UNIVERSIDAD AUTONOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BASICAS E INGENIERIA

ING. EN ELECTRONICA Y TELECOMUNICACIONES

TESIS

“IMPLEMENTACIÓN DE RED LAN EN EL H. AYUNTAMIENTO DE HUEYPOXTLA”

QUE PARA OBTENER EL TITULO DE INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

PRESENTAN
HERNANDEZ GOMEZ LUIS ANTONIO
OLGUIN ROJO ADIEL

ASESOR:
ING. SANDRA LUZ HERNANDEZ MENDOZA

PACHUCA DE SOTO HGO. DICIEMBRE DE 2008

ÍNDICE **PAG**

ÍNDICE DE FIGURAS **PAG**

Agradecimientos.

A mis padres y hermanos por su apoyo incansable,
Por el cariño y la paciencia que me han impulsado a
Cumplir con una meta más.

A mi Evita que me dio el regalo más lindo del mundo,
El apoyo incondicional en los momentos difíciles,
Por su paciencia, amor y cariño
A Gael el amor de mi vida por quien todo lo hago
Y a todas las personas que de alguna forma me
Ayudaron a llegar hasta aquí.

Adiel Olguín Rojo

.

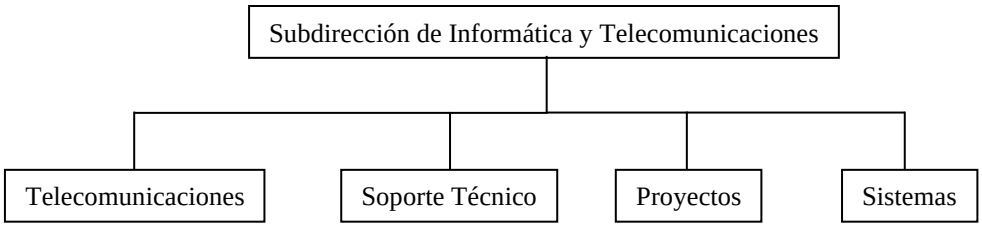
INTRODUCCIÓN.

La necesidad actual de las empresas en sus diferentes rubros, en materia de informática y telecomunicaciones es de vital importancia para sus operaciones financieras, políticas y administrativas, contar con tecnologías de la información de vanguardia que permitan dichos objetivos.

El H. Ayuntamiento de Hueypoxtla en el estado de México es una entidad gubernamental dedicada a la administración pública, servicios generales, recursos humanos, recursos materiales enfocados al bienestar y beneficio de la comunidad.

La demanda creciente de servicios para la población genera la necesidad de infraestructura en varios rubros (departamento de limpieza, obras públicas, seguridad, energía eléctrica, comunicaciones, recursos hidráulicos, drenaje).

En particular la subdirección de Informática y Telecomunicaciones está divida en cuatro departamentos.



La Dirección General del H. Ayuntamiento de Hueypoxtla en conjunto con la Subdirección de Informática y Telecomunicaciones dependiente de esta misma dependencia; han vislumbrado la necesidad real de contar con una red LAN sólida, estable, de vanguardia para realizar eficaz y oportunamente los diferentes procesos administrativos de las áreas demandantes. De esta forma se logra que cada empleado se sienta una parte fundamental y vital dentro del conjunto laboral.

La subdirección de Informática y Telecomunicaciones se convierte en una entidad activa en el fortalecimiento de utilización de la tecnología enfocada al apoyo, seguimiento y servicio a los usuarios para lograr las metas establecidas.

Tomando en cuenta los diversos diagnósticos, planes y programas elaborados con anterioridad, se explica la situación en que se encuentra el cableado estructurado, equipos de cómputo y de telecomunicaciones.

No existe un centro de cómputo y de telecomunicaciones institucional, en donde residan la información y los procesos de la misma, los equipos activos de telecomunicaciones que permitan una real integración de los equipos y sistemas de cómputo, así como un solo repositorio de datos. Para asegurar la información es necesario considerar los esquemas de ambientación, energía eléctrica, protección atmosférica y tierras físicas.

La red local existente en la subdirección de Informática y Telecomunicaciones, no cuentan con cableado estructurado la mayoría de los casos, situación que elimina la flexibilidad y calidad en la conectividad de las computadoras.

Los cableados adicionalmente instalados se basan en la conexión de los elementos que la componen, sin más pruebas que las físicas pasando por alto las lógicas (atenuación, NEXT, polarización del cable misma norma en los elementos) para asegurar una mayor eficiencia entre todos los nodos de la red local.

Por lo tanto se encontró con la necesidad de reubicar dichas oficinas, debido al espacio tan reducido y distante de las oficinas generales, por ende la premura y necesidad de generar un proyecto de cambio de inmueble.

Se propuso que se instalaran todas y cada una de las computadoras de la subdirección de Informática y Telecomunicaciones a la red del H. Ayuntamiento de Hueypoxtla sin afectar la calidad y cantidad de los servicios de red.

La ampliación de la subdirección de informática y telecomunicaciones se logro mediante la creación de un proyecto estructurado que a continuación de manera breve se describe.

El capítulo 1: Descripción de servicios necesarios para la ocupación del inmueble (energía eléctrica (regulada o no regulada), cableado estructurado voz-datos, sistemas de tierras, UPS unidad de respaldo de energía calculado en KVA, aire acondicionado, sistema contra incendios, iluminación).

El capítulo 2: Descripción de rutas de canalización muestra las trayectorias y sus derivaciones para cada departamento donde las especificaciones de canalización son diferentes para el cableado de energía eléctrica, equipos de computó, telefonía y unidades terminales de conexión (áreas de trabajo).

El capítulo 3: Descripción de configuración muestra los pasos a seguir para asignar una dirección única IP, puerta de enlace (Gateway), mascara de subred (Net-mask), DNS para acceso a Internet y se nombro un grupo de trabajo (work-group). Por último se realizaron pruebas de comunicación transmisión y recepción de paquetes de datos entre equipos.

Antecedentes.

El municipio de Hueypoxtla es una entidad que ha venido desarrollando actividades como es el manejo de recursos, obras públicas, administración del registro civil entre otros que requieren un manejo de información eficaz y oportuna.

En años anteriores el manejo de la información ha sido a través de documentación en papel, y la mayoría de esta no se encuentra digitalizada, esto en términos generales, si no se lleva un adecuado sistema de organización de la información, acarrea muchos problemas.

La información de obras realizadas y registro civil de administraciones pasadas se encuentra organizada en archiveros, el manejo de la información se ha venido realizando de esta manera. A últimas fechas con la adquisición de algunos equipos de cómputo repartidos en las diferentes áreas de esta dependencia, se ha digitalizado un porcentaje de la información que se tiene y de esta manera, se ha logrado un avance en cuanto a un mejor manejo y almacenamiento de ésta.

Caracterización del Ayuntamiento

El H. Ayuntamiento de Hueypoxtla se encuentra organizado de la siguiente manera.

Presidente municipal
1 Síndico procurador
6 Regidores de mayoría relativa
4 Regidores de representación proporcional

Principales Comisiones del Ayuntamiento

COMISIÓN	**RESPONSABLE**
Seguridad Pública	Presidente municipal
Normatividad Administrativa	Síndico
Comunicaciones y Transportes	Primer regidor
Obras Públicas	Segundo regidor
Agua y Saneamiento	Tercer regidor
Agricultura	Cuarto regidor
Educación, Cultura y Deporte	Quinto regidor
Desarrollo Urbano	Sexto regidor

Ecología	Séptimo regidor
Protección Civil	Octavo regidor
Salud Pública	Noveno regidor
Alumbrado Público	Décimo regidor

Descripción del departamento

La subdirección de Informática y Telecomunicaciones se convierte en una entidad activa en el fortalecimiento de utilización de la tecnología enfocada al apoyo, seguimiento y servicio a los usuarios para lograr las metas establecidas (Red LAN).

No existe un centro de cómputo y de telecomunicaciones institucional, en donde residan la información y los procesos de la misma, los equipos activos de telecomunicaciones que permitan una real integración de los equipos y sistemas de cómputo, así como un solo repositorio de datos. Para asegurar la información es necesario considerar los esquemas de ambientación, energía eléctrica, protección atmosférica y tierras físicas.

Descripción de Equipos

Grupo	Descripción
Equipo Activo	Equipo que se encarga de distribuir en forma activa la información a través de la red, como conmutadores y enrutadores.
Equipo Pasivo	Dispositivos o materiales para conexión de equipos de cómputo con equipo activo, entre ellos: • Cable UTP. • Canaletas. • Conectores. • Organizador de cables. • Patch panel. • Rack. • Otros

JUSTIFICACIÓN

Existen dos problemas básicos en el H. Ayuntamiento de Hueypoxtla del estado de México: la escasa accesibilidad a la información en las distintas áreas de este y la falta de dispositivos de Entrada/Salida (E/S) (impresoras, scanners, lector de huellas) vitales en el desarrollo de las labores diarias del personal. En consecuencia, muchos empleados se sienten desprovistos de materiales y herramientas, razón por la cual, la atención y servicio ofrecido por la institución tiende a ser lento o bien, se hace tedioso.

Pese a los programas de implementación de mejoras y a la creciente disponibilidad de recursos en línea el H. Ayuntamiento de Hueypoxtla no trabaja con tecnologías comunicación. Es por esto que es necesario implementar esta iniciativa de instalar una red de telecomunicaciones y así tener acceso mayor cantidad de información con mayor rapidez para poder ofrecer un servicio de calidad y más eficiente.

Es necesario informar y sensibilizar al personal que labora en esta dependencia para promover un uso sustentable de este recurso, en tanto esta es una tarea colectiva que exige convertirse en un objetivo comprendido y perseguido por todos. El problema de la escasa accesibilidad a la información no solo afecta a los empleados del Ayuntamiento, sino que también tiene alcance en la ciudadanía.

La instalación de una red LAN en el H. Ayuntamiento de Hueypoxtla, permite acceder a gran variedad de información y a su vez permite compartir recursos (impresoras, scanners) a una mayor cantidad de usuarios.

HIPÓTESIS

Con la implementación de una red de telecomunicaciones en el H. Ayuntamiento de Hueypoxtla se aceleran los servicios prestados en la dependencia en un porcentaje mayor, además de que se ahorra tiempo y se comparten recursos. Se consigue tener un mejor manejo y disponibilidad de la información en cualquier área que cuente con acceso a la red. También se completara de manera más eficiente la digitalización de la información de administraciones pasadas. Esto trae consigo una mejor atención por parte del personal que ahí labora y acelera los trámites y servicios que son llevados a cabo en cada departamento del Ayuntamiento.

OBJETIVOS

Objetivo General

Implementar una Red de Área Local con la finalidad de disponer de una red de computo que facilite o modernice, las tareas de la administración municipal, teniendo como fin brindar mejores servicios a la comunidad de Hueypoxtla, así como también cubrir necesidades generadas en cada una de las áreas administrativas.

Objetivos específicos

- Contar con la tecnología que permita cubrir con las expectativas de crecimiento de volúmenes de información a transmitir.

- Implementar más y mejores puntos de conexión mediante la instalación de sistemas de cableado estructurado, sus elementos que lo componen y basado en las normas internacionales que aseguren funcionalidad global, durabilidad y facilidad en los movimientos naturales de oficinas y equipos en las áreas.

- Lograr la interconexión de los equipos de las diferentes áreas del H. Ayuntamiento para optimizar y agilizar los tiempos de respuestas de los recursos humanos prestadores de servicio hacia lo comunidad demandante.

- Conceptualizar un proyecto estructurado de Telecomunicaciones con alto rendimiento operativo, funcionalidad y baja inversión de recursos materiales.

- Cubrir con las expectativas de transferencia de información del proyecto de modernización de la tecnología de información en el H. Ayuntamiento de Hueypoxtla.

- Contar con instalaciones integrables de cómputo y comunicaciones debidamente ambientadas para asegurar la información.

CAPÍTULO I: MARCO TEÓRICO REFERENCIAL

1.1 ESTADO DEL ARTE

El inicio del uso de redes locales, a finales de la década de 1970, fue un hecho significativo en el desarrollo del campo de la computación. Estas redes fueron desarrolladas por ingenieros que advirtieron que el empleo de técnicas de computación, más que de técnicas de telecomunicaciones, permitiría obtener grandes anchos de banda, bajas tasas de error y bajo costo. Las nuevas redes locales de banda ancha llegaron justamente cuando se les necesitaba, para permitir que las computadoras de bajo costo, que se estaban instalando en grandes cantidades, pudiesen compartir periféricos; al mismo tiempo, hicieron posible un nuevo enfoque del diseño de sistemas compartidos de computación.

Debido a la creciente cantidad de computadoras, se ha llegado a la necesidad de la comunicación entre ellas para el intercambio de datos, programas, mensajes y otras formas de información. Las redes de computadoras llegaron para llenar esta necesidad, proporcionando caminos de comunicación entre las computadoras conectadas a ellas.

Con el aumento de sistemas de computación y del número de usuarios potenciales, se llegó a la necesidad de un nuevo tipo de redes de comunicaciones. Al principio, las redes de área extendida (WAN, Wide Área Network), también conocidas como grandes redes de transporte, fueron un medio de conexión de terminales remotas a sistemas de computación. En estos sistemas de conexión, los dispositivos pueden funcionar como unidades independientes y se conectan por una red que cubre una gran área. Los medios de comunicación usados para la red pueden ser líneas telefónicas o cables tendidos específicamente para la red. La escala de redes de área extendida es ahora tan grande que ya existen enlaces intercontinentales entre redes, que establecen la comunicación vía satélite.

Las velocidades requeridas para tales sistemas pueden ser bastante lentas. Como el tamaño de los mensajes suele ser grande, el tiempo para recibir el reconocimiento puede ser largo. Las velocidades de operación típicas de este tipo de redes están en el intervalo de 10 a 50 Kbps, con tiempos de respuesta del orden de algunos segundos.

Se trata de redes de conmutación de paquetes que usan nodos de conmutación y el método de operación de almacenamiento y reenvío. La cantidad de sistemas computarizados ha crecido debido a los avances en microelectrónica, lo que ha dado lugar a la necesidad de un nuevo tipo de red de computadoras, llamada red de área local (LAN, Local Área Network). Las redes de área local se originaron como un medio para compartir dispositivos periféricos en una organización dada. Como su nombre lo indica, una red local cubre un área geográfica limitada y su diseño se basa en un conjunto de principios diferentes a los de las redes de área extendida.

1.2 CONCEPTO DE RED DE ÁREA LOCAL

En su nivel más elemental, una red consiste en dos ordenadores conectados mediante un cable para que puedan compartir datos. Toda red, no importa cuán sofisticada, procede de ese simple sistema.

Las redes empezaron siendo pequeñas, con quizás 10 ordenadores conectados junto a una impresora. La tecnología limitaba el tamaño de la red, incluyendo el número de ordenadores conectados, así como la distancia física que podría cubrir la red. Por ejemplo, en los primeros años 80 el más popular método de cableado permitía como 30 usuarios en una longitud de cable de alrededor de 200 metros (600 pies). Por lo que una red podía estar en un único piso de oficina o dentro de una pequeña compañía. Para muy pequeñas empresas hoy, ésta configuración es todavía adecuada. Este tipo de red, dentro de un área limitada, es conocida como una red de área local (Lan).

La definición más general de una red de área local (Local Área Network, LAN), es la de una red de comunicaciones utilizada por una sola organización a través de una distancia limitada, la cual permite a los usuarios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, etc.

Existe no obstante una definición oficial, la del Comité IEEE 802, quien define una Red local de la siguiente manera: Una Red local es un sistema de comunicaciones que permite que un número de dispositivos independientes se comuniquen entre si.

Una Red local, como su nombre indica, debe ser local en cuanto al ámbito geográfico, aunque local puede significar cualquier cosa, desde una oficina o un edificio de ocho plantas, hasta un complejo industrial con docenas de edificios con muchos pisos.

El término de red local incluye tanto el software con el hardware necesario para la conexión, gestión y mantenimiento de los dispositivos y para el tratamiento de la información.

1.3 COMPONENTES DE UNA RED

Una red de computadoras consta tanto de hardware como de software. En el hardware se incluyen: estaciones de trabajo, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad. En el software se encuentra el sistema operativo de red (Network Operating System, NOS).

1.3.1 Estaciones de trabajo

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma.

Una estación de trabajo no comparte sus propios recursos con otras computadoras. Esta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como Macintosh, Silicon Graphics, Sun.

1.3.2 Servidores

Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

1.3.3 Tarjeta de Interfaz de Red

Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC). Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo. Las tarjetas internas casi siempre se utilizan para las PC's, PS/2 y estaciones de trabajo como las SUN's. Las tarjetas de interfaz también pueden utilizarse en minicomputadoras y mainframes. A menudo se usan cajas externas para Mac's y para algunas computadoras portátiles. La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que la PC pueda entender y la envía a la PC.
Son ocho las funciones de la NIC:

Comunicaciones de host a tarjeta
Buffering
Formación de paquetes
Conversión serial a paralelo
Codificación y decodificación
Acceso al cable
Saludo
Transmisión y recepción
Estos pasos hacen que los datos de la memoria de una computadora pasen a la memoria de otra.

1.3.4 Cableado

La Red LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial.

Cable de par trenzado: Es con mucho, el tipo menos caro y más común de medio de red.

Cable coaxial: Es tan fácil de instalar y mantener como el cable de par trenzado, y es el medio que se prefiere para las LAN grandes.

