CAPÍTULO II

MARCO TEÓRICO

2.1- Definición de Red

Una red es un grupo de ordenadores y dispositivos periféricos conectados unos a otros para comunicarse y transmitir datos con el objetivo de compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico o inalámbrico. Una red utiliza protocolos de red para comunicarse.

2.1.1- Tipos de Redes

No existe una sola categorización de redes puesto que pueden clasificarse de acuerdo a varios parámetros como son:

Por extensión las redes pueden ser:

- ✓ **Área de red local (Local Area Network):** Consiste en una red que conecta los ordenadores y dispositivos en un área relativamente pequeña y predeterminada.
- ✓ **Área de red metropolitana MAN (Metropolitan Area Network):** Consiste en una interconexión de equipos informáticos distribuidos en una zona abarcada por varios edificios y generalmente trabaja a mayores velocidades que una LAN.

- ✓ **Área de red amplia WAN (Wide Area Network):** Consiste en una o más LAN que abarcan un área geográfica común.
- ✓ **Área de red personal PAN (Personal Area Network):** Son redes de pocos metros de distancia entre los ordenadores y dispositivos, los cuales son de uso personal.

Por relación funcional se clasifican en:

- ✓ Cliente – Servidor
- ✓ Igual-a-igual P2P (Per to per)

Por topología:

- ✓ Bus
- ✓ Estrella
- ✓ Malla
- ✓ Anillo
- ✓ Jerárquica

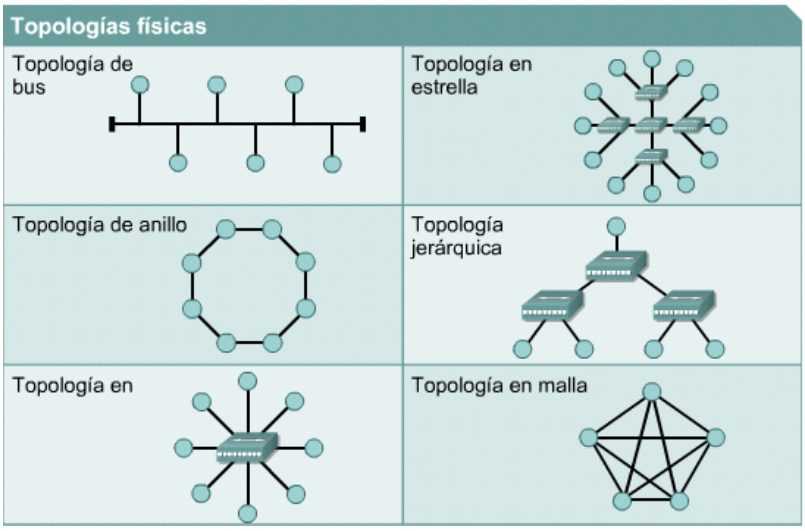

Figura 2.1: Topologías Físicas [1]

[1] Figura tomada de: Cisco, CCNA1 Versión 3.1. Modulo 1

Por estructura:

- ✓ Red OSI [1]
- ✓ Red TCP/IP

2.1.2- Intranet y Extranet

Además una red puede convertirse en una intranet o extranet:

Intranet

Red montada para el uso exclusivo dentro de una empresa u hogar. Puede o no tener acceso a Internet y sirve para compartir recursos entre computadoras.

Extranet

Intranet extendida (Extended Intranet). Es una red privada virtual resultado de interconectar dos o más intranets que utilizan Internet como medio de transporte de información entre sus nodos.

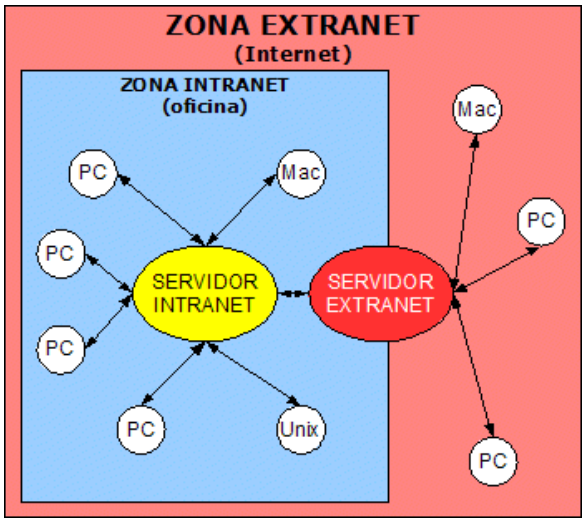

Figura 2.2: Ejemplo Zona Intranet y Extranet 2

[1] Modelo de referencia de Interconexión de Sistemas Abiertos (Open System Interconnection), creado por la ISO, nace de la necesidad de uniformizar los elementos para solucionar el problema de comunicación entre equipos de diferentes fabricantes. Es un modelo de referencia utilizado para describir redes y usos de la red.

[2]Figura tomada de: www.ls-interactive.com/cgi-bin/wa/GET?ACTION=intranet&DATA=intranet

2.2- Modelo TCP/IP

El modelo TCP/IP fue creado ante la necesidad de un modelo que pudiera trabajar bajo cualquier condición, o bajo cualquier medio.

Sin embargo TCP/IP fue creado como protocolo abierto, lo cual apresuro el desarrollo del mismo. El objetivo de TCP/IP consiste en establecer de común acuerdo un protocolo estándar que pueda funcionar en una diversidad de redes de diferentes características.

2.2.1- Capas de TCP/IP

TCP/IP se base en el modelo OSI, pero consta de cuatro capas:

1. **Aplicación**: Contiene protocolos de alto nivel como HTTP, FTP, SMTP, POP3 y IMAP.
2. **Transporte:** Provee control de errores y control de flujo. Se maneja protocolos TCP y UDP.
3. **Internet**: Define el formato del paquete, además maneja protocolo IP, que asegura que la dirección del equipo sea única en la red.
4. **Acceso a la red:** Provee de una interfaz con la capa física.

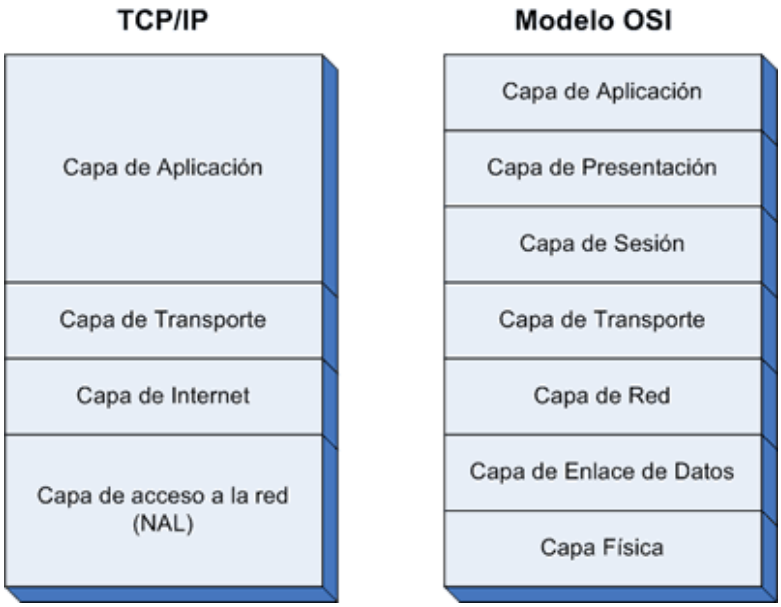

Figura 2.3: Capas del Modelo OSI y TCP/IP1

2.2.2- Protocolos TCP y UDP

Los protocolos TCP y UDP son manejados en la capa de transporte, TCP es confiable pero lento mientras que UDP al contrario es inseguro pero trabaja a mayores velocidades.

TCP

Protocolo orientado a la conexión, se establece una conexión antes de enviar los datos, la comunicación es monitoreada para asegurar que todos los datos llegaron completos y en el orden correcto.

UDP

Protocolo no orientado a la conexión, no necesita de ninguna comunicación antes de enviar los datos, y se considera más importante a la velocidad que la

[1] Figura tomada de http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

exactitud de entrega de los datos. El destino no confirma si llegaron bien los datos.

2.2.3- Diferencias entre los modelos OSI y TCP/IP

La perspectiva de ISO trata a las capas como grupos funcionales bastante reducidos, intentando forzar la modularidad al solicitar capas adicionales para funciones adicionales.

En los protocolos TCP/IP, un protocolo puede ser usado por otros protocolos en la misma capa, mientras que en el modelo OSI se definiría dos capas en las mismas circunstancias.

Las normas del modelo OSI tienden a ser prescriptivas, mientras que los protocolos TCP/IP tienden a ser descriptivos. Una ventaja importante de TCP/IP es que cada implementación concreta puede explotar características dependientes del sistema, se da así una mayor eficiencia.

2.3- Dispositivos de Red

Se conoce como dispositivos de red (networking devices) a los equipos que se enlazan directamente a un segmento de red.

Existen dos grupos:

Dispositivos de usuario final (hosts)

Permiten compartir, crear y obtener información, no necesitan de una red pero sin esta sus capacidades son restringidas. Se enlazan a traves de interfaces de red (NICs [1]) .

[1] Tarjeta de interfaz de red (Network Interface Card NIC): Es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard de un computador, o puede ser un dispositivo periférico

Entre estos dispositivos tenemos: computadores, impresoras, escáneres entre otros.

Dispositivos de Red

Transportan datos que deben transferirse entre hosts. Brindan el tendido de las conexiones de cable, la concentración de conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos.

2.3.1- Repetidor

Un repetidor es un regenerador de señal. Estos regeneran señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación. No toma decisiones inteligentes acerca del envío de paquetes.

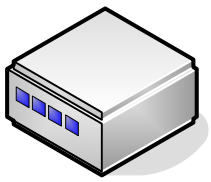

Figura 2.4: Repetidor

2.3.2- Hub

Un hub es un concentrador de conexiones. Permiten que la red trate un conjunto de hosts como una sola unidad. Los hubs activos no sólo concentran hosts, sino que además regeneran señales.

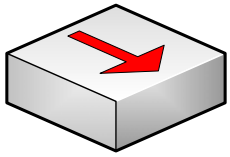

Figura 2.5: Hub

2.3.3- Puente

Los puentes convierten los formatos de transmisión de datos de la red y realizan la administración básica de la transmisión de datos. Proporcionan las conexiones entre LAN, sin embargo no sólo las conectan sino verifica los datos para determinar si les corresponde o no cruzar el puente aumentando la eficiencia de cada parte de la red.

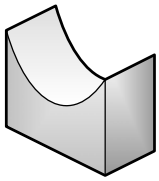

Figura 2.6: Puente

2.3.4- Switch y Temas Relacionados

Un switch es considerado un Hub inteligente. Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. Establece si los datos permanecen o no en una LAN y transfieren los datos únicamente a la conexión que corresponde. Un switch no convierte formatos de transmisión de datos.

