común, que definirá la densidad de cables con que contará la ruta en cuestión, y a su vez detallará las dimensiones de los ductos y su tipo.

  En cuanto a los ductos de *backbone* que conectan las plantas de un edificio, se deberán hacer consideraciones diferentes.

  Un comienzo será la identificación del cuarto de comunicaciones, nombrado como MDF que recibirá la conexión de servicios que vienen de fuera del edificio (POP), ya que éste será el que reciba las conexiones de los demás pisos. Esto también determinará otros detalles tales como la densidad de cableado que se llevará por una ruta común y la llegada de los servicios. Las rutas del *backbone* deberán ser lo más vertical posible, es decir, la ubicación de los cuartos de comunicaciones será óptima si se encuentran uno sobre otro y se colocarán los ductos por lo menos 3 tubos Conduit de 4” (según el estándar EIA/TIA569) que serán suficientes para el paso del cableado vertical. En los casos en que no se puedan colocar los cuartos alineados, se diseñará una ruta que los conecte y ésta no deberá tener más de dos curvas de 90° entre cada dos registros.

La topología que se utiliza cuando sólo es requerido un punto central de conexión es la de estrella. Cuando las conexiones se vuelven más complejas, es necesario más de un punto de conexión central, entonces la topología a usar es la de estrella extendida o de estrella jerárquica.

En la topología de estrella, el cableado horizontal finaliza en el IDF, a su vez todos los IDF se conectan a un solo punto central, el MDF. En la topología de estrella extendida, el cableado horizontal se termina en el “primer” IDF, éste a su vez se conecta al “segundo” IDF, que se

conecta al MDF. El "primer" IDF se nombra, en esta topología, HCC (horizontal cross-connect, conexión cruzada horizontal), y el "segundo" IDF se llama ICC (intermediate cross-connect, conexión cruzada intermedia).

A este punto se determinará, para los dos sistemas de backbone, el de conexión entre edificios y el de conexión entre los pisos de un edificio, qué tipo de cable se utilizará: de cobre o fibra óptica. Para el caso del cable de cobre se especificará que categoría es necesaria, el número de pares en total, el número de pares por cable y el total de cables. Para el caso de que se requiera fibra óptica se detallará el total de pares, el número de pares por cable, el total de cables y el tipo de fibra (monomodo o multimodo). La tabla 1 muestra las distancias máximas para cada uno de los medios recomendados por el estándar EIA/TIA568.

Es importante, la necesidad de redundancia del backbone. Sólo en los casos en que uno de los enlaces no sea muy confiable o que se requiera conexión continua por si alguno falla. Para esto se deberá tomar en cuenta si serán idénticos los enlaces o el enlace repetido será de emergencia con capacidades menores y si se necesitará diseñar una ruta diferente (como en las ocasiones en que el exceso sea considerado como opción de seguridad en caso de ataque, daño del enlace principal y serán hacia sitios alternos de conexión).

Tabla 1.: Distancias máximas para cada enlace con diferentes medios de transmisión

Tipo de medio de transmisión	Distancia del HCC al MCC	Distancia del HCC al ICC	Distancia del ICC al MCC
Fibra óptica 62.5/125 (Multimodo)	2,000 metros	500 metros	1500 metros
Fibra óptica monomodo	3,000 metros	500 metros	2,500 metros
UTP para voz	800 metros	500 metros	300 metros
UTP para datos	Para todos los casos será de 90 metros		

Un plano con las rutas del backbone del campus y el backbone de cada uno de los edificios será el resultado en el cual se indican las ubicaciones de los registros y los tubos existentes entre ellos así como sus características y acotaciones. De este plano se obtendrá la lista de los materiales a utilizar para su instalación. Los más comunes en este diseño serán tubos Conduit, de PVC, material de construcción para los registros o en su caso registros metálicos y las bases de los ductos

2.5.4 Cableado de Electricidad

Es muy importante que la instalación eléctrica esté muy bien hecha. De no ser así, se corren riesgos importantes.. Los problemas eléctricos suelen generar problemas intermitentes muy difíciles de diagnosticar y provocan deterioros importantes en los dispositivos de red.

Todos los dispositivos electrónicos de una red necesitan corriente eléctrica para su funcionamiento. Los ordenadores son dispositivos especialmente sensibles a perturbaciones en la corriente eléctrica. Cualquier estación de trabajo puede sufrir estas perturbaciones y perjudicar al usuario conectado en ese momento en la estación. Sin embargo, si el problema se produce en un servidor, el daño es mucho mayor, ya que está en juego el trabajo de toda o gran parte de una organización. Por tanto, los servidores deberán estar especialmente protegidos de la problemática generada por fallos en el suministro del fluido eléctrico.

Todos los dispositivos de red deben estar conectados a enchufes con tierra. Las carcasas de estos dispositivos, los armarios, las canaletas mecánicas, etc., también deben ser conectados a tierra. Toda instalación debe estar conectada a la tierra del edificio. Por tanto, habrá que comprobar que el número de picas de tierra que posee es suficiente para lograr una tierra aceptable.

Algunos factores eléctricos que influyen en el funcionamiento del sistema de red son los siguientes:

- ✓ Debe existir potencia eléctrica en cada nodo, especialmente en los servidores, que son los que soportan más dispositivos, por ejemplo, discos. A un servidor que posea una fuente de alimentación de 200 vatios no le podemos conectar discos y tarjetas que superen este consumo, o incluso que estén en el límite. Hay que guardar un cierto margen de seguridad si no queremos que cualquier pequeña fluctuación de corriente afecte al sistema. Los grandes servidores corporativos suelen tener fuentes de alimentación de mayor potencia con objeto de poder alimentar más hardware y, además, redundantes para evitar problemas en caso de fallos en la fuente.
- ✓ La corriente eléctrica debe ser estable. Si la instalación eléctrica es defectuosa, deberemos instalar unos estabilizadores de corriente que aseguren los parámetros básicos de la entrada de corriente en las fuentes de alimentación de los equipos. Por ejemplo, garantizando tensiones de 220 voltios y 50 Hz de frecuencia. El estabilizador

evita los picos de corriente, especialmente los producidos en los arran- ques de la maquinaria.

- ✓ Correcta distribución del fluido eléctrico y equilibrio entre las fases de corriente. En primer lugar, no podemos conectar a un enchufe de corriente más equipos de los que puede soportar. Encadenar ladrones de corriente en cascada no es una buena solución. Además, las tomas de tierra (referencia común en toda comunicación) deben ser lo mejores posibles.
- ✓ Si la instalación es mediana o grande, deben instalarse picas de tierra en varios lugares y asegurarse de que todas las tierras de la instalación tienen valores similares. Una toma de tierra defectuosa es una gran fuente de problemas intermitentes para toda la red, además de un importante riesgo para los equipos.
- ✓ Garantizar la continuidad de la corriente. Esto se consigue con un SAI (Sistema de Alimentación Ininterrumpida) o UPS.

  Normalmente, los sistemas de alimentación ininterrumpida corrigen todas las deficiencias de la corriente eléctrica: actúan de estabilizadores, garantizan el fluido frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etc.

  El SAI contiene en su interior unos acumuladores que se cargan en el régimen normal de funcionamiento. En caso de corte de corriente, los acumuladores producen la energía eléctrica que permite cerrar el sistema de red adecuadamente, guardar los datos que tuvieran abiertos las aplicaciones de los usuarios y cerrar ordenadamente los sistemas operativos.

  Si además no queremos vernos obligados a parar nuestra actividad, hay que instalar grupos electrógenos u otros generadores de corriente conectados a nuestra red eléctrica. Básicamente hay dos tipos de SAI:

  SAI de modo directo. La corriente eléctrica alimenta al SAI y éste suministra energía constantemente al ordenador. Estos dispositivos realizan también la función de estabilización de corriente.

  SAI de modo reserva. La corriente se suministra al ordenador directamente. El SAI sólo actúa en caso de corte de corriente. Los servidores pueden comunicarse con un SAI a través de alguno de sus puertos de comunicaciones, de modo que el SAI informa al servidor de las incidencias que observa en la corriente eléctrica.

Actividad 2.: Caso Práctico

Realiza un listado de requerimientos, evaluando hardware, software, tráfico, interconexión y seguridad para el análisis y diseño de redes, en los distintos tipos de modelos de negocios que se presentan a continuación:

1. Asesoría: Una asesoría cuenta con unordenador que se dedicará a consultas de tipo fiscal, laboral, contable y de telecomunicaciones. Para cada caso es necesario acceder a internet de forma segura y casi siempre se usarán productos distintos ´para los mismos clientes.

2. Empresa de diseño gráfico: Existen tres ordenadores que usan los diseñadores gráficos, cada uno está espespecializado en un aspecto en concreto: diseño vectorial, retoque forográfico y maquetación; por tanto, un mismp proyecto debe ser retocado por todos los diseñadores. Los archivos suelen ser muy grandes.

3. Empresa de desarrollo de software: En un edificio de la compañía trabajan distintos programadores que deben compartir muchas ideas, dudas, etc. Tienen sala de reuniones, sala de relajación, cafetería, etc. pero a veces desean comunicarse de forma rápida. Además debe existir una comunicación en tiempo real con otros edificios de la compañía ubicados alrededor del mundo.

III. DISEÑO FÍSICO

OBJETIVOS:

- Reconocer los elementos (canalizaciones, cableados, armarios, y rosetas, entre otros) de una instalación de infraestructura de red de un edifico a partir del diseño físico del proyecto.
- Seleccionar los elementos de conexión, arquitectura de red y topología más adecuados, a una determinada instalación de red de telecomunicaciones, según unas necesidades previas definidas

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

En esta sección de aprendizaje, veremos que para el diseño físico de la red, se deben contemplar documentos tales como planos de los edificios, plantas arquitectónicas con acotaciones, medidas y etiquetas o nombres de cada espacio en el plano. Además se deberá reunir información del tipo de paredes, pisos, techos y de las instalaciones existentes en el edificio (las instalaciones de energía eléctrica, de tierras físicas, de agua, drenaje, aire acondicionado, e incluso de cableado estructurado existente) que puedan influir en el desarrollo del proyecto. Estas, y otras evidencias, como la topología de la red, serán fundamentales para elaborar un diseño físico de la red acorde a los requerimientos presentados.

III. Diseño Físico

Introducción

La información inicial para el diseño físico será de gran importancia para la toma de decisiones a lo largo del proyecto. Esta información comprende muchos aspectos que se pueden dividir en 3: el aspecto físico, económico y de crecimiento de la organización.

La información con aspecto físico deberá reunir documentos tales como planos de los edificios, plantas arquitectónicas con acotaciones, medidas y etiquetas o nombres de cada espacio en el plano. Además se deberá reunir información del tipo de paredes, pisos, techos y de las instalaciones existentes en el edificio (las instalaciones de energía eléctrica, de tierras físicas, de agua, drenaje, aire acondicionado, e incluso de cableado estructurado existente) que puedan influir en el desarrollo del proyecto.

De la misma manera, se obtendrá la información de dónde serán instalados los equipos de cómputo en las áreas de trabajo, la densidad de personal en el área y la movilidad que éste tendrá a lo largo de su estancia en el edificio.

Conocer las aplicaciones que se implementarán en el sistema de comunicaciones, tales como telefonía, datos y video y sus requerimientos serán de vital importancia, ya que permitirá seleccionar características técnicas, de diseño y localización de los equipos y materiales a utilizar.

El perfil de crecimiento de la empresa, dará al diseño una flexibilidad que se ajuste a los cambios futuros y a que sea posible las ampliaciones y restructuraciones.

Toda esta información se obtendrá del personal de la empresa, se consultará a los técnicos para obtener diagramas, planos, esquemas y localizaciones de equipos, instalaciones y conductos; el personal administrativo podrá proporcionar información acerca del crecimiento de los últimos meses, incluso de los últimos tres años, tanto de personal como en las áreas de trabajo, así como del presupuesto y de los tiempos planeados para ejercerlo. Algunas recomendaciones para la obtención de información:

- ✓ Solicite la información siempre en formato escrito o electrónico.
- ✓ Nunca crea o asuma, siempre verifique.
- ✓ Siempre tenga a mano documentos como estándares de cableado o de seguridad.
- ✓ En los casos que no se tenga la información, solicite que la generen en el momento.
- ✓ Verifique que la información recibida sea lo más actualizada posible.

Para finalizar esta etapa y poder continuar, será necesario ordenar la información de acuerdo a ciertos criterios lógicos; por información financiera, de recursos humanos, documentación técnica, etc. Todo esto permitirá contrastar la información y tener un control absoluto sobre la misma y de esta manera poder observar qué se tiene y qué hace falta.

3.1 Plano General de la Empresa

Antes de instalar una red, los técnicos deben realizar un diseño previo en el que analizarán todos los espacios que recorreará a red, los obstáculos que pueden plantearse, las distancias entre puntos críticos, etc.

Para representar una red en un plano se utilizan los modelos de planos técnicos del edificio, la zona o la ubicación. Estos son diseñados por personal experto, que utilizan técnicas de diseño arquitectónico.

En un proyecto de construcción existen diferentes tipos de planos. Estos se agrupan según su categoría, entre las que se destacan las siguientes:

Tabla 2: Planos generales de una construcción

Plano eléctricos	Planos arquitectónicos	Planos de cañerías	Planos de telecomunicaciones
Comienzan con la letra “E”. Recogen todas las características del tendido eléctrico y puntos de suministro, distribución y terminación	Comienzan con la letra “A”. Reflejan las características de suelos, paredes y techos, entre otros. Son muy útiles para diseñar las canalizaciones.	Comienzan con “P”. Identifican todos los sistemas de cañerías instalados en el edificio. También resultan útiles para diseñar las canalizaciones.	Comienzan con la “T”. Representan los elementos de telecomunicaciones, así como la arquitectura de la red. Este es el tipo de planos que deberemos diseñar y con los que tendremos que trabajar.

Este conjunto de planos serán imprescindibles para el diseño físico de la red, de esta manera se podrán contemplar todos los elementos que conforman las áreas donde el sistema de red tendrá de una u otra forma impacto en la distribución de todos estos elementos; y como estos también impactarán el diseño y la implantación de la red.

3.1.1 Edificio

El edificio donde será instalada la red, debe ser recorrido y analizado con la compañía de personal experto en edificación y con los planos arquitectónicos, donde puede incluirse la red eléctrica, la red de conexión a tierra, etc.. Estos planos permitirán que el diseño físico se realice de la manera más precisa posible.

Es habitual que se haga una representación por planta, es decir, en un edificio de tres plantas habría tres planos de planta, uno por cada piso.

3.1.2 Pisos

Se deben hacer ciertas consideraciones a la hora de seleccionar el cableado horizontal y vertical, ya que contienen la mayor cantidad de cables en el diseño de la red; cada piso puede contener especificaciones, medidas y materiales distintos, estos deben ser analizados individualmente, marcando de manera especifica los requerimientos de diseño para cada uno de ellos.

Este anaálisis individual por piso, será también una guía para elegir el lugar apropiado para la instalación del cuarto de telecomunicaciones primario y demás distribución de los equipos. Los costes en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado, pueden ser muy altos. Para evitar estos costes, la distribución debe ser diseñada para facilitar el mantenimiento y la relocalización de áreas de trabajo.

3.1.3 Recinto

Se define como la **zona donde están los distintos puestos de trabajo** de la red. En cada uno de ellos habrá una roseta de conexión que permita conectar el equipo o equipos que se quieran integrar en la red.

El área de trabajo comprende todo lo que se conecta a partir de la roseta de conexión hasta los propios dispositivos a conectar (ordenadores e impresoras fundamentalmente). Están también incluidos cualquier filtro, adaptador, etc., que se necesite. Estos irán siempre conectados en el exterior de la roseta. La instalación se utiliza para transmitir voz, datos u otros servicios, cada uno de ellos deberá tener un conector diferente de la propia roseta de conexión.

Al cable que va desde la roseta hasta el dispositivo a conectar se le llama latiguillo y no puede superar los 3 metros de longitud.

3.2 Arquitectura de la red

La arquitectura de red es un marco para la especificación de los componentes físicos de una red y de su organización funcional y configuración, sus procedimientos y principios operacionales, así como los formatos de los datos utilizados en su funcionamiento.

En la telecomunicación, la especificación de una arquitectura de red puede incluir también una descripción detallada de los productos y servicios entregados a través de una red de comunicaciones, así como la tasa de facturación detallada y estructuras en las que se compensan los servicios.

La arquitectura de la red muestra una vista de alto nivel de la red, incluyendo la ubicación de los componentes principales o importantes.

La arquitectura de red no solo es necesaria para un diseño sólido, sino que también es esencial para mantener el rendimiento requerido en el tiempo.

La definición de la arquitectura de la red debe ser lo mas independiente posible del proveedor de equipo, es decir, debe ser expresada en términos funcionales. Durante el desarrollo de alternativas de diseño es necesario, antes que nada, escoger las posibles topologías con respecto a las especificaciones funcionales y ambientales (esto esta estrictamente relacionado con la elección del medio de transmisión). Después, es necesario acoplar cada topología con el medio de acceso mas apropiado.

Para definir la configuración física de la red se produce una representación visual de la red en la cual se presentan y localizan los componentes, volumen de trafico, tiempos de respuesta y aplicaciones que se ejecutan en cada localidad. Además, existen otros atributos que definen la información ambiental de cada componente de la red, tales como: tamaño del componente, tamaño en bytes de los datos (para calcular la memoria), distribución de canal y distribución de numero de dispositivos por canal en los sistemas de banda ancha, asignación de prioridades de acceso a los servicios, tipo de procesamiento, interconectividad o dependencia de otras tareas, etc.

El método para configurar una red es básicamente el mismo en todos los casos. Esencialmente, son tres los factores a considerar:

- ✓ El equipo a instalar en la periferia.
- ✓ El equipo a instalar en el o los centros.
- ✓ Las enlaces de comunicación que conectan los equipos.

Una vez que se tiene una vista preliminar de la red, se puede comenzar el diseño de la red física.

La red física se define en términos de un número de factores, incluyendo:

- ✓ Uso de enlaces de comunicación públicos o privados.
- ✓ Velocidad de los enlaces de comunicación.
- ✓ Colocación física de los enlaces de comunicación.
- ✓ Uso de concentradores y/o multiplexores.
- ✓ Número, capacidad y localización de los centros de procesamiento.
- ✓ Uso de procesadores frontales.
- ✓ Terminales y distribución de inteligencia.
- ✓ Colocación física de terminales.

Una vez que el diseño preliminar de la red se ha completado, el siguiente paso es optimizarlo. El propósito de la optimización es minimizar el costo y los tiempos de respuesta de la red, obteniendo la ruta mínima posible entre localidades, proporcionando varias alternativas de ruteo de la información (previendo que ciertas líneas se saturen o sufran algún accidente), equilibrar el trafico en la red y tratar de soportar la mayor cantidad de datos transmitidos.

3.2.1 Topología

Podemos considerar tres aspectos diferentes a la hora de considerar una topología:

- **La topología física,** que es la disposición real de los host y de los cables (los medios) en la red.
- **La topología lógica** de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring). La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet. La transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de

forma secuencial a cada host. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

- **La topología matemática**, donde los mapas de nodos y los enlaces a menudo forman patrones.

El término topología en redes, se refiere a la ubicación física de las computadoras, cables y otro componentes de la red. Topología es un término que muchos profesionales utilizan cuando se refieren al diseño básico de una red.

La elección de una topología sobre otra va a tener un fuerte impacto sobre:

- El tipo de equipo que la red necesita
- Las capacidades de este equipo
- Desarrollo de la red
- La forma en que la red es manejada

Sabiendo sobre las distintas topologías, se llega a entender más las capacidades de los distintos tipos de redes. Para que las computadoras puedan compartir archivos y poder transmitirlos entre ellos tienen que estar conectados. La mayoría de las redes usan un cable para conectar una computadora a otra, para hacer esto posible. Sin embargo, esto no es tan simple como conectar un cable de una computadora a otra. Diferentes tipos de cable requieren diferentes tipos de arreglos. Para que una topología en red funcione bien, necesita un diseño previo. Por ejemplo, una topología en particular puede determinar el tipo de cable que se necesita y como ese cableado recorre el piso, las paredes y el techo. Se debe especificar y plantear una topología de red que satisfaga los requerimientos de la empresa

3.2.2 Tecnología

La eleccción del tipo de tecnología a implementar dependerá de los requerimientos que han sido analizados anteriormente, tomándo en cuenta aspectos de tráfico, servicios proporcionados por la red, etc.

Una de las tecnologías más utilizadas en redes empresariales LAN son las del IEE 802.3. Hay diferentes variantes dentro del estándar IEEE 802.3, si lo que se busca es implementar una LAN; y esta tecnología da opciones de ancho de banda (10 Mbps, 100Mbps, 1000 Mbps, 10 Gigas, 100 Gigas, etc.).

La redes LAN que se han impuesto en el mercado por su buena relación costo-desempeño son las conocidas como Ethernet o estándar IEEE 802.3 (Ethernet, FastEthernet, GigabiEthernet, 10 Gigas, etc.). Luego de reconocer el estándar apropiado para su red, realice una selección del tipo de Red Ethernet / IEEE 802.3 que usted recomienda para la LAN de la dependencia y justifique su selección, comparándola con otras en cuanto a topología, costo-desempeño, ancho de banda, etc.

O sea, que la red o estructura de interconexión debe satisfacer la carga de tráfico previamente calculada para la cantidad de usuarios y aplicaciones.

Elabore una propuesta de ancho de banda (Mbps) requerido para la red, tomando en consideración la carga de tráfico de la red en dependencia de las aplicaciones, servidores, cantidad de usuarios, interacción típica y frecuencia de interacciones por usuario.

3.2.3 Componentes

Realice la selección del hardware y software necesario para la red, la cantidad requerida y características específicas; la ubicación exacta de cada uno de los componentes debe ser reproducido en el plano físico de la red. Entre los componentes tenemos: Tarjetas de Interfaz (NIC), Repetidores (Hub), transceptores (transceivers), Conmutadores (Switch), Enrutadores (Routers), Modems, fuentes de respaldo (UPS) , Cortafuegos o Firewalls, Servidores (sitios web, de correo , de ficheros, de bases de datos, etc) , estaciones de trabajo adicionales, etc.

A la hora de seleccionar los productos debe tener en consideración:

- Es importante la correcta selección de los servidores acorde a los servicios (sitios web, correo, de ficheros, de base de datos, DHCP, DNS etc.)
- Sistemas Operativos a emplear, de acuerdo a sus características incorporadas en ellos (Microsoft Windows, Linux, Ubuntu, etc.).
- Las estaciones de trabajo tienen que estar actualizadas con respecto a los sistemas operativos seleccionados.
- Las herramientas de hardware software para el monitoreo y gestión de la red.
- Componentes de seguridad asociados a los requerimientos y tecnologías propuestas.
- Identificar los productos específicos en el mercado para conocer sus cualidades técnicas y presupuesto.

- Determinar la necesidad y efectividad de la documentación de cada producto en perspectiva (si está completa, clara, etc).
- Considerar la reputación del fabricante y distribuidor.
- Hacer una selección comparando el presupuesto de lo que necesita el usuario y analizar la calidad de los productos y costos.
- Valorar el costo de los paquetes de software, su licencia de explotación, costo de actualizaciones, etc.
- Considerar las implicaciones de seguridad para: Acceso remoto, Acceso local, Acceso a ficheros, Acceso a hardware, Acceso a grabación etc.
- Verificar la compatibilidad de todos los componentes.