Cable de fibra óptica: Tiene mayor velocidad de transmisión que los anteriores, es inmune a la interferencia de frecuencias de radio y capaz de enviar señales a distancias considerables sin perder su fuerza. Tiene un costo mayor.

1.3.5 Equipo de conectividad

Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor.

Hubs o concentradores: Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella.

Repetidores: Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red.

Puentes: Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN.

Ruteadores: Los ruteadores son similares a los puentes, sólo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo sistema operativo de red, para poder conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring.

Compuertas: Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Podrá tenerse, por ejemplo, una LAN que consista en computadoras compatibles con IBM y otra con Macintosh.

1.3.6 Sistema operativo de red

Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red (Network Operating System, NOS), que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades. Algunos sistemas operativos se comportan excelentemente en redes pequeñas, así como otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias.

Los servicios que el NOS realiza son:

Soporte para archivos: Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.

Comunicaciones: Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.

Servicios para el soporte de equipo: Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etc.

1.4 TOPOLOGÍA

Una configuración de red se denomina topología de red. Por lo tanto, la topología establece la forma en cuanto a conectividad física de la red. El término topología se utiliza en geometría para describir la forma de un objeto. El diseñador de una red tiene tres objetivos al establecer la topología de la misma:

1. Proporcionar la máxima fiabilidad a la hora de establecer el tráfico (por ejemplo, mediante estacionamientos alternativos)

2. Encaminar el tráfico utilizando la vía de costo mínimo entre los ETD transmisor y receptor (no obstante, a veces no se escoge la vía de costo mínimo porque otros factores, como la fiabilidad, pueden ser más importantes.

3. Proporcionar al usuario el rendimiento óptimo y el tiempo de respuesta mínimo.

Una red tiene dos diferentes topologías: una física y una lógica.

1.4.1 La topología física.

Es la disposición física actual de la red, la manera en que los nodos están conectados unos con otros.

1.4.2 La topología lógica.

Es el método que se usa para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los diferentes nodos de la misma. Las topologías física y lógica pueden ser iguales o diferentes

Las topologías de red más comunes:

. La topología jerárquica (en árbol)

. La topología horizontal (en bus)

. La topología en estrella.

. La topología en anillo

. La topología en malla.

En este caso utilizaremos la topología en estrella. Una de las principales razones para su uso es fundamentalmente histórica. Todo el tráfico surge del centro de la estrella. El nodo A, típicamente un computador controla completamente los ETD conectados a él.

La topología estrella es una de las topologías más populares de un LAN (Local Área Network). Es implementada conectando cada computadora a un Hub central. El Hub puede ser Activo, Pasivo o Inteligente. Un hub pasivo es solo un punto de conexión y no requiere energía eléctrica. Un Hub activo (el más común) es actualmente un repetidor con múltiples puertos; impulsa la señal antes de pasarla a la siguiente computadora. Un Hub Inteligente es un hub activo pero con capacidad de diagnostico, puede detectar errores y corregirlos.

1.4.3 Comunicación en la Topología Estrella

En una red estrella típica, la señal pasa de la tarjeta de red (NIC) de la computadora que esta enviando el mensaje al Hub y este se encarga de enviar el mensaje a todos los puertos. La topología estrella es similar a la Bus, todas las computadoras reciben el mensaje pero solo la computadora con la dirección, igual a la dirección del mensaje puede leerlo.

1.4.4 Ventajas de la Topología Estrella

La topología estrella tiene dos ventajas grandes a diferencia de la topología Bus y Ring.

- Es más tolerante, esto quiere decir que si una computadora se desconecta o si se le rompe el cable solo esa computadora es afectada y el resto de la red mantiene su comunicación normalmente.

- Es fácil de reconfigurar, añadir o remover una computadora es tan simple como conectar o desconectar el cable.

1.4.5 Desventajas de la Topología Estrella

- Es costosa ya que requiere más cable que la topología Bus y Ring.
- El cable viaja por separado del Hub a cada computadora.
- Si el Hub se cae, la red no tiene comunicación.
- Si una computadora se cae, no puede enviar ni recibir mensajes.

Algunos sistemas poseen un nodo central de reserva, lo que incrementa considerablemente la confiabilidad del sistema. El cual se puede considerar para una opción futura o de contingencia.

1.5 EQUIPOS DE INTERCONEXIÓN DE REDES

En una LAN existen elementos de hardware y software, entre los cuales se pueden destacar: el servidor, estaciones de trabajo, sistema operativo, protocolos de comunicación y tarjetas de interface de red.

El servidor es el elemento principal de procesamiento, contiene el sistema operativo de red y se encarga de administrar todos los procesos dentro de ella, controla también el acceso a los recursos comunes como son las impresoras y las unidades de almacenamiento. Debe contar con una capacidad de procesamiento suficiente para responder a los requerimientos de las estaciones y con un disco duro de gran capacidad para almacenar el sistema operativo de la red, las aplicaciones y los archivos de los usuarios.

Las estaciones de trabajo, en ocasiones llamadas nodos, pueden ser computadoras personales o cualquier terminal conectada a la red. Son los sistemas de cómputo de usuario que comparten los recursos del servidor, realizan un proceso distribuido y se interconectan a la red mediante una tarjeta de interface de red. De esta forma trabaja con sus propios programas o aprovecha las aplicaciones existentes en el servidor.

El sistema operativo de red es un conjunto de programas y protocolos de comunicación que permite a varias computadoras interconectadas en una red compartir recursos de una manera organizada, eficiente y transparente. Con él se tiene acceso compartido a:

1. Servidores de archivo
2. Servidores de impresión
3. Servidores de comunicaciones

El sistema operativo de red tiene el control del acceso a los recursos en aspectos tales como:

1. Cuáles son los recursos disponibles para el usuario.
2. Qué puede hacer el usuario con estos recursos.
3. Qué privilegios y derechos tiene cada usuario.
4. Prevenir accesos múltiples

De los sistemas operativos de red disponibles comercialmente podemos mencionar:

1. LAN Manager de Microsoft
2. Netware de Novell
3. OS/2 LAN Server de IBM
4. Pathworks de DEC
5. VINES de Banyan

Los protocolos de comunicación son un conjunto de normas que regulan la transmisión y recepción de datos dentro de la red, el modelo OSI es la base para entender los protocolos utilizados.

Para tener comunicación la red, el servidor y las estaciones de trabajo deben contar con una tarjeta de interface de red o NIC (Network Interface Card), que puede encontrarse tanto en el interior como en el exterior del sistema de cómputo. Este adaptador será el apropiado para la topología que se desee usar.

El adaptador es una interface entre la red y la computadora, por lo tanto, debe cumplir con los protocolos adecuados para evitar conflictos con el resto de los nodos o con otros dispositivos conectados a la computadora como el monitor, el disco duro, etc.

Los requerimientos para la operación de un adaptador como interface de red son los siguientes:

1. Usan los protocolos adecuados según el tipo de red que se desee utilizar.

2. Tener el conector adecuado para adaptarse a la ranura de expansión o al puerto que se tenga disponible, en el caso de una computadora portátil como una laptop o notebook se utiliza generalmente el puerto paralelo.

Repetidor. Este dispositivo es el más rápido. Se usa para extender las longitudes físicas de las redes, pero no contiene inteligencia para funciones de enrutamiento. Un repetidor se utiliza cuando dos segmentos están acercando sus longitudes físicas máximas, las cuales son limitadas en cableado.

Puente. Trabaja en las capas físicas y de enlace de datos del modelo de referencia OSI, no cuida que los protocolos de red estén en uso, sólo prueba la transferencia de paquetes entre las redes. Con el empleo de un puente la información se intercambia entre los nodos por medio de direcciones físicas. El puente normalmente se utiliza para dividir una gran red dentro de áreas pequeñas, con lo que se reduce la carga de tráfico y se incrementa el rendimiento. Algunos modelos cuentan con 2 o más puertos LAN o una combinación de puerto de LAN y WAN.

Enrutador. Este dispositivo se emplea para traducir la información de una red a otra. La información se intercambia mediante direcciones lógicas. Funciona en la capa de red del modelo de referencia OSI; por lo que aunque un enrutador tiene acceso a la información física sólo se intercambia información lógica. Físicamente puede recibir dos o más puertos LAN, o una combinación de puertos LAN y WAN.

Compuerta. Se conoce también como un convertidor de protocolos y se emplea como interface de protocolos de redes diferentes. Se utiliza en una variedad de aplicaciones donde las computadoras de diferentes manufacturas y tecnologías deben comunicarse. La información que pasa a través de los gateways es información par a par que viene de las aplicaciones, de las interfaces y de los programas del usuario final. Estos dispositivos son lentos y delicados por lo que no se requieren para una alta velocidad de intercambio de información.

Conmutador de datos. Son dispositivos para proveer un enlace dedicado de alta velocidad entre segmentos de redes de cómputo. Los sistemas generalmente se utilizan en aplicaciones en las que el tráfico de una serie de estaciones de trabajo (Workstation), necesita alcanzar un simple servidor.

Los switches de datos trabajan en la capa de enlace de datos y, opcionalmente, dependiendo del fabricante, en la capa de red del modelo de referencia OSI. Los switches de datos, se emplean al conectar redes que acceden y comparten datos entre la misma serie de servidores y estaciones de trabajo.

CAPÍTULO II: ESTÁNDARES Y TECNOLOGÍAS DE LAS REDES LOCALES

2.1 ESTÁNDARES DE COMUNICACIÓN

Muchos fabricantes de software y hardware proporcionan productos para la conexión de equipos en red. Fundamentalmente, las redes son un medio de comunicación, de ahí que, la necesidad de los fabricantes de tomar medidas para asegurar que sus productos pudieran interactuar, llegó a ser aparentemente prematura en el desarrollo de la tecnología de redes. Como las redes y los proveedores de productos para redes se han extendido por todo el mundo, la necesidad de una estandarización se ha incrementado. Para dirigir los aspectos concernientes a la estandarización, varias organizaciones independientes han creado especificaciones estándar de diseño para los productos de redes de equipos. Cuando se mantienen estos estándares, es posible la comunicación entre productos hardware y software de diversos vendedores.

2.1.1 Estándares de redes

El Comité 802, o proyecto 802, del Instituto de Ingenieros en Eléctrica y Electrónica (IEEE) definió los estándares de redes de área local (LAN). La mayoría de los estándares fueron establecidos por el Comité en los 80´s cuando apenas comenzaban a surgir las redes entre computadoras personales.

Muchos de los siguientes estándares son también Estándares ISO 8802. Por ejemplo, el estándar 802.3 del IEEE es el estándar ISO 8802.3.

802.1 Definición Internacional de Redes. Define la relación entre los estándares 802 del IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI) de la ISO (Organización Internacional de Estándares). Por ejemplo, este Comité definió direcciones para estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única. Los vendedores de tarjetas de interface de red están registrados y los tres primeros bytes de la dirección son asignados por el IEEE. Cada vendedor es entonces responsable de crear una dirección única para cada uno de sus productos.

802.2 Control de Enlaces Lógicos. Define el protocolo de control de enlaces lógicos (LLC) del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación. La capa de Datos-Enlace en el protocolo OSI esta subdividida en las subcapas de Control de Acceso a Medios (MAC) y de Control de Enlaces Lógicos (LLC). En Puentes, estas dos capas sirven como un mecanismo de switcheo modular, como se muestra en la figura I-5. El protocolo LLC es derivado del protocolo de Alto nivel para Control de Datos-Enlaces (HDLC) y es similar en su operación. Nótese que el LLC provee las direcciones de Puntos de Acceso a Servicios (SAP’s), mientras que la subcapa MAC provee la dirección física de red de un dispositivo.

Las SAP's son específicamente las direcciones de una o más procesos de aplicaciones ejecutándose en una computadora o dispositivo de red.

El LLC provee los siguientes servicios:

- Servicio orientado a la conexión, en el que una sesión es empezada con un Destino, y terminada cuando la transferencia de datos se completa. Cada nodo participa activamente en la transmisión, pero sesiones similares requieren un tiempo de configuración y monitoreo en ambas estaciones.
- Servicios de reconocimiento orientado a conexiones. Similares al anterior, del que son reconocidos los paquetes de transmisión.
- Servicio de conexión sin reconocimiento. En el cual no se define una sesión. Los paquetes son puramente enviados a su destino. Los protocolos de alto nivel son responsables de solicitar el reenvío de paquetes que se hayan perdido. Este es el servicio normal en redes de área local (LAN's), por su alta confiabilidad.

802.3 Redes CSMA/CD. El estándar 802.3 del IEEE (ISO 8802-3), que define cómo opera el método de Acceso Múltiple con Detección de Colisiones (CSMA/CD) sobre varios medios. El estándar define la conexión de redes sobre cable coaxial, cable de par trenzado, y medios de fibra óptica. La tasa de transmisión original es de 10 Mbits/seg, pero nuevas implementaciones transmiten arriba de los 100 Mbits/seg calidad de datos en cables de par trenzado.

802.4 Redes Token Bus. El estándar token bus define esquemas de red de anchos de banda grandes, usados en la industria de manufactura. Se deriva del Protocolo de Automatización de Manufactura (MAP). La red implementa el método token-passing para una transmisión bus. Un token es pasado de una estación a la siguiente en la red y la estación puede transmitir manteniendo el token. Los tokens son pasados en orden lógico basado en la dirección del nodo, pero este orden puede no relacionar la posición física del nodo como se hace en una red token ring. El estándar no es ampliamente implementado en ambientes LAN.

802.5 Redes Token Ring. También llamado ANSI 802.1-1985, define los protocolos de acceso, cableado e interface para la LAN token ring. IBM hizo popular este estándar. Usa un método de acceso de paso de tokens y es físicamente conectada en topología estrella, pero lógicamente forma un anillo. Los nodos son conectados a una unidad de acceso central (concentrador) que repite las señales de una estación a la siguiente. Las unidades de acceso son conectadas para expandir la red, que amplía el anillo lógico. La Interface de Datos en Fibra Distribuida (FDDI) fue basada en el protocolo token ring 802.5, pero fue desarrollado por el Comité de Acreditación de Estándares (ASC) X3T9.
Es compatible con la capa 802.2 de Control de Enlaces Lógicos y por consiguiente otros estándares de red 802.

802.6 Redes de Área Metropolitana (MAN). Define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado Bus Dual de Cola Distribuida (DQDB). El bus dual provee tolerancia de fallos para mantener las conexiones si el bus se rompe. El estándar MAN esta diseñado para proveer servicios de datos, voz y vídeo en un área metropolitana de aproximadamente 50 kilómetros a tasas de 1.5, 45, y 155 Mbits/seg. DQDB es el protocolo de acceso subyacente para el SMDS (Servicio de Datos de Multimegabits Switcheados), en el que muchos de los portadores públicos son ofrecidos como una manera de construir redes privadas en áreas metropolitanas. El DQDB es una red repetidora que switchea celdas de longitud fija de 53 bytes; por consiguiente, es compatible con el Ancho de Banda ISDN y el Modo de Transferencia Asíncrona (ATM). Las celdas son switcheables en la capa de Control de Enlaces Lógicos.

Los servicios de las MAN son Sin Conexión, Orientados a Conexión, y/o isócronas (vídeo en tiempo real). El bus tiene una cantidad de slots de longitud fija en el que son situados los datos para transmitir sobre el bus. Cualquier estación que necesite transmitir simplemente sitúa los datos en uno o más slots. Sin embargo, para servir datos isócronos, los slots en intervalos regulares son reservados para garantizar que los datos llegan a tiempo y en orden.

802.7 Grupo Asesor Técnico de Anchos de Banda. Este comité provee consejos técnicos a otros subcomités en técnicas sobre anchos de banda de redes.

802.8 Grupo Asesor Técnico de Fibra Óptica. Provee consejo a otros subcomités en redes por fibra óptica como una alternativa a las redes basadas en cable de cobre. Los estándares propuestos están todavía bajo desarrollo.

802.9 Redes Integradas de Datos y Voz. El grupo de trabajo del IEEE 802.9 trabaja en la integración de tráfico de voz, datos y vídeo para las LAN 802 y Redes Digitales de Servicios Integrados (ISDN's). Los nodos definidos en la especificación incluyen teléfonos, computadoras y codificadores/decodificadores de vídeo (códecs). La especificación ha sido llamada Datos y Voz Integrados (IVD). El servicio provee un flujo multiplexado que puede llevar canales de información de datos y voz conectando dos estaciones sobre un cable de cobre en par trenzado. Varios tipos de diferentes de canales son definidos, incluyendo full dúplex de 64 Kbits/seg sin switcheo, circuito switcheado, o canales de paquete switcheado.

802.10 Grupo Asesor Técnico de Seguridad en Redes. Este grupo esta trabajando en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y encriptamiento. Los estándares propuestos están todavía bajo desarrollo en este momento.

802.11 Redes Inalámbricas. Este comité esta definiendo estándares para redes inalámbricas. Esta trabajando en la estandarización de medios como el radio de espectro de expansión, radio de banda angosta, infrarrojo, y transmisión sobre

líneas de energía. Dos enfoques para redes inalámbricas se han planeado. En el enfoque distribuido, cada estación de trabajo controla su acceso a la red. En el enfoque de punto de coordinación, un hub central enlazado a una red alámbrica controla la transmisión de estaciones de trabajo inalámbricas.

802.12 Prioridad de Demanda (100VG-ANYLAN). Este comité está definiendo el estándar Ethernet de 100 Mbits/seg. Con el método de acceso por Prioridad de Demanda propuesto por Hewlett Packard y otros vendedores. El cable especificado es un par trenzado de 4 alambres de cobre y el método de acceso por Prioridad de Demanda usa un hub central para controlar el acceso al cable. Hay prioridades disponibles para soportar envío en tiempo real de información multimedia.