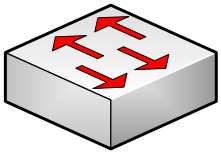

Figura 2.7: Switch

2.3.4.1- Spanning Tree

Definición

Spanning Tree es un protocolo que gestiona enlaces redundantes, previniendo bucles infinitos de repetición de datos en redes que presenten configuración redundante. STP es transparente a las estaciones de usuario. Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC.

BPDU

Los BPDUs (Bridge Protocol Data Units) son unidades de datos utilizados para lograr una topología libre de lazos.

Los bucles infinitos ocurren cuando hay rutas alternativas entre hosts. Estas rutas alternativas son necesarias debido a que, al proporcionar redundancia, dan una mayor fiabilidad ya que, al existir varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red.

Los switches envían entre sí BPDUs que tienen información para:

- ✓ Seleccionar un único switch que actúe como principal (root bridge)
- ✓ Calcular la ruta más corta entre él y el root bridge

- ✓ Determinar el “designated switch” que es el switch que comunicará todos los host de la LAN con el root bridge
- ✓ Seleccionar su “designated port” que es el puerto que lleva al camino más corto para llegar al root bridge
- ✓ Bloquear los otros puertos

Cuando la red se estabiliza, converge en un único “spanning-tree” en la red y se tiene como resultado:

- ✓ Un “root bridge” (Puente raíz) por red
- ✓ Un “root port” (Puerto raíz) por cada switch que no sea el principal
- ✓ Un “designated port” (Puerto designado) por segmento
- ✓ Puertos no designados sin uso.

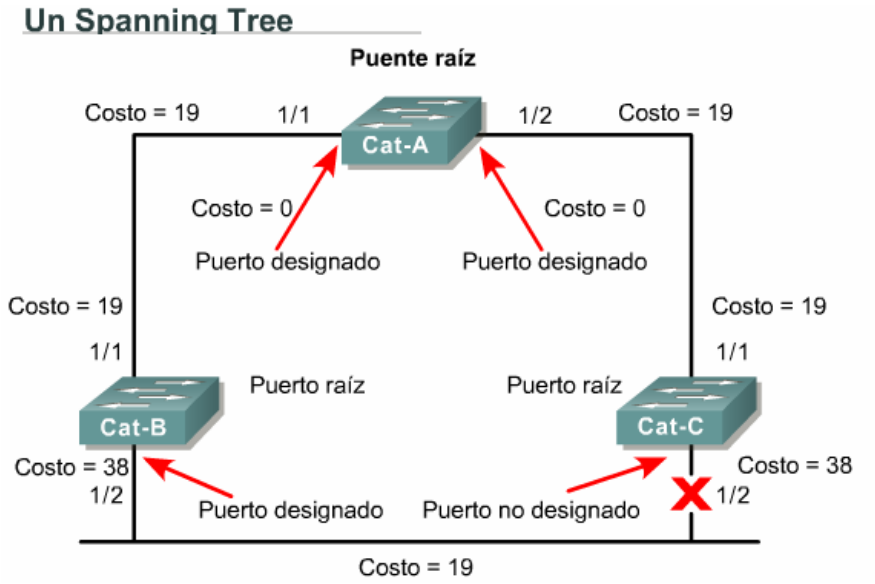

Figura 2.8: Un Spanning Tree [1]

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 7.

Los “root ports” y los “designated ports” envían datos de usuario. Se llaman “forwarding ports” (F). Los puertos no designados descartan los datos de usuario. Se llaman “blocking ports” (B).

Root bridge (Puente Raíz)

La primera decisión en una red con STP es la determinación del “root bridge”. Cuando se enciende un switch por primera vez, se considera como el “root bridge” y envía BPDUs cada 2 segundos con igual identificación en Root BID y Sender BID, consiste en: prioridad (32768 por defecto) y dirección MAC de switch.

Al intercambiar BPDUs con los otros switches se revisa el campo del Root BID de cada uno y se escoge al de menor valor recibido como el root bridge de la red. Se puede bajar el valor de prioridad para seleccionar un “root bridge” específico

Estado de puertos en Spanning-tree.

Los cambios topológicos en la red hacen que los puertos cambien de estado inactivo a activo y viceversa.

Hay una demora en este proceso llamado “propagation delay”. Si los puertos cambiaran de estado inmediatamente, se crearían más lazos.

Todo puerto en una red con STP está en uno de los cinco estados descritos a continuación:

- ✓ En el estado bloquear (blocking), el switch descarta paquetes de usuario, oye las BPDUs pero no aprende direcciones. Puede demorar hasta 20 segundos para cambiar al estado de escuchar.
- ✓ En el estado escuchar (listening), se determina si hay una ruta de menor costo al root. Si es así, se vuelve a bloqueo, sino va a estado aprender. No se envían datos de usuario ni se aprenden MACs. Máximo 15 segundos (forward delay).
- ✓ En el estado aprender (learning), no se envían datos de usuario, pero se aprenden las direcciones MAC de los equipos de la red y se procesan las BPDUs. Máximo 15 segundos (forward delay).
- ✓ En el estado enviar (forwarding), se envían datos de usuario y se aprenden direcciones MAC y procesan las BPDUs.
- ✓ En el estado deshabilitar (Disabling) es el estado en el cual el switch ha sido cerrado por el administrador o está dañado.

Hay un tiempo máximo de permanencia en cada estado que se calcula en un sistema de hasta 7 switches en cada rama de la red desde el root bridge.

2.3.4.2- VLAN

"Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico." [1]

Es así que una estación de trabajo en un grupo de VLAN se limita a comunicarse con los servidores en el mismo grupo de VLAN.

[1] Texto tomado de: Cisco CCNA3, versión 3. Modulo 8

2.3.4.2.1- Introducción a las VLAN

Una VLAN brinda facilidades para la administración de grupos lógicos de estaciones pues se comunican como si estuviesen en el mismo segmento físico de la red local proveendo de servicios de segmentación, que tradicionalmente lo proporcionaban por routers.

Una VLAN permite la segmentación lógica las redes conmutadas de acuerdo a las funciones de la organización, proporcionando escalabilidad, seguridad y gestión de red.

También una VLAN brinda facilitad de administración de adiciones y cambios en los miembros de esos grupos, provee la comunicación de estaciones de trabajo en una misma VLAN, sin importar la conexión física o la ubicación y la configuración de VLAN’s mediante el software sin necesidad de que los equipos de red se conecten físicamente.

Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no transmiten ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN. A continuación se muestra un ejemplo del diseño de una VLAN y sus límites físicos:

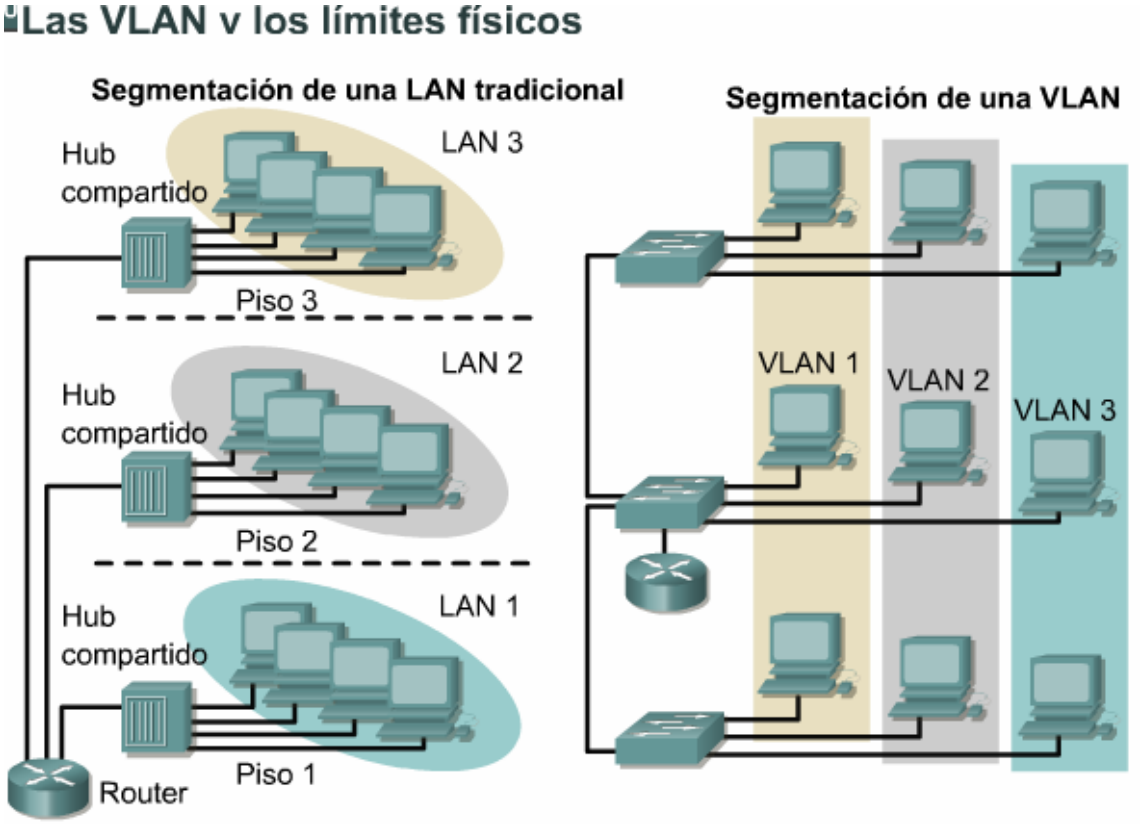

Figura 2.9: Las VLAN y los límites físicos [1]

Una VLAN esta conformada por una red conmutada lógicamente segmentada. Los puertos son asignados a una VLAN dependiendo de la necesidad de cada puerto del switch.

Los puertos que se encuentren en la misma VLAN comparten broadcasts[2] mejorando el desempeño puesto que se reduce los broadcasts innecesarios.

La VLAN por defecto es la VLAN 1, comúnmente llamada VLAN de administración. Esta no se la puede borrar y por lo menos un puerto debe ser asignado para poder administrar el switch. El resto de puertos en el switch puede reasignarse a otras VLAN.

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 8
[2] **Broadcast, o difusiones:** Estas se producen cuando una fuente envía datos a todos los dispositivos que encuentra en su red.