Para la selección de los equipos de interconexión (Router / Switch capa 3) hay que analizar varias opciones (no menos de tres) a fin de hacer comparaciones y fundamentar la selección. Igualmente para los servidores, pues debe recordarse que es un exigencia técnica y administrativa de evitar favoritismos e ilegalidades con determinados vendedores.

3.3 Planificación Estructurada del cableado

Los cambios que se deben realizar en las instalaciones de red, especialmente en su cableado, son frecuentes debido a la evolución de los equipos y a las necesidades de los usuarios de la red. Esto nos lleva a tener en cuenta otro factor importante: la flexibilidad.

Un sistema de cableado bien diseñado debe tener al menos estas dos cualidades: seguridad y flexibilidad. A estos parámetros se le pueden añadir otros, menos exigentes desde el punto de vista del diseño de la red, como son el coste económico, la facilidad de instalación, etc.

La estructuración del cable se consigue construyendo módulos independientes que segmenten la red completa en subsistemas de red, independientes pero integrados, de forma que un subsistema queda limitado por el siguiente subsistema. Estos subsistemas siguen una organización jerarquizada por niveles desde el sistema principal hasta el último de los subsistemas.

Podemos concluir que el cableado estructurado es una técnica que permite cambiar, identificar, mover periféricos o equipos de una red con flexibilidad y sencillez. Según esta definición, una solución de cableado estructurado debe tener dos características:

modularidad, que sirve para construir arquitecturas de red de mayor tamaño sin incrementar la complejidad del sistema, y flexibilidad, que permite el crecimiento no traumático de la red. El sistema de cableado puede ser centralizado o distribuido, en el mismo deben tomarse diferentes consideraciones tales como: si se requiere redundancia en diferentes lugares, si se requiere de múltiples fibras, o pares de cobre en un mismo cable, múltiples cables en un mismo conducto, múltiples conductos por un mismo camino etc.

A continuación, elaborar el plano físico de la red LAN con todos los detalles y con las medidas exactas en metros, tomando en cuenta:

- ✓ Tamaño de los locales, pisos, edificio, distancia entre edificios, etc.
- ✓ Ubicación de los usuarios y equipos
- ✓ Posición de las canaletas y distribuidores (techos, pisos, etc.)
- ✓ Precisar la posición de los armarios, gabinetes, etc.
- ✓ Closets de alambrado (racks, paneles, bandejas, etc.)
- ✓ Cuartos de conexión

El plano físico también debe ser preciso en el cuarto de control de la red, teniendo en consideración los elementos anteriores. A partir del plano físico se calculará la cantidad de cables, tomas de pared, armarios, cantidad de canaleta, etc.

Para determinar cuál es el mejor cable para un lugar determinado habrá que tener en cuenta distintos factores:

- ✓ Carga de tráfico en la red
- ✓ Nivel de seguridad requerida en la red
- ✓ Distancia que debe cubrir el cable
- ✓ Opciones disponibles del cable
- ✓ Presupuesto para el cable

Cuanto mayor sea la protección del cable frente al ruido eléctrico interno y externo, llevará una señal clara más lejos y más rápido.

3.3.1 Fundamento de Instalación del cable

El cableado y su instalación representa en la mayoría de las redes el 50% del costo total del sistema. Por lo que requiere de una administración efectiva. Para poder planear una instalación de cableado se debe responder preguntas tales como:

¿ Cual es la localización de los nodos?

¿ Cuál es el impacto de la dispersión geográfica?

¿ Los ductos actuales soportan cableado adicional?

¿ Que tan volátil es el ambiente (reubicaciones)?

¿ Existen fuentes de interferencia electromagnética?

Las reglas para una instalación de cableado exitosa son:

- ✓ Probar el cable (todos sus pares) y documentar los resultados.
- ✓ Elaborar planos para identificar rutas de cableado y equipos.
- ✓ Etiquetar cada conector y cada segmento de cable.
- ✓ Mantener el cable al menos 30 cms. lejos del cable eléctrico.
- ✓ Los cables de LAN's deberán correr perpendicular al cable eléctrico y separado a 30 cms.
- ✓ Para evitar averías al cable, debe ponerse en canaletas.
- ✓ Halar los cables en grupo, a un punto de distribución central.
- ✓ Asegurar los cables con "sostenedores".
- ✓ No colocar los cables sobre tos materiales del techo.
- ✓ No colocar los cables en donde la gente pueda pisarlos, tropezarse, romperlos o aplastarlos con muebles o sillas.

La instalación consiste en la ejecución ordenada, según las directrices del proyecto de instalación de un conjunto de tareas que revierten en proporcionar el servicio que necesitaba el cliente que solicitó la instalación.

Algunas de estas tareas se pueden superponer en el tiempo y habrá que tener esto en cuenta al confeccionar el calendario de instalación. A continuación describimos algunas de estas tareas:

- **Instalación de las tomas de corriente.** Esta tarea suele realizarla un electricista, pero desde el punto de vista del proyecto debemos asegurarnos de que hay suficientes tomas de corriente para alimentar todos los equipos de comunicaciones.
- **Instalación de rosetas y jacks.** Es la instalación de los puntos de red finales desde los que se conectarán los equipos de comunicaciones sirviéndose de latiguillos. La mayor parte de estas conexiones residirán en canaletas o en armarios de cableado.

- **Tendido de los cables.** Se trata de medir la distancia que debe recorrer cada cable y añadirle una longitud prudente que nos permita trabajar cómodamente con él antes de cortarlo. Debemos asegurarnos de que el cable que utilizaremos tenga la certificación necesaria.
- **Conectorización de los cables** en los patch panels y en las rosetas utilizando las herramientas de crimpado apropiadas. A esto se le denomina cross-connect.
- **Probado de los cables instalados.** Cada cable construido y conectorizado debe ser inmediatamente probado para asegurarse de que cumplirá correctamente su función.
- **Etiquetado y documentación del cable y conectores.** Todo cable debe ser etiquetado en ambos extremos, así como los conectores de patch panels y rosetas, de modo que queden identificados unívocamente.
- **Instalación de los adaptadores de red.** Gran parte de los equipos informáticos vienen ya con la tarjeta de red instalada, pero esto no es así necesariamente.
- **Instalación de los dispositivos de red.** Se trata de instalar los concentradores, conmutadores, puentes y encaminadores. Algunos de estos dispositivos deben ser configurados antes de prestar sus servicios.

Figura 3.: Algunos modelos de etiquetas para cables

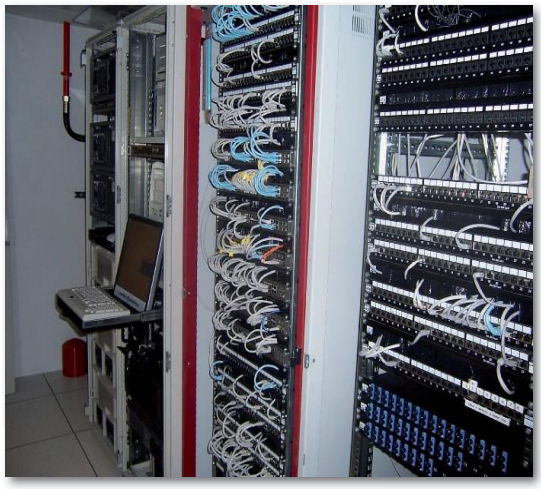

Figura 4.: Vista de un cuarto de comunicaciones instalado con cableado estructurado y certificado.

3.3.2 Montaje del cable

Durante el montaje del cableado, este se tiende desde el área de trabajo a las salas individuales. Se rotula cada cable en ambos extremos para permitir su identificación. En el área de trabajo, se debe tender cable adicional de modo que haya suficiente para trabajar durante la terminación. Si un cable va a pasar detrás de una pared, se saca en el extremo de terminación para que esté listo para la etapa siguiente. Una construcción nueva por lo general, representa un desafío menor que una remodelación, porque existen menos obstrucciones. La mayoría de las construcciones nuevas no requieren de una planificación especial. Las estructuras que sirven de apoyo a los cables y terminales se construyen, por regla general, según se necesiten. Sin embargo, es esencial la coordinación en el sitio de trabajo. Los otros trabajadores deben conocer las ubicaciones de los cables de datos para evitar que se dañen los que han sido instalados recientemente.

La operación de instalación de cableado comienza en el área de trabajo. Esta área por lo general se encuentra cerca del área de comunicación, ya que en ella se terminarán los extremos de todos los cables. La preparación adecuada del equipamiento ahorrará tiempo durante el proceso de tendido de cable. Los distintos tipos de tendidos de cable requieren diferentes configuraciones de equipo. El cableado de distribución de la red normalmente utiliza varios carretes pequeños de cable. El cableado backbone en general necesita un sólo carrete de cable grande.

- ✓ **Tendido de los cables hasta los jacks**

  En el área de trabajo, se deben tender los cables hasta un jack o toma. Si se utilizan conductos para tender cables detrás de la pared desde el techo hasta las tomas, se puede insertar una cinta pescacable o sonda dentro de la caja de la toma en un extremo del conducto y empujar hacia arriba por el conducto hasta el techo. Luego, se puede unir el cable directamente a la cinta pescacable y tirar hacia abajo desde el techo, y hacia fuera por la caja de toma. Algunas paredes, tales como las de hormigón o ladrillo, no pueden tener tendidos de cables detrás de ellas. En estos casos se utilizan canaletas para montar sobre la superficie. Antes de instalar los cables, las canaletas para montar sobre la superficie deben estar aseguradas contra la pared según indiquen las instrucciones del fabricante. Una vez que se ha tendido el cable hasta las tomas, el instalador vuelve a la TR para tirar del cable en ese extremo.

- ✓ **Fijación del cable**

  El último paso del proceso de preparación, es asegurar los cables de forma permanente. Existen muchos tipos de fijadores, como los ganchos J, y las ataduras de gancho y bucle. Nunca se deben atar los cables de la red a los de electricidad. Esta puede parecer la manera más práctica de hacer las cosas, en especial cuando se trata de cables individuales o pequeños grupos de cables. Sin embargo, esto viola los códigos sobre electricidad. Nunca se debe fijar cables a los caños de agua o del sistema de riego.

  Los cables de red de alto rendimiento tienen un radio mínimo de curvatura que no puede ser mayor que cuatro veces el diámetro del cable. Por lo tanto, se deben usar fijadores que admitan el radio mínimo de acodamiento. El espacio entre fijaciones puede definirse en las especificaciones del trabajo. Si no se especifica el espaciado, los fijadores deben estar colocados a intervalos no mayores de 1,5 m (5 pies). Si se instala en el techo una bandeja de cable o canasto, no se necesita una fijación permanente.

Figura 5.: Instalación de cableado estructurado

3.3.3 Recintos y estructura de un patch panel

Un patch panel es un dispositivo de interconexión a través del cual los cables instalados se pueden conectar a otros dispositivos de red o a otros patch panels.

Un Patch-Panel posee una determinada cantidad de puertos (RJ-45 End-Plug), donde cada puerto se asocia a una placa de circuito, la cual a su vez se propaga en pequeños conectores de cerdas. En estos conectores es donde se ponchan las cerdas de los cables provenientes de los cajetines u otros Patch-Panels. La idea del Patch-Panel además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan equipos en una red, de una mejor manera.

Sobre un armario se instalan patch panels que se conectan al cableado de la instalación por todo el edificio y otros patch panels que se conectan a los conectores de los dispositivos de red, por ejemplo a los hubs o conmutadores.

Figura 6.: Vistas de un rack para cableado estructurado.

Después, una multitud de latiguillos conectarán unos patch panels con los otros. De este modo, el cambio de configuración de cableado se realizará cambiando la conectividad del latiguillo sin tener que cambiar nada del cableado largo ni las conexiones a los dispositivos de red.

El cable largo instalado conectará las rosetas con los patch panels. Las rosetas (outlets) pueden adoptar multitud de formas dependiendo del lugar en que se fijen (canaleta, pared, etc.), del tipo de cable a conectar y del conector que el usuario utilizará. La roseta presenta

un conector por un lado y una estructura de fijación de los cables de pares por su reverso, a la que serán crimpados.

3.3.4 Distribución de los equipos

Para las salidas de los servicios se tomarán en cuenta detalles de ubicación en el área de trabajo, que deben adaptarse a la distribución del mobiliario, la cual se proyectará o en el caso de que ya esté instalada, observada y analizada, ya que la colocación de las salidas y de los ductos, ya sean canaletas o tubería perimetral dependerá de dónde estén ubicados los escritorios, divisiones modulares y otros muebles.

Éstas salidas deberán instalarse a una altura de no más de 30 cm. del piso y con suficiente accesibilidad a los usuarios. En los casos de que sean necesarios los MUTOs (*multi-user telecommunications outlet*, salida de telecomunicaciones multiusuarios) se podrán colocar a una altura mayor para evitar daño en los cables; asimismo se dispondrán en un área accesible a todos los usuarios que se conectarán a él para evitar que los cables pasen por encima de otros muebles, accesos o zonas transitadas. Es necesario considerar servicios para dispositivos tales como impresoras de red, fax automáticos, equipos de videoconferencia, entre otros, que no son propiamente un usuario pero requieren un servicio de red.

El resultado será un plano con la ubicación e identificación de cada una de las salidas de las áreas de trabajo, así como los tipos de servicio que tendrá cada uno (telefonía, datos, video, etc.)

3.3.5 Equipos para probar el cableado

Las herramientas de diagnóstico se utilizan para identificar los problemas potenciales y los existentes en una instalación de cableado de red. Los analizadores de cables se utilizan para descubrir circuitos abiertos, cortocircuitos, pares divididos y otros problemas de cableado. Una vez que el instalador haya terminado un cable, éste deberá ser conectado a un analizador de cable para verificar que la terminación haya sido correctamente realizada. Si el cable está asignado al pin incorrecto, el analizador de cable indicará el error en el cableado. La caja de herramientas de cada instalador de cable debería incluir un analizador de cables. Una vez analizados los cables para determinar su continuidad, pueden certificarse por medio de medidores para certificación.

Entre los equipos para probar el cableado están:

- ✓ **Ohmiómetro**

  Se utiliza para verificar las divisiones. Primero, verifique los pares para determinar la presencia de cortocircuitos. Si no hubiera cortocircuitos, genere uno en cada par. El ohmiómetro debería detectar un cortocircuito. Si se encuentra un circuito abierto, algo no está funcionando correctamente.

- ✓ **Generador de tonos**

  Se utiliza para determinar si está dividido o abierto. Los equipos de análisis de mayor calidad detectan los pares divididos midiendo la diafonía que se produce entre los pares.

- ✓ **Analizador de cables**

  Se utiliza para inspeccionar los pares divididos. Este tipo de analizador utiliza LED que notifican inmediatamente si hay un problema de polaridad o de continuidad.

- ✓ **Reflectómetro en el dominio del tiempo (TDR)**

  Envía un pulso a través del hilo y luego monitorea los ecos electrónicos que se producen debido a problemas en el cable. Los TDR determinan si hay una falla en el cable y si se trata de un circuito abierto o un cortocircuito. Los TDR también pueden medir la distancia desde el medidor hasta la falla. La señal es reflejada al alcanzar el extremo opuesto del cable, o en el momento en el que encuentra un defecto en el cable. La velocidad de la señal recibe el nombre de velocidad nominal de propagación. Esta es una medida conocida para distintos tipos de cables.

  Cuando un analizador conoce la velocidad a la que viaja la señal, puede medir la longitud del cable midiendo la cantidad de tiempo que lleva para que la señal llegue y sea reflejada. La lectura del TDR generalmente está calibrada en pies o en metros. Si está correctamente ajustado y se usa de manera adecuada, el TDR resulta una manera eficiente de identificar los problemas del cable.

Actividad 3.: Caso Práctico

Ana es una profesora del curso de Administración de redes que ha cambiado de Instituto. En el nuevo centro tienen una única red de ordenadores que consta de 20 equipos, más uno en secretaría, todos cableados con cable coaxial ancho, en una estructura de bus.

La secretaria se queja de que al compartir el acceso a internet con los alumnos, tiene muchos problemas con los virus, y los profesores se quejan de que cuando un equipo se avería, la red no funciona. Todos los equipos llevan sistemas operativos de más de 10 años de antigüedad. Tras hablar con el director. Han decidido comprar 90 equipos y montar tres salas de informática en aulas que no estén separadas más de 15 metros. Además quieren independizar la red de secretaría añadiendo un equipo para dirección, otro para los profesores y para registros académicos.

1.¿Quién usará la red?

2.¿Qué elementos de red desean compartir?

3.¿Crees que le conviene a Ana poner un servidor en la red?

4.¿Le interesa a Ana dejar el aula antigua con cableado coaxial?

5.¿Qué topología le recomiendas para la red alumnos?

6.¿Qué tipos de redes le interesa diseñar para el instituto?

7-¿Qué medio o medios de transmisión sería aconsejable utilizar?

8.¿Si Ana decide cablear con par trenzado, ¿Qué tipo le aconsejarías?, ¿Qué otros elementos del cableado estructurado necesitará para conectar las redes?

9.¿Le interesa cablear algún trozo de la red con fibra óptica?

IV. DISEÑO LÓGICO

OBJETIVOS:

- Diagnosticar el modelo de enrutamiento más adaptado a las especificaciones del proyecto de red que se quiere desarrollar.
- Conocer los tipos de protocolos de enrutamiento, sus características y las funcionalidades que estos le ofrecen a la red para la interconexión y la comunicación entre los usuarios.
- Evaluar los requerimientos del software para la administración de la red y sus herramientas integradas que permiten realizar las distintas tareas de gestión de red, de la forma más sencilla posible.
- Estudiar la situación actual de la red, desde el punto de vista de la seguridad, con el fin de determinar las acciones que se ejecutarán en función de las necesidades detectadas y con ello establecer políticas, objetivos y procesos de seguridad apropiados para gestionar el riesgo, posibilitando obtener resultados conformes con las políticas y objetivos globales de la organización.
- Adquirir destrezas en la elaboración de Diseños de Red (LAN / WAN) mediante la práctica.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Este capítulo comienza por la introducción al concepto y fundamentos de los planes de direccionamiento IP, los criterios a considerar para el diseño de redes de alta complejidad, se busca comprender la importancia de la definición de un buen plan de direccionamiento IP.

Posteriormente se hace referencia a los principios para evaluar un listado de requerimientos esenciales para todo software de administración de red, que incluya también aspectos como la seguridad, que mantengan la funcionalidad, interoperabilidad y la disponibilidad de los recursos de forma transparante para el usuario.

IV. Diseño Lógico

Introducción

El diseño lógico de una red es la forma en que los hosts se comunican a través del medio. Para ello hay que partir del tipo de red, o sea si es una red para oficinas, edificio o para un campus. Si la misma tendrá una topología en estrella o de anillo, si su jerárquica será de dos o tres niveles, totalmente conmutada o enrutada, etc.

En el diseño lógico de la red también forman parte los módulos para el direccionamiento y nombres, la selección de los protocolos de enrutamiento, la seguridad de la red y las estrategias de gestión entre otros. Por lo que se requiere de una planificación detallada de estos puntos.

Es importante conocer los planos de todas las conexiones lógicas existentes en la red (red y subredes), las características de los medios, equipos de interconexión, interfaces, servidores, etc. La figura 7 muestra un diagrama donde se puede apreciar el diseño lógico de una red corporativa.

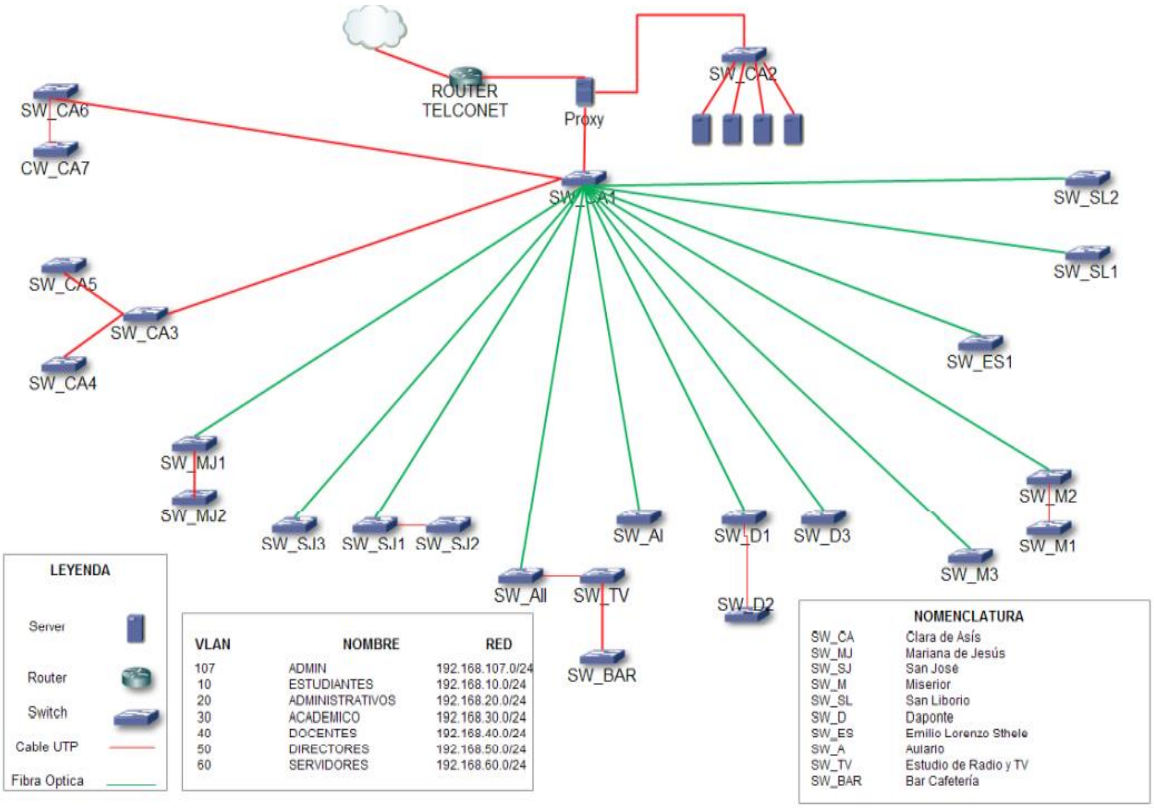

Figura 7.: Diseño lógico de una red

4.1 Esquema de direccionamiento y de nombre

Para continuar con el diseño lógico de la red, se debe implementar un plan de direccionamiento IP. En Internet, hay comités que asignan las direcciones IP con un método consistente y coherente para garantizar que no se dupliquen las direcciones, y establecen nombres que representan a grupos de direcciones.