2.1.2 Modelo OSI

La Organización Internacional de Estándares (ISO) diseñó el modelo de Interconexión de Sistemas Abiertos (OSI) como guía para la elaboración de estándares de dispositivos de computación en redes. Dada la complejidad de los dispositivos de conexión en red y a su integración para que operen adecuadamente, el modelo OSI incluye siete capas diferentes, que van desde la capa física, la cual incluye los cables de red, a la capa de aplicación, que es la interfaz con el software de aplicación que se esta ejecutando.

- Capa 1. Físico
- Capa 2. Enlace de datos
- Capa 3. Red
- Capa 4. Transporte
- Capa 5. Sesión
- Capa 6. Presentación
- Capa 7. Aplicación

Este modelo establece los lineamientos para que el software y los dispositivos de diferentes fabricantes funcionen juntos. Aunque los fabricantes de hardware y los de software para red son los usuarios principales del modelo OSI, una comprensión general del modelo llega a resultar muy benéfica para el momento en que se expande la red o se conectan redes para formar redes de aria amplia WAN.

Las siete capas del modelo OSI son la física, la de enlace de datos, la de red, la de transporte, la de sesión, la de presentación y la de aplicación. Las primeras dos capas (física y enlace de datos) son el hardware que la LAN comprende, como los cables Ethernet y los adaptadores de red. Las capas 3,4 y 5 (de red, de transporte, y de sesión) son protocolos de comunicación, como el sistema básico de entrada/salida de red (NetBIOS), TCP/IP y el protocolo medular NetWare (NCP) de Novell. Las capas 6 y 7 (de presentación y aplicación) son el NOS que proporciona servicios y funciones de red al software de aplicación.

2.1.2.1 Capa Física.

Define la interfaz con el medio físico, incluyendo el cable de red. La capa física maneja temas elementos como la intensidad de la señal de red, los voltajes indicados para la señal y la distancia de los cables. La capa física también maneja los tipos y las especificaciones de los cables, incluyendo los cables Ethernet 802.3 de instituto de ingenieros, eléctricos y electrónicos (IEEE) (Thick Ethernet, Thin Ethernet y UTP), el estándar de interfaz de datos distribuidos por fibra óptica (FDDI) del instituto nacional de estándares americanos (ANSI) para el cable de fibra óptica y muchos otros.

2.1.2.2 Capa de Enlace de Datos.

Define el protocolo que detecta y corrige errores cometidos al transmitir datos por el cable de la red. La capa de enlace de datos es la causante del flujo de datos de la red, el que se divide en paquetes o cuadros de información. Cuando un paquete de información es recibido incorrectamente, la capa de enlace de datos hace que se reenvíe. La capa de enlace de datos esta dividida en dos subcapas: El control de acceso al medio (MAC) y el control de enlace lógico (LLC). Los puentes operan en la capa MAC.

Los estándares basados en la capa de enlace de datos incluyen el estándar de enlace lógico 802.2 de IEEE, punto a punto (PPP), los estándares de la IEEE para el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), el estándar Token Ring y el estándar ANSI FDDI Token Ring.

2.1.2.3 Capa de Red.

Define la manera en que se dirigen los datos de un nodo de red al siguiente.

Los estándares que se requieren a la capa de red incluyen el protocolo de intercambio de paquetes entre redes (IPX) de Novell, el protocolo Internet (IP) y el protocolo de entrega de datagramas (DDP) de Apple. El IP es parte del estándar de protocolo TCP/IP, generado por el Departamento de la Defensa de Estados Unidos y utilizado en Internet. El DDP fue diseñado para computadoras Apple, como la Macintosh. Los enrutadores operen en esta capa.

2.1.2.4 Capa de Transporte.

Proporciona y mantiene el enlace de comunicaciones. La capa de transporte es la encargada de responder adecuadamente si el enlace falla o se dificulta su establecimiento.

Los estándares que pertenecen a la capa de transporte incluyen el protocolo de transporte (TP) de la organización internacional de estándares (ISO) y el protocolo de intercambio de paquetes en secuencia (SPX) de Novell. Otros estándares que ejecutan funciones importantes en la capa de transporte incluyen el protocolo de control de transmisión (TCP) del Departamento de la Defensa, que es parte de TCP/IP y de NCP de Novell.

2.1.2.5 Capa de Sesión.

Controla las conexiones de red entre nodos. La capa de sesión es responsable de la creación, mantenimiento y terminación de las sesiones de red.

El TCP ejecuta funciones importantes en la capa de sesión, así como hace NCP de Novell.

2.1.2.6 Capa de Presentación.

Es la encargada del formato de los datos. La capa de presentación traduce los datos entre formatos específicos para asegurarse de que los datos sean recibidos en un formato legible para el dispositivo al que se presenta.

2.1.2.7 Capa de Aplicación.

Es la mas alta definida en el modelo OSI. La capa de aplicación es la encargada de proporcionar funciones a las aplicaciones de usuario y al administrador de red, como es proporcionar al sistema operativo servicios como la transferencia de archivos.

2.2 CABLEADO ESTRUCTURADO

Hasta hace unos años para cablear un edificio se usaban distintos sistemas independientes unos de otros. Esto llevaba a situaciones como el tener una red bifilar para voz (telefonía normalmente), otra distinta para megafonía, otra de conexión entre ordenadores, etc. Con esta situación se dificulta mucho el mantenimiento y las posibles ampliaciones del sistema.

Un sistema de cableado estructurado es una red de cables y conectores en número, calidad y flexibilidad de disposición suficientes que nos permita unir dos puntos cualesquiera dentro del edificio para cualquier tipo de red (voz, datos o imágenes). Consiste en usar un solo tipo de cable para todos los servicios que se quieran prestar y centralizarlo para facilitar su administración y mantenimiento.

El cableado estructurado recibe nombres distintos para cada tipo de aplicación, aunque popularmente se generaliza y se le conoce con el nombre de P.D.S. Los nombres reales son:

- P.D.S. Sistemas de Distribución de Locales
- I.D.S. Sistemas de Distribución de Industria
- I.B.S. Control de Seguridad y Servicios

Al hablar de sistemas de cableado implícitamente se entiende cableado de baja corriente (telefonía, vídeo e informáticas), aunque la actitud sistemática que observamos ante este tipo de cableado, también se debería de aplicarse al conocido como cableado de alta corriente (sistema de 110v). Como se verá más adelante, es importante integrar en el diseño de un edificio ambos cableados para evitar interferencias entre ellos.

2.2.1 Beneficios

- El sistema de cableado estructurado nos va permitir hacer convivir muchos servicios en nuestra red (voz, datos, vídeo) con la misma instalación, independientemente de los equipos y productos que se utilicen.
- Se facilita y agiliza mucho las labores de mantenimiento.
- Es fácilmente ampliable.
- El sistema es seguro tanto a nivel de datos como a nivel de seguridad personal.
- Una de las ventajas básicas de estos sistemas es que se encuentran regulados mediante estándares, lo que garantiza a los usuarios su disposición para las aplicaciones existentes, independientemente del fabricante de las mismas, siendo soluciones abiertas, fiables y muy seguras. Fundamentalmente la norma TIA/EIA-568A define entre otras cosas las normas de diseño de los sistemas de cableado, su topología, las distancias, tipo de cables, los conectores, etc.
- Al tratarse de un mismo tipo de cable, se instala todo sobre el mismo trazado.
- El tipo de cable usado es de tal calidad que permite la transmisión de altas velocidades para redes.
- No hace falta una nueva instalación para efectuar un traslado de equipo.

2.2.2 Elementos que intervienen

Ya que el sistema de cableado recibe el nombre de estructurado, sería conveniente conocer su estructura. Al conjunto de todo el cableado de un edificio se le conoce con el nombre de SISTEMA y cada parte en la que se divide se da el nombre de SUBSISTEMA:

2.2.2.1 Área de trabajo: 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 dispositivo o dispositivos 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, que se necesite. Éstos irán siempre conectados en el exterior de la roseta. Si el cable se utiliza para compartir voz, datos u otros servicios, cada uno de ellos deberá de tener un conector diferente en 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.

2.2.2.2 Subsistema horizontal: Desde la roseta de cada uno de las áreas de trabajo irá un cable a un lugar común de centralización llamado panel de parcheo.

El panel de parcheo es donde se centraliza todo el cableado del edificio. Es el lugar al que llegan los cables procedentes de cada una de las dependencias donde se ha instalado un punto de la red. Cada roseta colocada en el edificio tendrá al otro extremo de su cable una conexión al panel de parcheo. De esta forma se le podrá dar o quitar servicio a una determinada dependencia simplemente con proporcionarle o no señal en este panel.

Se conoce con el nombre de cableado horizontal a los cables usados para unir cada área de trabajo con el panel de parcheo.

Todo el cableado horizontal deberá ir canalizado por conducciones adecuadas. En la mayoría de los casos, y en el nuestro también, se eligen para esta función las llamadas canaletas que nos permiten de una forma flexible trazar los recorridos adecuados desde el área de trabajo hasta el panel de parcheo. (Figura 2.1)

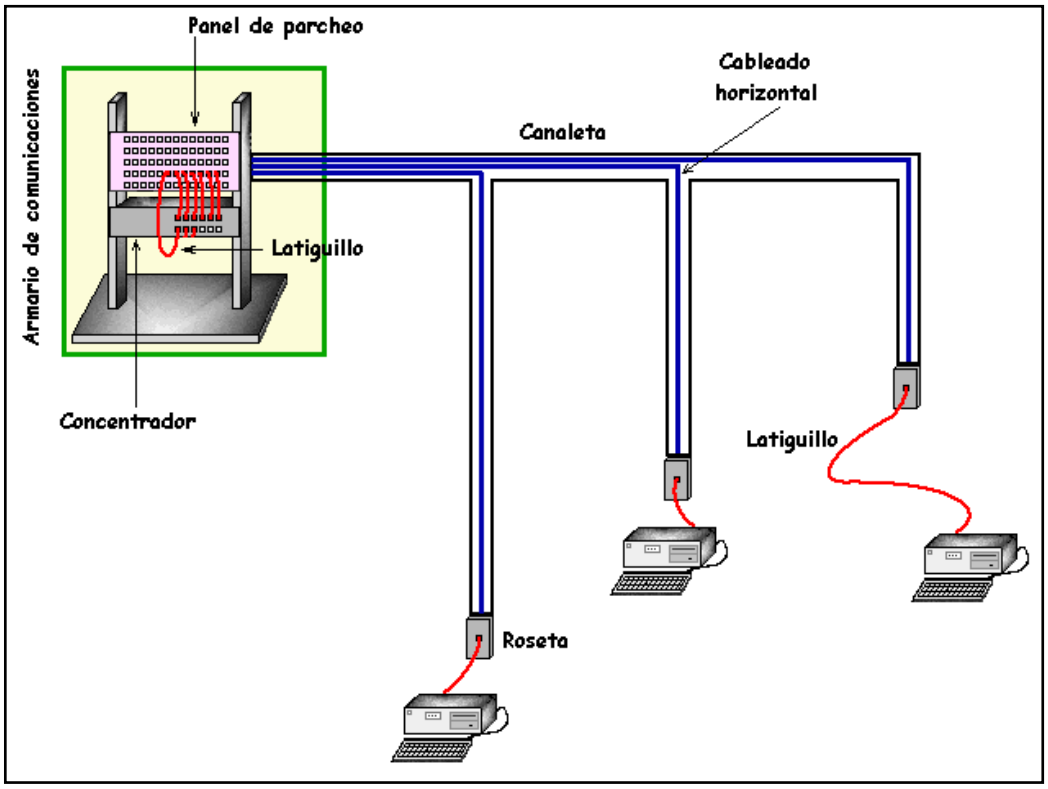


Figura 2.1 Subsistema horizontal

Las canaletas van desde el panel de parcheo hasta las rosetas de cada uno de los puestos de la red. Se podría dividir en dos tipos dependiendo del uso que se le dé:

- Las de distribución. Recorren las distintas zonas del edificio y por ellas van los cables de todas las rosetas.
- Las finales. Llevan tan solo los cables de cada una de las rosetas.

Es muy conveniente que el panel de parcheo junto con los dispositivos de interconexión centralizada (concentradores, latiguillos, router, fuentes de alimentación, etc.) estén encerrados un **armario de comunicaciones**. De esta forma se aíslan del exterior y por lo tanto de su manipulación "accidental". También facilita el mantenimiento al tenerlo todo en un mismo lugar.

Como se puede observar la topología usada es en estrella teniendo en cuenta que cada mecanismo de conexión en la roseta está conectado a su propio mecanismo de conexión en el panel de parcheo del armario de comunicaciones.

El subsistema horizontal incluye los siguientes elementos:

- El cable propiamente dicho.
- La roseta de conexión del área de trabajo.
- El mecanismo de conexión en el panel de parcheo del armario de comunicaciones.
- Los cables de parcheo o latiguillos en el armario de comunicaciones.
- Las canaletas.

Cada cable horizontal no podrá superar los 90 metros. Además los cables para el parcheo en el armario de comunicaciones no podrán tener más de 6 metros y no podrá superar los 3 metros el cable de conexión del puesto de trabajo a la roseta.

2.2.2.3 Subsistema Vertical

El cableado vertical (o de "backbone") es el que interconecta los distintos armarios de comunicaciones. Éstos pueden estar situados en plantas o habitaciones distintas de un mismo edificio o incluso en edificios colindantes. En el cableado vertical es usual utilizar fibra óptica o cable UTP, aunque en algunos casos se puede usar cable coaxial.

La topología que se usa es en estrella existiendo un panel de distribución central al que se conectan los paneles de distribución horizontal. Entre ellos puede existir un panel intermedio, pero sólo uno. (Figura 2.2)

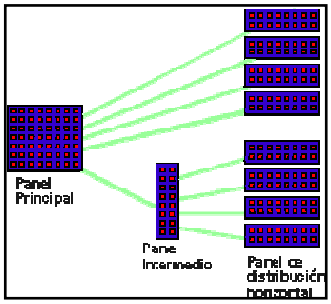


Figura 2.2 Subsistema vertical

En el cableado vertical están incluidos los cables del "backbone", los mecanismos en los paneles principales e intermedios, los latiguillos usados para el parcheo, los mecanismos que terminan el cableado vertical en los armarios de distribución horizontal.

2.2.2.4 Subsistema Campus

Lo forman los elementos de interconexión entre un grupo de edificios que posean una infraestructura común (fibras ópticas, cables de pares, sistemas de radioenlace).

2.2.2.5 Estándares

Todo el cableado estructurado está regulado por estándares internacionales que se encargan de establecer las normas comunes que deben cumplir todos las instalaciones de este tipo. Las reglas y normas comentadas en secciones anteriores están sujetas a estas normas internacionales.

Existen tres estándares, ISO/IEC-IS11801 que es el estándar internacional, EN-50173 que es la norma europea y ANSI/EIA/TIA-568A que es la norma de EE.UU. Éste último es el más extendido aunque entre todas ellas no existen diferencias demasiado significativas.

Todas ellas se han diseñado con el objeto de proporcionar las siguientes utilidades y funciones:

- Un sistema de cableado genérico de comunicaciones para edificios comerciales.
- Medios, topología, puntos de terminación y conexión, así como administración, bien definidos.
- Un soporte para entornos multiproveedor multiprotocolo.
- Instrucciones para el diseño de productos de comunicaciones para empresas comerciales.
- Capacidad de planificación e instalación del cableado de comunicaciones para un edificio sin otro conocimiento previo que los productos que van a conectarse.

El proceso de trabajo a seguir para realizar el cableado y conexionado de la red local del centro pasará por los siguientes puntos:

- Diseño y planificación de la red
- Montaje de la red
- Documentación de la red
- Mantenimiento del cableado de una red informática

2.3 PROTOCOLOS DE COMUNICACIÓN

Los protocolos son como reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet, para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación

Pueden estar implementados bien en hardware (tarjetas de red), software (drivers), o una combinación de ambos.

2.3.1 Funciones Principales de los Protocolos

- Definición de la asignación de pines en el interfaces físico
- Definición de la disciplina de línea a ser usada (Full dúplex – Half dúplex).
- Definición del medio e interfaces para acceso al medio.
- Detección y Corrección de errores en la transmisión.
- Definición de la señalización y codificación a ser usada.
- Proveer una secuencia para los paquetes de datos transmitidos.
- Establecer una técnica de enrutamiento dentro de la Red.
- Garantía confiable de la transmisión y recepción de los datos.
- Establecer una disciplina de dialogo para determinar quien transmite en un momento dado y por cuanto tiempo.
- Proveer un método para establecer y terminar una conexión.
- Establecer una técnica para compresión o encriptación de los datos.

2.3.2 Estandarización

Los protocolos implantados en sistemas de comunicación con un amplio impacto, suelen convertirse en estándares, debido a que la comunicación e intercambio de información (datos) es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo pre-existente. Esto ocurre tanto de manera informal como deliberada.

Existen consorcios empresariales, que tienen como propósito precisamente el de proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos.

2.3.3 Especificación de protocolo

Sintaxis: Se especifica como son y como se construyen.
Semántica: Que significa cada comando o respuesta del protocolo respecto a sus parámetros/datos.
Procedimientos de uso de esos mensajes: Es lo que hay que programar realmente(los errores, como tratarlos)

2.3.4 Definición de protocolo de aplicación

1. Definir el modelo de comunicación: Tenemos dos opciones: Orientado a conexión o No orientado a conexión
2. Definir el servicio de transporte: Que sea fiable o no. tenemos que definir la fiabilidad que tiene. Si queremos total fiabilidad: TCP, y si no, UDP.
3. Definir el tipo de sintaxis: Hay dos tipos. Nos fijamos en la unidad que va a ser capaz de comprender. Bits o Caracteres.