La cantidad de VLAN en un switch varía según diversos factores:

- ✓ Patrones de tráfico
- ✓ Tipos de aplicaciones
- ✓ Necesidades de administración de red
- ✓ Aspectos comunes del grupo
- ✓ Direccionamiento IP

2.3.4.2.2- Tipos de VLAN

VLAN de puerto central

Las VLAN de puerto central o basada en puertos es aquella en la que todos los nodos de una VLAN se conectan al mismo puerto del switch. El puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema conectado al puerto. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN. Este método es fácil de manejar porque no se requieren tablas de búsqueda complejas para la segmentación de VLAN. A continuación se muestra en un diagrama general de una VLAN de puerto central:

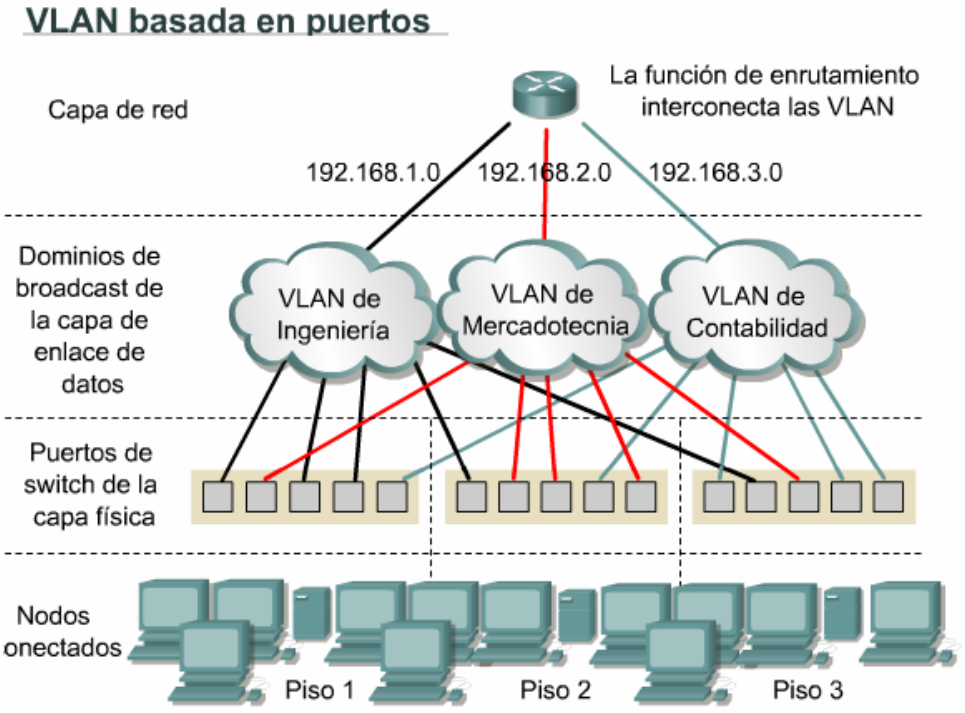

Figura 2.10: VLAN basada en puertos[1]

VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo. Las VLAN estáticas son puertos en un switch que el administrador de la red asigna manualmente a una VLAN. Esto se hace con una aplicación de administración de VLAN o configurarse directamente en el switch mediante la CLI[2]. Estos puertos mantienen su configuración de VLAN asignada hasta que se cambien manualmente. Este tipo de VLAN funciona bien en las redes que tienen requisitos específicos:

- Todos los movimientos son controlados y gestionados.
- Existe un software sólido de gestión de VLAN para configurar los puertos.

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 8
[2] La interfaz de línea de comandos (Command Line Interface, CLI) es un utilitario de configuración basado en texto que admita un conjunto de comandos y parámetros de teclado para configurar y gestionar un equipo.

- El gasto adicional requerido para mantener direcciones MAC de estación final y tablas de filtrado personalizadas no es aceptable.

La siguiente figura muestra un diagrama de una VLAN estática:

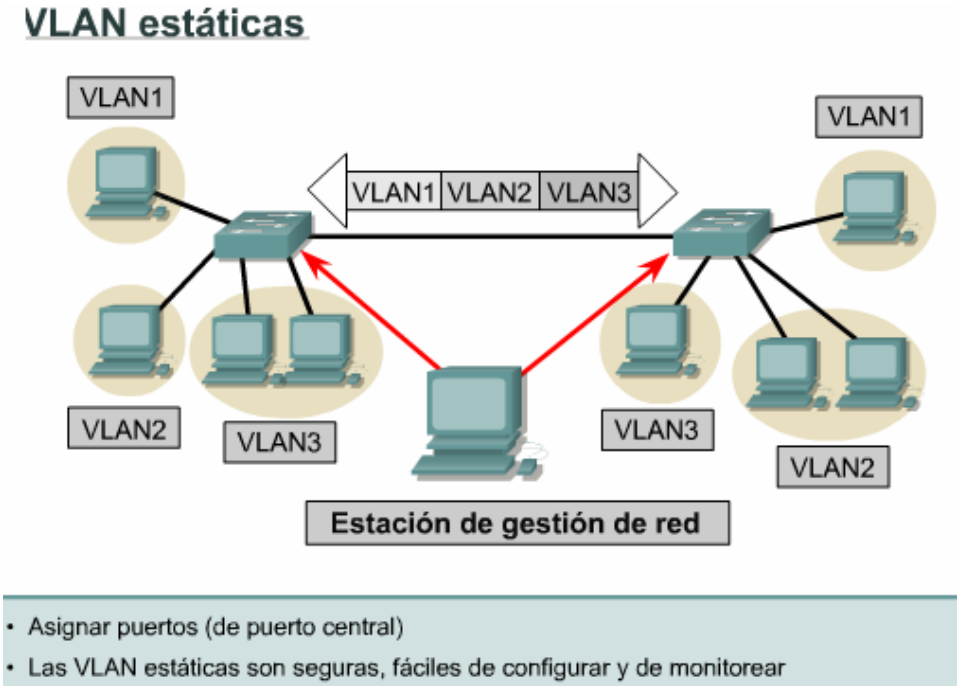

Figura 2.11: VLAN estáticas[1]

VLAN Por puerto

Se configura por una cantidad “n” de puertos en el cual se indica que puertos pertenecen a cada VLAN. Por ejemplo en la siguiente figura de un Switch 9 puertos el 1,5 y 7 pertenecen a la VLAN 1; el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3.

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 8

Cuadro 2.1 : Distribución de puertos para un switch de 9 puertos.

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1
6	3
7	1
8	2
9	3

Las ventajas de este tipo de VLAN son:

- ✓ Facilidad de movimientos y cambios.
- ✓ Microsegmentación y reducción del dominio de Broadcast.
- ✓ Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Mientras sus desventajas son:

- ✓ Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del switch al que esta conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

VLAN por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

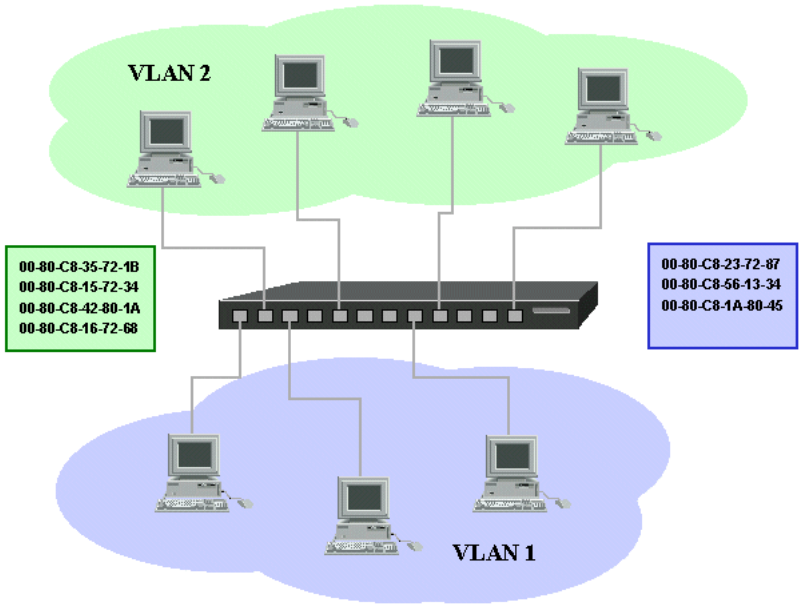

Figura 2.12: Diseño de VLAN por dirección MAC [1]

Las ventajas de una VLAN por dirección MAC son:

- ✓ Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- ✓ Multiprotocolo.
- ✓ Se pueden tener miembros en múltiples VLANs.

Las desventajas de este tipo de VLAN son:

- ✓ Problemas de rendimiento y control de Broadcast: el tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas las VLANs.
- ✓ Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

[1] Figura tomada de:
http://www.alaide.com/cours/reseaux/reseaux_locaux/equipements/images/vlan-1.gif

- ✓ Tiene impacto sobre desempeño, la escalabilidad y la administración.
- ✓ Ofrece flexibilidad pero aumenta el gasto.
- ✓ Necesita de un servidor de políticas de administración VLANs (VMPS[1]).

VLAN por protocolo

Este tipo de VLAN asigna a un protocolo una VLAN. El switch se encarga de la distribución dependiendo del protocolo por el cual pase la trama, designando a la VLAN correspondiente, como se muestra en la siguiente figura:

Cuadro 2.2 : Distribución para una VLAN por protocolo

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

Este tipo de configuración tiene las siguientes ventajas:

- ✓ Segmentación por protocolo.
- ✓ Asignación dinámica.

Sin embargo presenta las siguientes desventajas:

- ✓ Problemas de rendimiento y control de Broadcast: Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- ✓ No soporta protocolos de nivel 2 ni dinámicos.

[1] **VMPS** (VLAN Management Policy Server): Es un servidor de políticas de administración de VLANs que maneja la base de datos de todas las direcciones MAC.

VLAN por direcciones IP

Esta basado en el encabezado de la capa 3 del modelo OSI, llamada capa de red. Las direcciones IP a los servidores de VLAN configurados. No actúa como router, lo que hace es un mapeo de las direcciones IP que están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Ventajas de las VLAN por direcciones IP:

- ✓ Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo al tener asignada una dirección IP en forma estática no es necesario reconfigurar el switch.

Mientras que las desventajas de este tipo de VLAN son:

- ✓ El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.
- ✓ Perdida de tiempo en la lectura de las tablas.
- ✓ Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

VLAN por nombre de usuario

Estas VLAN se basan en la autenticación de usuarios y no en las direcciones MAC de los dispositivos.

Es así que estas VLAN tienen las siguientes ventajas:

- ✓ Facilidad de movimiento de los integrantes de la VLAN.

- ✓ Multiprotocolo.

Sin embargo sus desventajas son:

- ✓ En corporaciones muy dinámicas la administración de las tablas de usuarios se hace muy extensa.