Estos grupos de direcciones están divididas por "clases" como se muestra en la figura:

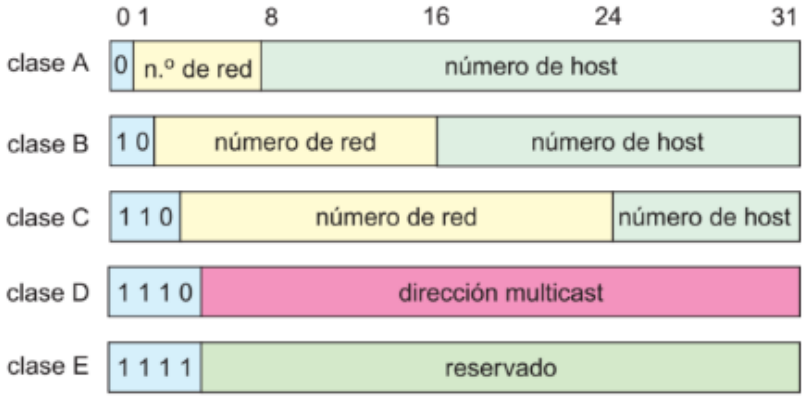

Figura 8.: Clases de direcciones IPv4

Las direcciones de clase A se asignan a las redes de tamaño extremo, ya que podrían tener más de 16 millones de hosts. Las direcciones 0.x.x.x y 127.x.x.x no se utilizan pues están reservadas para funciones de test. La dirección 127.0.0.1 identifica al host local (la dirección propia de la máquina) y se utiliza para las pruebas de bucle local (loopback). Los routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes hacia ellos mismos.

Las direcciones de clase B se asignan a las redes de tamaño medio, de hasta 65,534 host.

Las direcciones de clase C se asignan a las redes pequeñas , de hasta 254 hosts.

Las direcciones de clase D están reservadas para multicasting, que se usa para direccionar grupos de hosts en un área limitada. Esto permite que una máquina envíe paquetes a múltiples receptores.

Las direcciones de clase E las reserva el IETF para investigación.

No esta permitido utilizar como número de host las combinaciones formadas por todos los bits a 0 o a 1. Si el número de host está formado íntegramente por bits a 0 nos estamos refiriendo a la red en sí, mientras que si está formado íntegramente por bits a 1 se trata de una dirección de broadcast, es decir, que hace referencia a todos los equipos de la red. De

esta manera, la dirección 194.32.56.255 es la direccción broadcast de la red clase C 194.32.56.0.

Clase	Bits de mayor peso	Número de bits para la dirección de red	Número de redes	Número de bits para el host	Número de hosts por red	Valores del primer octeto
A	0	8	126	24	16.777.214	0-127
B	10	16	16.384	16	65.534	128-191
C	110	24	2.097.152	8	254	192-223
D	1110	No aplicable	No aplicable	No aplicable	No aplicable	224-239
E	1111	No aplicable	No aplicable	No aplicable	No aplicable	240-255

Figura 9: Número de redes y su tamaño para cada clase de dirección

La figura 9 muestra las clases de direcciones, su tamaño, el número posible de subredes y host para cada clase.

Al realizar el esquema de direccionamiento, se debe contemplar el número posible de sub redes y host para cada clase de red, ya que de esto dependerá que en el futuro el esquema de direccionamiento pueda ampliarse sin tener que reconfigurar todos lo equipos.

Algunas veces, un grupo de direcciones relacionadas se denomina espacio de direcciones. En Internet, ninguna persona u organización posee realmente estos grupos de direcciones porque las direcciones sólo tienen significado si el resto de la comunidad de Internet se pone de acuerdo sobre su uso. Mediante acuerdos, las direcciones son asignadas a organizaciones en relación con sus necesidades y tamaño. Una organización a la cual se le ha asignado un rango de direcciones, puede asignar una porción de ese rango a otra organización como parte de un contrato de servicio. Las direcciones que han sido asignadas de esta manera, comenzando con comités reconocidos internacionalmente, y luego repartidas jerárquicamente por comités nacionales o regionales, son denominadas direcciones IP enrutadas globalmente. Algunas veces es inconveniente o imposible obtener más de una dirección IP enrutada globalmente para un individuo u organización.

En este caso, se puede usar un técnica conocida como Traducción de Direcciones de Red o NAT (Network Address Translation). Un dispositivo NAT es un enrutador con dos puertos de red. El puerto externo utiliza una dirección IP enrutada globalmente, mientras que el puerto interno utiliza una dirección IP de un rango especial conocido como direcciones

privadas. El enrutador NAT permite que una única dirección global sea compartida por todos los usuarios internos, los cuales usan direcciones privadas. A medida que los paquetes pasan por él los convierte de una forma de direccionamiento a otra. Al usuario le parece que está conectado directamente a Internet y que no requieren software o controladores especiales para compartir una única dirección IP enrutada globalmente.

Por otro lado, muchos sitios permiten a los usuarios elegir los nombres de host para sus equipos. Los servidores también requieren como mínimo un nombre de host, asociado a la dirección IP de su interfaz de red principal.

Como administrador del sistema, debe asegurarse de que cada nombre de host de su dominio sea exclusivo. En otros términos, no puede haber dos equipos en la red que tengan el nombre de "fred". Sin embargo, el equipo "fred" puede tener múltiples direcciones IP.

Cuando planifique su red, realice una lista de las direcciones IP y sus nombres de host asociados para poder acceder a ellos fácilmente durante el proceso de configuración. Dicha lista le ayudará a verificar que todos los nombres de host sean exclusivos.

- ✓ **Selección de un servicio de nombres y de directorios:** algunos servicios de nombre pueden ser: archivos locales, NIS y DNS. Los servicios de nombres contienen información crítica sobre los equipos de una red, como los nombres de host, las direcciones IP, las direcciones Ethernet, etc. Los servicios de nombres NIS y DNS crean bases de datos de red en varios servidores de la red.
- ✓ **Uso de archivos locales como servicio de nombres:** Si no implementa NIS, LDAP o DNS, la red utiliza archivos locales para proporcionar el servicio de nombres. El término "archivos locales" hace referencia a la serie de archivos del directorio /etc que utilizan las bases de datos de red.
- ✓ **Nombres de dominio:** muchas redes organizan sus hosts y enrutadores en una jerarquía de dominios administrativos. Si utiliza el servicio de nombres NIS o DNS, debe seleccionar un nombre de dominio para la organización que sea exclusivo en todo el mundo. Para asegurarse de que su nombre de dominio sea exclusivo, debe registrarlo con InterNIC. Si tiene previsto utilizar DNS, también debe registrar su propio nombre de dominio con InterNIC.

  La estructura del nombre de dominio es jerárquica. Un nuevo dominio normalmente se ubica debajo de un dominio relacionado que ya existe. Por ejemplo, el nombre de

dominio para una compañía subsidiaria puede ubicarse debajo el dominio de su compañía principal. Si el nombre de dominio no tiene otra relación, una organización puede colocar su nombre de dominio directamente debajo de uno de los dominios que hay en el nivel superior.

A continuación se incluyen algunos ejemplos de dominios de nivel superior:

.com: compañías comerciales (de ámbito internacional)

.edu: instituciones educativas (de ámbito internacional)

.gov: organismos gubernamentales estadounidenses

.fr: Francia

Seleccione el nombre que identifique a su organización, teniendo en cuenta que debe ser exclusivo.

- ✓ **Subdivisiones administrativas:** Las subdivisiones administrativas están relacionadas con el tamaño y el control. Cuantos mas hosts y servidores haya en una red, más compleja será la tarea de administración. Puede configurar divisiones administrativas adicionales si es preciso. Agregue redes de una clase específica. Divida las redes existentes en subredes. La decisión de configurar subdivisiones administrativas para su red la determinan los factores siguientes:

  ¿Qué tamaño tiene la red?: Una única división administrativa puede controlar una única red de varios cientos de hosts, todo en la misma ubicación física y con los mismos servicios administrativos. Sin embargo, en ocasiones es preciso establecer varias subdivisiones administrativas. Las subdivisiones resultan especialmente útiles si tiene una red reducida con subredes y está repartida por un área geográfica extensa.

  ¿Los usuarios de la red tienen necesidades similares?: Por ejemplo, puede tener una red confinada a un único edificio que admita un número de equipos relativamente reducido. Estos equipos se reparten en una serie de subredes. Cada subred admite grupos de usuarios con diferentes necesidades. En este ejemplo, puede utilizar una subdivisión administrativa para cada subred.

4.2 Traducciones de direcciones de red

Network Address Translation (NAT) o Traducción de Direcciones de Red, es una técnica que modifica la información de dirección IP en la cabecera de un paquete IP mientras el mismo es transmitido de una red a otra por medio de un router. La necesidad de la traducción de direcciones IP surge cuando las direcciones IP privadas internas de la red no pueden ser usadas fuera de la red, o bien porque no son válidas en el exterior, o bien porque el direccionamiento interno debe mantenerse separado de la red externa. A fines prácticos, la traducción de direcciones permite, por lo general, que las máquinas de una red privada se comuniquen de manera transparente con destinos en una red externa y viceversa. Su principal uso hoy en día es el de permitir que las máquinas de una red privada puedan acceder a Internet utilizando una única dirección IP pública.

Respecto a la forma de trabajo de NAT, a continuación a partir del (posible) escenario planteado en la figura 10, analizaremos el funcionamiento de NAT. Dicha figura consiste en una red privada (red 1) con dos anfitriones (A y B) la cual posee una única dirección pública (200.13.147.43) que fue asignada al router X, el cual provee servicio de NAT. Ademá, hay dos máquinas (C y D) las cuales son externas a la red y la comunicación entre dichas máquinas y los anfitriones de la red se realiza vía Internet.

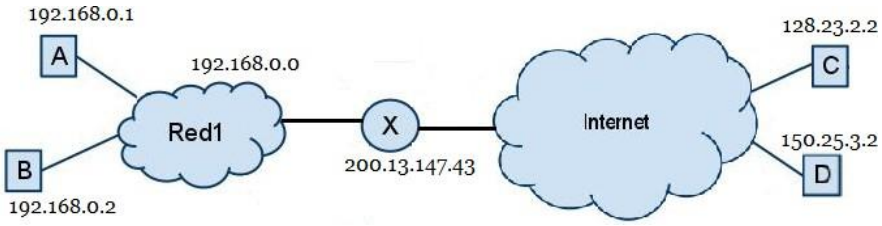

Figura 10.: Funcionamiento básico de NAT

NAT básico

En este tipo de NAT las sesiones son unidireccionales, salientes desde la red privada. El mismo, modifica dinámicamente las direcciones IP de los nodos finales (máquina emisora y máquina receptora) según corresponda y mantiene el estado de estos cambios en una tabla para que los paquetes pertenecientes a una sesión sean encaminados hacia el nodo final correcto en cualquiera de las redes (interna y/o externa).

Supongamos que el anfitrión A desea comunicarse con la máquina C y que el anfitrión B

quiere hacer lo propio con la máquina D. Cuando el router X reciba un paquete proveniente desde A o B deberá cambiar en el mismo la dirección privada del campo dirección del emisor por la dirección pública asignada a la red y guardar registro de dicha modificación.

Dirección Emisor	Dirección Pública	Dirección Receptor
192.168.0.1	200.13.147.43	128.23.2.2
192.168.0.2	200.13.147.43	150.25.3.2

Luego, cuando C le responda A o D haga lo propio con B, estas enviarán sus paquetes con el campo dirección destinatario seteado en 200.13.147.43 y X deberá encargarse de modificar dicho campo por la dirección de A o B según corresponda, para que la transmisión pueda seguir su curso. Ahora bien, ¿qué ocurre si mientras A se está comunicando con C, el anfitrión B desea hacer lo mismo? Si esto ocurriera, la tabla NAT de X quedará de la siguiente manera:

Dirección Emisor	Dirección Pública	Dirección Receptor
192.168.0.1	200.13.147.43	128.23.2.2
192.168.0.2	200.13.147.43	128.23.2.2

Entonces, cuando X reciba un paquete entrante no sabría a que anfitrión debería rutearlo. Para evitar este problema, cuando se utiliza NAT básico los anfitriones de la red privada no pueden comunicarse al mismo tiempo con la misma máquina exterior a la red.

4.1 Protocolos de enrutamiento

Este es el paso donde hay que decidir que protocolos de enrutamiento internos y externos se van a utilizar en la red: RIP, OSPF o EIGRP (internos) y BGP (externo).

Típicamente en las redes Empresariales o Corporativas se emplea el protocolo OSPF debido a su eficiencia en grandes redes, aunque en el caso de Redes con equipos Cisco se emplea mucho el protocolo EIGRP.

Igualmente hay que tener presente si se va a trabajar con IPv4 o IPv6.

Tipos de protocolo de enrutamiento dinámico

Existen tres grupos de protocolos de enrutamiento dinámico:

- **Según el propósito:** los encontramos como protocolos de gateway interior (IGP) y protocolos de gateway exterior (EGP).

  Antes de entrar a analizar estos protocolos se debe conocer un término que va de la mano de estos: sistema autónomo (AS) . Se denomina SA al grupo de redes administradas que poseen un encaminamiento dentro de una organización .

  IGP: se caracterizan por tener la capacidad de relacionarse al interior de una organización en un sistema autónomo . Los protocolos de enrutamiento IGP más conocidos son RIP, EIGRP y OSPF .

  EGP: se caracterizan por tener la capacidad de establecer relaciones entre sistemas autónomos; además, pueden coexistir en su funcionamiento varios protocolos IGP dentro de los EGP . Estos sistemas autónomos tienen una administración por separado, lo que beneficia el mantenimiento de la red . Los EGP utilizan unos routers conocidos como routers de borde, los cuales se encuentran al extremo de cada sistema autónomo . Los EGP utilizan el protocolo de enrutamiento dinámico BGP

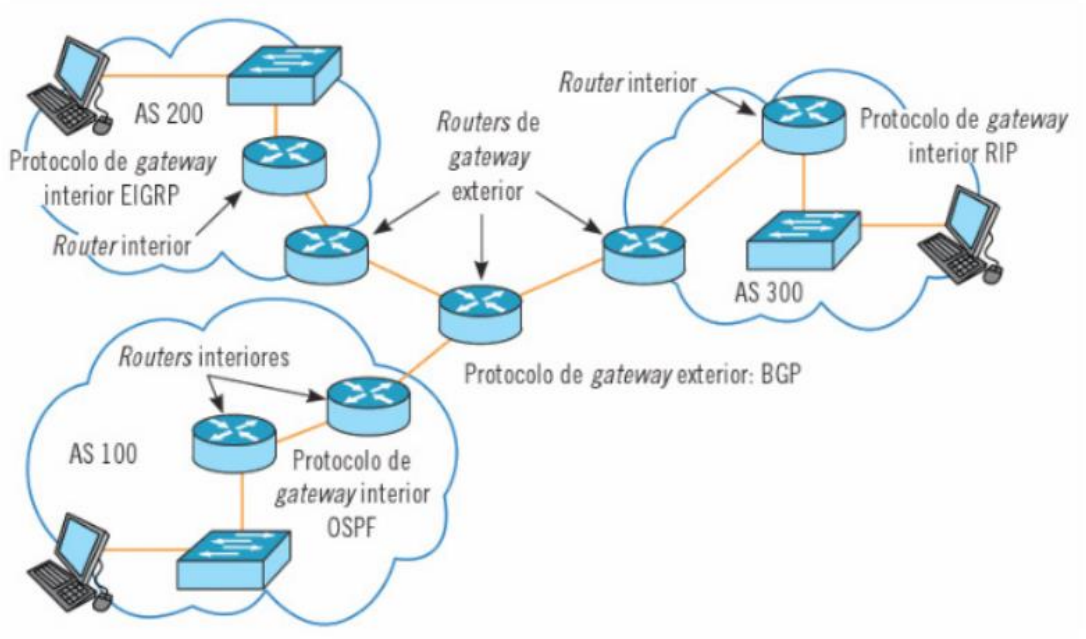

Figura 11.: Protocolos de enrutamiento exterior e interior

- **Según la operación:** los encontramos como vector distancia, protocolo de estado de enlace y protocolo vector de ruta .

  Protocolo vector distancia: se basa en dos parámetros implícitos en su nombre: la distancia, esta manifiesta el recorrido del origen al destino, y el vector, el cual identifica la dirección en que se encuentra ubicado el enrutador del siguiente salto o interfaz de salida hasta alcanzar el destino . El objetivo de los protocolos de vector distancia es identificar la ruta más corta determinando el sentido y la distancia en cualquier elemento de la red .

  Los routers que implementan vector distancia tienen conocimiento parcial del camino para llegar a su destino . En su totalidad, el router tiene conocimiento sobre la métrica . Los siguientes protocolos se identifican con IGP vector distancia IPv4: RIPv1, RIPv2, IGRP y Eigrp .

  Protocolo de estado enlace: se caracteriza por conocer toda la red . La manera en que se desempeñan los routers en este estado enlace les permite generar un mapa mediante el cual acceden a la mejor ruta para llegar al destino .

  Este protocolo funciona en una red donde se provee de un diseño jerárquico. Se trabaja en función de la convergencia . Los protocolos de enrutamiento que se desempeñan mediante estado enlace son OSPF e IS-IS .

  Protocolos de enrutamiento con clase y sin clase: estos protocolos se caracterizan por el manejo de la información . No comparten información de la máscara de subred en el enrutamiento, mientras que los protocolos de enrutamiento sin clase sí lo hacen .

  Los protocolos RIPv1 - EIGRP hacen parte de los protocolos con clase, debido a esto no manejan en su funcionamiento máscaras de subred de longitud variable, así como enrutamiento entre dominios sin clase (CIDR) .

  Los protocolos EIGRP, OSPF, BGP, etc ., hacen parte de los protocolos sin clase .

  Se puede decir que en la actualidad se maneja en las empresas enrutamiento sin clase . Estos protocolos aceptan VLSM y CIDR . Los protocolos IPv6 forman parte de estos protocolos sin clase.

4.1.1 Enrutamiento Estático

Enrutamiento estático es el término utilizado cuando la tabla de enrutamiento es creada por configuración manual. Algunas veces esto es conveniente para redes pequeñas, pero puede transformarse rápidamente en algo muy dificultoso y propenso al error en redes grandes. Peor aún, si la mejor ruta para una red se torna inutilizable por una falla en el equipo u otras razones, el enrutamiento estático no podrá hacer uso de otro camino.

El enrutamiento es fundamental en cualquier red de datos, ya que fija el camino que deben seguir los paquetes de información desde el nodo de origen hasta el nodo detino.

Los routers son lo dispositivos encargados de transferir paquetes de una red a otra, y conectan múltiples redes IP. La principal decisión de envío de los routers se basa en la información contenida en la capa de red del modelo OSI, es decir, la dirección Ip destino.

Los routers reenvían los paquetes mediante la detección de redes remotas y el mantenimeinto de información de enrutamiento. La información de enrutamiento que el router aprende desde sus fuentes de enrutamiento se coloca en su propia tabla de enrutamiento.

La tabla de enrutamiento del router sirve para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red. La tabla de enrutamiento determinará finalmente la interfaz de salida para reenviar el paquete y el router lo encapsulará en la trama de enalce de datos apropiada para dicha interfaz de salida.

Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar paquetes. Si las redes de destino no están conectadas directamente, el router debe aprender y calcular la ruta más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se construye mediante uno de estos métodos o ambos: manualmente, por el administrador de red que fija rutas concretas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino, o automáticamnte mediante procesos dinámicos que se ejecutan en la red.

Cuando el router debe enviar un paquete a una red que no aparece en su tabla de enrutamiento (es decir la desconoce) lo hace por defecto a una puerta de enlace de último recurso.

Las rutas estáticas se emplean habitualemente desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y de salida.

Con el enrutamiento estático se evita la sobrecarga de tráfico que genera un protocolo de enrutamiento. Las rutas estáticas permiten la programación manual de la tabla de enrutamiento.

4.1.2 Enrutamiento dinámico

Es un método en el cual los elementos de la red, en particular los enrutadores, intercambian información acerca de su estado y el estado de sus vecinos en la red, y luego utilizan esta información para automáticamente tomar la mejor ruta y crear la tabla de enrutamiento. Si algo cambia, como un enrutador que falla, o uno nuevo que se pone en servicio, los protocolos de enrutamiento dinámico realizan los ajustes a la tabla de enrutamiento. El sistema de intercambio de paquetes y toma de decisiones es conocido como protocolo de enrutamiento. Hay muchos protocolos de enrutamiento usados en Internet hoy en día, incluyendo OSPF, BGP, RIP, y EIGRP.

Para facilitar la administración de direcciones IP, es frecuente la utilización del protocolo DHCP (Dynamic Host Configuration Protocol) este es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un servicio cliente/servidor. Los servidores poseen una lista de direcciones IP disponibles y las van asignando a los clientes conforme las solicitan, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. DHCP se utiliza generalmente para otorgar a los dispositivos de red su dirección Ip y la correspondiente máscara, además de la puerta de enlace. Sin embargo, el protocolo permite configurar muchas más opciones como servidores DNS, servidores NTP, etc. DHCP minimiza los errores que se producen en la configuración manual (al duplicarse las direcciones) y permite al usuario trasladarse a cualquier punto de la red y obtener una configuración básica. Así mismo, permite asignar al cliente una dirección IP por un período configurable de riempo. Muchos routers tienen incorporada la funcionalidad de cliente/servidor DHCP.

Existen tres métodos de asignación en el protocolo DHCP:

Asignación manual: asigna una dirección IP a un equipo determinador. En la asignación se utiliza una tabla con direcciones Mac. Únicamente los equipos con una direccción MAC definida en dicha tabla recibirá la IP asignada en la misma tabla. Se utiliza cuando se desea

controlar la asignación de direcciones IP a cada equipo y así evitar que se conecten equipos no identificados.

Asignación automática: una dirección IP disponible dentro de un rango determinado se asigna permanentemente al equipo que la requiera. Se suele utilizar cuando el número de equipos en la LAN no varía demasiado.

Asignación dinámica: este método hace uso de la reutilización de direcciones IP. Mediante esta técnica, el servidor DHCP reinicia las tarjetas de red cada cierto intervalo de tiempo controlable, asignando unanueva dirección IP a los equipos. Demodo que la asihnación de direcciones IP es temporal y estas se reutilizan de forma dinámica

4.2 Requerimiento de software de administración de la red

Un software de administración de red es un conjunto de herramientas integradas que permite realizar las distintas tareas de gestión de red, de la forma más sencilla posible sobre todos, o la mayor parte, de los dispositivos de la red y los enlaces, independientemente de su naturaleza.

Entre las características generales que un software de administración de red debe cumplir están las siguientes:

- Descubrimiento automático de la topología de la red
- Herramientas de diagnóstico de la red
- Herramientas de seguridad
- Diagnostico de problemas
- Monitorización de la red
- Gestión de MIBs
- Gestión de direcciones de red

Los distintos tipos de requerimientos de los software de gestión de red, se pueden clasificar desde dos puntos de vista, requisitos técnicos y funcionales.

Requisitos técnicos

- Administración de entornos heterogéneos desde una misma plataforma.
- Administración de elementos de interconexión.
- Interfaces con grandes sistemas.
- Interfaz gráfico amigable.

- Evolución según las necesidades del cliente.

Requisitos funcionales

- Gestión del nivel de servicio para garantizar la disponibilidad, la atención a los usuarios, el tiempo de respuesta, etc.
- Gestión de problemas para facilitar la segmentación de los mismos resolviéndolos en etapas o niveles.
- Gestión de cambios para minimizar el impacto asociado habitualmente con los procesos de modificación de las configuraciones existentes.
- Apoyo a la toma de decisiones y facilitar que la gestión de red actúe de interfaz entre el personal técnico y la dirección, gracias a la facilidad de generar informes.
- Apoyo en la resolución de incidencias para preservar la experiencia del grupo de gestión, reduciendo el tiempo de resolución de problemas.