2.3.5 Niveles de abstracción

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI.

Según la clasificación OSI, la comunicación de varios dispositivos ETD se puede estudiar dividiéndola en 7 niveles, que son expuestos desde su nivel más alto hasta el más bajo:

Nivel	Nombre	Categoría
Capa 7	Nivel de aplicación	Aplicación
Capa 6	Nivel de presentación	
Capa 5	Nivel de sesión	
Capa 4	Nivel de transporte	
Capa 3	Nivel de red	Transporte de datos
Capa 2	Nivel de enlace de datos	
Capa 1	Nivel físico	

A su vez, esos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 4 capas superiores trabajan con problemas particulares a las aplicaciones, y las 3 capas inferiores se encargan de los problemas pertinentes al transporte de los datos.

Los protocolos de cada capa tienen una interfaz bien definida. Una capa generalmente se comunica con la capa inmediata inferior, la inmediata superior, y la capa del mismo nivel en otros computadores de la red. Esta división de los protocolos ofrece abstracción en la comunicación.

Una aplicación (capa nivel 7) por ejemplo, solo necesita conocer como comunicarse con la capa 6 que le sigue, y con otra aplicación en otro computador (capa 7). No necesita conocer nada entre las capas de la 1 y la 5. Así, un navegador web (HTTP, capa 7) puede utilizar una conexión Ethernet o PPP (capa 2) para acceder a la Internet, sin que sea necesario cualquier tratamiento para los protocolos de este nivel más bajo. De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador web, un archivo transferido vía FTP o un mensaje de correo electrónico.

Ejemplos de protocolos de red.

- **Capa 1: Nivel físico**
  - Cable coaxial o UTP categoría 5, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232.
- **Capa 2: Nivel de enlace de datos**
  - Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC.,cdp
- **Capa 3: Nivel de red**
  - ARP, RARP, IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, AppleTalk.
- **Capa 4: Nivel de transporte**
  - TCP, UDP, SPX.
- **Capa 5: Nivel de sesión**
  - NetBIOS, RPC, SSL.
- **Capa 6: Nivel de presentación**
  - ASN.1.
- **Capa 7: Nivel de aplicación**
  - SNMP, SMTP, NNTP, FTP, SSH, HTTP, SMB/CIFS, NFS, Telnet, IRC, ICQ, POP3, IMAP.

CAPÍTULO III: SEGURIDAD EN LAS REDES LOCALES

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “Hackers”, “crackers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

3.1 CONCEPTO DE SEGURIDAD EN LAS REDES

Ya que tratamos con conceptos que pueden tener múltiples interpretaciones, seria prudente acordar ciertos significados específicos. Así que, recurro a algunas definiciones.

- Seguridad: es “calidad de seguro”, y, seguro está definido como “libre de riesgo”.
- Información: es “acción y efecto de informar”.
- Informar: es “dar noticia de una cosa”.
- Redes: es “el conjunto sistemático de caños o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin”.

Uniendo todas estas definiciones, puedo establecer qué se entiende por Seguridad en redes.

Seguridad en Redes: es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin.

Uniendo los elementos anteriores se logra llegar a una definición más acertada:

Seguridad en redes. “Es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado”.

3.2 TIPOS DE SEGURIDAD

Los expertos afirman que la inversión en materia de seguridad siempre va a ser menor a las pérdidas que podría sufrir una empresa por un ataque que tenga gran impacto negativo.

3.2.1 Seguridad lógica:

Consiste en todas las soluciones de seguridad, tanto de hardware como de software, que impiden la entrada ilegal de usuarios a las redes de la empresa, herramientas que deben ser implementadas luego de un análisis de vulnerabilidad de la compañía, para que se adapten realmente a sus requerimientos.

3.2.2 Seguridad física:

Este tipo de seguridad está relacionada con garantizar la integridad de los centros de cómputo en caso de cualquier eventualidad, como, por ejemplo, un incendio, corto circuito, fallas en la energía eléctrica o que ningún usuario entre a la empresa sin un carnet que los identifique. Generalmente, este tipo de seguridad está aparte de la seguridad lógica, es por ello que los expertos recomiendan que las dos deban estar enlazadas, porque una es complemento de la otra.

3.2.3 Cifrado de los datos:

Las empresas utilizan la encriptación de la información para que cuando ésta viaje a través de la Red, no pueda conocerse su contenido en caso de ser interceptada por algún hacker. Hoy los sistemas de encriptación permiten hasta 128 bits.

3.2.4 Concientizar al personal de la empresa:

Es importante que las organizaciones le den a conocer a sus empleados el marco de referencia de sus políticas de seguridad y que éstos entiendan, por ejemplo, que no pueden escribir el password que le fue asignado en un papel y pegarlo en la pared, porque ya se estarían rompiendo las normas de seguridad.

3.3 NIVELES DE SEGURIDAD

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book (2), desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.
Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.
Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).
Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

3.3.1 Nivel D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

3.3.2 Nivel C1: Protección Discrecional

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso. Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario" quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.

- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

3.3.3 Nivel C2: Protección de Acceso Controlado

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.

Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

3.3.4 Nivel B1: Seguridad Etiquetada

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

3.3.5 Nivel B2: Protección Estructurada

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior.
La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

3.3.6 Nivel B3: Dominios de Seguridad

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones.

Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

3.3.7 Nivel A: Protección Verificada

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

3.4 IDENTIFICACIÓN DE ATAQUES.

Parte fundamental de una estrategia de seguridad eficaz consiste en realizar una valoración precisa de las amenazas a la red. Al igual que las organizaciones tienen distintos puntos de vista sobre lo que constituye un riesgo para la seguridad física, también tienen distinta opinión sobre los riesgos para los datos de red. Esta opinión depende de numerosos factores, como, por ejemplo, el sector en que opera la organización, el valor de los datos y si han sufrido ataques en la red con anterioridad.

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque.

Un "ataque" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Los ataques siempre se producen en Internet, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos.

Los ataques externos se producen de dos formas principales: ataques perpetrados por personas y los efectuados por aplicaciones malintencionadas. Ambos tipos tienen diferentes características y perfiles de amenaza. Los atacantes humanos pueden aprender detalles sobre la red de destino y modificar el ataque como sea pertinente, mientras que las aplicaciones malintencionadas pueden afectar a varios equipos y dejar puertas traseras para que las utilicen los atacantes.
Las aplicaciones malintencionadas incluyen varias amenazas posibles, como virus, gusanos y troyanos. Aunque estas aplicaciones pueden ser problemáticas y causar trastornos considerables, estos ataques son más sencillos de evitar que los perpetrados por personas.

La identificación de aplicaciones malintencionadas es de importancia considerable para las organizaciones de todos los sectores, aunque sobre todo para aquéllas que funcionan en el sector financiero o que deben cumplir normativas. Por ejemplo, ese tipo de organizaciones sienten más preocupación hacia la presencia de aplicaciones espía. Las aplicaciones espía pueden residir en un servidor o estación de trabajo y transmitir información confidencial a terceros externos.

La principal forma de identificar aplicaciones malintencionadas es realizar el seguimiento de procesos. Al hacerlo, se identifica cada programa que se inicia o se detiene en una estación de trabajo o servidor. La desventaja que presenta es que genera una gran cantidad de sucesos, la mayoría de los cuales carecen de interés.

Los problemas de seguridad que causan los ataques externos son considerables, ya que los atacantes disponen de gran flexibilidad para elegir el método de intrusión en la red. Los atacantes externos pueden penetrar las redes a través de los siguientes mecanismos:

- Intento de conseguir contraseñas
- Cambio o restablecimiento de contraseñas
- Explotación de vulnerabilidades
- Engaño a un usuario para que ejecute una aplicación malintencionada
- Uso de la elevación de privilegios para comprometer a equipos adicionales (lo que en inglés se denomina island hopping, saltos a otros sistemas)
- Instalación de un rootkit o troyano
- Uso de una estación de trabajo no autorizada
- Uso de un ataque phishing, en el cual una dirección de correo electrónico fraudulenta dirige a un sitio Web malintencionado

El principal método para detectar atacantes y aplicaciones malintencionadas consiste en realizar un seguimiento de los procesos. Se necesita aplicar este método con mucha atención e integrarlo con directivas de restricción de software en Directiva de grupo. Teniendo en cuenta que se deben definir directivas estrictas que estipulen qué programas se pueden ejecutar en los equipos dentro de las redes perimetrales.

Para bloquear estos ataques, es importante estar familiarizado con los principales tipos y tomar medidas preventivas.
Los ataques pueden ejecutarse por diversos motivos:

- para obtener acceso al sistema;
- para robar información, como secretos industriales o propiedad intelectual;
- para recopilar información personal acerca de un usuario;
- para obtener información de cuentas bancarias;
- para obtener información acerca de una organización (la compañía del usuario, etc.);
- para afectar el funcionamiento normal de un servicio;
- para utilizar el sistema de un usuario como un "rebote" para un ataque;
- para usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

3.4.1 Tipos de ataque

Los sistemas informáticos usan una diversidad de componentes, desde electricidad para suministrar alimentación a los equipos hasta el programa de software ejecutado mediante el sistema operativo que usa la red.

Los ataques se pueden producir en cada eslabón de esta cadena, siempre y cuando exista una vulnerabilidad que pueda aprovecharse.

Los riesgos se pueden clasificar de la siguiente manera:
Acceso físico: en este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos:

- Interrupción del suministro eléctrico.
- Apagado manual del equipo.
- Vandalismo.
- Apertura de la carcasa del equipo y robo del disco duro.
- Monitoreo del tráfico de red.

Intercepción de comunicaciones:

- Secuestro de sesión.
- Falsificación de identidad.
- Redireccionamiento o alteración de mensajes.

Denegaciones de servicio: el objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:

- Explotación de las debilidades del protocolo TCP/IP.
- Explotación de las vulnerabilidades del software del servidor.

Intrusiones:

- Análisis de puertos.
- Elevación de privilegios: este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de **desbordamiento de la memoria intermedia (búfer)** usan este principio.
- Ataques malintencionados (virus, gusanos, troyanos).

Ingeniería social: en la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.

Puertas trampa: son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador en todo momento.

Trashing (Cartoneo): Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema..."nada se destruye, todo se transforma".El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc. El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

Ataques de Monitorización: Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

Ataques de Autenticación Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

Ataques de modificación-daño:

Tampering o Data Diddling:

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aún así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por Insiders u Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor. Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva. Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA; o la reciente modificación del Web Site del CERT (mayo de 2001). Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.).

Borrado de Huellas:

El borrado de huellas es una de las tareas mas importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las Huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo. Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

Ataques Mediante Java Applets:

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java. Estos Applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con

archivos a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques.

Ataques Mediante JavaScript y VBScript

JavaScript (de la empresa Netscape®) y VBScript (de Microsoft®) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

Es por ello que los errores de programación de los programas son corregidos con bastante rapidez por su diseñador apenas se publica la vulnerabilidad. En consecuencia, queda en manos de los administradores (o usuarios privados con un buen conocimiento) mantenerse informados acerca de las actualizaciones de los programas que usan a fin de limitar los riesgos de ataques.

Ataque por rebote

Cuando se ejecuta un ataque, el pirata informático siempre sabe que puede ser descubierto, por lo que generalmente privilegia los ataques por rebote (en oposición a los ataques directos). Los primeros consisten en atacar un equipo a través de otro para ocultar los rastros que podrían revelar la identidad del pirata (como su dirección IP) con el objetivo de utilizar los recursos del equipo atacado.

Esto comprueba la importancia de proteger su red o PC, ya que podría terminar siendo "cómplice" de un ataque y, si las víctimas realizan una denuncia, la primera persona cuestionada será el propietario del equipo que se utilizó como rebote.

Con el desarrollo de las redes inalámbricas, este tipo de situación podría ser cada vez más común ya que estas redes no son demasiado seguras y los piratas ubicados en sus inmediaciones podrían usarlas para ejecutar un ataque.

3.4.2 Hacker

El término "**hacker**" se usa con frecuencia para referirse a un pirata informático. A las víctimas de piratería de redes informáticas les gusta pensar que han sido atacadas por piratas con experiencia quienes han estudiado en detalle sus sistemas y desarrollaron herramientas específicas para sacar provecho de sus vulnerabilidades.

El término *hacker* ha tenido más de un significado desde que surgió a fines de la década de 1950. Al principio, está palabra se usó con una connotación positiva para describir a los expertos en programación. Luego, en la década de 1970, se la usó para describir a los revolucionarios informáticos. Muchos de ellos se convirtieron en los fundadores de las empresas de IT más importantes.

En la década de 1980, esta palabra se usó para agrupar a personas involucradas en la piratería de videojuegos que desactivaban las protecciones de estos juegos y revendían copias.

En la actualidad, con frecuencia se la usa erróneamente para referirse a personas que irrumpen en sistemas informáticos.

Los diferentes tipos de piratas

En realidad existen varios tipos de "*atacantes*" divididos en categorías de acuerdo a sus experiencias y motivaciones.

- "Los "**hackers de sombrero blanco**", hackers en el sentido noble de la palabra y cuyo objetivo es ayudar a mejorar los sistemas y las tecnologías informáticas, son casi siempre los responsables de los protocolos informáticos y las herramientas más importantes usadas actualmente, por ejemplo el correo electrónico;
- "Los "**hackers de sombrero negro**", más comúnmente llamados *piratas*, son personas que irrumpen en los sistemas informáticos con propósitos maliciosos;
    - "Los "**script kiddies**" (también conocidos como *crashers*, *lamers* y *packet monkeys*) son jóvenes usuarios de la red que utilizan programas que han encontrado en Internet, casi siempre de forma incompetente, para dañar sistemas informáticos por diversión.
    - "Los "**pherakers**" son piratas que usan la red telefónica conmutada (RTC) para hacer llamadas gratis a través de circuitos electrónicos (llamados *cajas*, como la *caja azul*, la *caja violeta*, etc.) que conectan a la línea telefónica para manipular su funcionamiento. Por lo tanto, la palabra "**phreaking**" se usa para el pirateo de líneas telefónicas.
    - "Los "**carders**" principalmente atacan sistemas de tarjetas inteligentes (en especial tarjetas bancarias) para entender su funcionamiento y aprovechar sus vulnerabilidades. El término **carding** se refiere a los piratas de tarjetas inteligentes.
    - "Los "**crackers**" no son galletitas de queso sino personas que crean herramientas de software que permitan el ataque de sistemas informáticos o el craqueo de la protección anticopia del software con licencia. Por consiguiente, el "crack" es un programa ejecutable creado para modificar (o *actualizar*) el software original con el fin de quitarle su protección.
- "Los "**hacktivistas**" (contracción de *hackers* y *activistas*) son hackers con motivaciones principalmente ideológicas. Este término ha sido muy usado por la prensa para transmitir la idea de una comunidad paralela (en general llamada *underground*, en referencia a las poblaciones que vivían bajo tierra en las películas de ciencia ficción).

De hecho, estos tipos de distinciones no son muy claras ya que algunos *hackers de sombrero blanco* han sido alguna vez *hackers de sombrero negro* y viceversa. Es común ver a usuarios de listas de distribución y foros discutiendo sobre la diferencia que debería hacerse entre un *pirata* y un *hacker*. El término *trol* se usa en general para referirse a temas delicados que buscan provocar reacciones intensas.

Algunos ejemplos de troles:

- Me ha atacado un hacker.
- ¿Windows es más fuerte que Mac?
- ¿Qué es mejor, PHP o ASP?
- etc.

Las raíces de sus motivaciones

Los *hackers de sombrero negro* (piratas) pueden actuar por varias razones:

- el atractivo de lo prohibido;
- interés financiero;
- interés político;
- interés ético;
- deseo de reconocimiento;
- venganza;
- deseo de dañar (destruir datos, hacer que un sistema no funcione)

Los *hackers de sombrero blanco* (hackers) por lo general tienen uno de estos objetivos:

- aprender;
- optimizar los sistemas informáticos;
- probar las tecnologías hasta el límite para llegar a un ideal más eficiente y fiable.

Cracker:

Experto que entra en los sistemas informáticos de forma furtiva y con malas intenciones. Suele contar con tecnologías avanzadas para cometer sus acciones y es capaz de deteriorar complejos sistemas.

3.4.3 Virus:

Un *virus informático es un programa de computadora*, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego. Obviamente ahí termina todo su parecido con estos típicos programas que casi todo el mundo tiene instalados en sus computadoras. Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a auto replicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible. Ya se ha dicho antes que los virus informáticos guardan cierto parecido con los biológicos y es que mientras los segundos infectan células para poder replicarse los primeros usan archivos para la misma función. En ciertos aspectos es una especie de "burla tecnológica" hacia la Naturaleza. Mientras el virus se replica intenta pasar lo más desapercibido que puede, intenta evitar que el "huésped" se dé cuenta de su presencia... hasta que llega el momento de la "explosión".

Es el momento culminante que marca el final de la infección y cuando llega suele venir acompañado del formateo del disco duro, borrado de archivos o mensajes de protesta. No obstante el daño se ha estado ejerciendo durante todo el proceso de infección, ya que el virus ha estado ocupando memoria en la computadora, ha ralentizado los procesos y ha "engordado" los archivos que ha infectado.