VLAN dinámicas

Las VLAN de asociación dinámica son creadas mediante software de administración de red, permiten la asociación basada en la dirección MAC del dispositivo. Cuando se conecta un equipo, el switch busca en una base de datos en el Servidor de Configuración de VLAN para la asociación. En la siguiente figura se visualiza un ejemplo de VLAN dinámica:

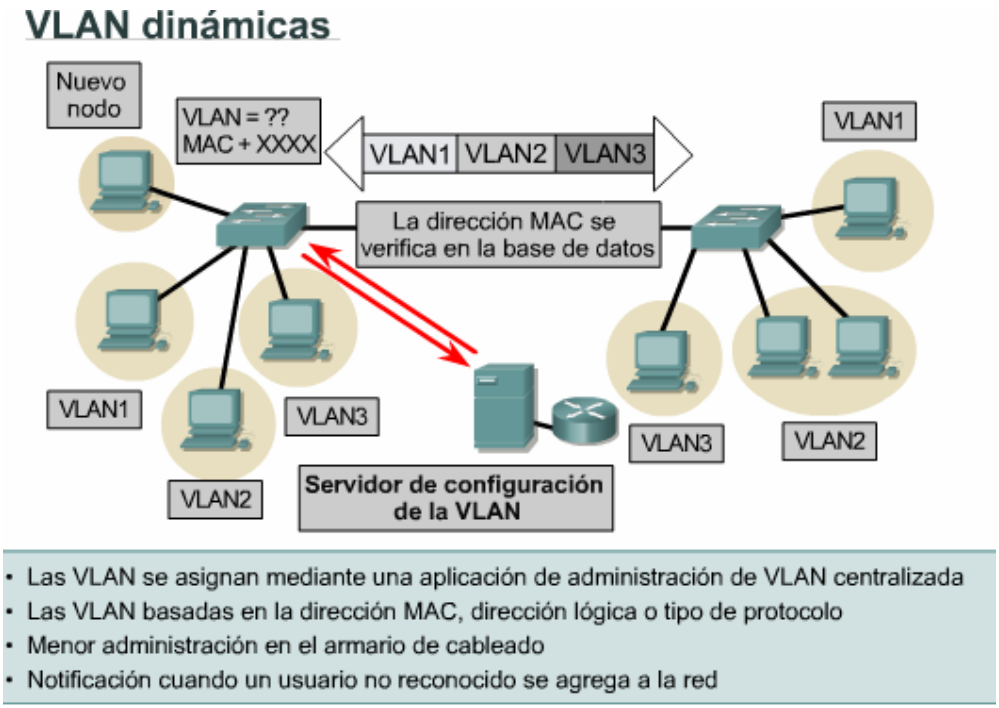

Figura 2.13: VLAN dinámicas[1]

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 8

2.3.4.2.3- Funcionamiento

A medida que los paquetes son recibidos por el switch desde cualquier dispositivo de estación final conectado, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los switches o routers correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es eliminado del paquete por el switch adyacente y es enviado al dispositivo conectado. El etiquetado de paquetes brinda un mecanismo para controlar el flujo de broadcasts y aplicaciones, mientras que no interfiere con la red y las aplicaciones. La emulación de LAN (LANE) es una forma en que una red de Modo de Transferencia Asíncrona (ATM) simula una red Ethernet. No hay etiquetado en LANE, pero la conexión virtual utilizada implica un ID de VLAN.

Cada VLAN debe tener una dirección única de red de Capa 3 asignada a ella. Esto permite que los routers intercambien paquetes entre VLAN. Las VLAN pueden existir como redes de extremo a extremo, o pueden existir dentro de las fronteras geográficas.

2.3.4.2.4- Ventajas de las VLAN

- ✓ Proporcionan seguridad de grupo de trabajo y de red
- ✓ Reducen los costes administrativos relacionados con la resolución de los problemas asociados con los traslados, adiciones y cambios
- ✓ Proporcionan una actividad de difusión controlada

2.3.4.2.5- Seguridad en VLAN

Las VLAN representan una técnica de administración económica y sencilla para aumentar la seguridad es segmentar la red en múltiples grupos de broadcast que permiten:

- ✓ Limitar la cantidad de usuarios en un grupo de VLAN
- ✓ Evitar que otro usuario se conecte sin recibir antes la aprobación de la aplicación de administración de red de la VLAN.
- ✓ Configurar todos los puertos no utilizados en una VLAN de bajo servicio por defecto.

2.3.4.2.6- VLAN y Enlaces Troncales

Un enlace troncal es una conexión física y lógica entre dos switches a través de la cual viaja el tráfico de red.

Los protocolos de enlace troncal se desarrollaron para administrar la transferencia de tramas de distintas VLAN en una sola línea física de forma eficaz. Los protocolos de enlace troncal establecen un acuerdo para la distribución de tramas a los puertos asociados en ambos entremos del enlace troncal

El enlace troncal proporciona un método eficaz para distribuir la información del identificador de VLAN a otros switches.

Los dos tipos de mecanismos de enlace troncal estándar que existen son el etiquetado de tramas y el filtrado de tramas. El etiquetado de tramas ofrece una solución más escalable para la implementación de las VLAN. El estándar IEEE

802.1Q establece el etiquetado de tramas como el método para implementar las VLAN.

El etiquetado de trama de VLAN se ha desarrollado específicamente para las comunicaciones conmutadas. El etiquetado de trama coloca un identificador único en el encabezado de cada trama a medida que se envía por todo el backbone de la red. El identificador es comprendido y examinado por cada switch antes de enviar cualquier broadcast o transmisión a otros switches, routers o estaciones finales. Cuando la trama sale del backbone de la red, el switch elimina el identificador antes de que la trama se transmita a la estación final objetivo. El etiquetado de trama funciona a nivel de la Capa 2 del modelo OSI, llamada capa de Enlace de datos, y requiere pocos recursos de red o gastos administrativos.

Es importante entender que un enlace troncal no pertenece a una VLAN específica. Un enlace troncal es un conducto para las VLAN entre los switches y los routers.

ISL[1] es un protocolo que mantiene la información de VLAN a medida que el tráfico fluye entre los switches. Con ISL, la trama Ethernet se encapsula con un encabezado que contiene un identificador de VLAN.

[1] **Inter Switch Link** (**ISL**) es un protocolo propietario de Cisco que mantiene información sobre VLANs en el tráfico entre routers y switches.

2.3.4.3- VTP Protocolo de enlace troncal de VLAN (VTP: *VLAN Trunking Protocol*)

El protocolo de enlace troncal de VLAN (VLAN Trunk Protocol VTP) fue creado por Cisco para resolver los inconvenientes operacionales en una red conmutada con VLAN. Es un protocolo propietario de Cisco.

Los dos problemas más comunes incluyen VLAN interconectadas provocadas por incoherencias de configuración y mala configuración en los dispositivos.

Con VTP, la configuración de VLAN se mantiene unificada dentro de un dominio administrativo común. Un dominio VTP se compone de uno o más dispositivos interconectados que comparten el mismo nombre de dominio VTP. Un switch puede estar en un solo dominio VTP. Cuando se transmiten mensajes VTP a otros switches en la red, el mensaje VTP se encapsula en una trama de protocolo de enlace troncal como por ejemplo ISL o IEEE 802.1Q.

Los switches VTP operan en uno de estos tres modos:

- ✓ Servidor
- ✓ Cliente
- ✓ Transparente

Estos incluyen el servidor que puede crear, modificar y eliminar VLAN así como los parámetros de configuración de una VLAN para todo el dominio, cliente que procesa los cambios de la VLAN y envía mensajes VTP por afuera de todos

los puertos de enlace troncal y transparente, que envía publicaciones VTP pero que ignora la información que contiene el mensaje.

A continuación se muestra una tabla de comparación entre los modos de VTP:

Comparaciones de modo VTP

Característica	Servidor	Cliente	Transparente
Mensajes VTP origen	Sí	Sí	No
Escuchar mensajes VTP	Sí	Sí	No
Crear las VLAN	Sí	No	Sí*
Recordar las VLAN	Sí	No	Sí*

*Sólo significativo localmente

Figura 2.14: Comparación de modo VTP [1]

Con VTP, cada switch publica en los puertos de sus enlaces troncales, su dominio de administración, el número de revisión de configuración, las VLAN que conoce y algunos parámetros para cada VLAN conocida.

Estos son dos tipos de publicaciones VTP; peticiones de clientes y respuestas de servidor. Generan tres tipos de mensajes VTP incluyendo una petición de publicación, publicación de resumen y una publicación de subconjunto. Con las peticiones de publicación los clientes solicitan información de la VLAN y el servidor responde con publicaciones de resumen y de subconjunto. Por defecto, los switches de servidor y de cliente emiten publicaciones de resumen cada determinado tiempo. Los servidores informan a los switches vecinos lo que consideran como el número de revisión VTP actual. Ese número se compara y si existen diferencias, se solicita nueva información sobre la VLAN. Las publicaciones de subconjunto contienen información detallada sobre las VLAN,

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 8

como por ejemplo el tipo de versión VTP, el nombre de dominio y los campos relacionados así como el número de revisión de configuración.

2.3.5- Router

Un router regenerar señales, concentra múltiples conexiones, convierte formatos de transmisión de datos, y maneja transferencias de datos. Permite conexión a una WAN, enlazando LAN's separadas por grandes distancias generalmente. Es el único dispositivo de red con estas capacidades.

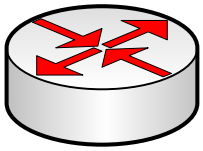

Figura 2.15: Router

2.4- Ethernet

Ethernet es una tecnología de redes ampliamente aceptada con conexiones disponibles para PCs, estaciones de trabajo científicas y de alta desempeño. La tecnología Ethernet fue adoptada para su estandarización por el comité de redes locales de la IEEE como IEEE 802.3. Esta norma fue adoptada por la ISO, siendo así un estándar de redes internacional.

El estándar IEEE 802.3 provee un sistema tipo Ethernet basado en el estándar DIX[1] original.

Los objetivos originales de Ethernet son:

- ✓ Simplicidad
- ✓ Compatibilidad
- ✓ Bajo Costo
- ✓ Direccionamiento flexible
- ✓ Equidad
- ✓ Bajo retardo
- ✓ Arquitectura en Capas
- ✓ Facilidad de mantenimiento

Los objetivos principales de Ethernet son consistentes con los que se han convertido en los requerimientos básicos para desarrollar y usar las redes LAN.

Las redes Ethernet no hacen uso de un dispositivo central de control. Todos los dispositivos son conectados a un canal de comunicaciones de señales compartidas.

Los campos de direcciones en una trama Ethernet llevan direcciones de 48 bits, tanto para la dirección de destino como la de origen. El estándar IEEE administra parte del campo de las direcciones mediante el control de la asignación un identificador de 24 bits conocido como OUI (Organizationally Unique Identifier, identificador único de organización).

[1] DIX (Digital Intel Xerox). Término usado para la Ethemet original, dado que la norma fue desarrollada conjuntamente por las tres compañías.

Existen una gran variedad de implementaciones de IEEE 802.3. Para distinguir entre ellas, se ha desarrollado una notación. Esta notación especifica tres características de la implementación:

- ✓ La tasa de transferencia de datos en Mb/s
- ✓ El método de señalización utilizado
- ✓ La máxima longitud de segmento de cable en cientos de metros del tipo de medio.