4.2.1 Sistema Operativo

Cuando planificamos la infraestructura de una red, la selección del SO de red se puede simplificar de forma significativa si primero se determina la arquitectura de red (cliente/servidor o grupo de trabajo) que mejor se ajusta a nuestras necesidades.

Para decidir qué tipo de infraestructura queremos montar nos basaremos en varios parámetros:

- **Nivel de seguridad de la red.** Esta decisión se basa en los tipos de seguridad que se consideran más adecuados. Las redes basadas en servidor permiten incluir más posibilidades relativas a la seguridad que las que nos ofrece un simple grupo de trabajo. Por otro lado, cuando la seguridad no es una propiedad a considerar, puede resultar más apropiado un entorno de red del tipo grupo de trabajo
- **Número de usuarios de la red.** Cuando el número de usuarios es pequeño, a veces resulta más práctico y fácil de administrar un grupo de trabajo que una red en entorno cliente/servidor ya que el mantenimiento, actualización y gestión de los recursos será pequeño.
- **Número de equipos de la red**. Al igual que en el caso anterior y por los mismos motivos, si disponemos de pocos equipos en la red, tal vez será mejor trabajar en un grupo de trabajo que en un entorno de red cliente/servidor.

- **Evaluar la interoperabilidad de la red.** Después de identificar las necesidades de seguridad, usuarios y equipos de la red, el siguiente paso es determinar los tipos de interoperabilidad necesaria en la red para que se comporte como una unidad. Debemos saber que a la hora de montar una infraestructura de red siempre podremos mezclar equipos de uno y otro tipo sin ningún tipo de problema si conocemos las características que nos ofrece cada uno de ellos y el diseño y necesidades que tengamos en nuestra red. Si miramos la Figura 12, podemos ver un sistema informático en red en el que existe una interoperabilidad total entre sistemas clientes y servidores.

  Cada sistema operativo de red considera la interoperabilidad de forma diferente y, por eso, resulta muy importante recordar nuestras propias necesidades de interoperabilidad cuando se evalúe cada sistema operativo de red.

  Si la opción es grupo de trabajo, disminuirán las opciones de seguridad y de interoperabilidad debido a las limitaciones propias de esta arquitectura. Si la opción seleccionada se basa en la utilización de un entorno cliente/servidor, es necesario realizar estimaciones futuras para determinar si la interoperabilidad va a ser considerada como un servicio en el servidor de la red o como una aplicación cliente en cada equipo conectado a la red.

  La interoperabilidad basada en servidor es más sencilla de gestionar puesto que, al igual que otros servicios, se localiza de forma centralizada.

  La interoperabilidad basada en cliente requiere la instalación y configuración en cada equipo. Esto implica que la interoperabilidad sea mucho más difícil de gestionar.

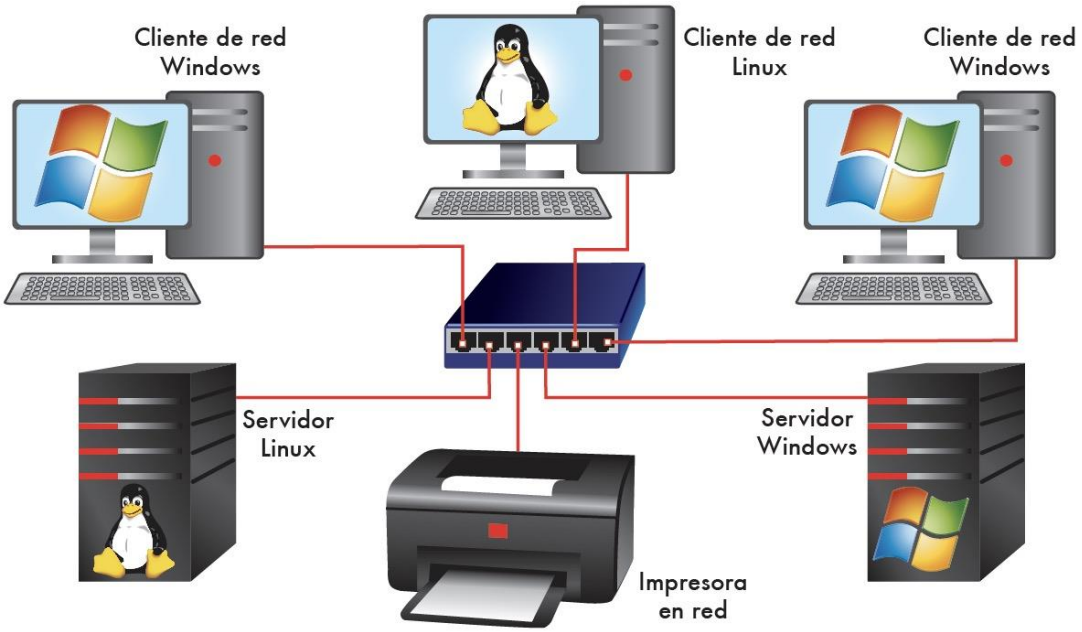

Figura 12.: Interoperabilidad en Sistema informático en red

Seleccionado el SO en red que queremos instalar, a continuación se determinan los servicios de red que se requieren. Recordemos que los servicios de red son programas que se ejecutan de forma permanente en los SO y que determinan qué es lo que se puede hacer sobre el sistema. Como por ejemplo, los servicios de impresión. En una red Windows Server, cualquier servidor o cliente puede funcionar como servidor de impresión. La diferencia es que si el servicio de impresión está montado en un cliente, el administrador de la red no tendrá control total sobre el mismo. Lo normal es instalar estos servicios en el servidor y gestionarlos desde ese equipo.

Otros servicios de red. que ayudan a la gestión global de un entorno de red son:

Servicio de mensajería. Monitoriza la red y recibe mensajes emergentes para el usuario.

Servicio de alarma. Envía las notificaciones recibidas por el servicio de mensajería.

Servicio de exploración. Proporciona una lista de servidores disponibles en los dominios y en los grupos de trabajo.

Servicio de estación. Se ejecuta sobre una estación de trabajo y es responsable de las conexiones con el servidor.

Servicio de servidor. Proporciona acceso de red a los recursos de un equipo.

Otros servicios adicionales que se pueden incluir a la hora de configurar y gestionar un SO en red son soportes de interoperabilidad para conexiones con otros sistemas operativos, servicios de gestión de red, políticas de seguridad, automatización de procesos, etc.

4.2.2 Recursos compartidos

Compartir es el término utilizado para describir los recursos que públicamente están disponibles para cualquier usuario de la red. La mayoría de los sistemas operativos de red no solo permiten compartir, sino también determinar el grado de compartición. Las opciones para la compartición de recursos incluyen:

- Permitir distintos usuarios con diferentes niveles de acceso a los recursos (privilegios).
- Coordinación en el acceso a los recursos asegurando que dos usuarios no utilicen el mismo recurso en el mismo instante.
- Indicar que en este punto, por ejemplo, habrá usuarios de la red que podrán acceder a determinados documentos, solamente para poder leerlos. En cambio, otros además de leerlos, podrán modificarlos e incluso habrá usuarios que no tengan ni permisos para poder leer esos archivos. Estos privilegios o permisos son concedidos por el administrador a los usuarios de la red.

4.2.3 Aplicaciones

El administrador debe valorar el modo en que trabajarán los usuarios, con información local o centralizada, de esto dependerá el medio en el que los usuarios accederán a las aplicaciones. Podemos encontrarnos con tres tipos de configuraciones para los clientes:

- Los programas y aplicaciones están instalados en el disco duro local de la estación y no son compartidos por la red. Cada usuario tiene una copia de cada aplicación. Los datos residen también de modo habitual en el disco local, aunque es posible centralizar la información en los servidores.
- Los programas están instalados en el servidor y todos los usuarios acceden al servidor para disparar sus aplicaciones. Por tanto, se instala una única copia de las aplicaciones, lo que ahorra espacio en disco. Hay que tener en cuenta, no obstante, que no todas las aplicaciones permiten esta operativa de trabajo. Los datos de usuario

pueden seguir estando distribuidos por las estaciones clientes, aunque también pueden residir en el servidor.

Hay un caso particular de esta configuración: los clientes ligeros o las estaciones que no poseen disco local (o que poseyéndolo, no lo utilizan para almacenar aplicaciones o datos) y que deben arrancar remotamente a través de la red desde un servidor de sistemas operativos.

- La instalación de aplicaciones distribuidas exige la colaboración del cliente y del servidor, o entre varios servidores, para completar la aplicación. Por ejemplo, una aplicación de correo electrónico consta de una parte denominada cliente, que se instala en la estación cliente, y una parte denominada servidor, que se instala en el servidor de correo.

  Otros ejemplos de aplicaciones distribuidas son las construidas según la tecnología cliente-servidor, como las bases de datos distribuidas.

La clasificación anterior está muy simplificada. La realidad es mucho más compleja. Lo habitual en el mundo de los sistemas de red son combinaciones de todas estas posibilidades y, por ejemplo, máquinas que son servidoras con respecto de un tipo de servicio son clientes con respecto de otros.

De la eficacia al diseñar esta estructura de red depende el éxito del administrador de red dando un buen servicio a los usuarios de la red que administra.

4.2.4 Software de administración de la red

La administración de red requiere de la habilidad para supervisar, comprobar, sondear, configurar y controlar los componentes hardware y software de una red.

Dado que los dispositivos de red son distribuidos, el administrador debe ser capaz de recopilar datos, para la supervisión de entidades remotas, así como realizar cambios sobre ellas, para controlarlas. Para llevar a cabo actividades como las anteriores, se requiere de una arquitectura de software de administración de redes, que se compone de los siguientes elementos:

- **Entidad administradora:** aplicación con control humano que se ejecuta en una estación centralizada de administración de red, en el NOC, Centro de Operaciones de Red (Network Operations Center) éste es el lugar donde se realiza la actividad de la

administración de la red, controla la recolección, procesamiento, análisis y visualización de la información de administración. En el NOC se inician las acciones que controlan el comportamiento de la red y donde el administrador de red interactúa con los dispositivos que la conforman.

- **Dispositivo administrado:** es una parte del equipamiento de la red, incluido el software, que reside en la red administrada. Un dispositivo administrado puede ser un host, un router, un switch, un puente, un hub, una impresora o un módem. En el dispositivo hay diversos objetos administrados, por ejemplo: el hardware como una tarjeta de interfaz de red y el conjunto de parámetros de configuración de los dispositivos hardware y software.
- **Base de información de administración (MIB):** lugar donde se almacenan los datos referentes a los objetos administrados. Es una colección de objetos, que representan de forma abstracta los dispositivos de la red y sus componentes internos, estos objetos incluyen direcciones de red, tipos de interfaz, contadores y datos similares. De esta manera los protocolos de gestión no operan directamente sobre el objeto a administrar, sino que operan sobre la MIB, convirtiéndose esta en el reflejo de dicho objeto. El estándar MIB de Internet define 126 objetos relacionados con los protocolos TCP/IP.
- **Agente de administración de red:** proceso residente que se ejecuta en cada dispositivo administrado y que se comunica con la entidad administradora, realizando acciones locales bajo el control de los comandos de la entidad administradora.
- **Protocolo de administración de red:** éste se ejecuta entre la entidad administradora y el dispositivo administrado permitiendo a la entidad administradora consultar el estado de los dispositivos e indirectamente realizar acciones en dichos dispositivos a través de los agentes. Ejemplo de este, es el protocolo SNMP (Protocolo Simple De Administración de Red).

Algunos ejemplos de software para la administración de redes son:

- **Nagios:** es una herramienta de monitorización de red de código abierto. Está licenciado bajo la GNU General Public License Version 2. Como herramienta de monitorización, vigila que los equipos de la red funcionan como deberían. Nagios

comprueba constantemente si los dispositivos funcionan correctamente. Es capaz de verificar si determinados servicios, en los diferentes equipos, están activos.

Además, acepta los informes de estado de otros procesos o equipos, por ejemplo, un servidor web puede informar directamente a Nagios si no está sobrecargado. La monitorización de sistemas en Nagios se divide en dos categorías de objetos: hosts o equipos y servicios. Los equipos representan un dispositivo físico o virtual en la red (servidores, routers, estaciones de trabajo, impresoras, etc.) Los servicios son funcionalidades específicas, por ejemplo, un servidor SSH (Secure Shell) puede definirse como un servicio monitorizado. Cada servicio se asocia con el equipo en el que está corriendo. Además, los equipos pueden asociarse en grupos de equipos (hostgroups)

Nagios realiza todas sus comprobaciones de estado a través de plugins. Éstos son componentes externos que pasan la información a Nagios sobre los servicios que deben comprobarse y sobre sus límites. Los plugins son responsables de la realización de las comprobaciones y de analizar los resultados. La salida de una comprobación (output), es el estado y un texto adicional describiendo la información del servicio en detalle. Nagios incorpora un conjunto de plugins por defecto que permiten realizar comprobaciones de estado para una amplia gama de servicios.

Una característica muy importante de Nagios es el sistema de dependencia. Este se basa en los niveles de dependencia entre los equipos de la red, es decir, qué equipo está conectado a qué otro u otros. Esto permite posteriormente reflejar la topología real de la red. Y de tal forma, Nagios no realizará una petición a un dispositivo dependiente de otro que se encuentre apagado, ya que no podrá ser fructífera si no existe otro camino.

- **Zabbix:** fue creado por Alexei Vladishev, y actualmente es desarrollado y respaldado activamente por Zabbix SIA,es una solución de monitoreo distribuido de código abierto de clase empresarial. Este software monitorea numerosos parámetros de una red y la salud e integridad de los servidores. utilizando un mecanismo de notificación flexible que permite a los usuarios configurar alertas basadas en correo electrónico para prácticamente cualquier evento. Esto permite una reacción rápida a los problemas del servidor, ofrece excelentes funciones de informes y visualización de

datos basadas en los datos almacenados. Esto hace que Zabbix sea ideal para la planificación de la capacidad.

Zabbix admite tanto el sondeo como la captura. Se accede a todos los informes y estadísticas, así como a los parámetros de configuración, a través de una interfaz web. Una interfaz basada en la web garantiza que el estado de su red y el estado de sus servidores puedan evaluarse desde cualquier ubicación. Con una configuración adecuada, esta herramienta puede desempeñar un papel importante en el monitoreo de la infraestructura de TI. Esto es igualmente cierto para organizaciones pequeñas con pocos servidores y para grandes empresas con multitud de servidores.

Algunas características de la herramienta zabbix son:

- Interfaz web centralizada y fácil de utilizar.
- Servidor que funciona bajo la mayoría de los sistemas operativos basados en Unix, incluyendo Linux, AIX, FreeBSD, OpenBSD y Solaris.
- Agentes nativos para la práctica mayoría de los anteriores sistemas basados en Unix y para las versiones de Windows.
- Desarrollo de gráficos integrado y diversas prestaciones de visualización.
- Notificaciones que permiten una fácil integración con otros sistemas.
- Envío de alertas vía e-mail, SMS y servicios de mensajería instantánea.
- Ejecución de comandos remotos desde el servidor central.
- Configuración flexible incluyendo la definición de plantillas.

- **Solarwinds** SIEM - Correlacionador de Eventos- Lem (Solar Winds). SolarWinds LEM permite el Análisis proactivo de registros de los dispositivos de la red, como también la correlación de eventos de la red, sistemas, aplicaciones, máquinas virtuales e infraestructura de almacenamiento con casi 700 reglas de correlación incorporadas y un constructor de reglas personalizable para crear y compartir reglas con otros administradores de TI.

  La herramienta en la entidad se utiliza para efectuar el registro de los Log en los servidores, si hay una alerta critica envía un correo notificando. Las alertas críticas

en la entidad son aquellas que están relacionadas con la caída de un servicio, el llenado de un disco duro, problemas de memoria, alta ocupación de procesadores; como también notifica acerca de intrusiones de seguridad en el caso de ingresos de usuarios no autorizados, esto permite a través del Network Performance Monitor (NPM), proveer una completa plataforma para la administración de fallas y monitorización de desempeño que permite ver la disponibilidad de cada uno de los componentes de la infraestructura tecnológica en tiempo real y los históricos de estadísticas desde un Web Browser, mientras se monitorea, se recolectan y analizan datos de enrutadores, switches, firewalls, servidores y cualquier otro dispositivo con el protocolo SNMP habilitado. La herramienta en la Entidad se utiliza para:

- Se utiliza para realizar un escaneo o analices de la red permitiendo la detección, el diagnóstico y la resolución de problemas de la red antes de que se produzca un corte del servicio.
- También es utilizado por el administrador de la red para hacer seguimiento del tiempo de respuesta, tiempo de actividad y para analizar la disponibilidad (routers, los conmutadores y otros dispositivos con SNMP habilitado) de los dispositivos y elementos que componen la infraestructura del área Tecnológica.
- Para analizar la capacidad y utilización de ancho de banda de switches, enrutadores e interfaces de red.
- Para monitorear la red en busca de trafico excesivo o inusual que llega al sistema.

4.3 Configuración de MAN/WAN

Los administradores de redes de la actualidad, deben administrar redes WANs complejas, para soportar el número creciente de aplicaciones de software que se desarrollan en torno al protocolo IP y la Web. Estas WAN exigen una gran cantidad de recursos de la red, y necesitan tecnologías de networking de alto desempeño. Las WAN son entornos complejos que incorporan múltiples medios, múltiples protocolos, e interconexión con otras redes, como Internet. El crecimiento y la facilidad de administración de estos entornos de red, se logran mediante la compleja interacción de protocolos y funciones.

A pesar de las mejoras en el desempeño de los equipos y las capacidades de los medios, el diseño de una WAN es una tarea cada vez más difícil. El diseño cuidadoso de las WAN, puede reducir los problemas asociados con los entornos crecientes de networking. Para diseñar WAN confiables y escalables, los diseñadores de red deben tener en mente, que cada WAN posee requisitos de diseño específicos.

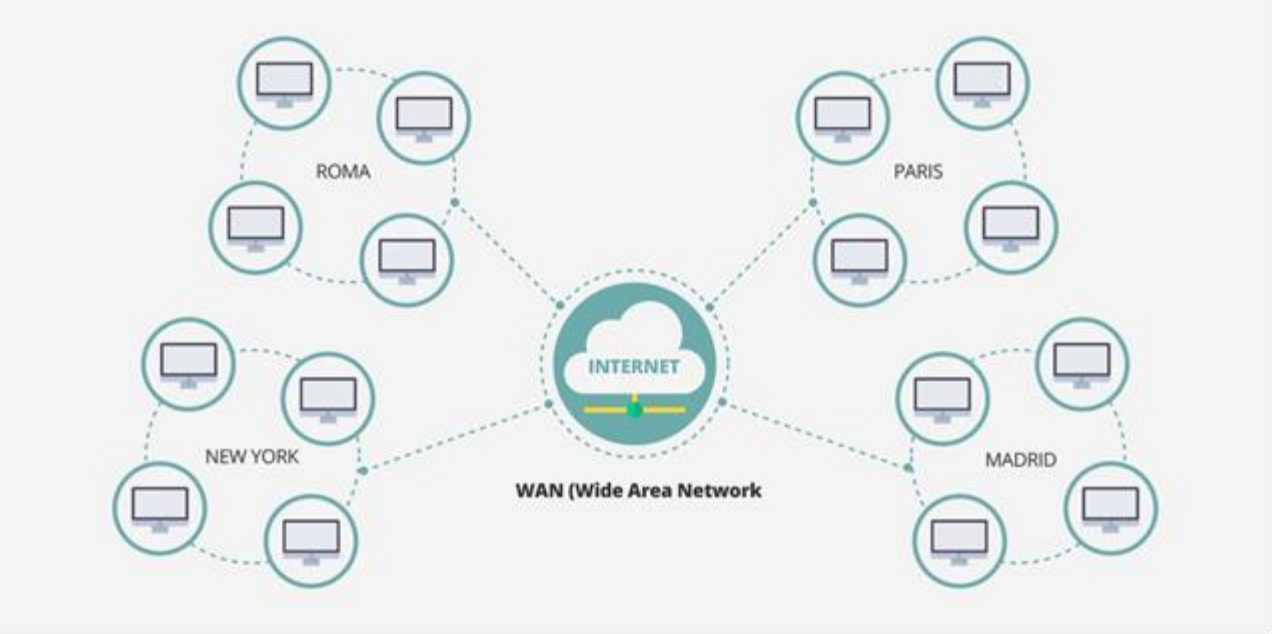

Figura 13.: Ejemplo de red WAN

Cuando se implementa correctamente, la infraestructura de la WAN puede optimizar la disponibilidad de las aplicaciones y permitir el uso económico de los recursos de red existentes.

El objetivo general del diseño WAN es minimizar el costo basándose en distintos elementos (equipos, tráfico, rendimiento, topologías, capacidad de línea, etc), proporcionando servicios que no comprometan los requisitos de disponibilidad establecidos. Hay dos aspectos fundamentales: disponibilidad y costo. Estos aspectos se encuentran esencialmente en posiciones antagónicas. Cualquier aumento en la disponibilidad en general debe reflejarse en un aumento en los costos. Por lo tanto, se debe analizar cuidadosamente la importancia relativa de la disponibilidad de recursos y el costo general.

El primer paso en el proceso de diseño, es comprender los requisitos de la empresa. Los requisitos de la WAN deben reflejar los objetivos, características, procesos empresariales y políticas de la empresa en la que opera.

Las conexiones WAN también se caracterizan por el costo del alquiler de los medios (los cables) a un proveedor de servicios para conectar dos o más sitios entre sí. Como la infraestructura WAN a menudo se arrienda a un proveedor de servicio, el diseño WAN debe optimizar el costo y eficiencia del ancho de banda. Por ejemplo, todas las tecnologías y funciones utilizadas en las WAN son desarrolladas para cumplir con los siguientes requisitos de diseño: optimizar el ancho de banda de WAN, minimizar el costo y maximizar el servicio efectivo a los usuarios finales.

Las nuevas infraestructuras WAN deben ser más complejas, deben basarse en nuevas tecnologías y deben poder manejar combinaciones de aplicaciones cada vez mayores (y en rápido proceso de cambio), con niveles de servicio requeridos y garantizados.

Los diseñadores de redes están usando las tecnologías WAN para soportar estos nuevos requisitos. Las conexiones WAN generalmente manejan información importante y están optimizadas en el aspecto del precio y desempeno del ancho de banda. Los routers que conectan campus, por ejemplo, generalmente aplican optimización del tráfico, múltiples rutas para redundancia, respaldo de discado para la recuperación de desastres y calidad de servicio para las aplicaciones críticas.

El trabajo de los diseñadores de redes de datos será parcialmente intuitivo y parcialmente analítico. Mientras que el único camino para tomar ventaja de lo intuitivo es a través de la experiencia, el entrenamiento y la utilización de herramientas analíticas para el trabajo.

- **Congestión en WAN: Configuración Encolamiento y Compresión**

  Con las aplicaciones actuales, hambrientas de banda ancha, la necesidad de ancho de banda de un sitio remoto también aumentará, aun cuando no se requiera ancho de banda en el sitio central.