Bucaneros
Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos " Crackeados " pasan a denominarse " piratas informáticos " así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo para beneficio económico personal.

Esfuerzo de protección
La seguridad del sistema de un equipo generalmente se denomina "asimétrica" porque el pirata informático debe encontrar sólo una vulnerabilidad para poner en peligro el sistema, mientras que el administrador debe, por su propio bien, corregir todas sus fallas.

3.5 HERRAMIENTAS DE SEGURIDAD

Además, existen ciertos dispositivos (firewalls, sistemas de detección de intrusiones, antivirus) que brindan la posibilidad de aumentar el nivel de seguridad.

A continuación describo algunos.

3.5.1 Firewalls
Un **cortafuegos** (o ***firewall*** en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.
También es frecuente conectar al cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.
Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente.

Tipos de cortafuegos
Hay dos tipos según la arquitectura: A nivel de hardware. A nivel de software.

Cortafuegos de capa de red o de filtrado de paquetes
Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI) como el puerto origen y destino, o a nivel de enlace de datos (NO existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Cortafuegos de capa de aplicación
Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuegos a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a Internet de una forma controlada.

Cortafuegos personal
Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

Ventajas de un cortafuegos

Protege de intrusiones. El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

- **Protección de información privada.** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- **Optimización de acceso.-** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un cortafuegos
Un cortafuegos no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.

- El cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (diskettes, memorias) y sustraigan éstas del edificio.
- El cortafuegos no puede proteger contra los ataques de Ingeniería social

- El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.
- El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

3.5.2 Kerberos

Es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar eavesdropping y ataques de Replay.
Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

3.5.3 Criptografía

(del griego κρύπτω *krypto*, «ocultar», y γράφω *graphos*, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.
Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.
Otro método utilizado para ocultar el contenido de un mensaje es ocultar el propio mensaje en un canal de información, pero en puridad, esta técnica no se considera criptografía, sino esteganografía. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en blanco usados para justificar un texto.

La esteganografía no tiene porqué ser un método alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea para dificultar aún más la labor del criptoanalista.
En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

En la Jerga de la criptografía, la información original que debe protegerse se denomina *texto en claro*. El *cifrado* es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* (también llamado *cifra*) se basa en la existencia de una *clave*: información secreta que adapta el *algoritmo de cifrado* para cada uso distinto. Cifra es una antigua palabra arábiga para designar el número cero; en la antigüedad cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso.
Las dos técnicas más sencillas de *cifrado*, en la criptografía clásica, son la *sustitución* (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la *trasposición* (que supone una reordenación de los mismos); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.
El *descifrado* es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El *protocolo criptográfico* especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, en conjunto es lo que constituyen un *criptosistema*, que es con lo que el usuario final trabaja e interactúa.
Existen dos grandes grupos de *cifras*: los algoritmos que utilizan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*, y los que utilizan una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los primeros se denominan *cifras simétricas*, de *clave simétrica* o de *clave privada* y son la base de los algoritmos de cifrado clásico. Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y forman el núcleo de las técnicas de cifrado modernas.
En el lenguaje cotidiano, la palabra *código* se usa de forma indistinta con *cifra*. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los *códigos* son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar "atacar al amanecer". Por el contrario, las *cifras* clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje -letras, dígitos o símbolos-; en el ejemplo anterior, "rcnm arcteeaal aaa" sería un criptograma

obtenido por *transposición*. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un *libro de códigos*.
Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como *encriptado* y *desencriptado*, aunque ambos son neologismos -anglicismos de los términos ingleses *encrypt* y *decrypt*- todavía sin reconocimiento académico. Hay quien hace distinción entre *cifrado/descifrado* y *encriptado/desencriptado* según estén hablando de criptografía simétrica o asimétrica, pero la realidad es que la mayoría de los expertos hispanohablantes prefieren evitar ambos neologismos hasta el punto de que el uso de los mismos llega incluso a discernir a los aficionados y novatos en la materia de aquellos que han adquirido mas experiencia y profundidad en la misma.

3.6 HERRAMIENTAS DE MONITOREO

Todos sabemos que una de las cosas más interesantes es monitorear una red. A veces nos interesa saber qué es lo que entra y sale necesitamos conocer el tráfico de paquetes que se encuentran en actividad.

Veremos, a continuación, una serie de herramientas que nos ayudarán a proteger nuestro sistema. Para conseguirlo, tenemos dos tipos de herramientas. Las primeras, se basan en chequeos a los archivos. Las segundas, nos alertan de posibles modificaciones de archivos y de programas "sospechosos" que puedan estar ejecutándose en la máquina de forma camuflada.

Veremos, en primer lugar, las que chequean la integridad de los sistemas de archivos.

COPS (Computer Oracle and Password System)

Cops es un conjunto de programas diseñado por la Universidad de Purdue que chequea ciertos aspectos del sistema operativo UNIX relacionados con la seguridad.

Existen dos versiones de este paquete: una versión escrita en "sh" y "C" y otra versión escrita en "perl", aunque su funcionalidad es similar. Este programa es fácil de instalar y configurar y se ejecuta en gran cantidad de plataformas UNIX.

En el primer caso, necesitaremos un compilador de lenguaje C y un shell estándar (sh). En el segundo, nos bastará con tener instalado el interprete de perl (versión 3.18 o superior). Entre las funcionalidades que tiene Cops podemos destacar.

- Chequeo de modos y permisos de los archivos, directorios y dispositivos
- Passwords pobres. En el caso que tengamos una herramienta como crack, podemos comentar la línea de chequeo de passwords.
- Chequeo de contenido, formato y seguridad de los archivos de "password" y "group".
- Chequeo de programas con root-SUID.

- Permisos de escritura sobre algunos archivos de usuario como ".profile" y ".cshrc"
- Configuración de ftp "anonymous".
- Chequeo de algunos archivos del sistema como "hosts.equiv", montajes de NFS sin restricciones, "ftpusers", etc.

Tiger
Es un software desarrollado por la Universidad de Texas que está formado por un conjunto de shell scripts y código C que chequean el sistema para detectar problemas de seguridad de forma parecida a COPS.

Una vez chequeado el sistema, se genera un archivo con toda la información recogida por el programa. Tiger dispone de una herramienta (tigexp) que recibe como parámetro dicho archivo y da una serie de explicaciones adicionales de cada línea que generó el programa anterior. El programa viene con un archivo de configuración donde es posible informarle qué tipo de chequeo se quiere realizar. Podemos comentar las operaciones más lentas y ejecutar éstas de forma menos continuada, mientras que las más rápidas pueden ser ejecutadas más frecuentemente.

Entre la información que chequea el programa tenemos:

- Configuración del sistema.
- Sistemas de archivos.
- Archivos de configuración de usuario.
- Chequeo de caminos de búsqueda.
- Chequeos de cuentas.
- Chequeos de alias.
- Comprueba la configuración de ftp "anonymous".
- Chequeo scripts de cron.
- NFS.
- Chequeo de servicios en el archivo /etc/inetd.conf
- Chequeo de algunos archivos de usuario (.netrc, .rhosts, .profile, etc)
- Comprobación archivos binarios (firmas). Para poder chequear éstos es necesario disponer de un archivo de firmas.

Crack
Este paquete de dominio público realizado por Alex Muffet permite chequear el archivo de contraseñas de UNIX y encontrar passwords triviales o poco seguras.

Para ello, usa el algoritmo de cifrado (DES) utilizado por el sistema UNIX y va comprobando a partir de reglas y de diccionarios las passwords que se encuentran en el archivo de contraseñas, creando un archivo con todos los usuarios y palabras descubiertas. Se realiza una serie de pasadas sobre el archivo de contraseñas, aplicando la secuencia de reglas que se especifique.

Estas reglas se encuentran en dos archivos (gecos.rules y dicts.rules) y pueden ser modificadas utilizando un lenguaje bastante simple. Para una mayor efectividad pueden utilizarse diccionarios complementarios (existen en gran diversidad servidores ftp) en diferentes idiomas y sobre diversos temas.

Experiencias realizadas en la Universidad Carlos III de Madrid sobre diversas máquinas han arrojado resultados de 16% de passwords triviales en máquinas donde no se tenía ninguna norma a la hora de poner contraseñas de usuario.

Es una buena norma pasar de forma periódica el crack para detectar contraseñas poco seguras, además de tener una serie de normas sobre passwords, tanto en su contenido como en la periodicidad con que deben ser cambiadas.

Tripwire

Este software de dominio público desarrollado por el Departamento de Informática de la Universidad de Purdue, es una herramienta que comprueba la integridad de los sistemas de archivos y ayuda al administrador a monitorizar éstos frente a modificaciones no autorizadas.

Esta herramienta avisa al administrador de cualquier cambio o alteración de archivos en la máquina (incluido binarios). El programa crea una base de datos con un identificador por cada archivo analizado y puede comparar, en cualquier momento, el actual con el registrado en la base de datos, avisando ante cualquier alteración, eliminación o inclusión de un nuevo archivo en el sistema de archivos.

La base datos está compuesta por una serie de datos como la fecha de la última modificación, propietario, permisos, etc. con todo ello se crea una firma para cada archivo en la base de datos.

Esta herramienta debería ser ejecutada después de la instalación de la máquina con el objeto de tener una "foto" de los sistemas de archivos en ese momento y puede ser actualizada cada vez que añadimos algo nuevo. Dispone de un archivo de configuración que permite decidir qué parte del sistema de archivos va a ser introducida en la base de datos para su posterior comprobación.

Chkwtmp

Es un pequeño programa que chequea el archivo "/var/adm/wtmp" y detecta entradas que no tengan información (contienen sólo bytes nulos).

Estas entradas son generadas por programas tipo "zap" que sobrescriben la entrada con ceros, para, de esta manera, ocultar la presencia de un usuario en la máquina. Este programa detecta esa inconsistencia y da un aviso de modificación del archivo y entre qué espacio de tiempo se produjo.

Chklastlog

Es parecido al programa anterior. Éste chequea los archivos "/var/adm/wtmp" y "/var/adm/lastlog". El primero, es la base de datos de login, y el segundo, la información del último login de un usuario. En el segundo archivo nos indica qué usuario ha sido eliminado del archivo.

Spar

Software de dominio público diseñado por CSTC (Computer Security Technology Center) realiza una auditoría de los procesos del sistema, mucho más flexible y potente que el comando lastcomm de UNIX.

El programa lee la información recogida por el sistema y puede ser consultada con una gran variedad de filtros como usuario, grupo, dispositivo, admitiendo también operadores (=, >, <, >=, &&...).

Por defecto, el programa obtiene la información del archivo "/var/adm/pacct". No obstante, se le puede indicar otro archivo. La información puede ser mostrada en ASCII o en binario para su posterior proceso con spar.

lsof (List Open Files)

Este programa de dominio público creado por Vic Abell, nos muestra todos los archivos abiertos por el sistema, entendiendo por archivo abierto: un archivo regular, un directorio, un archivo de bloque, archivo de carácter, un archivo de red (socket, archivo NFS).

CPM (Check Promiscuous Mode)

Este pequeño programa realizado por la Universidad de Carnegie Mellon, chequea la interfaz de red de la máquina descubriendo si está siendo utilizada en modo promiscuo (escuchando todo el tráfico de la red).

Está herramienta es muy útil, porque nos alerta de la posible existencia de un "sniffer" (olfateador) que intente capturar información en nuestra red como puedan ser las passwords. Este programa debería ser ejecutado de forma periódica para detectar lo antes posible el estado promiscuo en la placa de red. Una forma útil de utilizarlo es mandarnos el resultado vía correo electrónico.

Es importante tener en cuenta que muchos de los programas descritos en este documento, pueden poner la placa en modo promiscuo con lo que deberemos asegurarnos que no son nuestros programas los que producen esa alerta.

Generalmente los programas tipo "sniffer" suelen estar ejecutándose como procesos camuflados en el sistema.

Ifstatus
Software de dominio público creado por Dave Curry, permite, al igual que el anterior, descubrir si un interfaz de red está siendo utilizada en modo promiscuo para capturar información en la red. Sirven todas las recomendaciones mencionadas anteriormente.

Osh (Operator Shell)
Creado por Mike Neuman, este software de dominio público es una shell restringida con "setuid root", que permite indicar al administrador mediante un archivo de datos qué comandos puede ejecutar cada usuario.

El archivo de permisos está formado por nombres de usuario y una lista de los comandos que se permite a cada uno de ellos. También es posible especificar comandos comunes a todos ellos. Este shell deja una auditoría de todos los comandos.
Ejecutados por el usuario, indicando si pudo o no ejecutarlos. Dispone, además, de un editor (vi) restringido.

Este programa es de gran utilidad para aquellas máquinas que dispongan de una gran cantidad de usuarios y no necesiten ejecutar muchos comandos, o para dar privilegios a determinados usuarios "especiales" que tengan algún comando que en circunstancias normales no podrían con un shell normal.

Noshell
Este programa permite al administrador obtener información adicional sobre intentos de conexión a cuentas canceladas en una máquina.

Para utilizarlo basta sustituir el shell del usuario en el archivo /etc/password por éste programa. A partir de ahí, cada intento de conexión generará un mensaje (vía email o syslog) indicando: usuario remoto, nombre de la computadora remota, dirección IP, día y hora del intento de login y tty utilizado para la conexión.

Trinux
Trinux contiene las últimas versiones de las más populares herramientas de seguridad en redes y es usado para mapear y monitorear redes TCP/IP.

El paquete es muy interesante pues, básicamente, se compone varios discos, con los cuales se bootea la máquina que se va a dedicar a realizar el trabajo y corre enteramente en RAM.

CAPÍTULO IV: IMPLEMENTACIÓN DE LA RED

4.1 DESCRIPCIÓN DEL ÁREA

Para la instalación de los equipos de telecomunicaciones, se encontró que el lugar de trabajo se divide en diferentes áreas como se indica, la subdirección de informática, telecomunicaciones, soporte técnico, proyectos, sistemas, *pool* secretarial, dos baños donde muestra las entradas y salidas de cada área como lo indica el diagrama. Figura 4.1.

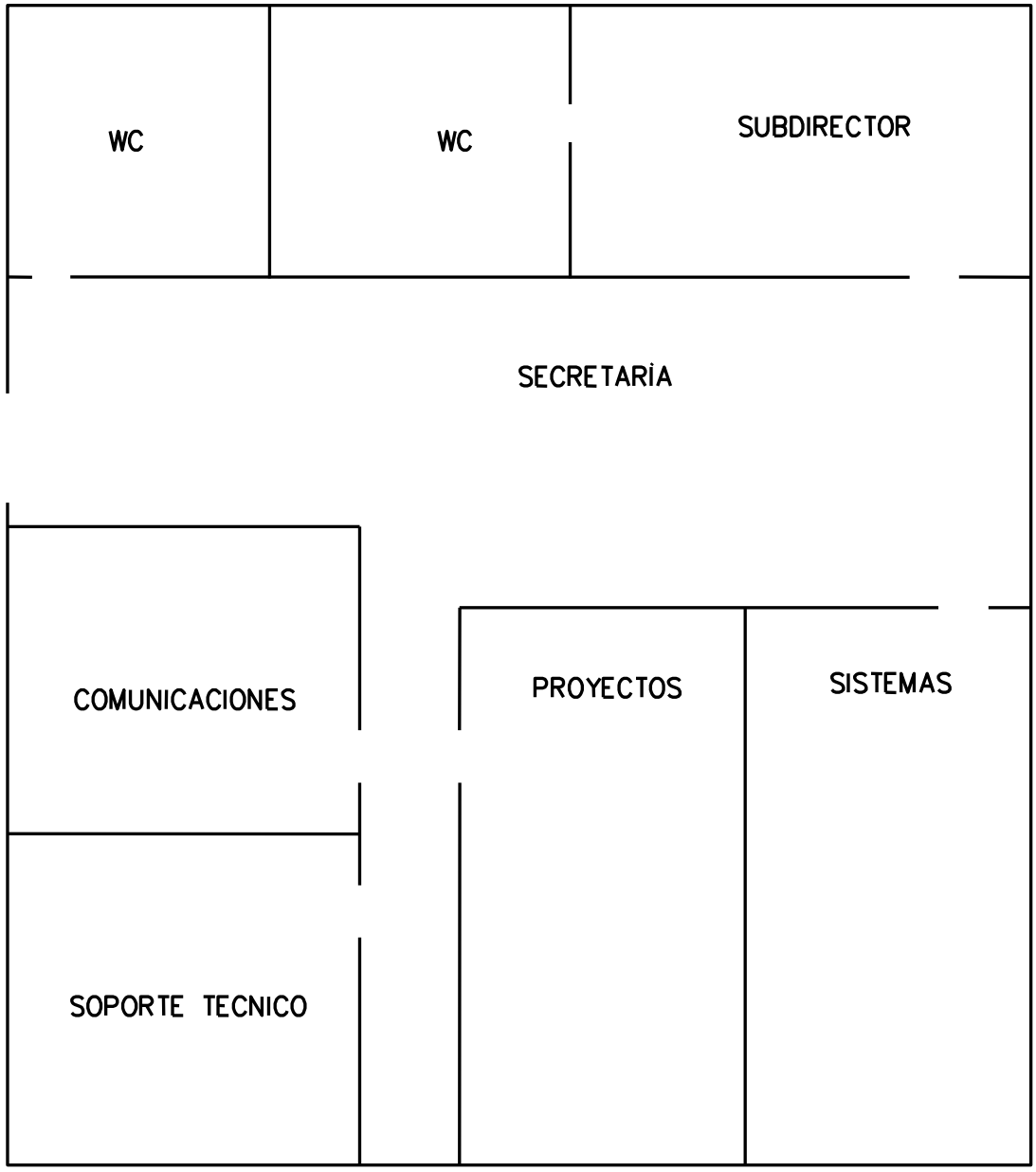


Figura 4.1 Croquis de la oficina de trabajo

4.1.1 Ubicación de los equipos

Se indicó y proporcionó un diagrama de la cantidad y tipo de equipos (veinte computadoras personales, tres impresoras, seis teléfonos) que serán interconectados y anexados a la red, la ubicación y el lugar donde se instaló el cableado estructurado, *patch panel, switch* para conectar los equipos ya mencionados en red como lo muestra la figura 4.2.