2.5- Voz sobre IP

La tecnología de voz sobre el Internet o VoIP (Voice over Internet Protocol), es un sistema de enrutamiento de conversaciones de voz mediante paquetes basados en IP por la red de Internet. Esta tecnología permite hacer y recibir llamadas telefónicas utilizando una conexión de Internet en lugar de una línea telefónica corriente.

Es así que VoIP convierte la señal de voz del teléfono en una señal digital que viaja a través del Internet hasta su destino. Al llamar a un número de teléfono fijo corriente, la señal se reconvierte al llegar a quien recibe la llamada. Convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales.

VoIP representa el avance de la transmisión conmutada por circuitos a la transmisión basada en paquetes, esta toma el tráfico de la red pública telefónica y lo ubica en redes IP. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET.

2.5.1- Funcionamiento

La telefonía IP, requiere un elemento que se encargue de transformar las ondas de voz en datos digitales y que divida en paquetes susceptibles de ser transmitidos haciendo uso del protocolo IP. Este elemento es conocido como Procesador de Señal Digital (DSP) [1].

Un DSP segmenta la señal de voz en tramas y las almacena en paquetes de voz. Los DSP son claves en la compresión y descompresión de voz. Los paquetes son transportados a través de IP, usando un estándar para comunicación de voz, como H.323, SIP, etc.

Cuando los paquetes alcanzan el Gateway de destino se produce el mismo proceso a través del DSP pero a la inversa con lo cual el receptor podrá recibir la señal analógica correspondiente a la voz del emisor.

2.5.2- Arquitectura de red

Se definen tres elementos fundamentales en la estructura de la arquitectura de red:

2.5.2.1- Terminales

Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

[1] **Digital Signal Processing.-** Un microprocesador digital de señal especializado que realiza cálculos o digitaliza señales originalmente analógicas. Su gran ventaja es que son programables. Entre sus principales usos está la compresión de señales de voz. Son la pieza clave de los codec.

2.5.2.2- Gatekeepers

Representan el núcleo de toda la organización VoIP, y el sustituto de las actuales centrales telefónicas. Por lo tanto los Gatekeepers son la unidad central de control que gestiona las prestaciones en una red de VoIP, o de aplicaciones multimedia y de videoconferencia. Proporcionan la inteligencia de red, incluyendo servicios de resolución de direcciones, autorización, autenticación, registro de los detalles de las llamadas para tarificar y comunicación con el sistema de gestión de la red. También monitorizan la red para permitir su gestión en tiempo real, el balanceo de carga y el control del ancho de banda utilizado, el cual es un elemento básico al introducir servicios suplementarios. Usualmente se implementan en software y todas las comunicaciones pasarían a través del mismo.

2.5.2.3- Gateways

Es el enlace con la red telefónica tradicional, desenvolviéndose de forma transparente para el usuario.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. El Gateway se considera como una caja que por un lado tiene una interfase LAN y por el otro dispone de uno o varios de las siguientes interfaces:

- ✓ FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
- ✓ FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
- ✓ E&M. Para conexión específica a centralitas.
- ✓ BRI. Acceso básico RDSI (2B+D).

- ✓ PRI. Acceso primario RDSI (30B+D).
- ✓ G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps.

2.5.2.4- Protocolos

Los protocolos representan el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión; siendo parte esencial ya que de la misma depende la eficacia y la complejidad de la comunicación.

Algunos de los principales protocolos son:

- ✓ H.323 - Protocolo definido por la ITU-T
- ✓ SIP - Protocolo definido por la IETF
- ✓ Megaco (También conocido como H.248) y MGCP - Protocolos de control
- ✓ Skinny Client Control Protocol - Protocolo propiedad de Cisco
- ✓ MiNet - Protocolo propiedad de Mitel
- ✓ CorNet-IP - Protocolo propiedad de Siemens
- ✓ IAX
- ✓ Skype - Protocolo propiedad peer-to-peer utilizado en la aplicación Skype
- ✓ Cliconnect - Proveedor de Servicio VOIP Cliconnect
- ✓ Jajah - Protocolo propiedad peer-to-peer utilizado en los teléfonos-Web Jajah SIP, IAX y compatibles.
- ✓ Jingle - Protocolo abierto utilizado en tecnología Jabber

A continuación se muestra el diseño de una Red VoIP, donde se visualiza la arquitectura de red anteriormente detallada así como los elementos de una red VoIP:

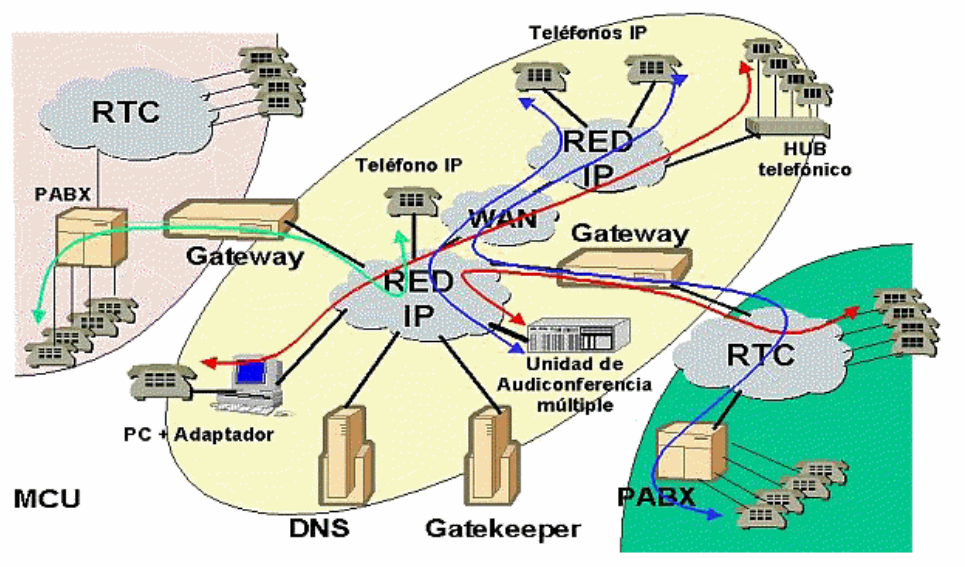

Figura 2.16: Diseño de una Red VoIP[1]

2.5.3- Parámetros de la VoIP

El principal problema que se presenta al implementar tanto VoIP como todas las aplicaciones de IP son los parámetros. Actualmente no es factible garantizar la calidad de servicio sobre una red IP por medio de retardos y ancho de banda, por ello que se presentan diversos inconvenientes al momento de garantizar la calidad del servicio.

Los parámetros de la VoIP son:

2.5.3.1- Códecs

La voz se codifica para poder ser transmitida por la red IP. El uso de Códecs garantiza la codificación y compresión del audio o del video para continuar con la decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.

[1] Figura tomada de : www.monografias.com/trabajos3/voip/voip.shtml

2.5.3.2- Retardo o latencia

Una vez determinados los retardos de procesado, retardos de tránsito y el retardo de procesamiento, la conversación se considera aceptable por debajo de los 150 milisegundos.

2.5.3.3- Calidad del servicio

La calidad de servicio se la alcanza en base a los siguientes criterios:

- ✓ La supresión de silencios, otorga más eficiencia al realizar una transmisión de voz, pues se aprovecha mejor el ancho de banda al transmitir menos información.
- ✓ Compresión de cabeceras aplicando los estándares RTP/RTCP.
- ✓ Priorización de los paquetes que demanden menor latencia.
- ✓ La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

2.5.4- Beneficios de VoIP

Varios de los servicios VoIP incluyen planes de llamadas ilimitadas locales y de larga distancia por un precio fijo y una variedad de características o funciones como por ejemplo:

- ✓ Sistemas integrados de mensajes de correo de voz y correo electrónico, esto permite escuchar los mensajes telefónicos en la PC o consultar el correo electrónico en el teléfono.
- ✓ La posibilidad de tener más de un número de teléfono, incluso números de teléfono con códigos de área diferentes.

- ✓ Portabilidad, es posible llevarse el sistema VoIP, pues mediante programas software y hardware especiales las llamadas personales o comerciales le serán enviadas al lugar donde se encuentre.
- ✓ Integración sobre su Intranet de la voz como un servicio más de su red, tal como otros servicios informáticos.
- ✓ Las redes IP constituyen la red estándar universal para Internet, Intranets y extranets.
- ✓ Estándares efectivos (H.323)
- ✓ Interoperabilidad de diversos proveedores
- ✓ Uso de las redes de datos existentes
- ✓ Independencia de tecnologías de transporte (capa 2), asegurando la inversión.
- ✓ Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay)
- ✓ No paga SLM ni Larga Distancia en sus llamadas sobre IP.

2.5.5- Protocolo H.323

H.323 es una recomendación del ITU-T[1] , que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

El IMTC[2] permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz, se

[1]**Unión Internacional de Telecomunicaciones (International Telecommunication Union).-** La es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

[2]**Internacional Multimedia Telecommunications Consortium (IMTC).-** es una comunidad internacional de compañías que trabajan en conjunto para facilitar la disponibilidad en tiempo real, de rich-media comunicaciones entre la gente en múltiples lugares alrededor del mundo.

decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP. VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia.

H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

2.5.5.1- Direccionamiento

El direccionamiento en H.323 permite a las estaciones localizarse entre ellas. Los protocolos utilizados para este proceso son:

Registro, Admisión y Estado (RAS Registration, Admision and Status).- Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.

Servicio de resolución de Nombres (DNS Domain Name Service).- Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

2.5.5.2- Señalización

H.323 se basa en tres protocolos fundamentales para manejar la ejecución de la llamada, cada uno de ellos tienen una función específica, estos son:

Cuadro 2.3 : Protocolos de señalización en H.323

Protocolo	Función
Q.931	Encargado de la señalización inicial de llamada.
H.225	Encargado del control de llamada: señalización, registro y admisión, y paquetización / sincronización del flujos de voz.
H.245	Protocolo de control para especificar mensajes de apertura y cierre de canales para flujos de voz.

2.5.5.3- Compresión de Voz

Para comprimir la voz H.323 necesita de los siguientes protocolos:

Protocolos requeridos: G.711 y G.723

Protocolos opcionales: G.728, G.729 y G.722

2.5.5.4- Transmisión de Voz

La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

2.5.5.4.1- Protocolo de Tiempo Real (RTP Real Time Protocol)

Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

Control de la Transmisión: RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

A continuación se muestra la pila de protocolos en VoIP donde se visualiza la ubicación del protocolo RTP :

Figura 2.17: Pila de protocolos en VoIP

2.5.6- Configuraciones para VoIP

2.5.6.1- VoIP PC-PC

En este tipo de configuraciones se requiere que ambos equipos tengan instalada la misma aplicación la cual esta encargada de gestionar la llamada telefónica, y estar conectados a la red IP, Internet para poder efectuar una llamada IP. El paquete de software o una tarjeta DSP debe constar de:

- ✓ Codec de Voz
- ✓ Unidad de control de la tasa binaria del codec

- ✓ Encapsulador de tramas de voz a datagramas IP.
- ✓ Detector de actividad (VAD).
- ✓ Cancelador de ecos.