  Cuando las demandas de ancho de banda de un sitio remoto excedan la capacidad del enlace, la mejor solución es proveer de más ancho de banda. Sin embargo, en algunos casos, arrendar una línea adicional o aumentar el número de circuitos, puede no ser práctico, sobre todo si las demandas de ancho de banda son súbitas e inesperadas.

Entonces, para manejar la congestión de los enlaces WAN, se dispondrá de dos técnicas: el encolamiento (queuing) y la compresión, particularmente sobre enlaces que ofrecen anchos de banda menores.

Existen muchas estrategias y técnicas para optimizar el tráfico sobre enlaces WAN, incluyendo encolamiento y listas de acceso (ACLs). Sin embargo uno de los métodos más efectivos es la compresión.

El encolamiento se refiere al proceso por el cual un dispositivo (un router por ejemplo) usa, para transmisión, paquetes estacionados (en espera en un buffer) durante los períodos de congestión. Se puede configurar un router congestionado para que priorice y envíe primero aquellos paquetes de misión crítica y de tráfico sensible al retardo, aun cuando existan paquetes, de baja prioridad, que hayan llegados primeros o, puede darse el caso de que se descarten paquetes debido al exceso. En muchos casos se requiere de más ancho de banda. El encolamiento, en realidad, aumenta los problemas de performance porque demanda ciclos de CPU adicionales y fuerza al router a aplicar un encolado lógico a cada paquete. Además, el encolamiento es una solución temporaria o una solución para aquellas raras ocasiones cuando las sesiones interactivas fallan por problemas de latencia o descarte de paquetes.

Por otro lado, la compresión de datos trabaja identificando patrones o modelos en una corriente o flujo (stream) de datos, y escogiendo un método más eficaz de representar la misma información. Esencialmente, se aplica a los datos un algoritmo para remover o quitar tanta redundancia como sea posible. La eficacia y efectividad de un esquema de compresión se mide por su tasa de compresión, la tasa o proporción del tamano de datos no comprimidos a datos comprimidos.

Para comprimir datos existen disponibles muchos algoritmos diferentes. Algunos se diseñan para tomar ventaja de un medio específico y encontrar las redundancias, pero por otro lado realizan un pobre trabajo cuando se aplican a otras fuentes de datos. Por ejemplo, la norma MPEG fue diseñada para tomar ventaja de la diferencia, por otro lado hace un trabajo terrible para comprimir texto.

Sin embargo, en la teoría de compresión existe un límite teórico que especifica cuánto puede comprimirse una fuente de datos.

La tecnología de compresión de datos maximiza el ancho de banda e incrementa el throughput (rendimiento) del enlace WAN (al reducir el tamano del frame permite transmitir más datos sobre el enlace).

4.3.1 Encapsulamiento

En cada conexión WAN, se encapsulan los datos en las tramas antes de cruzar el enlace WAN. Para asegurar que se utilice el protocolo correcto, se debe configurar el tipo de encapsulación de capa 2 correspondiente. La opción de protocolo depende de la tecnología WAN y el equipo de comunicación. Las siguientes son descripciones breves de tipos de protocolo WAN:

- **HDLC:** es el tipo de encapsulación predeterminado en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuitos cuando el enlace utiliza dos dispositivos de Cisco. Ahora, HDLC es la base para PPP síncrono que usan muchos servidores para conectarse a una WAN, generalmente Internet.
- **PPP:** proporciona conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos. PPP funciona con varios protocolos de capa de red, como IPv4 e IPv6. PPP utiliza el protocolo de encapsulación HDLC, pero también tiene mecanismos de seguridad incorporados como PAP y CHAP.
- **Protocolo de Internet de línea serial (SLIP):** es un protocolo estándar para conexiones seriales punto a punto mediante TCP/IP. PPP reemplazó ampliamente al protocolo SLIP.
- **Procedimiento de acceso al enlace balanceado (LAPB) X.25:** es un estándar del UIT-T que define cómo se mantienen las conexiones entre un DTE y un DCE para el acceso remoto a terminales y las comunicaciones por computadora en las redes de datos públicas. X.25 especifica a LAPB, un protocolo de capa de enlace de datos. X.25 es un antecesor de Frame Relay.
- **Frame Relay:** es un protocolo de capa de enlace de datos conmutado y un estándar del sector que maneja varios circuitos virtuales. Frame Relay es un protocolo de última generación posterior a X.25. Frame Relay elimina algunos de los procesos prolongados (como la corrección de errores y el control del flujo) empleados en X.25.

- **ATM:** es el estándar internacional de retransmisión de celdas en el que los dispositivos envían varios tipos de servicios (como voz, video o datos) en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento se lleve a cabo en el hardware, lo que disminuye las demoras en el tránsito. ATM aprovecha los medios de transmisión de alta velocidad, como E3, SONET y T3.

4.3.2 Traducción de protocolos

Actualemente, IPv4 e IPv6 coexisten en internet y lo seguirán haciendo durante bastantes años. Por este motivo son necesarios mecanismos que permitan dicha coexistencia y una migración progresiva de un protocolo a otro, tanto de las redes como de los equipos de usuarios. Este tipo de mecanismo se conoce como traducción de protocolos, y es necesario cuando un nodo que solo soporta IPv4 intenta comunicarse con otro que solo soporta IPv6 y viceversa. Esta situación también puede ocurrir con otros tipos de protocolos.

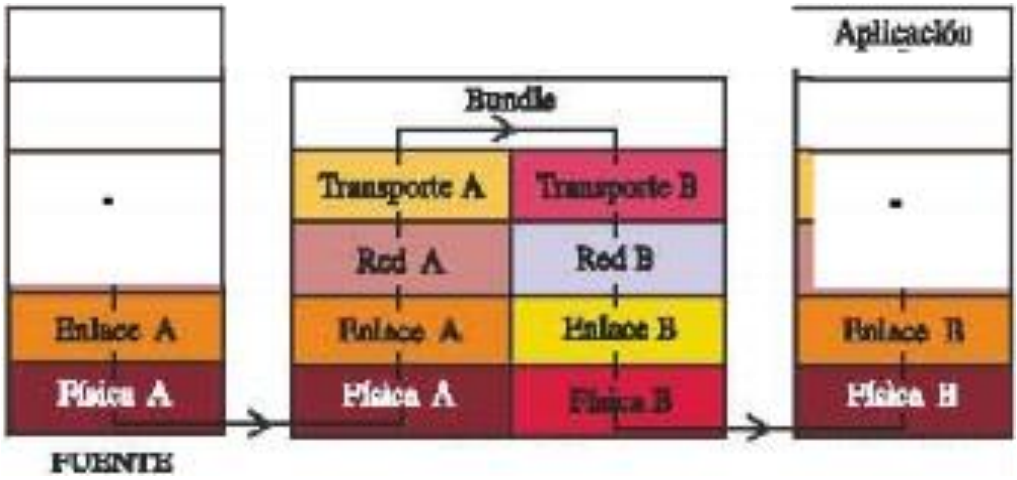

Figura 14: Traducción de protocolos

4.4 Seguridad de la red

Para realizar un diseño para la seguridad de la red, se debe estudiar la situación actual desde el punto de vista de la seguridad, con el fin de determinar las acciones que se ejecutarán en función de las necesidades detectadas y con ello establecer políticas, objetivos y procesos de seguridad apropiados para gestionar el riesgo, posibilitando obtener resultados conformes con las políticas y objetivos globales de la organización.

Los bienes informáticos de que dispone una entidad no tienen el mismo valor, e igualmente, no están sometidos a los mismos riesgos, por lo que es imprescindible la realización de un **Análisis de Riesgos** que ofrezca una valoración de los bienes informáticos y las amenazas a las que están expuestos, así como una definición de la manera en que se gestionarán dichos riesgos para reducirlos.

Como resultado, se establecerán las prioridades en las tareas a realizar para minimizar los riesgos. Puesto que los riesgos nunca desaparecen totalmente, la dirección de la entidad debe asumir el **riesgo residual**, o sea el nivel restante de riesgo después de su tratamiento.

- **Recopilar información de seguridad**

  Durante el proceso de preparación se reunirá toda la información que facilite el diseño e implementación de los mecanismos para ofrecer seguridad a la red, para lo cual se utilizan los documentos normativos y metodológicos que existan sobre el tema; documentación de aplicaciones y sistemas en explotación en la organización; documentación de incidentes ocurridos en la entidad o en otras organizaciones afines; tendencias de seguridad nacionales e internacionales, así como otros materiales que faciliten su realización.

- **Determinación de las necesidades de protección**

  Las necesidades de protección del sistema se establecen mediante la realización de un análisis de riesgos, que es el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.

La realización del análisis de riesgos debe proporcionar:

- Una detallada caracterización del sistema informático objeto de protección.

- La creación de un inventario de bienes informáticos a proteger.
- La evaluación de los bienes informáticos a proteger en orden de su importancia para la organización.
- La identificación y evaluación de amenazas y vulnerabilidades.
- La estimación de la relación importancia-riesgo asociada a cada bien informático (peso de riesgo).

En el proceso de análisis de riesgos se pueden diferenciar dos aspectos:

a) **La Evaluación de Riesgos** orientada a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valorando los riesgos y estableciendo sus niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la entidad. Consiste en el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar su importancia.

b) **La Gestión de Riesgos** que implica la identificación, selección, aprobación y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones destinadas a:

- Reducir la probabilidad de que una amenaza ocurra.
- Limitar el impacto de una amenaza, si esta se manifiesta.
- Reducir o eliminar una vulnerabilidad existente.
- Permitir la recuperación del impacto o su transferencia a terceros.

La gestión de riesgos implica la clasificación de las alternativas para manejar los riesgos a que puede estar sometido un bien informático dentro de los procesos en una entidad. Implica una estructura bien definida, con controles adecuados y su conducción mediante acciones factibles y efectivas. Para ello se cuenta con las técnicas de manejo del riesgo siguientes:

- **Evitar:** Impedir el riesgo con cambios significativos por mejoramiento, rediseño o eliminación, en los procesos, siendo el resultado de adecuados controles y acciones realizadas.
- **Reducir**: Cuando el riesgo no puede evitarse por dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más

bajo posible. Esta opción es la más económica y sencilla y se consigue optimizando los procedimientos y con la implementación de controles.

- **Retener**: Cuando se reduce el impacto de los riesgos pueden aparecer riesgos residuales. Dentro de las estrategias de gestión de riesgos de la entidad se debe plantear como manejarlos para mantenerlos en un nivel mínimo.
- **Transferir**: Es buscar un respaldo contractual para compartir el riesgo con otras entidades, por ejemplo, alojamiento, hospedaje, externalización de servicios, entre otros. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo.

La necesidad de la actualización permanente del análisis de riesgos estará determinada por las circunstancias siguientes:

- Los elementos que componen un sistema informático en una entidad están sometidos a constantes variaciones: cambios de personal, nuevos locales, nuevas tecnologías, nuevas aplicaciones, reestructuración de entidades, nuevos servicios, etc.
- La aparición de nuevas amenazas o la variación de la probabilidad de ocurrencia de alguna de las existentes.
- Pueden aparecer nuevas vulnerabilidades o variar o incluso desaparecer alguna de las existentes, originando, modificando o eliminando posibles amenazas.

En resumen, durante la determinación de las necesidades de protección del sistema de red es necesario:

- Caracterizar el sistema informático.
- Identificar las amenazas potenciales y estimar los riesgos sobre los bienes informáticos.
- Evaluar el estado actual de la seguridad.

Una posible agrupación por categorías que puede ayudar a la identificación de los bienes informáticos a proteger podría ser la siguiente:

a) **Hardware:** redes de diferente tipo, servidores y estaciones de trabajo, computadoras personales (incluyendo portátiles), soportes magnéticos y ópticos, medios

informáticos removibles, líneas de comunicaciones, módems, ruteadores, concentradores, entre otros.

b) **Software:** programas fuentes, programas ejecutables, programas de diagnóstico, programas utilitarios, sistemas operativos, programas de comunicaciones, entre otros.

c) **Datos:** durante la ejecución, almacenados en discos, información de respaldo, bases de datos, trazas de auditoría, en tránsito por los medios de comunicaciones, entre otros.

d) **Personas:** usuarios, operadores, programadores, personal de mantenimiento, entre otros.

e) **Documentación:** de programas, de sistemas, de hardware, de procedimientos de administración, entre otros.

Una vez identificados los bienes informáticos que necesitan ser protegidos se determinará su importancia dentro del sistema informático y se clasificarán según la misma.

Bienes informáticos críticos

Como resultado de la evaluación anterior se determinarán los bienes informáticos críticos para la gestión de la entidad en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos. Se consideran bienes informáticos críticos aquellos sin los cuales el trabajo de la entidad no tuviera sentido o no puede ser ejecutado. Por ejemplo:

- El servidor principal de una red.
- Los medios de comunicaciones de un centro de cobros y pagos remoto.
- El sistema de control de tráfico aéreo de un aeropuerto.
- El sistema contable de una entidad.

Para lograr la seguridad en la red es necesario describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde dónde), es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación).

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines. Los piratas de la era cibernética que reclaman un acceso libre e irrestricto a los medios de comunicación electrónicos.

Como administradores del sistema debemos disponer de herramientas para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté probando. Todos los movimientos del sistema son registrados en archivos, que los operadores revisan diariamente.

Evidentemente las redes, como otros sistemas son susceptibles a múltiples ataques que pueden distorsionar el efecto de la información transmitida o capturarla simplemente. Al aumentar la complejidad de las redes se hace cada vez más patente la necesidad de articular mecanismos de seguridad y protección. El tema es muy amplio por lo que, esquemáticamente, puede decirse que los servicios de seguridad más significativas son: la autenticación, el control de acceso, la confidencialidad de datos y la integridad de datos.

- **La autenticación:** proporciona la verificación de la identidad de la fuente de los datos.
- **El control de acceso**: proporciona protección contra el uso no autorizado de recursos accesibles a través de la red.
- **La confidencialidad de los datos:** proporciona protección de datos, por ejemplo, mediante mecanismos de tipo criptográfico.
- **La integridad de datos**: proporciona una validación de la integridad de la información, detectando cualquier modificación, inserción o eliminación de datos.

Pueden añadirse algunas medidas de protección adicionales contra el uso no autorizado de manera especifica en redes, como devolución de llamadas, certificados digitales y firewalls.

4.4.1 Selección de seguridad

Antes de considerar el tratamiento de los riesgos, la organización decidirá los criterios para determinar si pueden ser aceptados o no. Un riesgo puede ser aceptado si, por ejemplo, se determina que es bajo o que el costo de su tratamiento no es rentable para la organización.

Para cada uno de los riesgos identificados se tomará una decisión sobre su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

- **Aplicar controles apropiados** para reducir los riesgos.
- **Aceptar riesgos** de manera consciente y objetiva, siempre que satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
- **Evitar riesgos**, no permitiendo las acciones que propicien los riesgos.
- **Transferir los riesgos** a otras partes, por ejemplo, aseguradores o proveedores.

Los controles de seguridad que se seleccionen para la reducción de los riesgos a un nivel aceptable cubrirán adecuadamente las necesidades específicas de la organización. La elección de los controles de seguridad depende de una decisión organizacional basada en los criterios para la aceptación del riesgo, las opciones para el tratamiento de mismo, y el acercamiento a su gestión general aplicada a la organización, y también estará conforme a toda la legislación y regulaciones nacionales e internacionales vigentes.

Los controles de seguridad informática serán considerados en las etapas de especificación de requisitos y de diseño de sistemas y aplicaciones. El no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y en el peor de los casos, imposibilidad de alcanzar la seguridad adecuada.

Estos controles serán establecidos, implementados, supervisados y mejorados cuando sea necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

Hay que tener presente que ningún sistema de controles puede alcanzar la seguridad completa y que acciones adicionales de gestión deben implementarse para supervisar, evaluar, y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la

organización.

La seguridad informática se logra implantando un conjunto adecuado de controles, que incluyen políticas, procesos, medidas, procedimientos, estructuras organizativas y funciones de hardware y software.

Las medidas y procedimientos de seguridad que se implementen en correspondencia con las políticas definidas conforman el cuerpo del sistema de seguridad diseñado y representan la línea de defensa básica de protección de los bienes informáticos, por lo cual es sumamente importante su selección adecuada, de forma tal que cubran las amenazas identificadas durante el proceso de evaluación de riesgos, implementándolas de una manera rentable.

Si la mayor amenaza al sistema es un acceso remoto, tal vez no tenga mucha utilidad el empleo de dispositivos técnicos de control de acceso para usuarios locales. Por otro lado, si la mayor amenaza es el uso no autorizado de los bienes informáticos por los usuarios habituales del sistema, probablemente será necesario establecer rigurosos procedimientos de monitoreo y de gestión de auditoría.

La seguridad será implementada mediante el establecimiento de múltiples barreras de protección, seleccionando controles de diferentes tipos de forma combinada y concéntrica, logrando con ello una determinada redundancia que garantice que, si una medida falla o resulta vulnerada, la siguiente medida entra en acción continuando la protección del activo o recurso. No es conveniente que el fallo de un solo mecanismo comprometa totalmente la seguridad.

La implementación de múltiples medidas simples puede en muchos casos ser más seguro que el empleo de una medida muy sofisticada. Esto cobra mayor validez cuando determinada medida no puede ser aplicada por alguna limitación existente, como pueden ser, por ejemplo: las insuficiencias del equipamiento, que impiden la implementación de una medida técnica. En este caso serán consideradas medidas o procedimientos complementarios de otro tipo que garanticen un nivel de seguridad adecuado.

Hay que tener en cuenta también que el uso del sentido común y una buena gestión son las herramientas de seguridad más apropiadas. De nada vale diseñar un sistema de medidas muy complejo y costoso si se pasan por alto los controles más elementales. Por ejemplo, independientemente de cuan sofisticado sea un sistema de control de acceso, un simple usuario con una clave pobre o descuidada puede abrir las puertas del sistema.

Otro elemento importante para considerar, al implementar las medidas y procedimientos es aplicar el principio de proporcionalidad o racionalidad, que consiste en ajustar la magnitud de estas al riesgo presente en cada caso. Por ejemplo, la salva de la información puede tener diferentes requerimientos en distintas áreas y en una misma área para distintos tipos de datos o programas.

Las medidas de seguridad se clasifican de acuerdo con su origen en: administrativas; de seguridad física, técnica o lógica; de seguridad de operaciones; legales y educativas. A su vez, por su forma de actuar, las medidas pueden ser: preventivas, de detección y de recuperación.

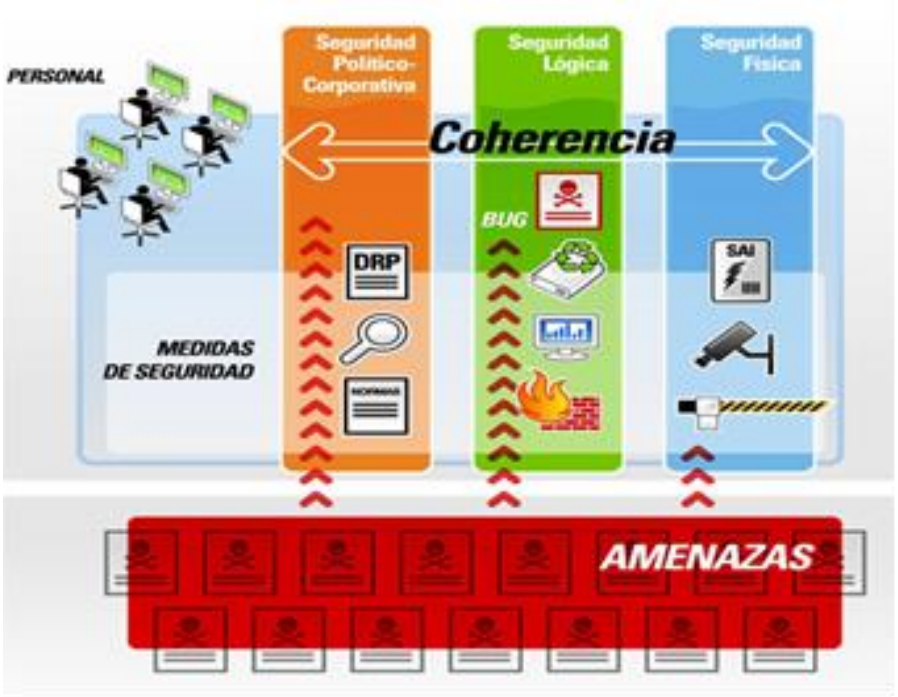

Figura 15.: Medidas de seguridad para la red

- **Medidas administrativas.** Las medidas administrativas, frecuentemente no son apreciadas en toda su importancia, a pesar de que la práctica ha demostrado que un elevado porcentaje de los problemas de seguridad se puede evitar con medidas de esta naturaleza. Se establecen por la dirección de cada entidad mediante las regulaciones comprendidas dentro de sus facultades y por tanto, son de obligatorio cumplimiento por todo el personal hacia el cual están dirigidas.

- **Medidas de seguridad física**. Constituyen la primera barrera de protección en un sistema de seguridad de red e introducen un retardo que incrementa el tiempo de materialización de un acto doloso o accidental.

  Se aplican a los locales donde se encuentran las tecnologías de información y directamente a estas mismas tecnologías e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.
- **Medidas técnicas o lógicas**. Son las de mayor peso dentro de un sistema de seguridad. Pueden ser implementadas por software, a nivel de sistemas operativos y de aplicaciones o por hardware. El uso combinado de técnicas de software y hardware aumenta la calidad y efectividad en la implementación de este tipo de medidas. Algunos tipos de medidas técnicas son empleadas para identificar y autentificar usuarios, protección criptográfica, protección contra virus y otros programas dañinos y registro de auditoría, entre otros.
- **Medidas de seguridad de operaciones**. Están dirigidas a lograr una eficiente gestión de la seguridad mediante la ejecución de procedimientos definidos y deben garantizar el cumplimiento de las regulaciones establecidas por cada entidad y por las instancias superiores a la misma.
- **Medidas legales**. Representan un importante mecanismo de disuasión que contribuye a prevenir incidentes de seguridad y sancionar adecuadamente a los violadores de las políticas establecidas por la entidad. Se establecen mediante disposiciones jurídicas y administrativas, en los cuales se plasman: deberes, derechos, funciones, atribuciones y obligaciones, así como se tipifican las violaciones y tipos de responsabilidad administrativas, civiles, penales u otras.
- **Medidas educativas**. Están dirigidas a inculcar una forma mental de actuar, mediante la cual el individuo esté consciente de la existencia de medidas de para mantener la seguridad en la red.
- **Medidas de recuperación.** Están dirigidas a garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos ante cualquier eventualidad que pueda ocurrir, que afecte o ponga en peligro el normal desarrollo de estos. Se establecen a partir de la identificación de los posibles incidentes o fallos que puedan causar la interrupción o afectación de los procesos informáticos y garantizan

las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios para ello.

Algunos procedimientos de seguridad que pueden ser implementados son:

a) De administración de cuentas de usuarios.

b) De asignación y cancelación de permisos de acceso a las tecnologías y sus servicios.

c) De asignación y cancelación de derechos y privilegios.

d) De gestión de incidentes.

e) De gestión de contraseñas.

f) De realización de auditorías.

g) De acceso a las áreas.

h) De entrada y salida de las tecnologías y sus soportes.