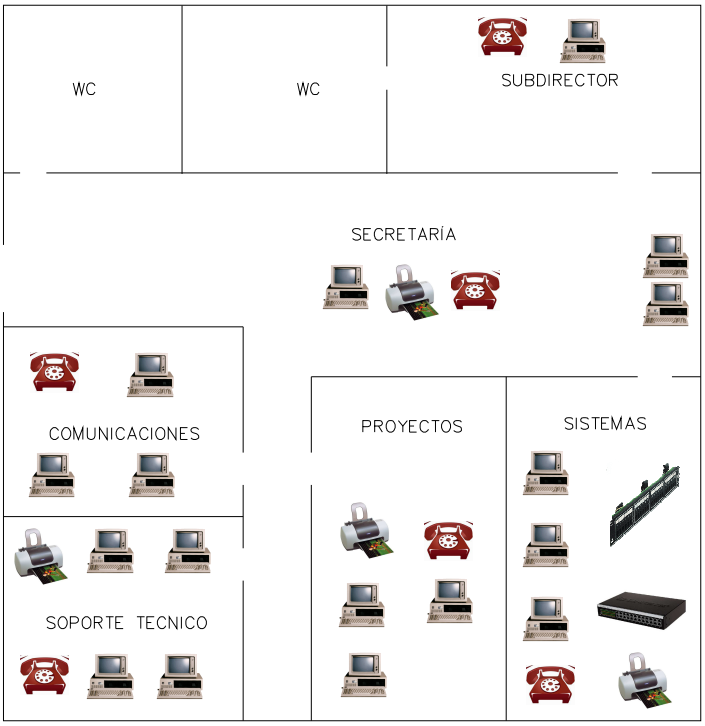


Figura 4.2 Esquema de la red LAN

4.1.2 Revisión y prevención del equipo

Se revisa todo el equipo que se va a interconectar en la red de manera externa para saber si se encontraba en buenas condiciones. El equipo se examinó detalladamente para ver si todo funcionaba correctamente con respecto al *hardware*.

A continuación se muestran algunos cuidados físicos internos que se recomiendan a la subdirección de informática.

- Para evitar sobrecargas eléctricas en los equipos se tendrá que proteger con un regulador de voltaje (NO-BREAK) o una unidad de respaldo (UPS Unit Power Supply) y así como la tierra física que no deberá exceder de 1 *volt* de AC. Los equipos mantendrán corriente regulada para su alimentación.

- Proteger los equipos de polvo, humedad y campos magnéticos en lugares cerrados de un área aproximada a 1.60 metros cuadrados (sitios *on-line*).

- Realizar mantenimiento preventivo y correctivo a equipos de comunicaciones (voz, datos) por lo menos una vez por año.

- Instalar los equipos de cómputo como *Main Frame*, Servidores, RAS (*Remote Acces Server*) *Router, Switches, Hubs, Modems*, Descanalizadores, PBX, ETO (Equipo Terminal Óptico)), ya que siempre es recomendable en estos casos que el centro de cómputo se ubique en un lugar aislado a la humedad, campos magnéticos, movimientos vibratorios, público o contingentes por seguridad y si se encuentra en un edificio en la parte central de éste.

- Regular la temperatura la sala de cómputo y contar con extintores para cualquier contingencia en los equipos.

- Tener en cuenta una buena instalación de electricidad que regule los picos de corriente eléctrica como pueden ser reguladores, UPS, NO BREAK, etc. Esto ayuda a mantener un buen funcionamiento de los equipos de cómputo.

4.2 CONFIGURACIÓN DEL EQUIPO

4.2.1 Limpieza

Los equipos fueron revisados uno por uno para comprobar su funcionalidad interna, se realizo una limpieza con aire comprimido y brochas para liberarlos de toda clase de polvo. Una vez limpios los equipos se realizaron chequeos completos (a las PC) y se verificó que todos los dispositivos internos estuvieran bien conectados a la *motherboard*.

4.2.2 Conexión de tarjetas de red (NIC)

Para conectar ordenadores en red de área local es necesario instalar una tarjeta de red (SMC EZ 10/100 PCI) en cada uno de ellos, habilitar la configuración correspondiente y realizar la conexión física con un cable cruzado o normal, (uno a uno).

El siguiente paso es desconectar el cable de alimentación de energía (AC), desensamblar el chasis del ordenador, revisar los slots (PCI) disponibles para la inserción de la tarjeta, como lo muestra la figura 4.3

Figura 4.3 Inserción de tarjeta de red en slot (PCI)

4.2.3 Inspección del sistema operativo y formateo

Se revisó que todos los equipos contaran con un solo sistema operativo estandarizado (Windows XP Profesional). Una vez confirmada la estandarización del Sistema Operativo se prosiguió al formateo de todas las máquinas para lograr la optimización de funcionalidad de los ordenadores.

4.2.4 Formateando un disco duro del ordenador

Se utiliza el Comando (Format C:) y la pantalla despliega la leyenda:

ADVERTENCIA: todos los datos del disco no extraíble
C: se perderán.
¿Desea formatear (S/N)?

Como se muestra en la figura 4.4, una vez terminado el proceso de formateo se tendrá que reiniciar el ordenador.

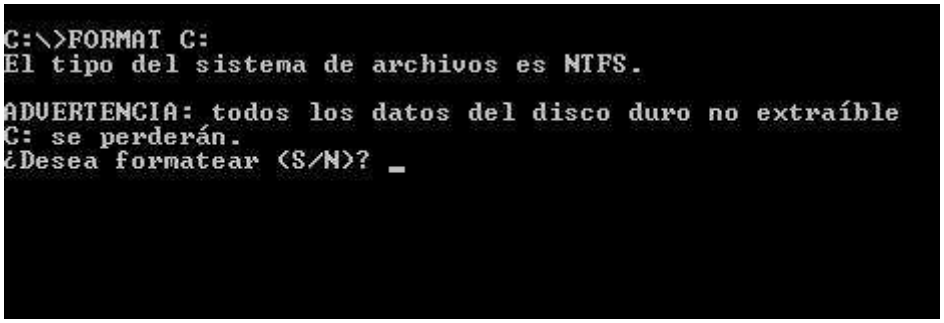


Figura 4.4 Comando Format

4.2.5 Procedimiento de instalación del Sistema Operativo

Para poder instalar el Sistema Operativo (Windows XP Profesional) se deben seguir los siguientes pasos:

1. Insertar el disco de Windows XP Profesional en la unidad de CD.

   - Nota: el ordenador pedirá la partición del disco duro (Hard Disk) correspondiente y será configurado de acuerdo a las necesidades del usuario

2. Aparecerán las tres siguientes opciones:

   - ✓ Instalación de Windows XP profesional.
   - ✓ Instalación con compatibilidad con CD.
   - ✓ Instalación sin compatibilidad con CD.

Si se ejecuta la primera opción, automáticamente la unidad del disco CD-ROM, llamará al asistente que guía al usuario durante el proceso de su instalación, si se ejecuta la opción número 2 se deberá hacer uso de comandos en línea y por último se utiliza la opción 3 no se podrá tener acceso a la unidad de CD-ROM.

Instalación de paqueterías o utilerías.

Para instalar una paquetería o programa (software) es necesario llevar a cabo los siguientes pasos:

1) posibilidad de instalación mediante el análisis de espacio disponible en Disco Duro (Hard Disk)
   - ➢ Posicionar el cursor en icono del botón **inicio** y presionar la tecla **enter.**
   - ➢ Posicionar el cursor en icono del botón mi PC y presionar la tecla **enter.**
   - ➢ Posicionar el cursor en icono del botón Unidad C: y hacer “clic” con el botón derecho del Mouse.
   - ➢ Posicionar el cursor en el menú contextual y seleccionar la opción de *Propiedades*. Donde desplegará la información necesaria para la toma de decisión de la instalación de dicho *programa*.
2) Insertar el disco que contenga los programas deseados para su instalación en Unidad de CD-ROM.
3) Posesionar el cursor en el icono del CD-ROM que se encuentra en *Mi PC* para ver el contenido.
4) Una vez visualizada la información contenida en la unidad de CD-ROM, se busca el botón install.exe, setup, autorun o instalar y se selecciona y se presiona la tecla **enter.**

A continuación en la siguiente figura 4.5 se muestra el botón seleccionado para poder instalar en este caso la paquetería.

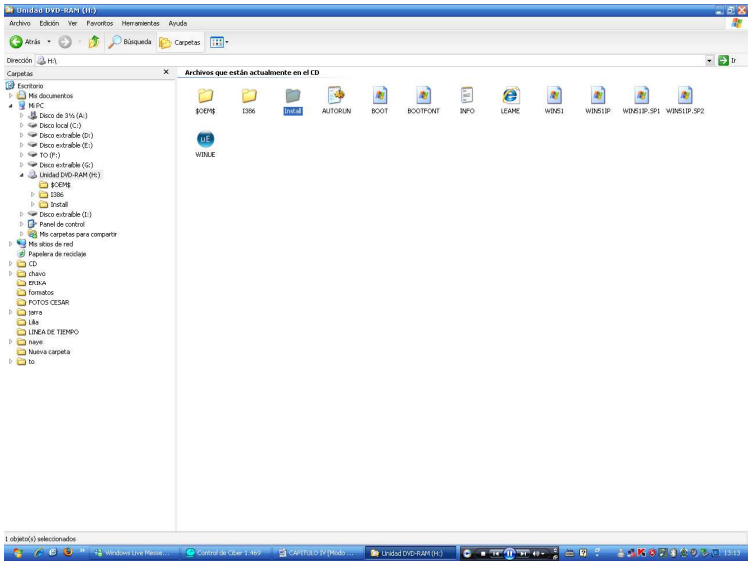


Figura 4.5 botón instalar

Seguir los pasos de la ayuda para recabar la información necesaria.

5) Introducir el número de serie o clave del producto.

4.3 TENDIDO DEL CABLEADO

4.3.1 Introducción

Las redes de área local (LAN) se componen de computadoras, tarjetas de interfaz de red, medios de *networking*, dispositivos de control del tráfico de red y dispositivos periféricos. Las ALN hacen posible que las empresas que utilizan tecnología informática compartan de forma eficiente elementos tales como archivos e impresoras y permiten la comunicación, por ejemplo, a través del correo electrónico, unen entre sí: datos, comunicaciones, servidores de computador y de archivo.

Una WAN (red de área amplia) opera en la capa física y la capa de enlace de datos del modelo de referencia OSI. Interconecta las LAN que normalmente se encuentran separadas por grandes áreas geográficas. Las WAN llevan a cabo el intercambio de paquetes y tramas de datos entre routers y puentes y las LAN que soportan.

4.3.2 Instalación del cableado eléctrico (AC)

Antes de empezar a instalar el cableado estructurado para la red LAN, se tiene que instalar el cable de la corriente eléctrica. Se propuso que para energizar las seis áreas de la oficina adecuadamente, deberían existir por lo menos dos chalupas con tres contactos, cada una por área.

Para empezar con el trabajo de la instalación del cableado eléctrico se elaboró un diagrama del lugar donde se tendrían que colocar los contactos eléctricos basándose en dicho diagrama, se prosiguió a tomar las medidas correspondientes

de las áreas y hacer los cortes respectivos de la tubería. Además se utilizó como símbolo de un contacto eléctrico la siguiente figura 4.6.

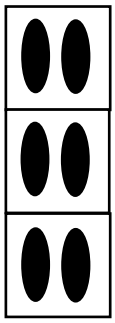


Figura 4.6 Símbolo de una chalupa eléctrica

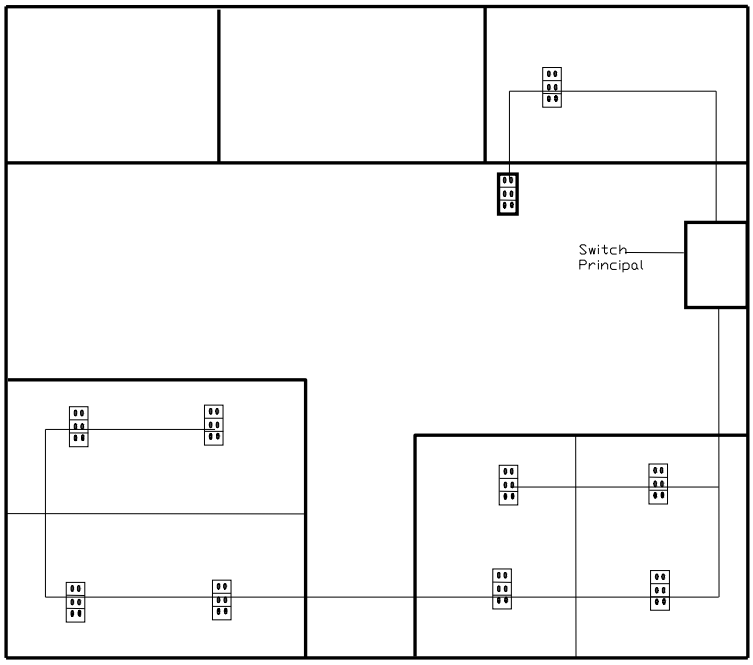


Figura 4.7 Diagrama del tendido del cable eléctrico

Después de ver la ubicación de cada una de las conexiones donde serían colocadas, se prosiguió a hacer las conexiones respectivas como a continuación se indican. Se cortaron los tubos galvanizados con sus respectivas medidas por donde pasarían los tres hilos del cable, se introdujo una guía dentro del tubo para poder pasar por dentro los cables. Una vez introducido y medido el cable dentro del tubo con la chalupa ya colocada, se hicieron los cortes correspondientes, se colocaron los tres colores del cable según el caso (neutro, carga y tierra física)

figura 2.3, se atornillaron todas las chalupas, tapas y el tubo se fijo al muro a una distancia del suelo de cinco centímetros y finalmente se verificaron todas las conexiones con el multímetro para verificar si existía continuidad en el cable como se muestra en la figura 4.8

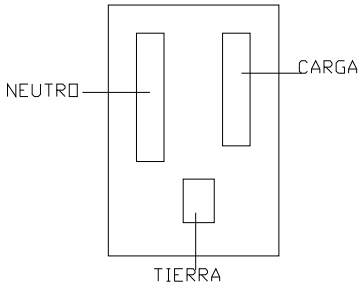


Figura 4.8 clavija de conexión de energía

4.3.3 Instalación del cableado estructurado (Datos)

Para empezar con el tendido del cableado de red, la oficina de informática proporcionó cinco bobinas de cable UTP categoría 5de 250 metros de distancia. Se iniciaron los trabajos de instalación en el área de telecomunicaciones debido que era el área más distante del *Rack* de comunicaciones. Se instaló canaleta plástica dos vías de (5 x 2.5 cm) por la periferia del inmueble hasta el área de instalación, se tomaron tres bobinas de cable UTP y se acometieron sobre la misma. En la figura 4.9 se muestra la trayectoria de cableado estructurado para el área de Telecomunicaciones.

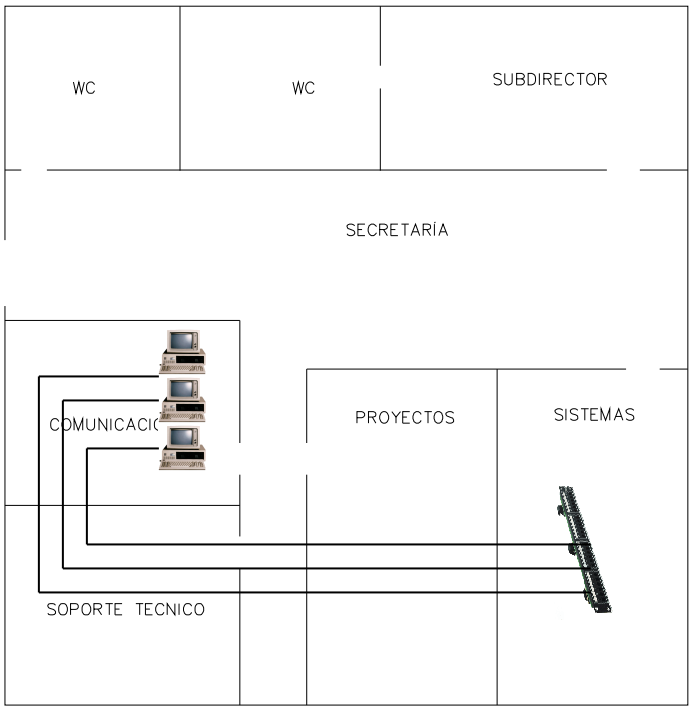


Figura 4.9 Cableado estructurado del área de Telecomunicaciones

Una vez instalada la canaleta plástica dos vías de (5 x 2.5 cm) hasta el área de Telecomunicaciones, se midieron y cortaron los cables necesarios para los servicios solicitados (Soporte Técnico, Proyectos y Sistemas). En las figuras (4.10, 4.11 y 4.12) se muestran las trayectorias del cableado.