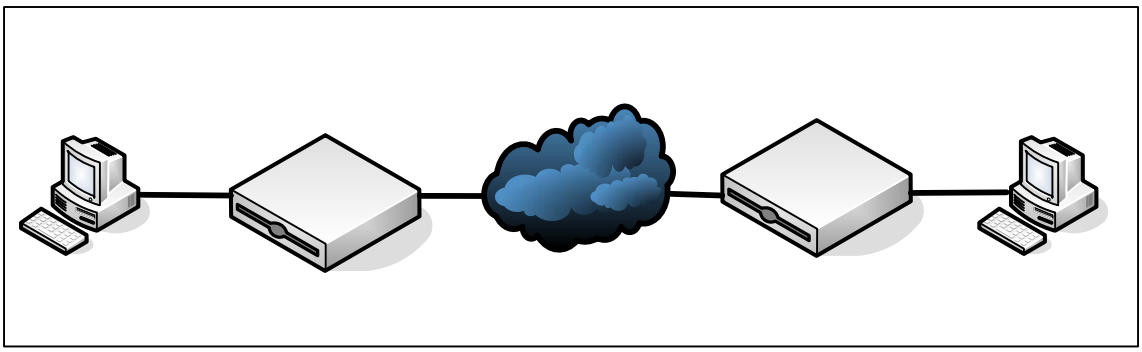

Figura 2.18: Diagrama VoIP PC-PC

2.5.6.2- VoIP pasarela-pasarela

Al realizar una llamada se utiliza el teléfono tradicional accediendo a una pasarela o gateway de voz la cual convierte la voz entrante por la RTC a datagramas para enviar por la red IP.

2.5.6.3- VoIP teléfono-teléfono

En este caso los dispositivos telefónicos operan directamente sobre la red IP. Tanto el origen como el destino necesitan ponerse en contacto con un gateway. Si el teléfono A solicita efectuar una llamada a B, el gateway de A solicita información al gatekeeper sobre como alcanzar a B, y éste le responde con la dirección IP del gateway que da servicio a B. Entonces el gateway de A convierte la señal analógica del teléfono a en un caudal de paquetes IP que encamina hacia el gateway de B, este regenera la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B.

El gateway de B se encarga de enviar la señal analógica al teléfono B, por tanto es una comunicación telefónica convencional entre el teléfono a y el gateway que le da servicio (gateway A), una comunicación de datos a través de una red IP, entre el gateway A y el B, y una comunicación telefónica convencional entre el gateway que da servicio al teléfono B (gateway B), y éste. Se puede decir entonces que se trata de dos llamadas telefónicas convencionales, y una comunicación IP.

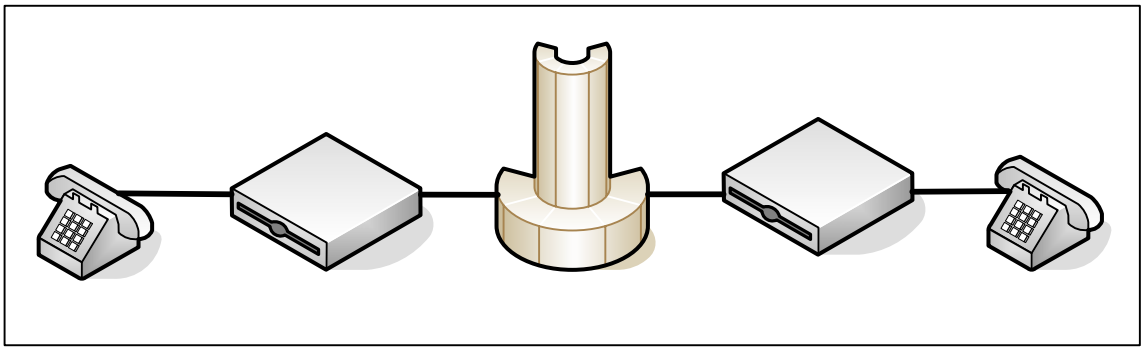

Figura 2.19: Diagrama VoIP teléfono-teléfono

2.6- Central Telefónica IP

2.6.1- Definición

Una Central Telefónica IP brinda las mismas características que una central telefónica convencional, incluyendo mayores funciones, y representando menor costo. Las extensiones o internos pueden ser dispositivos VoIP. Esto brinda portabilidad, puesto que es posible colocar una extensión de la central, sin importar su ubicación geográfica.

Gateway A

A

Las centrales telefónicas IP se interconectan mediante la red de Internet. De acuerdo a las características de la misma, es posible acceder a diferentes

servicios tales como transferencia, conferencia, voice mail, número universal, seguridad, entre otras.

Las centrales telefónicas personales o de pequeñas empresas (centralitas telefónicas), se denominan PBX (Private Branch eXchange: Equipo de Intercambio Privado). Una PBX es un conmutador telefónico localizado en el equipo terminal del usuario que primeramente establece circuitos a través de líneas conectadas entre usuarios individuales y la Red telefónica conmutada. Una PBX se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior. Hace que las extensiones tengan acceso desde el exterior, desde el interior, y ellas a su vez tengan acceso también a otras extensiones y a una línea externa.

Existen soluciones de software para implementar una central telefónica IP o se puede acceder a soluciones de hardware propias que ofrecen mayores y mejores capacidades así como servicios.

En el caso particular de PETROCOMERCIAL, la empresa posee una central telefónica IP propia, el equipo es de marca “Mitel”, Modelo 3300 y tiene una capacidad de 700 extensiones.

A continuación se muestra la Central Telefónica IP Mitel 3300:

Figura 2.20: Central Telefónica IP. Controlador Mitel 3300

2.6.2- Servicios de las Centrales Telefónicas IP

Las Redes Privadas IP le brindan servicios adicionales de avanzada tales como:

- ✓ Conferencia
- ✓ Servicio De Voice-Mail
- ✓ Numero Universal
- ✓ Seguridad
- ✓ Transferencia
- ✓ Crecimiento Modular Por Software
- ✓ Cableado Estructurado IP
- ✓ Concentrador De VPN's
- ✓ Extensiones Virtuales

2.7- Modelo Jerárquico Cisco

Cisco diseño un modelo jerárquico de construcción de LAN que permita satisfacer de mejor manera los requerimientos de las organizaciones:

1. Capa Núcleo: Backbone
2. Capa de Distribución: Routing
3. Capa de Acceso: Switching

A continuación se visualiza el modelo de diseño jerárquico Cisco:

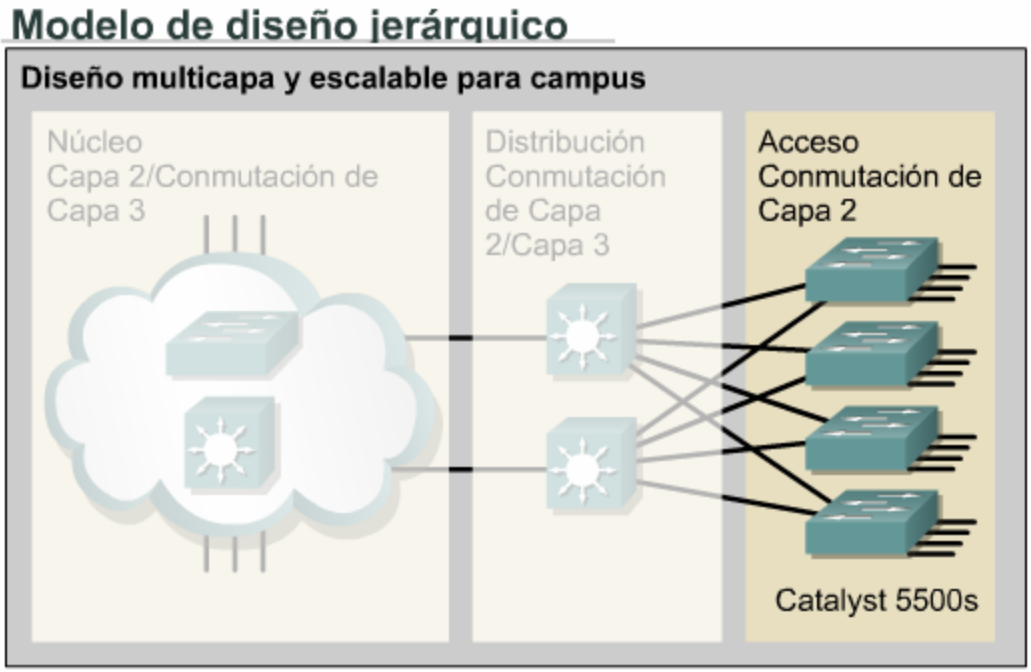

Figura 2.21: Modelo de diseño Jerárquico Cisco [1]

2.7.1- Capa Núcleo

Es el backbone de conmutación, fue diseñado para conmutar paquetes a alta velocidad, se encarga de la transferencia de grandes cantidades de tráfico y lo hace de manera confiable. En esta capa es esencial tanto la velocidad como la latencia.

Las consideraciones que se deben tomar para esta capa son:

- ✓ Diseñar el núcleo para alta confiabilidad. Tomar en cuenta las tecnologías de enlace de datos que facilitan tanto la velocidad como la redundancia, tales como: FDDI, Frame Relay, ATM[2], etc.
- ✓ Diseñar el núcleo para altas velocidades. La latencia debe ser mínima.
- ✓ Seleccionar protocolos de enrutamiento con tiempo de convergencia bajos.

[1] Figura tomada de: Cisco CCNA3, versión 3. Modulo 5.
[2] Modo de Transferencia asíncrona (Asyncronous Transfer Mode)

En esta capa no se debe realizar ningún tipo de manipulación de paquetes, tal como usar listas de control de acceso, enrutamiento entre redes de área local virtuales (VLAN) o filtro de paquetes, etc. La capa no soporta accesos de grupo de trabajo y es importante evitar expandir el núcleo cuando la red crece. Si el desempeño es un problema en el núcleo, son preferibles las actualizaciones en lugar de las expansiones.

2.7.2- Capa de Distribución

Es el punto de comunicación entre la capa de acceso y el núcleo. Las principales funciones de la capa de distribución son el proveer enrutamiento, filtros, accesos WAN y determinación de como los paquetes acceden al núcleo si es necesario. En esta capa se implementan las políticas para la red.

Además esta capa de encarga de:

- ✓ Enrutamiento
- ✓ Implementación de listas de control de acceso o filtro de paquetes.
- ✓ Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y firewalls.
- ✓ Calidad de Servicio, en base a las políticas definidas.
- ✓ Redistribución entre protocolos de enrutamiento, incluyendo rutas estáticas.
- ✓ Enrutamiento entre VLANs y otras funciones que soportan los grupos de trabajo.
- ✓ Definición de dominios de broadcast y multicast.
- ✓ Posible punto para acceso remoto.
- ✓ Traslado de medios de comunicación.