4.4.2 Tecnología de seguridad

Una empresa necesita de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad.

Las políticas y una estimación preliminar de los riesgos son el punto de partida para establecer una infraestructura organizativa apropiada, es decir, son los aspectos esenciales desde donde se derivan los demás.

La mayoría de las organizaciones no tiene los recursos para diseñar e implantar medidas de control desde cero. Por tal razón a menudo escogen soluciones proporcionadas por los fabricantes de productos de seguridad y luego intentan adaptar esos productos a las políticas, procedimientos, normas y demás esfuerzos de integración dentro de la organización. Esto se realiza a menudo sin conocer o entender suficientemente los objetivos y las metas de seguridad. Como resultado, los productos de seguridad escogidos y su aplicación pueden no resultar adecuados a las verdaderas necesidades de la organización.

Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía la gerencia en lo que a seguridad se refiere.

De manera que tales políticas, pueden ser una manera de garantizar de que se está apropiadamente seleccionando, desarrollando e implantando las tecnologías de seguridad.

Algunas tecnologías y configuraciones que se pueden añadir al diseño de la red para proporcionar seguridad están:

a) Red de area local virtual

Una VLAN (Red de Área Local Virtual) es una agrupación lógica de dispositivos o servicios de red, en base a funciones, departamentos, equipos de trabajo o aplicaciones, sin considerar la localización física o conexiones de red. La función de las VLan's es una segmentación lógica de la red en diferentes dominios de broadcast, es decir que los paquetes son solamente conmutados entre puertos que han sido asignados a la misma VLAN. Así como solo los routers proveen conectividad entre diferentes segmentos LAN, también solo los routers o equipos que operen en la capa tres del modelo OSI, proveen conectividad entre diferentes segmentos VLAN. Los routers en topologías VLAN proveen filtrado de broadcast, seguridad y administración del flujo de tráfico.

Ventajas de las VLAN's

- Incrementan el desempeño de la red agrupando estaciones de trabajo, recursos y servidores según su función, sin importar si ellos se encuentran en el mismo segmento físico LAN. (Mejor desempeño, facilidad de administración).
- Facilidad en la administración de adición, movimiento y cambio de estaciones de trabajo en la red. (Flexibilidad, Escalabilidad, Facilidad de Administración).
- Mejoran la seguridad de la red, porque solamente las estaciones de trabajo que pertenezcan a la misma VLAN podrán comunicarse directamente (sin enrutamiento).
- Incrementan el número de dominios de broadcast mientras éstos decrecen en su tamaño. (Mejor desempeño).
- Facilitan el control de flujo de tráfico, porque permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que éstos por defecto son filtrados desde todos los puertos que no son miembros de la misma VLAN en un Switch.(Mejor desempeño).

- La configuración o reconfiguración de VLan's se realiza a través de software, por lo tanto esto no requiere de movimientos o conexiones físicas de los equipos de red. (Facilidad de Administración).
- Las VLan's proveen flexibilidad, escalabilidad, seguridad, facilidad de administración y mejor desempeño de la red.

b) Listas de control de acceso – ACL

Las listas de control de acceso (ACL / Access Control List) incluyen una de descripción de los usuarios y grupos de usuarios con diferentes permisos sobre los archivos y carpetas de un volumen NTFS (New Technology File System).

Aparecer en la lista ACL significa tener derecho de acceso sobre el archivo o carpeta. El tipo de permiso definido en la entrada de un usuario o grupo de usuarios especifica el nivel de privilegio sobre el objeto (lectura, escritura, etc.).

Cada vez que un usuario accede a un archivo o carpeta se verifica si el usuario o el grupo de usuarios al que pertenece tienen al menos una entrada en la lista ACL del objeto. De no ser así, el sistema le niega el derecho sobre el objeto; en cambio, si posee uno o más entradas, el usuario podrá acceder al objeto con los privilegios especificados por los permisos asociados a las entradas.

c) Servidor AAA – Radius

Es un protocolo de autorización y autentificación para aplicaciones de acceso a red, utiliza el puerto 1812 UDP, a su vez facilitara la administración de usuarios y su acceso a dispositivos de red, se encargara de reforzar la seguridad a nivel lógico.

Cumplirá las siguientes funciones:

- Servicio de Autenticación y Encriptación a un cliente
- Usuarios y contraseñas personalizadas por cada cliente.
- Uso de certificados para asegurar la autenticación.

d) Muros de fuego (firewalls)

Básicamente un firewall es una computadora que se encarga de filtrar el tráfico de información entre dos redes. El problema no es el controlar a los usuarios de un sistema sino el prevenir accesos no autorizados de hackers que pudieran atacar la seguridad.

La ventaja de construir un firewall entre una red confiable y una insegura, es la de reducir el campo de riesgo ante un posible ataque. Un sistema que no cuente con este tipo de protección es propenso a sufrir un acceso no autorizado en cualquier nodo que compone la red confiable. En el momento de proteger el sistema con un firewall, el peligro se reduce a un solo equipo.

La mejor manera de proteger una red interna es vigilando y con un firewall bien diseñado obtenemos esta ventaja. Este medio nos puede proveer información de los paquetes de datos que entran a la red, los que son rechazados, el número de veces que tratan de entrar, cuantas veces un usuario no autorizado ha querido penetrar en la red, etc. Con esta información se puede actualizar el sistema de seguridad y prevenir una posible violación al mismo.

Un firewall debe proveer los fundamentos de seguridad para un sistema, pero no es lo único que necesitamos para proteger la red ya que no esta exento de ser pasado por un hacker. Esencialmente se instala entre la red interna y la Internet. El firewall previene el acceso del resto del mundo al sistema y sobre todo a la información que circula por la Intranet. Un firewall combina hardware y software para proteger la red de accesos no autorizados.

e) Kerberos

Es un sistema de autentificación en red. Permite a los usuarios comunicarse sobre las redes computacionales enviando su identificación a los otros, previniendo la escucha indiscreta. Tiene como principio el mantener un servidor de la red seguro o confiable. Provee confidencialidad de la información usando la encriptación y también una autentificación en tiempo real dentro de un ambiente distribuido inseguro.

El modelo de kerberos esta basado en un protocolo de autentificación a través de un servidor confiable ya que este sistema considera que toda la red es una región de riesgo grande excepto por éste servidor. Trabaja proporcionando a los usuarios y a los servicios boletos que pueden usar para identificarse a sí mismos, además de llaves encriptadas secretas proporcionando cierta seguridad en la comunicación con los recursos de la red.

f) SATAN

SATAN es una herramienta de búsqueda y generación automática de reportes acerca de las vulnerabilidades de una red, la cual provee un excelente marco de trabajo para continuar creciendo. Es conocido con dos diferentes nombres: SATAN (Security Analysis Tool for Auditig Networks) lo cual significa herramienta de análisis de seguridad para la auditoría de redes y santa (Security Analysis Network Tool For Administrators) herramienta de análisis de la seguridad en red para los administradores.

SATAN es un programa bajo UNIX que verifica rápidamente la presencia de vulnerabilidades en sistemas remotos, ofrece una forma fácil de que el usuario normal examine en corto tiempo la seguridad en red de los sistemas computacionales.

g) ISS (Internet Security Scanner)

El programa del autor Christopher Klaus es un explorador de seguridad de multinivel del mismo tipo que SATAN, que verifica un sistema UNIX en búsqueda de un número conocido de huecos de seguridad, tales como los problemas en el sendmail, o una de compartición de archivos NFS configurada impropiamente.

Actividad 4.: Caso de estudio

Direccionamiento de IP

En este ejercicio, vamos a ver las direcciones IP de la red de la Compañía ABC.

Red de la Compañía ABC

El administrador de la red de ABC necesita decidir un nuevo esquema de direcciones IP para la redes nuevas de la compañía. Se le pide una propuesta para la compañía.

Las necidades expresadas por los departamentos incluyen:

- Trabajadores en la sede principal, realmente sólo necesitan acceso al sistema de la red interna de la Compañía ABC más la habilidad de navegar el Internet.
- El equipo de desarrollo necesitan acceso completo al Internet.
- El equipo de ingenieros esta preparado para considerar cualquier propuesta pero están preocupados acerca de costos de equipos y quien va a dar soporte a toda la infraestructura de la red.
- ABC cuenta con 3 sucursales más en el país.
- Debe considerarse el acceso remoto a los equipos
- El acceso a través de wifi es indispensable para el equipo de ventas a través de smarthphone.

Preguntas a considerar:

1. **¿**Debe ABC usar una red de clase A, B o C o múltiples redes de una clase en particular?

2. ¿Cómo se asignaran números de redes a las redes en su diseño?

3. ¿Debe ABC considerar establecer una intranet para ahorrarse direcciones IP?

4. ¿Qué otras opiniones son arrojadas de estas consideraciones?

Evaluará también para el diseño los aspectos de la **Seguridad de la Red de la Compañía ABC.**

Usted es el administrador de la red.

Aquí se le provee las necesidades de diferentes departamentos de la Compañía ABC, y usted está en el deber de proveer estas necesidades pero siempre tomando en cuenta la necesidades de seguridad. Trate de responder las siguientes preguntas:

1.- ¿Cuáles medidas de seguridad de la red puede usted usar?

2.- La oficina principal esta expuesta al Internet. ¿Qué tipos de defensas son apropiadas para estos sistemas?

3.- El departamento de Ingeniería necesita la máxima protección. ¿Qué sugiere usted aquí en este caso?

4.- El equipo de desarrollo necesita acceso rápido y fácil a recursos en línea pero posee datos sensibles que no pueden ser robados. ¿Puede usted pensar en una solución que satisfaga ambas de estas necesidades?

5.- También considere que otras sugerencias y medidas de seguridad puede usted tomar para asegurar que nuestra oficina no sea blanco de ataque.

Actividad 5.: Caso de Estudio

Karen y Luis son dos técnicos en sistemas microinformáticos y redes, que quieren presentar un proyecto a un concurso de adjudicación promovido por su municipio.

El proyecto es para la instalación de una red en unas aulas de formación.

Los técnicos de su localidad les han facilitado los planos de las aulas y del edificios, así como un plan de montaje lógico con las necesidades que deben cumplirse en el proyecto.

Ellos saben que necesitan dar cobertura inalámbrica y cableada a unos 80 ordenadores (en tres aulas distintas) que den estar separados varios metros entre sí.

También conocen la existencia de una habitación que debe usarse de cuarto de TIC, por lo que están sopesando aprovechar los cuatro conmutadores de 8 puertos que ya existen en esas aulas, o bien migrar a un sistema sobre un armario rack.

Algunos equipos no tienen tarjetas de red o las tienen averiadas.

En el caso de los portátiles del aula de idiomas, éstos poseen adaptadores inalámbricos poco potentes en su rececpción (pocos metros).

Además, existe la necesidad de segmentar la red por motivos de seguridad y velocidad en las siguientes partes:

Aula de informática

Aula de teledocumentación e internet

Aula de ofimática

Aula de idiomas

Portátiles de los profesores

Con los datos suministrados, responder el siguiente cuestionario

1¿Cómo deben interpretar el diseño lógico de la red? (esquema de direccionamiento estático o dinámico).

2.¿Qué tipo de tarjetas de red son las más adecuadas para la red cableada?

3.¿Qué tipos de dispositivos de interconexión de redes deben elegir y cuáles desechar?

4.¿Que tipo de conmutador o switch es el idóneo actualmente?

5.¿Cómo deben segmentar las redes?

6.¿Qué normas deben cumplir los dispositivos de interconexión de redes inalámbricas?

7.¿Qué tipos de dispositivos de interconexión de redes necesitarán presumiblemente?

8.¿Dónde deben colocar los dispositivos de interconexión?

9.¿Les interesa más hacer una red cableada, inalámbrica o mixta? y Por qué.

10.¿Qué tipos de tecnologías de seguridad es conveniente implementar y por qué?

V. DISEÑO DE ADMINISTRACIÓN DE LA RED

OBJETIVOS:

- Determinar las acciones de administración sobre un determinado escenario de una red de telecomunicaciones.
- Identificar los elementos críticos de una red de telecomunicaciones en términos generales de la administración, como un conjunto de acciones, métodos, herramientas y procedimientos que se llevan a cabo para mantener la operación continua de una red.
- Valorar que la administración de la seguridad brinda un tratamiento basado en la confidencialidad, integridad y disponibilidad de toda la información que se utiliza en las operaciones internas, además fomenta y desarrolla las mejores prácticas en las diversas áreas operativas, buscando cumplir las políticas de seguridad propuestas.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

La administración de redes como tal, consiste en una serie de actividades o requisitos que se deben cumplir para tener un mejor control sobre la red, garantizando su debida operatividad. En esta área se han impuesto diversas soluciones y mecanismos, que propicien una administración ágil, ya sea centralizada o distribuida, gestionando desde los usuarios, permisos y políticas de seguridad, hasta los equipos y las aplicaciones que son parte del sistema de red.

V. Diseño de Administración de la Red

Introducción

Las necesidades de incrementar y mejorar el uso de las redes de información ha provocado que la administración y monitoreo de las mismas sea un factor preponderante en el campo de las telecomunicaciones, para que se pueda mantener un adecuado funcionamiento.

Para completar el diseño de una red de datos es indispensable establecer normas de administración y mantenimiento de red, con el fin de que esta siga teniendo un nivel aceptable de funcionamiento.

Los objetivos del diseño para la administración de red son los siguientes:

- Proporcionar herramientas automatizadas y manuales de administración de red para controlar posibles fallas o degradaciones en el desempeño de la misma.
- Disponer de estrategias de administración para optimizar la infraestructura existente, optimizar el rendimiento de aplicaciones y servicios. Además, prever los crecimientos en la red esperados debido al cambio constante en la tecnología.

5.1 Modelo de una administración

La estandarización del empleo de una variedad de herramientas de red, aplicaciones y dispositivos para la administración de red, se le conoce como modelo de administración de red. Este modelo permite que los componentes (de distintos fabricantes o proveedores) que conforman una red, y los sistemas operativos de los hosts puedan interoperarse con el Sistema de Administración de Red.

Para la Administración de Red existen tres modelos fundamentales:

- Administración de Red OSI.
- Administración Internet.
- Arquitectura TMN (Telecommunications Management Network).

Administración de Red OSI. Definido por ISO, con el objetivo de lograr la administración de los recursos según el modelo de referencia OSI.

El modelo de gestión OSI (Open System Interconection) provee a los fabricantes de un conjunto de estándares que aseguran una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnologías de red utilizados por las empresas a nivel mundial. Proporciona una estructura de red organizada, para conseguir la interconexión de los diversos tipos de

sistemas de Operación y equipos de telecomunicación usando una arquitectura estándar e interfaces normalizadas.

Define una arquitectura Física: estructura y entidades de red; un modelo funcional: servicios, componentes y funciones de gestión; modelo de información: definición de recursos gestionados y un modelo organizativo: niveles de gestión

La finalidad es tener una visión general del modelo de gestión OSI. Los conceptos encerrados en dicho modelo tienen plena vigencia y son la base para la comprensión de otras soluciones de gestión. Propone tres formas distintas de llevar a cabo la gestión en entornos OSI:

- ✓ **Gestión de Sistemas:** Pretende llevar a cabo la gestión de toda la torre de comunicaciones OSI, de una manera específica por medio de protocolos del nivel de aplicación.
- ✓ **Gestión de Nivel:** Pensado para permitir el intercambio de la información de gestión entre elementos de red, que no implementan toda la torre de protocolos OSI. Ejemplo: puentes, repetidores, etc.
- ✓ **Operación en Nivel:** Tiene como objetivo el monitorizar y controlar la comunicación entre los distintos niveles de la torre OSI.

La gestión basada en (OSI) CMIP define un verdadero Sistema de Gestión de Red orientado a objeto basado en la arquitectura de comunicaciones de OSI de siete capas, (el modelo de referencia OSI se define en las series de recomendaciones X.200 de CCITT/ITU-T, y en estándar 7498 de ISO).

Los Sistemas de Gestión de Red basados en (OSI) CMIP pueden ser aplicados para gestionar redes de área local (LANs), redes corporativas y redes privadas de área amplia (WANs), redes nacionales e internacionales. El protocolo de séptima capa (aplicación) utilizado por la gestión OSI es el protocolo común de información de gestión (Common Management Information Protocol: CMIP).

Administración Internet. Definido por la Fuerza de Tareas de Ingeniería de Internet IETF (Internet Enginnering Task Force) y la IAB (Internet Activities Board), para administrar según la arquitectura de red TCP/IP (Protocolo de Control de Transporte/ Protocolo de Internet, Transport Control Protocol / Internet Protocol).

Arquitectura TMN (Red de Administración de Telecomunicaciones). Definida por la ITU-T (Unión Internacional de Telecomunicaciones). Más que un modelo de red, define una estructura de red basada en los modelos anteriores. Es una arquitectura orientada a objeto, que permite una amplia aplicabilidad. Esta fue definida por varios estándares, basando su estructura principalmente en el modelo de comunicaciones de OSI. Su enfoque esta destinado para dar soluciones de gestión a redes de telecomunicaciones, teniendo como eje central el nivel de servicio que debe brindar la red.

Niveles y Arquitectura Lógica de TMN

En el estándar TMN se definen una serie de capas o niveles de gestión mediante las cuales se pretende abordar la gran complejidad de la gestión de redes de telecomunicación. Cada uno de estos niveles agrupa un conjunto de funciones de gestión

- ✓ **Niveles de Elementos de red:** Incluye las funciones que proporciona la información en formato TMN de equipamiento de red, así como las funciones de adaptación para proporcionar interfaces TMN a elementos de red.
- ✓ **Nivel de Gestión de Elementos:** Referente a la gestión remota e individual de cualquier elemento de red que se precise para el establecimiento de conexiones entre dos puntos finales, proporcionando un servicio dado. Este nivel suministra las funciones de gestión para monitorizar y controlar elementos de gestión individuales, en la capa de elemento de red.
- ✓ **Nivel de Gestión de Red:** Proporciona el control, supervisión, coordinación y configuración de grupos de elementos de red, constituyendo redes y subredes para la realización de una conexión.
- ✓ **Nivel de Gestión de Servicio:** Contiene las funciones que proporcionan un manejo eficiente entre los puntos finales de la red, asegurando un óptimo aprovisionamiento y configuración de los servicios prestados a los usuarios.
- ✓ **Nivel de Gestión de Negocio:** Soporta la gestión completa de explotación de la red, incluyendo contabilidad, gestión y administración, basándose para ello en las entradas procedentes de niveles de gestión de servicios y de gestión de red.

Los modelos OSI e Internet se refieren a redes de hosts, mientras que el modelo TMN es de utilidad para los grandes operadores de redes de telecomunicaciones.

5.2 Administración Distribuida

La gestión distribuida sustituye el centro de control de red, con estaciones de gestión locales en las LANs de la organización, cooperando entre ellas. Esto permite a los gestores de los departamentos mantener las redes, sistemas y aplicaciones de sus usuarios locales.

Mediante la gestión distribuida es posible controlar redes de gran extensión de una manera más efectiva, dispersando entre varias estaciones de gestión las tareas de monitorización, recogida de información y toma de decisiones .En esta línea se están realizando esfuerzos para integrar la arquitectura de objetos distribuidos CORBA (Common Object Request Broker Architecture) en los modelos de gestión tradicionales (CMIP/SNMP). Ya que CORBA es más potente que SNMP y menos complejo que CMIP. Añadiendo ha esto la ventaja que supone su proximidad a C++ y Java, dos lenguajes de gran difusión.

La siguiente grafica muestra la interacción de los distintos componentes de una arquitectura de sistemas de gestión distribuida.

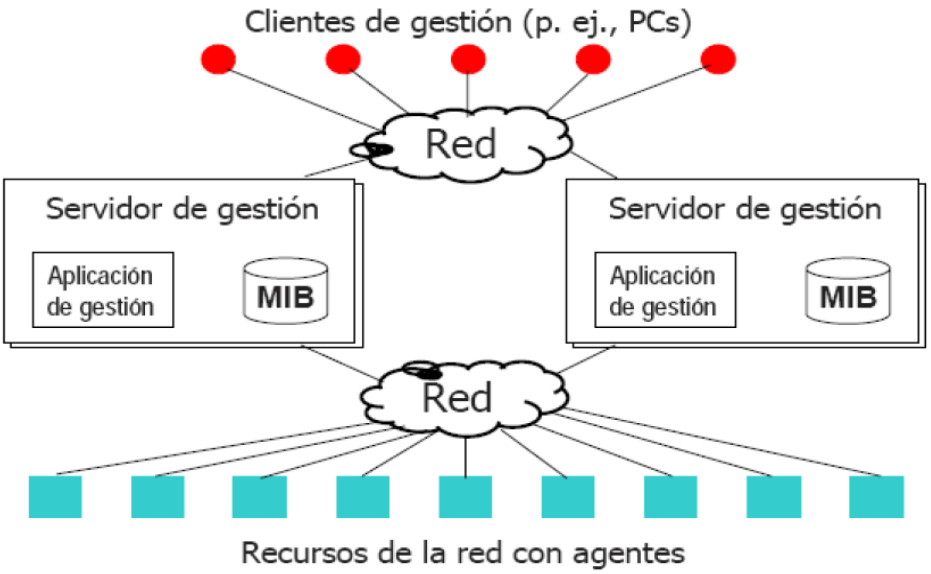

Figura 16.: Interacción de los elementos de la arquitectura de sistemas de Gestión distribuida.

5.3 Administración de una red

La administración de una red abarca las actividades necesarias para operar y mantener la red en las condiciones necesarias para que a través de su vida útil satisfaga las necesidades de los usuarios; tales como disponibilidad, eficiencia y estabilidad y las necesidades del negocio; las nuevas aplicaciones, los nuevos clientes, adoptar nueva tecnología, operación remota, cambios y crecimiento. En términos generales la administración de una red consiste de un conjunto de acciones, métodos, herramientas y procedimientos que se llevan a cabo para mantener la operación continua de una red. Sus objetivos principales son:

- ✓ Lograr la operación continua y eficiente de los sistemas de comunicación
- ✓ Mejorar la productividad de la red.
- ✓ Obtener un mejor rendimiento de los recursos.
- ✓ Mejorar la calidad de servicio ofrecido a los usuarios.
- ✓ Anticiparse a los problemas; evitarlos, minimizar inconvenientes y controlar los daños.
- ✓ Planear crecimiento futuro.
- ✓ Reducir costos.

Las responsabilidades principales del administrador de la red son:

- ✓ Mantenimiento preventivo y correctivo.
- ✓ Actualización tanto en hardware como en software.
- ✓ Resolver problemas de la red.
- ✓ Predecir crecimiento de la red.
- ✓ Seguridad en el sistema.
- ✓ Contabilización de recursos.
- ✓ Mantener registro histórico de fallas.

El administrador de la red se encuentra ante la problemática de que los componentes de las redes en una empresa generalmente son de distintos proveedores y se encuentran en una situación geográfica dispersa en constante crecimiento y con aplicaciones y datos distribuidos. Por lo que el proceso de administración, tiene como elementos fundamentales las herramientas de monitoreo y los procedimientos.