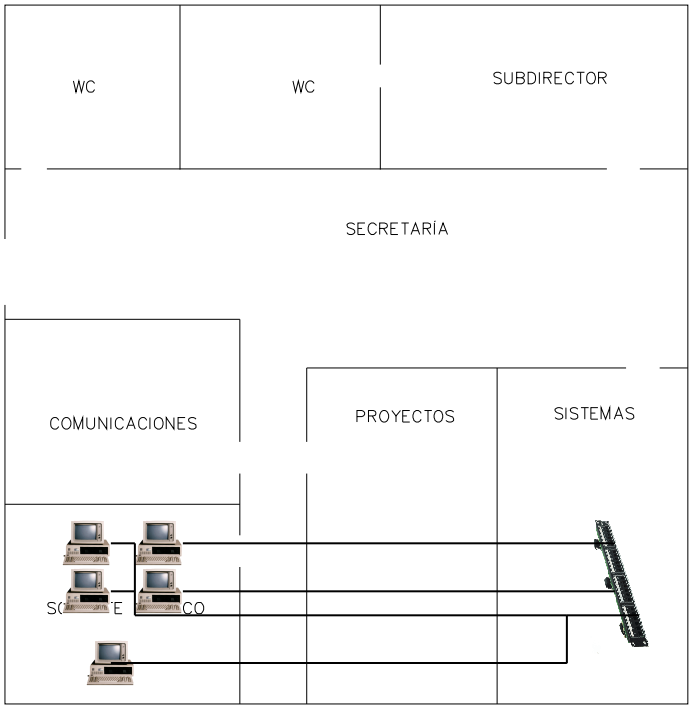


Figura 4.10 Cableado Estructurado del área de Soporte Técnico

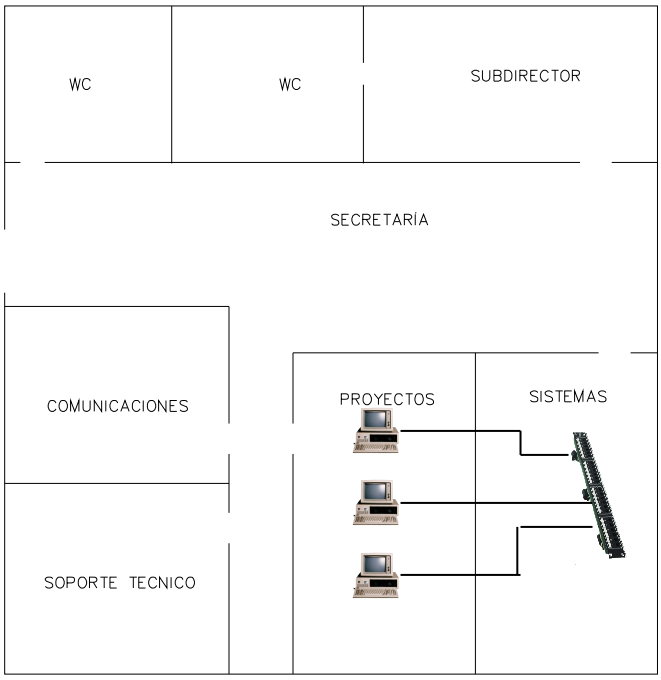


Figura 4.11 Cableado Estructurado del área de Proyectos

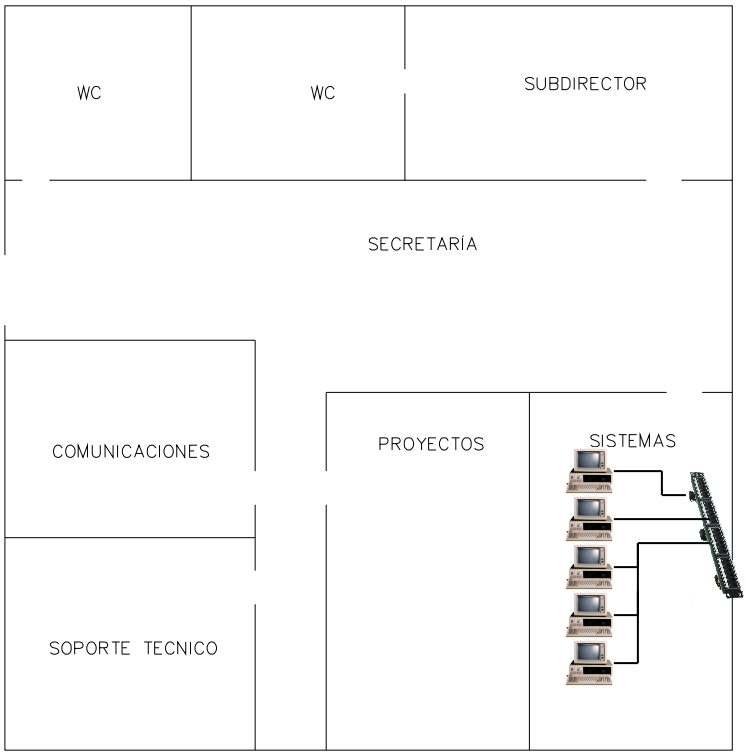


Figura 4.12 Cableado Estructurado del área de Sistemas

Para el área de la subdirección de informática y telecomunicaciones y su secretaría se instaló canaleta plástica de dos vías (5 x 2.5 cm.), se midió y se cortaron los cables necesarios para los servicios solicitados y se acometieron hasta la estación de trabajo como lo muestra la figura 4.13

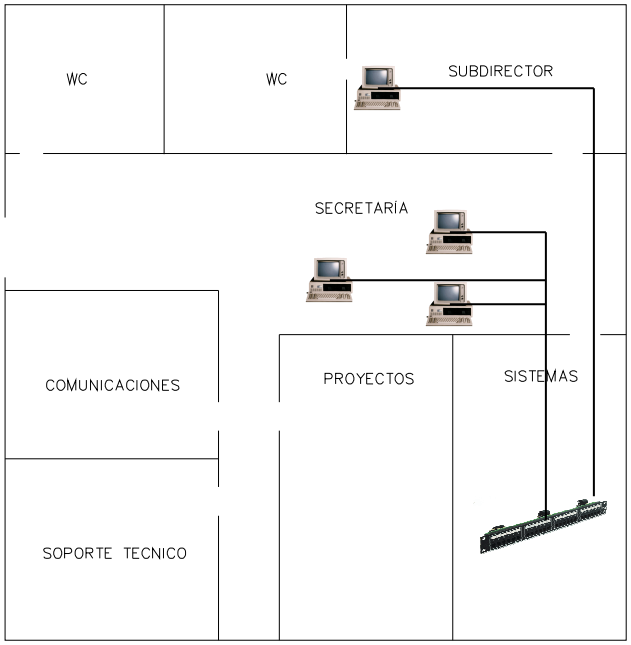


Figura 4.13 Cableado Estructurado del área de la Secretaría y el Subdirector

4.3.4 Instalación del cableado estructurado (Voz)

Para la instalación del cableado de voz se utilizaron 2 cables UTP CAT 5 para la conexión. En el siguiente diagrama de la figura 4.14 se muestra la trayectoria del cableado hasta las estaciones de trabajo.

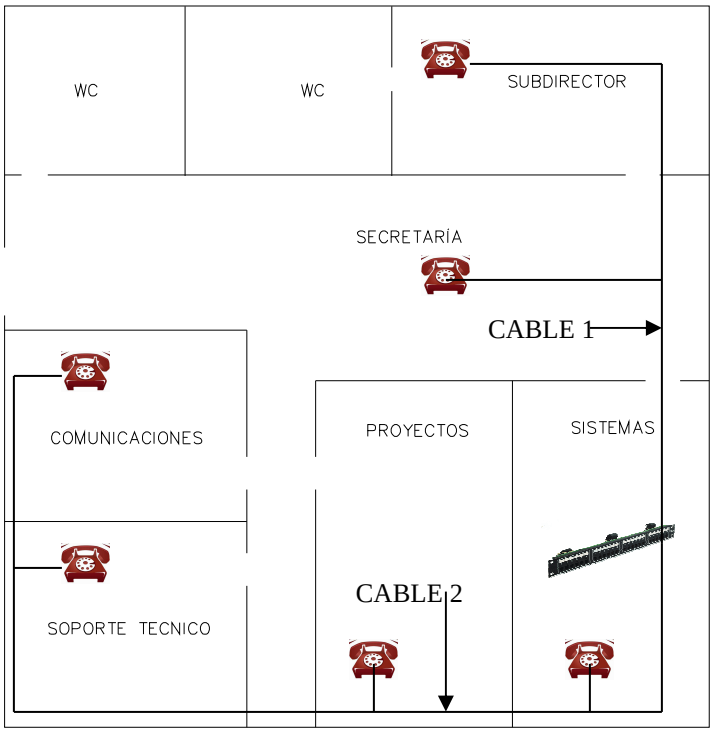


Figura 4.14 Cableado Estructurado de voz

4.3.5 Instalación de cableado entre dos edificios

Para realizar la conectividad de datos entre los edificios se utilizó un cable FTP CAT 5 blindado. Se instalaron tres cables entre los edificios a una distancia de 90 metros con sus respectivas conexiones (Instalación del Switch en el Rack). En el siguiente diagrama de la figura 4.15 se muestran los edificios a (H. Ayuntamiento), b (subdirección de informática)) y la calle donde se instaló el cable para anexar la oficina de informática a la red de telecomunicaciones WAN.

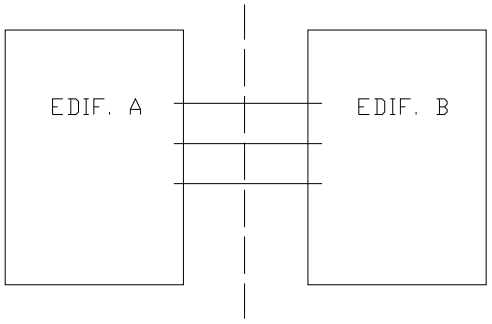


Figura 4.15 Enlace entre edificios

Nota: la necesidad de interconexión entre edificios para el abastecimiento de comunicaciones (Voz, datos) fue realizada mediante tendidos aéreos con tres cables blindados FTP (Protocolo de transferencia de archivos) debido a la inexistencia de acometida subterránea entre los mismos.

Los requerimientos y especificaciones necesarios para la operación óptima de las comunicaciones aéreas a intemperie es la recomendada para usar este tipo de conductor, figura 4.16.

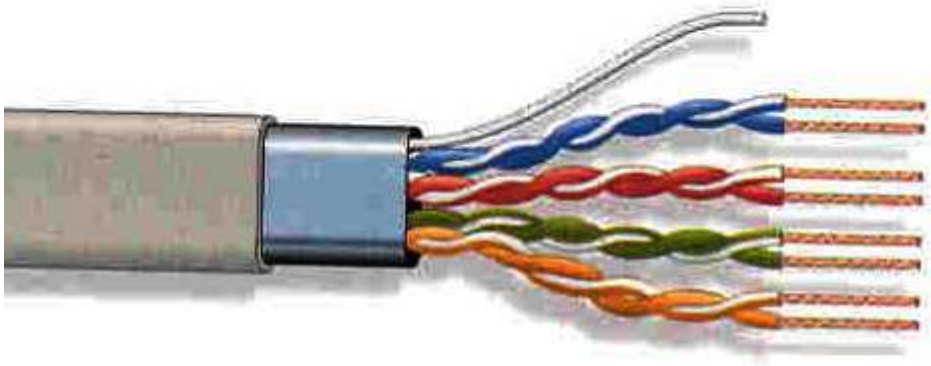


Figura 4.16 Cable FTP (Protocolo de Transferencia de Archivos) blindado

4.3.6 Conexiones en los cables

Para la instalación de los conectores RJ-45 y Jacks se utilizó la norma de colores estandarizada T-568 B como lo muestra la figura 4.17 (Muestra la norma que se utilizó para las conexiones que envían los datos).

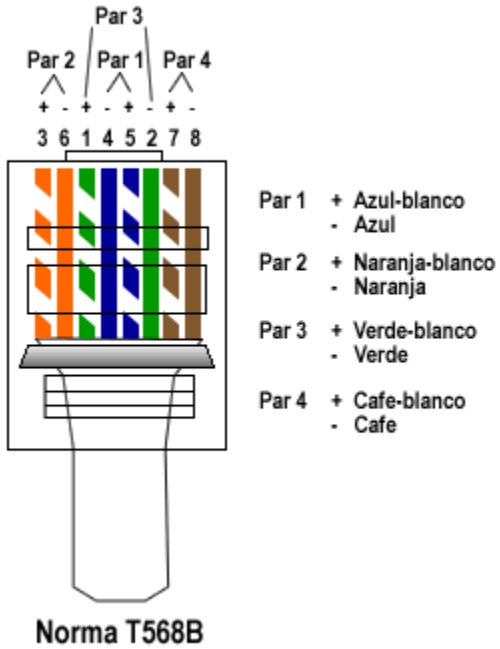


Figura 4.17 Norma de colores en los cables a utilizar (568 B)

En las figuras 4.18 y 4.19 se muestran los tipos de conexiones y conectores que se utilizaron en el cableado de 90 metros entre los edificios y en las áreas de las oficinas.

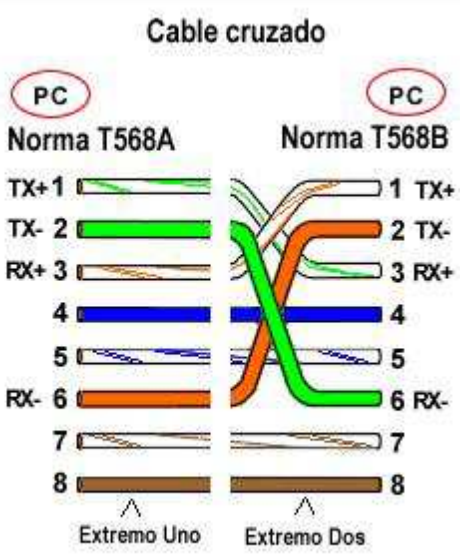


Figura 4.18 Conexión entre los cables con la norma 568 B

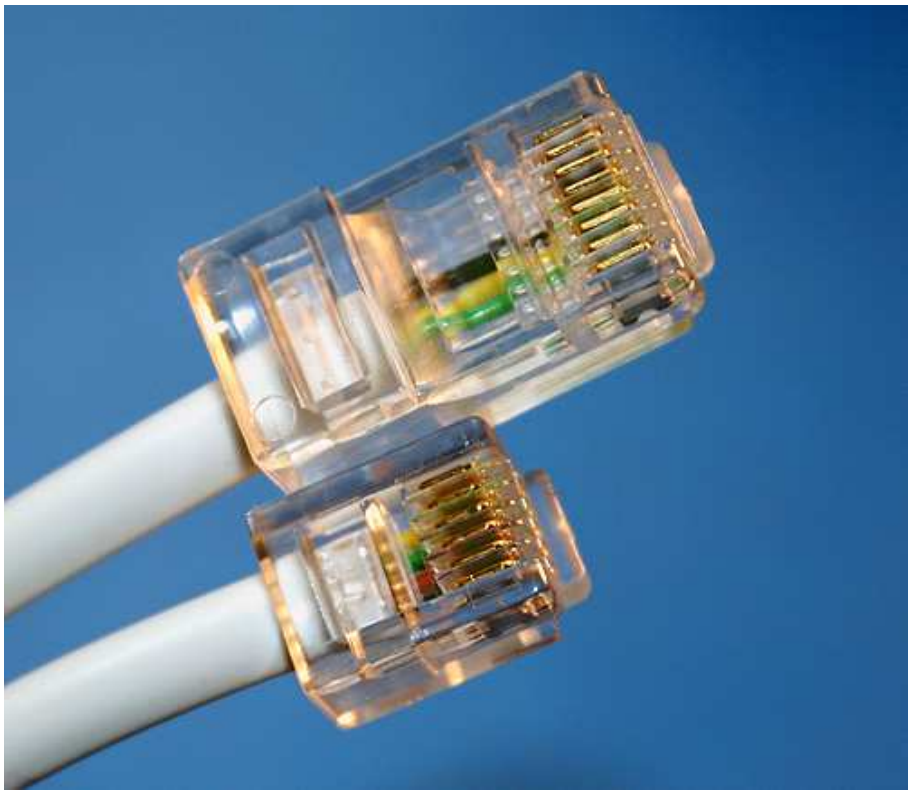


Figura 4.19 Conectores RJ-45 y RJ-11

Una vez instalado el cableado estructurado voz-datos, se prosiguió a instalar los jacks RJ-45 para que se pudieran conectar los equipos desde su misma área respectiva. En la figura 4.20 se muestra como se conectaron los cables hacia un Jack RJ-45.

Figura 4.20 Conectando un cable RJ-45 hacia un Jack

Para poder hacer las conexiones con los jacks y conectores, se utilizaron pinzas de impacto y pinzas para conectores RJ-45, y RJ-11 que se muestran en la figura 4.21.

Figura 4.21 Pinzas ponchadoras y pinzas de impacto

4.4 CONFIGURACIÓN DEL *SWITCH* Y EL ORDENADOR

4.4.1 Procedimiento para activar una Hyper Terminal

Para poder configurar el *switch* se utiliza una herramienta que viene incluida en el S.O. (Sistema Operativo) de Windows XP que se llama Hyper Terminal. Esta herramienta proporciona una ventana en modo lineal donde se introducen los comandos correspondientes para dicha configuración. A continuación se siguen los siguientes pasos previos para la configuración correspondiente.