2.7.3- Capa de Acceso

La capa de acceso es el punto en el cual los usuarios finales son conectados a la red. Utiliza listas de acceso o filtros para optimizar las necesidades de un grupo particular de usuarios si fuese necesario. Esta capa también es conocida como “desktop layer”.

La capa de acceso se encarga de:

- ✓ Continúa el control de acceso y políticas (desde la capa de distribución)
- ✓ Creación de dominios de colisión separados (micro-segmentación)
- ✓ Conectividad de los grupos de trabajo dentro de la capa de distribución.
- ✓ Habilitar filtros de direcciones MAC
- ✓ También es posible tener acceso a grupos de trabajo remotos.
- ✓ Presta servicios de asignación de VLANs a nivel de capa 2 del modelo OSI.

2.8- Cableado Estructurado

“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. “[1]

El actual desarrollo de las tecnologías de comunicación ha hecho necesario el uso de sistemas de cableado estructurado, que sean capaces de soportar todas las aplicaciones de comunicación.

[1] Texto tomado de:
http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/cableado.htm

2.8.1- Ventajas del cableado estructurado

El cableado estructurado posee numerosas ventajas, las principales son las siguientes:

- ✓ Convivencia de varios tipos de servicios bajo las mismas instalaciones.
- ✓ Se facilita el mantenimiento y mejoran los servicios de mantenimiento.
- ✓ Brinda seguridad a la red.
- ✓ Es fácilmente escalable.
- ✓ Sus normas son reguladas bajo estándares internacionales.
- ✓ Se ahorran recursos y tiempo de instalación.
- ✓ Provee de orden y coherencia al diseño de la red.
- ✓ Una buena instalación permite altas velocidades de transmisión.
- ✓ Los recursos son reutilizables para varios equipos y diseños.
- ✓ Permite una mejor administración de redes

2.8.2- Normas del cableado estructurado

El cableado se rige a normas y estándares internacionales. Los principales estándares y normas para los sistemas de cableado estructurado son:

2.8.2.1- Estándar ANSI/TIA/EIA-568-A

"Norma para construcción comercial de cableado de telecomunicaciones".

Permite una planeación e instalación de cableado sin tener mucha información acerca de los equipos de comunicación que podrían ser instalados posteriormente, tomando en cuenta lo beneficioso que resulta la implantación de sistemas de cableado estructurado durante la construcción o renovación de edificios.

2.8.2.2- Estándar ANSI/TIA/EIA-569-A

"Norma de construcción comercial para vías y espacios de telecomunicaciones”

Esta norma se refiere al diseño especifico sobre la dirección y construcción, los detalles del diseño para el camino y espacios para el cableado de telecomunicaciones y equipos dentro de edificios comerciales.

2.8.2.3- Estándar ANSI/TIA/EIA-606

"Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales"

Brinda normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado.

2.8.2.4- Estándar ANSI/EIA/TIA-569

“Norma de construcción comercial para vías y espacios de telecomunicaciones"

Proporciona directrices para conformar ubicaciones, áreas, y vías donde se instalan los equipos y medios de telecomunicaciones.

2.8.2.5- Estándar ANSI/TIA/EIA/TIA 607

"Requisitos de aterrizado y protección para telecomunicaciones en edificios comerciales"

Define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y proteger los elementos del sistema estructurado

2.9- Políticas de Seguridad

Las Políticas de Seguridad son las normas y procedimientos que reglamentan la forma en que una organización protege y maneja su información, además de prevenir y protegerla ante los diversos tipos de ataques informáticos.

Las tres preguntas fundamentales que debe responder cualquier política de seguridad son las siguientes:

¿Qué queremos proteger?

¿Contra quién?

¿Cómo?

El objetivo de la definición de políticas de seguridad es notificar al mayor detalle a los usuarios, empleados y gerentes acerca de las reglas y mecanismos que se deben efectuar, cumplir y utilizar para proteger los recursos y componentes de los sistemas de la empresa u organización, en especial la información.

Los componentes que una política de seguridad debe contemplar son:

- ✓ Política de privacidad
- ✓ Política de acceso
- ✓ Política de autenticación
- ✓ Política de contabilidad
- ✓ Política de mantenimiento para la red
- ✓ Política de divulgación de información.

Otros aspectos muy importantes a incorporar en la política de seguridad son :

- ✓ Procedimientos para reconocer actividades no autorizadas.
- ✓ Definir acciones a tomar en caso de incidentes.
- ✓ Definir acciones a tomar cuando se sospeche de actividades no autorizadas.
- ✓ Conseguir que la política sea refrendada por el estamento más alto posible dentro de la organización.
- ✓ Divulgar la política de forma eficiente entre los usuarios y administradores.
- ✓ Articular medidas de auditoria de nuestro propio sistema de seguridad.
- ✓ Establecer plazos de revisión de la política en función de resultados obtenidos.

2.10- Delitos Informáticos

"Delito informático es toda conducta que revista características delictivas, es decir sea típica, antijurídica, y culpable, y atente contra el soporte lógico o Software de un sistema de procesamiento de información, sea un programa o dato relevante".[1]

En otras palabras, los delitos informáticos son los actos que agravian o perjudican a personas, entidades o instituciones y son ejecutados por medio del uso de computadoras a través de Internet o directamente por dispositivos electrónicos sofisticados.

Además este tipo de delitos son realizados totalmente a través de las computadoras y en casos especiales con la colaboración de terceros, inclusive en forma física en determinadas eventualidades.

[1] Tomado de: http://html.rincondelvago.com/delitos-informaticos_1.html

Algunos de los más conocidos delitos informáticos son:

2.10.1- Propagación de Virus informáticos

Los servicios de Internet más comúnmente empleados para la propagación masiva de virus, son el correo electrónico con archivos adjuntos, mensajería instantánea**,** redes “Igual-a-igual”, el IRC (Internet Relay), vía FTP (Protocolo de Transferencia de archivos), HTTP es decir visitando páginas web con códigos malignos previamente configuradas, el servicio Telnet, el mismo que aprovecha las vulnerabilidades de los sistemas operativos, e ingresa a los sistemas con generadores de contraseñas o forzando al sistema.

2.10.2- Estafas y Fraudes

Las estafas y fraudes se han convirtiendo en prácticas habituales por quienes se aprovecharse del descuido, negligencia o ingenuidad del resto de usuarios que utilizan el Internet no solo como vía de consulta o uso de sus servicios, sino también para adquirir productos en línea.

2.10.3- Pishing

El pishing consiste en falsificar una página web que simula pertenecer a un Portal de Pagos o hasta de un Banco y al cual el usuario, previo mensaje de correo electrónico conminatorio es convencido a ingresar los datos de su tarjeta de crédito, con el propósito de una supuesta regularización, a causa de un supuesto error.

Esta información es posteriormente utilizada para realizar compras ilegales a través de Internet.

2.10.4- Scamming

El Scamming es la típica labor que conduce a una estafa. Usualmente empieza con una carta enviada en forma masiva con el nombre del destinatario, y en la cual le pueden ofrecer una serie de oportunidades al usuario como ganar dinero, premios, préstamos a bajo interés, oportunidad del cobro, etc.

Una vez que el usuario proporciona sus datos o hace alguna transferencia de dinero, el vendedor o la página web de la supuesta organización o empresa, desaparece.

2.10.5- Otros delitos informáticos

Otros delitos comunes son:

- ✓ El envío masivo de correo no deseado o **SPAM.** Spam es la denominación usada en Internet para el Correo Electrónico Comercial no Solicitado que está inundando la red.
- ✓ La suplantación de los Remitentes de mensajes con la técnica **Spoofing.** Spoofing es un sistema de diseminación de virus a través del e-mail.
- ✓ Envío o ingreso subrepticio de archivos espías o **Keyloggers.** Los keyloggers son programas para espionaje, plantean problemas éticos y legales. Son utilizados muy a menudo en las oficinas de trabajo para espiar a los empleados sin el conocimiento de estos
- ✓ Uso de **Troyanos/Backdoors** para el control remoto de sistemas o robo de información. Los troyanos son programas potencialmente peligrosos, se ocultan dentro de otro para evitar ser detectado e instalarse de forma permanente en el sistema, permiten el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información

- ✓ Uso de **Rootkits** para los mismos fines anteriores y daños irreversibles. Un rootkits es una herramienta usada para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema.
- ✓ **Piratería** de software, CD musicales, películas o videos en formato DVD.
- ✓ Ataques a servidores con el objeto de sabotearlos, conocidos como **Cracking** o **Defacing** . Cracking es es el ataque o intromisión no autorizada desde el exterior al equipo. Sucede al tener una conexión permanente a la Internet, sobre todo con direcciones IP fijas
- ✓ **Robo directo de información** considerada estratégica o de secreto tecnológico.
- ✓ Interceptación de paquetes de datos enviados por Internet o **Sniffing.** Sniffing es un tipo de ataque en el cual se busca recavar información para posteriormente analizar el tráfico de red y obtener información confidencial

Dada la complejidad de los delitos informáticos y los de alta tecnología no es fácil establecer un marco legal apropiado y eficiente**.** Pero es esencial conocer cuales son y como funcionan para brindar soluciones a la organización que permitan proteger y precautelar la seguridad de la información.

2.11- Seguridad Perimetral

La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Define niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y deniega el acceso a intrusos.

La seguridad perimetral es entonces la correcta implementación de los equipos de seguridad que controlan y protegen todo el tráfico y contenido de entrada y salida entre todos los puntos de conexión o el perímetro de la red a través de una correcta definición de las políticas de seguridad y una robusta configuración de los dispositivos de protección.

La solución de Seguridad Perimetral protege a las redes de ataques informáticos como crackers, ataques de negación de servicio (Denied of Service - DoS)[1], virus, gusanos[2], troyanos, spam, contenido malicioso en correos y páginas web, protegiendo a la red en todos los enlaces, puntos de conexión o perímetro de la misma, incluyendo VPN´s[3] y enlaces a Internet.

2.11.1- Zona Desmilitarizada (DMZ)

Una DMZ o zona desmilitarizada *(*Demilitarized zone*)* es una subred situada entre la red interna, como puede ser una LAN, y entre una red externa, por ejemplo Internet.

Usualmente la DMZ contiene servicios accesibles desde Internet, como pueden ser el acceso a contenidos de paginas web, transferencia de archivos mediante servidor FTP, servicios de dominio de nombres DNS, etc. El objetivo de la DMZ es permitir las conexiones desde la red interna y la externa a la DMZ, pero

[1] **DoS.-** es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

[2] **Gusanos.-** son programas muy similares a los virus, también hacen copias de sí mismos y tienen efectos dañinos para los ordenadores, pero se diferencian en que no necesitan infectar otros ficheros para reproducirse.