Funciones de administración de red

Las funciones de administración de red se basan en dos procedimientos que ayudan a llevar a cabo numerosas tareas, estos procedimientos son los siguientes:

- **Monitoreo.** El monitoreo es un proceso eminentemente pasivo, el cual se encarga de observar el estado y comportamiento de la configuración de red y sus componentes. También se encarga de agrupar todas las operaciones para la obtención de datos acerca del estado de los recursos de la red.
- **Control.** El control es un proceso que se lo considera activo, debido a que permite tomar información de monitoreo y actuar sobre el comportamiento de los componentes de la red administrada. Abarca la configuración y seguridad de la red, como por ejemplo, alterar parámetros de los componentes de la red.

5.4 Cómo y dónde está la administración

La administración de redes como tal, consiste en una serie de actividades o requisitos que se deben cumplir para tener un mejor control sobre la red, garantizando su debida operatividad. En esta punto se han impuesto diversas soluciones y mecanismos, los cuales han pasado por un largo proceso de adaptación. A consecuencia, se han propuesto diferentes áreas dónde se detallan el dónde y cómo se debe aplicar la administración de la red. Estás áreas son:

- **Administración de prestaciones.**

  Es medir la calidad de funcionamiento, proveer información disponible del desempeño de la red (hardware y software), asegurar que la capacidad y prestaciones de la red correspondan con las necesidades de los usuarios, analizar y controlar parámetros como: utilización, rendimiento, tráfico, cuellos de botella, tiempo de respuesta, tasa de error, throughput, etc.; esto de los distintos componentes de red como switches, ruteadores, hosts, etc., para poder ajustar los parámetros de la red, mantener el funcionamiento de la red interna en un nivel aceptable, poder efectuar análisis precisos y mantener un historial con datos estadísticos y de configuración, predecir puntos conflictivos antes de que éstos causen problemas a los usuarios.

  El conocimiento de esta información nos permite en el futuro tomar acciones correctivas como balanceo o redistribución de tráfico, establecer y reportar tendencias para ser utilizadas en la toma de decisiones y planificación del crecimiento.

Se debe definir claramente los parámetros de funcionamiento o desempeño alrededor de los cuáles, se van a organizar las tareas de Administración de prestaciones como las siguientes:

- Obtención de la información de funcionamiento de la red a través del monitoreo sobre los recursos disponibles.
- Análisis de la información recolectada para determinar los niveles normales de utilización de la red.
- Comparación entre los valores obtenidos y los normales, para generar acciones de inicio de alarmas que pueden generar la toma de medidas preventivas o correctivas.

- **Administración de problemas o fallas.**

  Aquí se maneja las condiciones de error que hacen que los usuarios pierdan toda la funcionalidad de un recurso de la red. La administración de fallas se lleva a cabo en cinco pasos: determinación del problema, diagnostico del problema, recuperación y desvió del problema, resolución del problema, rastreo y control del problema.

  La determinación del problema consiste en detectar un problema y dar todos los pasos necesarios para comenzar el diagnostico del problema, como confinar el problema a un subsistema en particular.

  El diagnostico del problema consiste en determinar la causa precisa del mismo y la medida que es necesario tomar para resolverlo.

  El desvió y recuperación del problema son intentos para desviar el problema, parcial o totalmente. Solo da una solución temporal y depende del modulo de resolución de problemas para resolverlo permanentemente.

  La resolución del problema es la suma de los esfuerzos para eliminarlo. En general comienza una vez terminado el diagnostico del problema y suele implicar acciones correctivas, como el reemplazo de hardware o software en estado de falla.

  El rastreo y control de problemas consiste en el rastreo de cada uno de ellos hasta llegar a su solución final. La información vital que describe el problema se almacena en una base de datos de problemas.

Los objetivos de esta área son: detección, aislamiento, corrección, registro y notificación de los problemas existentes en la red, sondeo periódico en busca de mensajes de error y establecimiento de alarmas.

Las consecuencias de estas fallas pueden causar tiempo fuera de servicio o la degradación inaceptable de la red, por lo que es deseable su pronta detección y corrección.

La diferencia entre falla y error esta en que un error es un evento aislado como la pérdida de un paquete o que éste no llegue correctamente, pero una falla es un funcionamiento anormal que requiere una intervención para ser corregido. La falla se manifiesta por un funcionamiento incorrecto o por exceso de errores.

Las acciones o procedimientos para esta corrección son:

- Determinar exactamente dónde está la falla.
- Aislar el resto de la red, para que pueda seguir operando sin interferencia.
- Reconfigurar la red para minimizar el impacto de operar sin el componente averiado.
- Reparar o reemplazar el componente averiado para devolver la red al estado inicial.
- Si es posible, ejecutar un proceso de corrección automática y lograr el funcionamiento óptimo de la red.
- Registrar la detección y la resolución de fallas.
- Hacer seguimiento de la reparación de fallas.

Una buena política de Administración, es la prevención, es decir, debe adelantarse a los posibles problemas y resolverlos antes de que se produzcan.

- **Administración de contabilidad.**

Esta función proporciona información respecto al funcionamiento de los recursos de red. Las funciones de los equipos de administración de desempeño y contabilidad incluyen el monitoreo de los tiempos de respuesta de los sistemas; la medición de los recursos disponibles; la sintonía, rastreo y control del desempeño de la red. La información recabada por las funciones de administración de la contabilidad y el desempeño es útil para determinar si se están alcanzando los objetivos de desempeño

de la red o si, con base en el desempeño se deben iniciar procedimientos de determinación de problemas.

Su objetivo es controlar el grado de utilización de los recursos de red, controlar el acceso de usuarios y dispositivos a la red, obtener informes, establecer cuotas de uso, asignar privilegios de acceso a los recursos.

Finalmente, se debe hacer un seguimiento del uso de recursos de la red por parte de un usuario o grupo de usuarios. Todo esto para regular apropiadamente las aplicaciones de un usuario o grupo y además permitir una buena planificación para el crecimiento de la red.

Los objetivos de la función de administración de contabilidad son:

- Vigilancia de abuso de privilegios de acceso.
- Evitar sobrecargas en la red y perjuicios a otros usuarios.
- Uso ineficiente de la red.
- Modificar la forma de trabajo para mejorar prestaciones.
- Planificación del crecimiento de la red.
- Saber si cada usuario o grupo tiene lo que necesita.
- El aumento o disminución de derechos de acceso a recursos.

- **Administración de configuraciones.**

  El objetivo es controlar la información que describe las características físicas y lógicas de los recursos de la red, así como las relaciones entre dichos recursos. Un sistema de administración central almacena los datos en la base de datos de la administración de la configuración e incluye información como los números de versión del software del sistema o micro código; números de serie del hardware y software; ubicación física de los dispositivos de red; nombre, direcciones y números telefónicos de contactos. Los elementos de la administración de la configuración ayudan a llevar un inventario de los recursos de la red y asegurar que los cambios en la configuración de la red se reflejen en la base de datos de la administración de la configuración.

  Los sistemas de administración de problemas utilizan esta información para comparar las diferencias en versión y para ubicar, identificar y verificar las características de los recursos de la red.

Las funciones de ésta administración son: inicialización, desconexión o desactivación ordenada de la red o de parte de ella, mantenimiento y adición de componentes, reconfiguraciones, definición o cambio de parámetros de configuración, denominación de los elementos de la red, conocimiento de que dispositivos hay en la red, hardware y configuraciones de software de dichos dispositivos.

Las tareas que se presentan en la administración de configuración son:

- Es deseable que el arranque y parada de componentes específicos, se puedan realizar de forma remota.
- Definir información de configuración de recursos.
- Mantener ésta información, por si se sufre un ataque, poder realizar una comprobación de la información de configuración para asegurar que permanece en un estado correcto.
- Modificación de propiedades de recursos e información al usuario de estos cambios.
- Control de versiones de software.
- Actualización de software.
- Establecer qué usuarios pueden utilizar qué recursos.
- Inicialización y finalización de servicios de red.

Las herramientas típicas para ésta administración son: monitorear la red para ver qué elementos hay activos y con qué características obtener la información, para saber de qué modo están conectados entre sí los diferentes elementos, ésta información se mantiene para ayudar a otras funciones de administración.

- **Administración de Operaciones.**

  Consiste en administración distribuida de los recursos de la red desde un punto central por medio de dos conjuntos de funciones: servicios de administración de operaciones y servicios de operaciones comunes. Los servicios de administración de operaciones permiten controlar los recursos remotos centralmente por medio de las funciones siguientes: activación y desactivación de recursos, cancelación de comandos y configuración del reloj.

Los servicios de administración de operaciones se pueden iniciar automáticamente en respuesta a ciertas notificaciones de problemas en el sistema. Los servicios de operaciones comunes permiten la administración de recursos que no son manejados explícitamente por otras áreas de administración, por medio de una comunicación especializada a través de aplicaciones nuevas y más capaces. Los servicios de operaciones comunes proporcionan dos servicios importantes, el comando ejecutar y la administración de recursos. El comando ejecutar representa una forma estándar para ejecutar comandos remotos.

La administración de operaciones rastrea los cambios en la red y mantiene archivos de modificaciones en los nodos remotos. Los cambios en la red ocurren principalmente por dos razones: cambios en los requerimientos del usuario y evitar problemas. Los cambios en los requerimientos del usuario incluyen las actualizaciones en hardware y software, nuevas aplicaciones, servicios y otros factores que modifican constantemente las necesidades de los usuarios de la red. Evitar problemas es necesario para enfrentar cambios inesperados producidos como resultado de la falla de hardware, software u otros componentes de la red. La administración de operaciones tiene como objetivo minimizar los problemas promoviendo de manera ordenada los cambios de la red y administrando los archivos de cambios, los cuales guardan una bitácora de las modificaciones realizadas en la red.

5.5 Administración de la seguridad

La administración de la seguridad es la encargada de brindar un tratamiento a la información, basado en la confidencialidad, integridad y disponibilidad de toda la que se utiliza en las operaciones internas, además fomenta y desarrolla las mejores prácticas en las diversas áreas operativas, buscando cumplir las políticas de seguridad propuestas.

El objetivo de la administración de la seguridad es controlar el acceso a los recursos de la red con respecto a las normas de consulta locales, de modo que la red no pueda ser saboteada (intencionalmente o involuntariamente) y que la información que es vulnerable no pueda ser utilizada por aquellos sin una autorización apropiada.

La administración de seguridad, por ejemplo, entre sus funciones está vigilar a los usuarios que entran a un recurso de la red, rechazando el acceso aquellos que introduzcan códigos de acceso no validos. Dividir los recursos de la red en áreas autorizadas y en áreas no autorizadas. Identificar los recursos de la red que son vulnerables (incluso los sistemas, archivos y otras entidades) y determinar la relación entre estos recursos y su utilización.

La administración de la seguridad se compone de 4 procesos básicos:

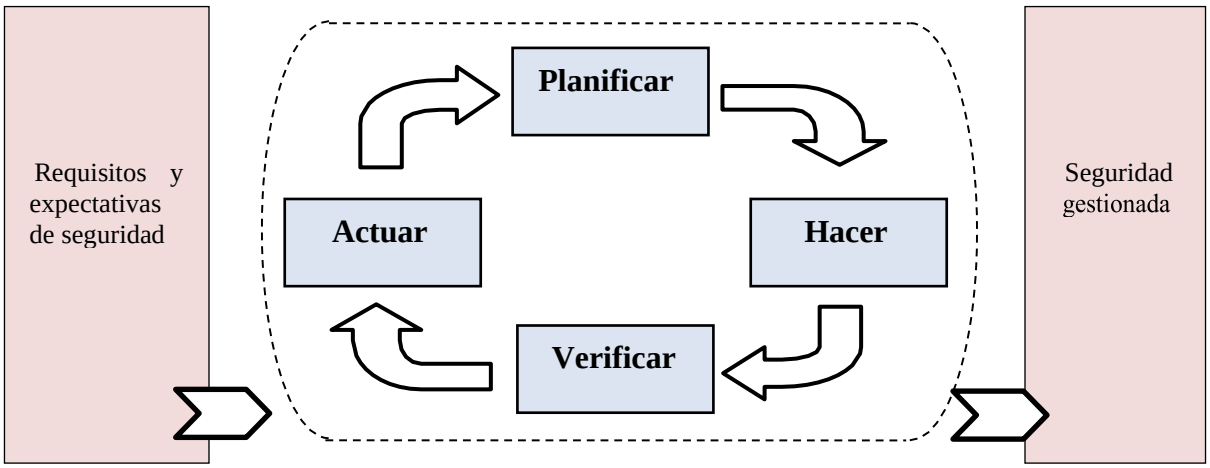

Figura 17.: Procesos básicos de la administración de la seguridad

Planificar	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización.
Hacer	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos.
Verificar **Revisar y dar seguimiento**	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política, los objetivos de seguridad y la experiencia práctica, también reportar los resultados a la dirección, para su revisión.
Actuar **Mantener y mejorar**	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua.

El segumiento de estos procesos, asociados a los requerimientos de seguridad de la red, le proyectan una vía confiable al administrador de la red para realizar un exitoso plan de administración para mantener la seguridad de la red.

El administrador de la red debe también tomar en cuenta que la seguridad está dividida en: Seguridad física, Control de acceso y Seguridad de transmisión. Para cada uno de los tipos de seguridad, el administrador de la red debe tomar medidas para prevenir e impedir que de alguna u otra forma, se ponga en riesgo la seguridad de la información.

- ✓ **Seguridad Física.** La seguridad física trata de proteger a la red de daños ocasionados por personas o causas naturales.

  Por ejemplo, la principal amenaza para el cable de una red parecen ser los trabajadores que ignoran cual es el cable estropeado y cortan uno que no era. Marcar la localización de los cables puede ofrecer una medida de protección contra esto. Los mismos usuarios pueden dañar los cables desconectándolos o enroscándolos, particularmente si estos están expuestos en las oficinas donde se conecto una terminal. La mejor solución para esto es tener una salida en la pared a la cual se conecta la terminal. Existen cierto riesgo de que el cable sea dañado por los animales, como roedores. Una zanja profunda o salidas con cubiertas muy fuertes pueden ayudar en estas situaciones.

  La integridad de la red puede ser afectada también por causas naturales como inundaciones e incendios los cuales pueden dañar cables y o servidores. Los servidores se pueden dañar por exceso de calor o humedad es necesario una cuidadosa planeación de la instalación de cable y servidores.

- ✓ **Control de Acceso**. Las funciones principales de control de acceso son autorizadas a ciertos usuarios para que utilicen los recursos de la red e impide que los usuarios no autorizados hagan uso de la red.

  El mecanismo más comúnmente empleado es el uso de passwords. Los passwords pueden ser usados para limitar el acceso algunos o todos los recursos de la red. Cada dispositivo o recurso puede tener su propia lista de passwords, de tal manera que el usuario tenga que dar varios passwords durante una sesión o tener un password para accesar todos los recursos autorizados. Frecuentemente los passwords no resultan

efectivos, porque los usuarios no tienen cuidado de elegir un password apropiado o protegerlo de que los descubran. Una política de seguridad efectiva puede ser:

Asignar passwords a través del sistema o por una persona de seguridad.

Incluir una mezcla de caracteres alfabéticos y no desplegables (return, escape, etc.).

Cambiar regularmente los passwords.

Enfatizar a los usuarios la necesidad de proteger los passwords y quizá penalizar la falta de cuidado.

Los procedimientos para administrar los passwords, incluyendo como deben ser definidos y distribuidos y que tan frecuentemente deben ser cambiados, debe ser parte del plan de administración de la seguridad de la red.

Es conveniente realizar una revisión periódica de los puntos vulnerables de la red para evitar que por medio de ellos se introduzcan usuarios sin autorización. Estos puntos más vulnerables son: Cuartos de equipo y gabinetes de cables.

Como puntos de concentración de una gran cantidad de circuitos, los cuartos de equipo y gabinetes de cables son particularmente vulnerables. Estos deben permanecer bien cerrados y asignar las llaves a personas autorizadas.

Niveles de Seguridad en Base de Datos. Una base de datos puede ser programada para aceptar acceso a los archivos solo desde las terminales autorizadas además, como es difícil asegurar que personas no autorizadas utilicen estas termínales, es conveniente que además de códigos de terminales se tengan passwords en una base de datos se pueden manejar las siguientes clasificaciones:

- Los archivos personales solo pueden ser accesados por sus dueños.

- Los archivos privados solo pueden ser accesados para lectura y escritura por la lista de passwords autorizados.

- Los archivos compartidos pueden ser leídos por todos, pero escritos solo por un grupo limitados.

- Los archivos públicos pueden ser leídos por todos lo que tengan acceso a la base de datos.

- ✓ **Seguridad de la transmisión.** Las redes están diseñadas para compartir el mismo medio de transmisión. Los dispositivos son capaces de copiar todos los mensajes y descartar los mensajes dirigidos a otros dispositivos. Los analizadores de protocolos

pueden monitorear todo el trafico de la red y fácilmente desplegar el contenido de los mensajes. La encriptación es la mejor solución a este problema.

La seguridad en la transmisión se refiere a la protección de la información en transito en la red de las amenazas de fugas o inyección de información. Fugas de información se refiere al acceso no autorizado con el fin de obtener información de la red. Esto comúnmente sucede a través de conexiones secretas pasivas. Inyectar información se refiere introducir información señales en la red, las cuales se disfrazan como señales auténticas o alteran las señales auténticas. La inyección es una característica de una conexión secreta activa. La encriptación es una de las soluciones tanto para la fuga como inyección de información. Con la encriptación los mensajes son traducidos a otro código en la estación origen y transmitidos al otro extremo, donde al recibir el mensaje se descifra. Sin el conocimiento del proceso de encriptación usado, el mensaje es ilegible. Cuando se usa una encriptación, la fuga de información deja de ser un problema porque el mensaje es ilegible para la persona no autorizada que lo pretende leer. La inyección de información también se previene porque el perpetrador no conoce las reglas que debe seguir para encriptar correctamente.

Al desarrollar un plan de seguridad para la red es conveniente atacar los siguientes puntos: Protección Operacional, Encriptación, Manejo de llaves, Autenticación, Numeración secuencial de los paquetes transmitidos, Procedimientos de Log - on y password.

La Seguridad en las redes puede verse afectada por dos tipos de ataques:

- **Ataques Activos.**

  En este tipo de ataques existe evidencia del hecho por mal funcionamiento de componentes o servicios, o por sustitución de usuarios en ejecución de tareas orientados a tratar de conseguir información privilegiada o interrumpir un servicio crítico para la organización, puede ser desde el interior o del exterior.

  Ejemplos de estos ataques son: modificación del contenido de los datos que circulan por la red, alteración del orden de llegada de los datos, supresión de mensajes con un destino particular, saturación de la red con datos inútiles para degradar la calidad de servicio, engaño de la identidad de un host o usuario para acceder a datos confidenciales, desconfiguraciones para sabotaje de servicios.

- **Ataques Pasivos.**

  Ataques difíciles de detectar, ya que no se produce evidencia física del ataque pues no hay alteración de datos ni mal funcionamiento o comportamiento fuera de lo habitual de la red, escucha o "intercepción del tráfico de la red y los servicios involucrados", estudio de parámetros de configuración de manera ilegal por parte del intruso, robo de información sensible para las organizaciones.

Para cualquiera de los tipos de ataques se puede prevenir o solucionar a través de las siguientes actividades:

- Fortalecer políticas de administración y asignación de claves.
- Historiales de seguridad, para posterior análisis.
- Uso de cortafuegos para monitorear y controlar los puntos de acceso internos y externos a la red.
- Encriptar o cifrar de la información enviada por la red.
- Localizar la información importante.
- Registrar los usuarios que consultan dicha información y durante qué períodos de tiempo, así como los intentos fallidos de acceso.
- Señales de alarma.
- Establecimiento de mecanismos y políticas de prevención.
- Sistemas de detección de intrusos.
- Sensibilización de seguridad en el usuario.
- Mantenimiento del sistema operativo y sus aplicaciones relacionadas.
- Utilizar herramientas de monitoreo en los diferentes niveles.
- Configurar de manera segura los elementos y servicios de red.

Actividad 6.: Implementación del Nuevo Producto de Administración de Red.

Su tarea como administrador es planificar la implementación del nuevo producto de administración de red, en toda la empresa ABC, y el caso de Karen y Luis en el instituto, presentados en el capítulo anterior,. Le será necesario tomar en consideración los siguientes puntos:

1.- ¿Cuáles parámetros del sistema y de la red debe usted medir?

2.- ¿Cuáles son los nodos críticos en la red existente en la compañía en este momento?

3.- ¿Dónde tiene sentido colocar la estación de trabajo que efectuará la administración?

4.- ¿Existen algunas situaciones de red comunes que usted puede programar cierto tipo de respuesta automatizada?

5- ¿Es necesario realizar un plan para la administración de estos casos específicos? Presente una propuesta del plan y el software o sistema que utilizará para ejecutarlo.

VI. VALIDACIÓN, PRUEBA Y OPERACIÓN

OBJETIVOS:

- Determinar las acciones para llevar a cabo pruebas de verificación y validación sobre un determinado escenario de una red de telecomunicaciones.
- Conocer los principales métodos de resolución de averías en una red.
- Identificar los síntomas en una red y las posibles averías asociadas, así como las soluciones más probables.
- Comprobar que los servicios de la red mantienen su funcionalidad.
- Registrar las operaciones y pruebas realizadas siguiendo las buenas prácticas de gestión de documentación.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Este capítulo tiene como propósito definir y estandarizar los procedimientos para la activación de pruebas de verificación y validación relativas a los servicios que ofrece la red, como pueden ser, las interconexiones entre las redes, las condiciones de las interfaces del equipo de transmisión, la interoperabilidad entre los equipos, la recepción y envío de paquetes en los tiempos requeridos, la disponibilidad de los servicios, etc.

Estas pruebas tendrán como objetivo evaluar las condiciones y la funcionalidades de la red, con respecto a los requerimientos que definieron a los diseños físicos y lógicos de la red.

Por último, se da un pantallazo a los problemas más comúnes y las soluciones frecuentes a distintas situaciones que ocurren en las redes de datos.

VI. Validación Prueba y Operación

Introducción

Se dice que el mejor diseño sólo es bueno como lo es su implementación. Es por esto, que no es suficiente diseñar la red para cumplir con los requisitos. También se debe comprobar que cada paso del esfuerzo de diseño cumpla con los requisitos adecuados como se definió en la especificación de requerimientos.

Estas actividades se llaman verificación, validación, prueba y demostración. La verificación tiene lugar en cada paso en el ciclo de vida del proyecto, mientras que la validación ocurre después de que se instala el sistema y antes de ponerlo en servicio. Las pruebas y la demostración ocurren con todos los servicios levantados y en operación.

Estas actividades le ayudan a quitar tantas fallas sistemáticas del sistema como sea posible. Las fallas sistemáticas son las que están “integradas” al sistema como resultado de errores humanos, contrario a las fallas aleatorias que ocurren cuando el equipo se descompone.

Dichas actividades proporcionan un alto nivel de garantía de que el sistema de red funcionará de acuerdo con su especificación de requisitos; y las prácticas de dcumentación le pueden ayudar a producir (y mantener) la prueba de que el sistema de red está diseñado e implementado adecuadamente.