1. Con el cursor del *Mouse* se presiona el botón *inicio*, se selecciona *programas, accesorios, comunicaciones* y el ícono de *Hyper Terminal* (figura 4.22) se oprime el botón *enter*

Figura 4.22 Icono de Hyper Terminal

2. Una vez oprimido el icono de *Hyper Terminal* aparecerá una ventana (Figura 4.23) donde se indicará que escriba el nombre de la Terminal y el icono correspondiente; posteriormente se oprime el botón *Aceptar.*

Figura 4.23 Descripción de la conexión

3. Después aparecerá una ventana donde se pedirá que se elija el modo de conexión (COM1), que se utilizará para conectarse con la *Hyper Terminal.* En la ventana *propiedades de COM1* se tomaron los siguientes datos que se muestran en la figura 4.24

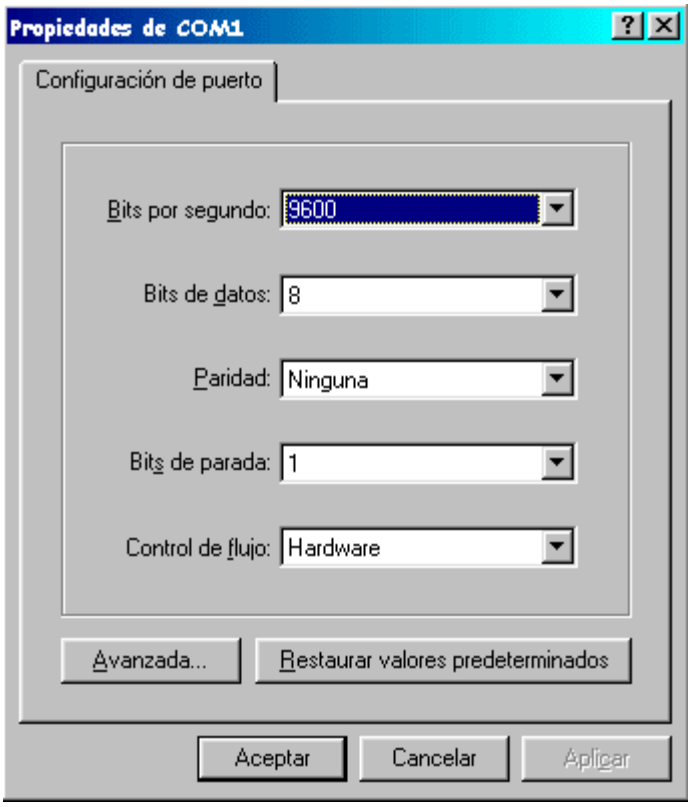


Figura 4.24 Propiedades de COM1

4.4.2 Configuración del *Switch*

Cuando se habilita la conexión de una *Hyper Terminal* se muestra un menú de inicio de dos opciones ([K], [M]) donde pide la forma en la que se va a acceder al *Switch* de manera predeterminada se elige la opción [K] que es la de modo comando; posteriormente aparecerá el *promont* de modo usuario (>). En esta modalidad se tienen ciertas restricciones de configuración. Para poder configurar el *Switch* sin restricciones se escribe el comando ***enable*** y con esto se habilita el modo privilegiado (#) donde se tienen todos los permisos de configuración.

Una vez ya en el modo privilegiado, para poder asignarle un nombre al *Host* (Switch) se utiliza el comando *Hostname*, pero para poder asignar este comando en este modo se utiliza el comando *configure terminal*; este modo es global, en otras palabras el modo de configuración.

Para asignarle una dirección lógica (IP) al *host* se utiliza el comando *ip address.* Posteriormente para entrar a una interfaz primero se escribe en el modo global el

comando *Interface Ethernet* 0/0 de a cuerdo a los puertos correspondientes del *Switch*; para activar dicha interfaz se escribe el comando *shutdown*.

4.4.3 Configuración del Ordenador

Para configurar un ordenador en red se deben seguir los siguientes pasos:

- Dirección IP válida.
- Máscara de Subred.
- Puerta de Enlace y domino de red.
- Servidores DNS

Como el *subneting* ya se había hecho con anterioridad, se prosiguió a seguir los pasos correspondientes para otorgarles sus direcciones IP correspondientes a cada ordenador.

1) Se selecciona del escritorio el icono *Entorno de Red* y con el botón derecho del *Mouse* se elige la opción *Propiedades*. Si no se encuentra debe dirigirse al botón de inicio, seleccionar Configuración – *Panel de control* y presionar el icono *Red*. La ventana que se despliega es la mostrada en la figura 4.25

Figura 4.25 Menú contextual del Entorno de Red

2) Se selecciona *Protocolo TCP/IP* y se presiona el botón *propiedades* figura 4.26.

Figura 4.26. Protocolo TCP/IP

3) En la carpeta *General,* se activa la opción *Usar la siguiente dirección IP* figura 4.27

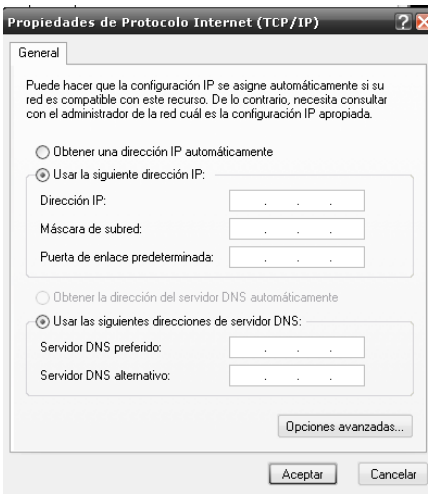


Figura 4.27 Carpeta de Direcciones

Se asignan los octetos correspondientes, proporcionados por los *carriers* (Prestadores de servicio), *Internet* y otros tipos de servicios ISDN (*Interface Service Digital Network*). Posteriormente se presiona el botón Aceptar y se le indica que reinicie la máquina para que la configuración quede activada (figura 3.1)

4) Al iniciar la máquina, se puede probar la conexión a la red de la siguiente manera:

   - Ir al botón *Inicio*, seleccionar *Ejecutar* y escribir una dirección x.x.x.x; presione el botón *Aceptar*.
     Con esto se abrirá una ventana en la que debe aparecer un mensaje parecido al mostrado en la figura 4.28

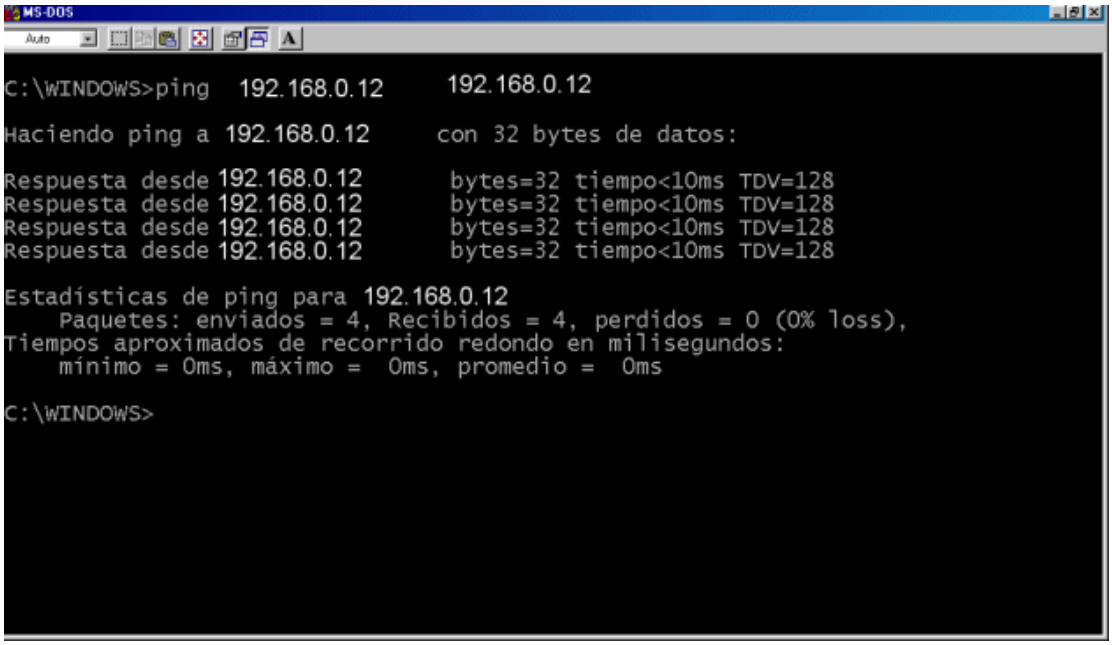


Figura 4.28 Comando *Ping*

Si se escribe un mensaje de respuesta similar, la configuración esta lista, si no, es que puede existir algún problema de configuración o del cableado estructurado.

ANEXOS

Figura A.1 Material utilizado en la colocación de los nodos.

Figura A.2 Área de proyectos.

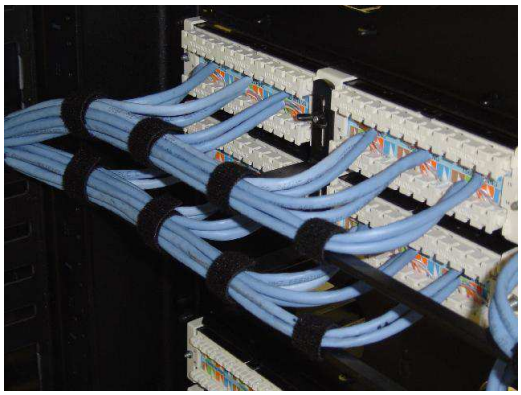


Figura A.3 Conexión final en Patch panel.

Figura A.4 Limpieza de los equipos.

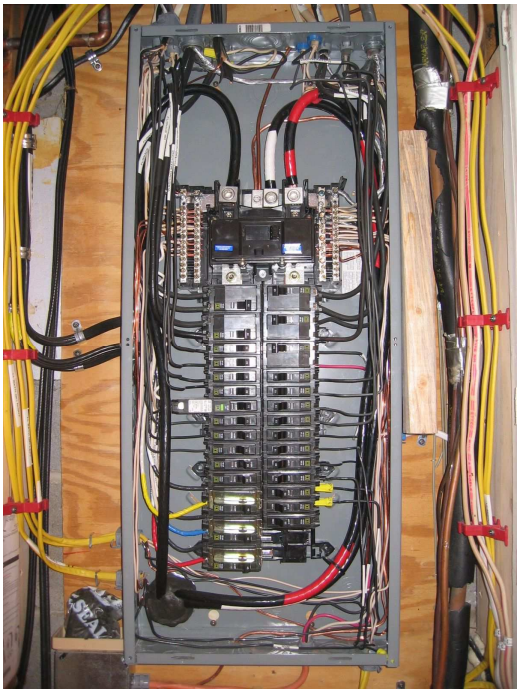


Figura A.5 Centro de carga de la instalación eléctrica

Figura A.6 Montado del rack

CONCLUSIONES

Al implementar la red en el H. Ayuntamiento de Hueypoxtla del Estado de México se cumplió satisfactoriamente con los objetivos fijados al inicio del proyecto gracias a que fueron proporcionados, dentro de lo posible, los elementos y herramientas necesarias para trabajar, como software, tarjetas de red, cable, rosetas, Patch panel, switch entre otros, incluyendo también el material necesario para la instalación eléctrica (cable, chalupas, tubería . dejando así en condiciones óptimas y funcionales la subdirección de informática, ya que se contó con apoyo de asesores quienes siempre tuvieron la disposición de informar y enseñar los procedimientos a seguir para llevar a cabo el proyecto.
Con esta infraestructura de telecomunicaciones se obtiene ahorros en consumibles de impresión, papel, discos flexibles, posiciona a la administración municipal en la modernidad y coadyuva a la eficiencia operativa en conjunto.

Finalmente los resultados esperados de tal reubicación de las oficinas fueron cumplidas en tiempo y forma, resolviendo problemas técnicos y administrativos inherentes al programa establecido por la subdirección de Informática y Telecomunicaciones.

GLOSARIO

Ancho de banda	Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. También se utiliza éste término para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.
Broadcast	Transmisión abierta. Mensajes que se mandan sin destino.
Colisión	Definido como un exceso en portadora eléctrica. Sucede en Ethernet cuando dos o más estaciones hablan al mismo tiempo y las señales de datos se pierden.
Concentrador	Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.
CPU	Unidad Central de Proceso. Director y principal realizador de procesos de la computadora. Circuito microprocesador que realiza los procesos de datos básicos y controla el funcionamiento general de la computadora.
Data Address	Localización física dentro del dispositivo de almacenamiento.
Dominio	Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.
Driver	Manejador. Es el programa que contiene el algoritmo de manejo de un tercer elemento para poder manejarlo como otro dispositivo (ejemplo: el programa que permite manejar una tarjeta de red como otro dispositivo es el driver).
DTE	En redes son los equipos en donde los datos tienen origen y destino.
E0	Término utilizado para referirse a los canales de ISDN de 64 Kbps en estándar Americano.
E1	Estándar Europeo de transmisión de datos 2.048 Mbps.

E3	Canal de comunicación Digital de 34 Mbps.
E-mail	Correo que se establece vía electrónica mediante Internet. Cada persona tiene una dirección asignada en su computadora de tal manera que puede enviar y recibir mensajes.
Ethernet	Estándar de red más popular e implementada. Utiliza CSMA/CD con una velocidad de 10 Mbps.
Firewall	Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizada. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.
Frame Relay	Paquetes retrasados. Protocolo de comunicación asíncrono con dispositivo especial que atrasa el envío de grupos de información para mandarlos en paquetes de tamaño físico.
Hardware	Se utiliza vocablo inglés para denominar al conjunto de componentes físicos que forman un ordenador, incluyendo los periféricos.
Host	Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir Usuarios.
Hub	Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con funciones inteligentes de retraso de señal (retiming), retransmisión de la misma (repeating).
Interface	Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para los dos sistemas diferentes.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino y éste envía sin acuse de recibido.
LAN	Red de Área Local. Red de datos de alta velocidad y

	bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y la señalización en la capa física y la capa de enlace de datos del modelo de referencia OSI. Ethernet, FDDI y Token Ring son tecnologías de LAN ampliamente utilizadas. Comparar con MAN y WAN.
Modelo OSI	Modelo de referencia para interconexión de sistemas abiertos. Modelo de arquitectura de red desarrollado por ISO e UIT-T. el modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales.
NetBios	Interfaz estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
Ordenador	Computadora Personal.
Paquete	Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. El término “paquete” se usa con mayor frecuencia para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.
Ping	Instrucción utilizada por el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de red. Éste es un mecanismote prueba sumamente básico.
PC cards	Dispositivos periféricos que agregan una amplia variedad de posibilidades a las computadoras: almacenamiento, memoria, manejo de periféricos, fax, red, comunicaciones, etc. Existen tres tipos de acuerdo a su tamaño.
Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.

Repetidor	Dispositivo que transmite y amplifica la señal de la red.
Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje.
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
Segmento	1. en una LAN que usa topología de bus, un segmento es un circuito eléctrico continuo que a menudo está conectado a otros segmentos similares a través de repetidores. 2. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.
Software	Está formado por aquellos programas de diversos tipos o elementos lógicos, como el Sistema Operativo, que hacen funcionar un ordenador o una red que se ejecutan en ellos, en contraposición con los elementos físicos de la red o el ordenador. El término software está en oposición al de hardware, duro-blando, por lo que se refiere a la intangibilidad de los programas y la realidad física del ordenador.
Trama	Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado y la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se utilizan para describir las agrupaciones de información lógica en las distintas capas del modelo de referencia OSI y en distintos círculos de tecnología.
TCP/IP	Protocolos definidos por catedráticos en el proyecto Arpanet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.

Usuario	Persona que trabaja con la estación de trabajo. El que realiza tareas de acceso a los recursos de la red, pero no los modifica sustancialmente.
WAN	Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.

BIBLIOGRAFIA

Referencias de texto.

- D Bertsekas y R. Gallager, Data Networks, 2ª Ed., New Jersey, Prentice Hall.

- Corner, D. E., Internetworking con TCP/IP, volumen 1,2. Ed., Prentice Hall.

- Stalling, W. Comunicaciones y Redes de computadoras, 6ta. Edición. Prentice Hall, 2000.

- S. Feit, TCP/IP Architecture, protocols and implementatio, Nueva York, Mc Graw-Hill.

- GS Comunicaciones, Telecomunicaciones: Redes de datos, México, Mc Garw-Hill.

- St-P. Armand y S. William, Redes Locales e Internet, México, Trillas.

- León García, A; Widjaja, I, Redes de Comunicación, Conceptos Fundamentales y arquitecturas básicas, 1ra. Edición, Mc Graw-Hill, 2001.

- Stalling, W. Comunicaciones y Redes de Computadoras, 6ta. Ed., Prentice Hall.

- w. Stallings, Local ¡ Metropolitan Area Networks, New Jersey, Prentice Hall.

- Protocolos de Internet. Diseño e implementaciçon en sistemas UNIX, 2000 ALFAOMEGA Grupo Editor, S.A. de C.V.

Referencias Electrónicas

- http://www.uib.es/edured/redes-intro.html
- http://www.aprendaredes.com
- http://es.wikipedia.org/wiki/protocolo_de_red
- http://www.forest.ula.ve/mana/cursos/redes/clasifica.html
- http://www.monografias.com
- http://www.um.es/docencia/barzana/IATS/lats2003.html
- http://www.eveliux.com/telecom/protocolos.html
- http://neo.lcc.uma.es
- http://es.wikipedia.org/wiki/FTP