6.2 Verificación

Para verificar la red diseñada, se pueden utilizar distintas aplicaciones o herramientas tanto de hardware como de software, éstas permitirán realizar pruebas de verificación de conectividad de los equipos y otras pruebas para responder a las interrogantes siguientes:

¿Están siendo los paquetes IP v4 e IP v6 encaminados correctamente?

¿Está trabajando bien el NAT interno y externo?

¿Está trabajando correctamente los protocolos RIP y OSPF?

¿Están todas las redes incluidas en las tablas de rutas?

¿Funcionan bien los servidores (web, mail, ftp, VoIP, video, etc.)?

¿Funcionan bien las políticas de seguridad, en especial las ACL?

¿Funcionan bien las redes LAN virtuales (VLAN)?

¿Están trabajando correctamente los túneles y dobles pilas IP V4 – IP V6?

¿Está funcionando adecuadamente el Cortafuegos (Firewall)?

¿Están funcionando bien los servidores Proxies?

Estas y otras interrogantes ayudarán a verificar el estado de la red.

La verificación se puede realizar mediante análisis, pruebas o una combinación de ambos. Las actividades podrían incluir:

- ✓ Revisión de documentos de todas las fases del ciclo de vida del sistema de red, para garantizar el cumplimiento con los objetivos y requisitos.
- ✓ Revisión del diseño
- ✓ Pruebas de los productos diseñados para garantizar que funcionen de acuerdo con su especificación.
- ✓ Pruebas de integración realizadas cuando se juntan diferentes partes del sistema.

Las actividades de verificación y sus resultados se documentan completamente para mostrar no sólo que el diseño ha cumplido con los requisitos, sino también que usted ha comprobado para asegurarse de que así sea y que ha hecho las correcciones necesarias

Los procedimientos de verificación y comprobación se dividen en tres partes: rendimiento de enlace (sobre el cableado), transmisión (sobre los componentes del cableado) y medidas de los componentes.

- El equipo del proyecto deberá formar un equipo de trabajo para efectuar las pruebas necesarias. Es muy importante tener la aprobación del usuario, quien deberá revisar y aprobar que las pruebas propuestas son esenciales para el funcionamiento del sistema. Se deben involucrar analistas, diseñadores, representantes de usuarios y expertos de pruebas del sistema. En caso de que el resultado de las pruebas conduzca a cambios en el diseño. Se deben usar procedimientos formales y documentos para evaluar y obtener la aprobación final a cada cambio propuesto. Además, se debe asegurar que el sistema funciona de acuerdo a los tiempos de respuesta esperados en el diseño. Y finalmente, se debe escribir la aprobación, con el objeto de identificar modificaciones y establecer el nivel de confianza del sistema. Algunas de las pruebas que debe ser aplicadas en este proceso incluyen:
- Probar las capacidades de transferencia de archivos con todos los tipos de archivos soportados.
- Probar que todos los equipos funcionen adecuadamente con los diferentes tipos de Sistemas Operativos.

- Si la red lo soporta, enviar múltiples archivos a nodos únicos simultáneamente, para probar sincronización y acceso a la red.
- Si es soportado el software de terminal virtual, se debe probar la conexión con diferentes sistemas y aspectos de enlace (edición de pantallas, formas, graficas, etc).
- Escribir programas "muestras" para probar librerías y futuras aplicaciones.
- Probar las facilidades ofrecidas por el software de control o administración de la red. (desconectar equipos y observar)
- Probar las aplicaciones que actualmente se encuentran operacionales. Para observar compatibilidad con el nuevo sistema.
- Desconectar nodos y verificar estabilidad de la red. Esto se hace a mitad de una sesión para verificar el control de error y recuperación.
- Probar el rendimiento del sistema: a) Tiempo de establecimiento de sesión o conexión. b) Tiempo de respuesta en la transmisión de datos / archivos. c) Medición del "throughput" del sistema. d) Medición de los "time out's".

Estas verificaciones deben realizarse durante la ejecución de cada fase del proyecto, y si las pruebas de verificación arrojan la necesidad de cambios en el diseño y configuración de la red, estos cambios deben ser ejecutados de ser necesario para cumplir con los objetivos y requerimientos.

6.3 Validación

La validación se basa en las actividades de verificación agregando pruebas completas de la red, para comprobar que todo funcione como debe. Esto demuestra que cada función de la red, así como los equipos y sistemas en sí, cumplen con todos los requisitos contenidos en la especificación de requisitos.

Mientras que la verificación se hace en todo el proyecto y se puede realizar donde se está haciendo el trabajo, la validación ocurre sólo en sitio, después de que se ha instalado y comisionado el sistema.

Entre otras cosas, las pruebas de validación pueden incluir la confirmación de que …

- ✓ La red funciona adecuadamente en todos los modos de operación relevantes.
- ✓ El sistema de red funciona satisfactoriamente bajo los modos de operación normal y anormal como se define en la especificación de requisitos de seguridad.

- ✓ La interacción en la red con distintos tipos de equipos y software conectados no afecta o restringe la habilidad de respuesta del sistema
- ✓ Los enlaces, y elementos finales de control (incluyendo canales redundantes) funcionan como se requiere.
- ✓ La comunicación en la red sigue funcionando como está diseñada cuando ocurre pérdida y restauración de servicios públicos, tales como energía eléctrica.

La validación requiere una planificación precisa para identificar y documentar los procedimientos, medidas y pruebas que se usarán, así como el orden y programa de las pruebas y las aptitudes requeridas del personal que las realizará.

6.4 Prueba y Demostración

Cada fase de las pruebas debe confirmar que la fase de desarrollo correspondiente ha cumplido completamente con cada uno de sus objetivos. Para alcanzar esa meta se requiere una completa y rigurosa planificación.

Por ejemplo, se debe asegurar de considerar y documentar lo siguiente:

- ✓ **Estrategia de pruebas:** incluyendo los escenarios de pruebas, resultados esperados y cómo lidiar con la corrección de discrepancias.
- ✓ **Proceso de pruebas:** incluyendo criterios para declarar que una prueba está completa.
- ✓ **Requisitos de personal:** cuántos, por cuánto tiempo y con qué habilidades.
- ✓ **Requisitos de tecnología:** herramientas, analizadores y software de soporte necesario.

Aunque generalmente los administradores de la red, junto con el equipo de diseño e implementación de la red, son los responsables de ejecutar las pruebas, es una buena idea que las pruebas sean conducidas por gente diferente a la que diseñó e implementó el sistema. Alguien independiente que haga las pruebas tiende más a emplear el equipo y software en maneras que el diseñador y el que implementó el sistema no anticiparon, tales como introducir valores de datos válidos y no válidos.

Las pruebas son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- ✓ **Pruebas de conectividad física.**

  Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- ✓ **Pruebas de conectividad lógica.**

  Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

- ✓ **Pruebas de medición.**

  Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

Una vez culminada las pruebas, estas deben documentarse. Para que la documentación se pueda usar y se le pueda dar mantenimiento, debe estar bien organizada. Las buenas prácticas de documentación, tales como las que se definen en la norma de gestión de la calidad ISO 9000, están diseñadas para garantizar el control de la creación, revisión, aprobación, distribución y almacenamiento de documentos. Entre los documentos que se deben incluir estan:

- Resultados de la evaluación de peligros, riesgos y amenazas.
- Suposiciones usadas cuando se determinaron los niveles de seguridad, velocidad, etc.
- Especificaciones de requisitos.
- Trazabilidad entre los documentos y la especificación de requisitos de seguridad
- Documentación del diseño
- Información y/o documentación de las modificaciones
- Registros de verificación y validación de calificación
- Procedimiento(s) para la validación del sistema
- Procedimientos de operación del sistema
- Procedimientos de mantenimiento del sistema
- Procedimientos de pruebas de aceptación por parte de los usuarios
- Resultados de evaluaciones y auditorías

6.5 Solución de Problemas

El momento culminante del proyecto es cuando el sistema entra en operación. Sin embargo antes de la puesta en operación del sistema se deben contar con los siguientes requerimientos;

Mecanismo de soporte de problemas:

Cuando algo no funciona o se tiene duda ¿Quién resuelve los problemas?.

- Actualizar las políticas de administración de la seguridad en un ambiente de redes.
- Finalizar los contratos de mantenimiento y soporte con el proveedor. Comunicar estos al grupo de soporte interno.
- Producir, copiar y distribuir guías y manuales de usuario. Estos son documentos de consulta rápida.
- Establecer los procedimientos de control y administración. Esto sirve para saber como es controlada la red, como se hacen las actualizaciones, los respaldos y las otras tareas relacionadas a la administración.
- Crear o modificar los planes de recuperación en caso de desastre. Para reflejar la necesidad y utilización de la red en una operación de recuperación siguiendo a un desastre.
- Otros elementos relacionados.

Principios Generales para Localizar Averías

Hay muchas metodologías para localizar averías.

- **Reconozca los síntomas**. Muy a menudo, uno no puede solucionar el problema porque uno no lo ha identificarlo correctamente.
- **Investigue el problema.** Debe siempre asegurarse de identificar donde y cuando el problema comenzó tan bien como cuántos sistemas pueden ser afectados semejantemente.
- **Adquiera Información** Este paso puede ser una consecuencia del paso anterior. Se cerciora de siempre usted tener toda la información disponible de las fuentes, de la gente, y de los sistemas implicados.
- **Pruébelo**. sea seguro interpretando sus resultados.

- **No salte a las Conclusiones**. A menudo el primer impulso que usted tiene puede curar el síntoma pero no el problema subyacente. Asegúrese siempre de usted haber cavado profundamente bastante para aislar la fuente del problema.
- **Encuentre la Avería**. Este paso se podía también llamar encontrar la causa a los efectos descubiertos.
- **Lista de lo qué Podría Ser**. No subestime la reunión de reflexión y la suerte en este paso. Ayuda a menudo a conseguir varios diversos pares de ojos y la habilidad fija implicado en identificar causas posibles.
- **Elimine los Problemas Uno Por Uno**. Cuando usted no sabe cuál es el problema, pero usted sabe lo que podría ser, comienze a eliminar las menos probables. Usted puede encontrar a menudo que las causas son aisladas mejor con el proceso de la eliminación que intentando corregir lo que no es el problema. Recuerde que mientras más causas, no posibles son eliminadas, menos el trabajo que tendrá que efectuar para corregir el problema.
- **Corrija la Avería**. Ésta es normalmente la parte fácil. Cerciórese de que usted cure la enfermedad, no apenas el síntoma.
- **Analice la Falla**. Ahora que no hay presión puesto que pudo corregir el problema, haga las preguntas importantes: ¿Se repetirá? ¿Es un síntoma de otros problemas? ¿Qué contribuyó a este suceso? ¿Cómo prevengo esto en el futuro?

Caja de Herramientas para Corregir Averias

Recuerde que mientras más herramientas de corregir fallas posea mejor serán sus chances de éxito. Herramientas para corregir fallas de ambas indole de software y de hardware, asi como la preparación fundamentada y la experiencia de quien le pueda ser de asistencia, pueden hacer la resolución de problemas más rápida y más fácil.

Herramientas De Software Entre algunas de las herramientas de software útiles para asistir en la resolución de problemas TCP/IP se pueden incluir: ping, netstat, traceroute, ifconfig, lsmod, route, ps. Los ficheros del log pueden también ser especialmente útiles. Revise siempre y cuando sea posible los ficheros de diario, por existencia de los mensajes de error. Incluso los mensajes no relacionados con el problema particular que usted está tratando de solucionar pueden resultar provechosos asi como pueden asistirle a no perseguir pistas

erróneas y evitar así perder un tiempo valioso en aíslar la causa principal del problema. Siempre y cuando pueda habilite el servicio de log de mensajes, particularmente los críticos.

Herramientas De Hardware. Los analizadores de red pueden ser particularmente útiles en el diagnóstico de problemas de red, y en algunos casos, pueden hastas recomendar curso de acción para remediar los problemas. Los analizadores de red disponibles pueden ser basados en hardware o software y dedicado o no dedicados. Los fragmentos de paquete capturados (y por lo general interpretados) por los analizadores de red son el mejor método para determinarse qué realmente está sucediendo en su red. Al hacer su investigación siempre recuerde que los administradores de sistema, los usuario e incluso las máquinas y los softwares pueden mentir, pero el cable nunca mintirá.

Otras Herramientas No se olvide de que su herramienta más útil es su cerebro y los otros cerebros que usted puede integrar a la solución del problema.

Consejos de resolución de problemas de red generales

Uno de los primeros signos de que hay problemas en una red es una pérdida de comunicación de uno o varios hosts. Si un host no aparece la primera vez que se añade a la red, el problema puede ser uno de los archivos de configuración. También puede deberse a una tarjeta de interfaz de red defectuosa. Si un único host comienza a dar problemas de manera repentina, la interfaz de red puede ser la causa. Si los hosts de una red pueden comunicarse entre ellos pero no con otras redes, el problema podría estar en el enrutador. O también podría estar en otra red.

Puede usar distintos comandos según el sistema que este usando para obtener información sobre interfaces de red, ver las estadísticas de protocolo y tablas de enrutamiento. Los programas de diagnóstico proporcionan varias herramientas de resolución de problemas.

Las causas de problemas que afectan al rendimiento de la red resultan más difíciles de identificar. Puede usar herramientas como ping para evaluar problemas como la pérdida de paquetes de un host.

Problemas Físicos Comunes.

Problemas fisíos que involucran conectividad y enrutamiento.

- ✓ **Conectividad**. Pongale mucha atención a las cosas más simples y obvias. Muy a menudo la resolución de un problema de alto nivel puede ser simplificado observando deficiencias obvias en el sistema.

  Primero, ¿Están todos los cables conectados correctamente? ¿se encuentran conectados el teclado y el ratón? ¿está el cable de red en el lugar correcto y en perfecto estado? Se han dedicado muchas horas inecesarias localizando el problema de red. Esto ocurre muchas veces, cuando sólo era un cable desconectado, por accidente u otras fallas simples. Siempre haga las cosas simples primero y busque lo obvio y no lo complejo inicialmente al empezar a localizar averías.

- ✓ **Enrutamiento**. Si usted se encuentra en una red enrutada, lo que es la generalidad de hoy en día, la resolución de problemas en su caso llega a ser un poco más compleja para usted determinar en qué segmento o subred está la avería. La detección de esto puede implicar muchos pasos, incluyendo (pero no limitado a):

  ¿Muestra el ping pérdida de paquetes?

  Una conexión lenta puede ser la causa de éstas pérdidas. O no trabajar del todo.

  Si sus manejadores de red se cargan como módulos en el kernel, puede ser que necesite utilizar el comando lsmod para asegurarse de que el módulo apropiado este cargado en el kernel. Luego, revise las tablas de enrutamiento para verificar que estén válidas y correctas. Utilice el comando route para comprobar sus tablas de enrutamiento IP. Usted puede utilizar el comando netstat para visualizar el estado de las conexiones de red actuales y con la opción -a para imprimir todos los sockets, incluyen los que se encuentra escuchando por peticiones. Asegurse de detener conexiones en ambos puntos. Los paquetes pueden fluir desde un punto pero no desde el otro, causando la confusión y enmascarándo donde sucede el problema.

- ✓ **Problemas Lógicos Comunes**. Los problemas lógicos conciernen con archivos de configuración, un proceso del servidor, la pila del TCP/IP, servicio de nombre y archivos de diario. Archivos de Configuración ¿Le parecen aceptables? Sea especialmente cuidadoso de los cambios recientes, especialmente ésos que coinciden sobre preguntas relacionadas con el problema en cuestión. Procesos del servidor debe preguntarse ¿Se encuentra el servidor en cuestión ejecutándose? Para determinar esto, intente conectar se con él con una sesión de telnet. Utilice el comando ps -ax para

visualizar los procesos actualmente ejecutándose. ¿Es el proceso en ejecusión el proceso correcto (es decir, está el servidor en ejecusión corriendo el proceso que se supone? No se olvide asegurarse que todos los sistemas no tengan ningún servicio extraño o innecesario ejecutándose. Éstos podrían estar interfiriendo con los servicios necesarios, y no todos los sistemas tienen todos los servicios habilitados.

Actividad 7.: Escenarios de resolucion de problemas

Hay algunos problemas que usted va a enfrentar más a menudo que otros:

- Dificultad de poner hardware a funcionar correctamente
- Problemas de resolución de nombre
- Conexiones intermitente entre los hosts
- Ninguna conexión entre ciertos host
- Perdida de paquetes.
- Disminunción de la velocidad de transferencia
- Violación a la seguridad física y lógica de la red
- Acabo de Instalar un Nuevo NIC, Pero No Puedo Interconectar
- Sólo Puedo Interconectar Usando Direcciones IP
- ¿Por Qué Son Algunos Host en Mi Red Inalcanzables?
- Puedo Interconectarme, Pero Pierdo 50 Por Ciento De Mis Paquetes
- ¿Por qué Consigo Conexiones De Red Intermitentes?

Esta actividad incluye procedimientos que usted puede seguir al tratar de solucionar problemas de averías en la red.

Presente al menos 3 posibles soluciones para cada uno de los casos.

VII. CASO DE ESTUDIO

OBJETIVOS:

- Formar a los participantes en los principios de análisis y diseño de redes para encontrar los criterios que favorezcan la actividad en función de sus objetivos, con un enfoque en la lógica de manera holística, y en las mejores prácticas y modelos de diseño de redes IP.
- Adquirir destrezas en la elaboración de Diseños de Red (LAN / WAN) mediante la práctica.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Este último capítulo proporciona al participante, la libertad de emitir un análisis crítico personal, tomando el papel de diseñador de redes de datos, mediante el desarrollo de un caso de estudio como una herramienta de investigación y una técnica de aprendizaje que le permitirá comprender la particularidad de la situación para distinguir cómo funcionan las partes y las relaciones con el todo.

VII. Caso de Estudio

En una Empresa X, con una plataforma tecnológica básica en la cual funcionan los servicios de Internet tradicional como mensajería, para poder gestionar los pedidos, navegación por Internet, inventario, entre otras. Actualmente necesitamos una red con un conjunto de hardware y software en la cual se puedan comunicar las computadoras para compartir recursos como programas, impresión, discos, etc. Para esto necesitamos empezar con un diagnóstico de nuestro espacio y los requerimientos, en este análisis abarca la parte física y lógica, permitiendo identificar las necesidades y las ventajas de la infraestructura que vamos a implementar.

El hecho de realizar un análisis de los requerimientos de la infraestructura nos permite determinar una solución con los recursos técnicos disponibles.

Actualmente no cuenta con ninguna infraestructura tecnológica de comunicación por lo que poder administrar la red en un solo sistema, permitirá agilizar los trámites y procesos para que los usuarios obtengan la información actualizada, sistematizada y en tiempo real agilitando las funciones.

Nota: Se le solicita realizar un Diseño y Configuración de una Red LAN, con crecimiento a una Wan a futuro; usted debe presentar un diseño físico y lógica de la red, mecanismos para proporcionar seguridad y administrar la red de la Empresa X. Además, se solicita implementar la red desde cero y como administrador en redes va a recomendar que deben implementar (tecnologías, arquitectura, topologías, protocolos, componentes hardware y software, esquema de direccionamiento, tipo de cableado, cantidad de material a utilizar, sistema operativo, software para administrar la red, herramientas para la seguridad, políticas de seguridad, etc.)

Ademas, debe presentar un presupuesto y cronograma para el proyecto.

Usted debe considerar los siguientes aspectos:

1. No cuentan con un cuarto de comunicación
2. Debe proponer un direccionamiento IP fijo o DHCP
3. La red no está bien configurada.
4. Tienen acceso a internet simétrico.
5. Los equipos no son adecuados. (switch, router..etc)

6. No cuentan con ninguna seguridad.

7. La estructura del edificio se basa en 3 alturas con una estructura de planta como sigue:

Planta baja: con dos departamentos (4 oficinas), recepción, informática aseo y cuarto de mantenimiento.

Planta primera: con dos departamentos (cuatro oficinas y sala de reuniones) contabilidad, almacén, sala de reuniones.

Planta segunda: con tres departamentos (tres oficinas),ventas, recursos humanos, gerencia y sala de eventos.

8. Los invitados al edificio deben contar con acceso wifi, especialmente en el área de recepción y sala de eventos.

9. Actualmente cuentan con un estimado de posibles usuarios de la red de 30 personas.

10. Debe estructurar en 3 zonas (futuro a una WAN, LAN Y WIFI)

Bibliografía

- Beas, J., Gallego, J., (2019). Intalación y mantenimiento de redes para transmisión de datos. Editex, S.A. España.
- Santos, M. (2014). Diseño de Redes Telemáticas. España. Editorial RA-MA.
- Stallings, W.; (2000). "Comunicaciones y Redes de Computadores". 6ª Edición; Prentice-Hall.
- Tanenbaum, A.S.;(1996). "Computer Networks".3ª Edición; Prentice-Hall.
- León García, A.; Widjaja, I.; (2001). "Redes de Comunicación. Conceptos fundamentales y arquitecturas básicas". 1ª Edición, Mc-Graw Hill.
- Kurose, J.F, Ross, K.W; (2001). "Computer Networking, a top-down approach featuring the Internet". Addison-Wesley.
- Schwarts, M; (1983). "Redes de Telecomunicación : protocolos, modelado y análisis". Adison Wesley.
- Ramirez, Jesús. (2020). Tecnologías e interconexiones de redes de telecomunicaciones. Tesis para optar al grado de Maestro en ciencias de la ingeniería eléctrica con especialidad en telecomunicaciones. Universidad Autónoma de Nuevo León. México.
- Carlos Valdivia Miranda.(2015). Sistemas de Telecomunicaciones e Informáticos. Electricidad y Electrónica. Redes Telemáticas. Primea edición. España. Ediciones Paraninfo, S.A.
- Barbancho, J., Benjumea, J., Rivera, O., Ropero, J., Sánchez, G., Sivianes, F., (2014). Sistemas Microinformáticos y Redes. Redes Locales. Segunda edición, España, Ediciones Paraninfo, S.A.
- Andréu Joaquin. (2011).Redes Locales. Madrid. Editorial Editex, S.A., 312 pág.
- Carlos V. Galarza-Macancela. (2017). Diseño e implementación de una red de datos segura para la Pontificia Universidad Católica del Ecuador, Santo Domingo. Revista Científica. Dominio de la Ciencia. Vol. 4, núm. 2, abril, 2018, pp. 123-137. Dom. Cien., ISSN: 2477-8818.
- López, R., (2018). Enrutamiento y Configuración de Redes. Fundación Universitaria del Área Andina. Bogotá. ISBN 978-958-5462-80-9.

- Gamez, D., (2012). Metodología para el Análisis y Diseño de Redes Fundamentados en ITIL 4, para empresas de servicio. Tesis para optar al Título de Ingeniero en sistemas e informática. Universidad Libre de Colombia. Bogotá. 91 páginas.
- Ibarra, M. M., Orozco, L. M., & Calderón, O. J. (2012). Opciones de Interconexión, Requerimientos y Procesos de Pruebas en el Nivel de Transporte de la NGN. Ingenium, 71-83.
- Kurose, J., Ross, K., (2010). Redes de Computadoreas: Un enfoque descendente. Madrid. Pearson Educación, S.A. ISBN: 978-84-7829-119-9. 844 Pág.