[3] **VPN.-** Es una red privada, fue construida sobre la infraestructura de una red pública normalmente Internet. En lugar de utilizarse enlaces dedicados se utiliza la infraestructura de Internet, una vez que las redes están conectadas es transparente para los usuarios.

las conexiones desde la DMZ sólo se permiten a la red externa, es decir que los equipos en la DMZ no pueden conectarse con la red interna, por lo tanto pueden dar servicios a la red externa y además protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. La zona desmilitarizada brinda confianza a la red interna y esta protegida de la red externa.

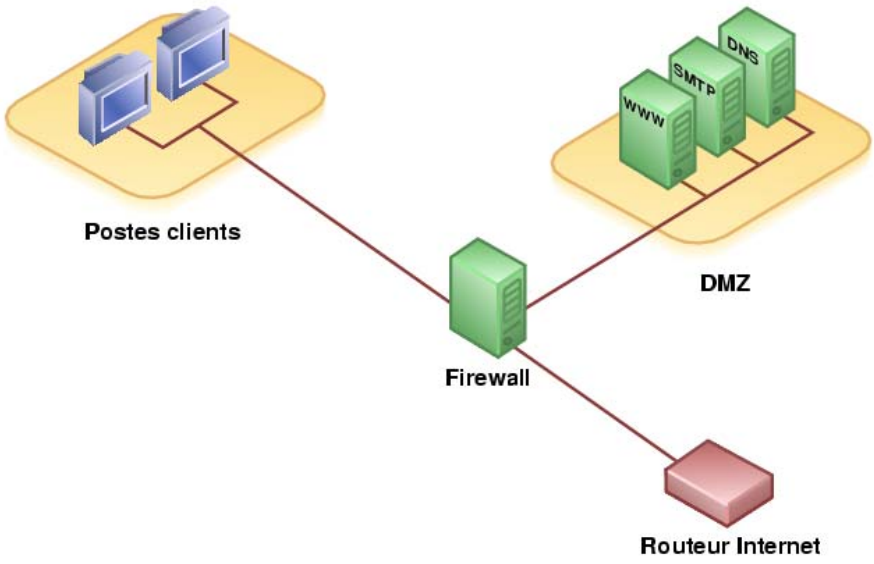

Figura 2.22: Diagrama de una Zona Desmilitarizada

2.11.2- Seguridad en Internet

La seguridad en Internet protege los recursos de la organización frente a posibles riesgos y amenazas como resultado de conectarse a Internet.

Es fundamental para toda empresa tener una salida a Internet, sin embargo si la red corporativa posee usuarios externos es esencial tomar medidas para controlar y prevenir posibles rupturas en la seguridad.

Los recursos, usuarios y todo el sistema informático varían constantemente, es así que la seguridad en internet trata de proteger a la red frente a cualquier tipo de

agresión externa. Existe además seguridad interna, como la seguridad física de los equipos, es decir protección frente a usuarios malintencionados.

Los componentes fundamentales de la seguridad en Internet son:

1. Identificación y Autentificaron

Se basa en mecanismos de autentificación para el control de acceso al sistema.

2. Control de acceso

Permite o deniega recursos como lectura, escritura, ejecución, creación, etc .

3. **Integridad**

Mantiene al sistema sin corrupción frente a alteraciones.

4. Confidencialidad

Es la capacidad para mantener oculta o secreta información frente a usuarios o sistemas ajenos.

2.12- El Firewall

"Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Un cortafuegos es una colección de elementos, tanto software como de hardware, destinado a filtrar todo el tráfico desde la Internet hacia nuestra red como de nuestra hacia la Internet." [1]

El firewall o cortafuegos actúa a modo de barrera que se interpone entre el servidor e Internet, examinando todos los paquetes de datos que entran o salen de su servidor.

[1] Texto tomado de: http://www.dei.uc.edu.py/tai2002-2/firewall/firewalls.html

El firewall funciona mediante la definición de políticas de seguridad. Posteriormente el propio firewall se encargará de verificar que todos y cada uno de los paquetes con destino al servidor se cumplan, descartando aquellos que no lo hagan.

Las políticas de seguridad se basan sobre todo en reglas utilizadas para:

- ✓ Impedir el acceso a los puertos del servidor (excepto a los que vayan a utilizarse) para evitar que un intruso pueda tomar el control del servidor aprovechando vulnerabilidades de aplicaciones de comunicaciones o un puerto abierto por un virus o gusano.
- ✓ Parar los ataques de denegación de servicio para evitar que un ataque basado en una gran cantidad de peticiones al servidor (fuerza bruta) pueda llevarlo al colapso. El firewall detectaría el intento y cortaría el flujo de datos sin dejar que llegase al servidor. También se detectan y cortan muchos más tipos de ataques sofisticados cuya intención es colapsar los servicios de red del servidor.

Un firewall contiene usualmente ya configuradas las principales políticas de seguridad generales para cualquier organización sin embargo le permite definir sus propias reglas de seguridad.

2.12.1- Funcionamiento del Firewall

Un firewall funciona de acuerdo a la siguiente secuencia:

1. Se utiliza un dispositivo con capacidad para ruta, puede ser el equipo donde funcionara la aplicación de software del firewall, un equipo de hardware que

funcione como firewall, o una solución de software y hardware. En este se ubican dos interfaces de red (interfaces de serie, ethernet, paso de testigo en anillo, etc.)

2. Se deshabilita el reenvío de paquetes IP (IP forwading)

3. Se conecta una interfaz a Internet .

5. Se conecta la otra interfaz a la red que se desea proteger.

2.12.2- Arquitecturas básicas de un firewall

Los elementos para la construcción de un firewall son innumerables, sin embargo existen algunos elementos esenciales que se deben tomar en cuanta al seleccionar los tipos de firewall.

1. Control de daños
2. Zonas de riesgo
3. Modo de fallo
4. Facilidad de uso
5. Políticas de seguridad por defecto
6. Manejo de "Stateful inspection"[1]
7. Sistema de Prevención contra Intrusiones (IPS Instrusion Protection System).
8. Anti-spam
9. Filtrado Web
10. Protección Anti-malware (bloquea toda clase de amenazas de contenidos (virus, gusanos, troyanos, spyware, intentos de phishing, etc.)
11. Soporte de VPN (Redes privadas virtuales)

[1] Stateful Inspection.- Es un tipo de filtrado que realiza un seguimiento del estado y contexto de las comunicaciones, básico en todos los protocolos y avanzado en FTP, PPTP, L2TP, IPSEC, estado de la comunicación, timeouts, conexiones relacionadas.

12. Sistema de detección de intrusos (IDS Instrusion Detection System), entre otros.

Las arquitecturas básicas de un firewall son:

'Screening Routers'

El filtrado se realiza solo con un router de selección. Existe la posibilidad de comunicación entre algunos ordenadores de la red e Internet. Es bastante vulnerable.

'Dual Homed Gateway'

Es un firewall implementado sin router de selección (usando IP Forwading). En caso de caída del firewall se podría deshabilitar el IP Forwading, con lo que la red quedaría totalmente vulnerable a Internet.

'Screened Host Gateway'

Es una de las configuraciones más utilizadas, emplea un router de selección y un host bastión[1].

'Screened Subnet'

Se crea una subred aislada, situada entre Internet y la red privada. Normalmente, esta red se aísla usando routers de selección, con los que se pueden implementar varios niveles de filtrado. Se configura de forma que Internet y la red privada tengan acceso a dicha subred, pero que el tráfico no pueda fluir directamente entre las dos subredes. Si un firewall es destruido, el atacante tiene que reconfigurar el enrutamiento entre las tres subredes, sin desconcertase o bloquearse, posible pero muy difícil.

[1] **Host bastión.-** es un ordenador en una red que ofrece un único punto de entrada y salida a internet desde la red interna y viceversa.

2.12.3- Tipos de Firewall

2.12.3.1- Firewalls basados en filtrado de paquetes

Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), dejan pasar a una red a través de paquetes IP en función de unas determinadas reglas. Estos firewalls conceptualmente trabajan a nivel de red, y son capaces de filtrar tráfico en función de direcciones de IP, protocolos, y números de puerto de TCP o UDP.

Normalmente, esta misión la pueden desempeñar tanto hosts con dos tarjetas de red, como routers. En el caso de firewalls basados en filtrado de paquetes, los dispositivos de la red interna han de configurarse con la ruta por defecto apuntando a este dispositivo, que en función de sus reglas, dejará pasar estos paquetes o los rechazará.

El principal problema de este tipo de firewalls es la limitación al configurar reglas complejas y la falta de flexibilidad en la capacidad de log, o registro de actividad. Otra desventaja fundamental es la imposibilidad de filtrar tráfico en función de información contenida en niveles superiores, tales como URL's, o esquemas de autenticación fuertes.

2.12.3.2- Firewalls basados en proxies

Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), no dejan pasar a una red a través de paquetes IP. La comunicación se produce por medio de proxies, que se ejecutan en el firewall.

Desde el punto de vista conceptual, este tipo de firewalls funciona a nivel de aplicación.

Un usuario interior que desee hacer uso de un servicio exterior, debe conectarse primero al firewall, donde el proxy atenderá su petición, y en función de la configuración impuesta en dicho firewall, se conectará al servicio exterior solicitado y hará de puente entre el servicio exterior y el usuario interior. Es importante mencionar que para la utilización de un servicio externo, se deben establecer dos conexiones o sockets.

En el caso de este tipo de firewalls, los programas clientes deben estar configurados para redirigir las peticiones al firewall en lugar de al host final. Esto es trivial en navegadores WWW, como Netscape, Internet Explorer o Linux, y en clientes FTP entre otros. Mientras, las aplicaciones tipo TELNET, no suelen incluir este tipo de soporte, y para ello, lo habitual es conectar directamente con el firewall y desde allí, el proxy permite especificar el destino final de telnet, que en este caso, sería encadenado.

La capacidad del registro de actividad es mucho mayor con este tipo de dispositivos. La información usualmente registrada por estos sistemas va desde el nombre de usuario que ha conseguido autentificarse satisfactoriamente, hasta los nombres y tamaños de ficheros transmitidos vía FTP, pasando por los URL's solicitados a través del proxy HTTP.

2.12.3.3- Firewalls con transparencia o de tercera generación

La característica primordial de estos sistemas es que admiten paquetes no destinados a ellos mismos, de forma similar a como lo hacen los routers, y en

función de una serie de reglas y configuraciones, son capaces de arrancar los proxies correspondientes automáticamente y conectar con el destinatario inicial.

Aparentemente para el usuario, se ha conectado con el servidor final, aunque realmente lo ha hecho con el proxy, que le devuelve los paquetes con dirección IP origen la del servidor final. Esto implica, que el programa cliente del usuario no requiere ningún tipo de configuración. En definitiva, se trata de firewalls basados en proxies, pero con apariencia y funcionalidad similar a los basados en filtrado de paquetes.

2.12.4- Seguridad en profundidad en la red externa

Las medidas fundamentales tomadas en el perímetro exterior se pueden resumir en:

- ✓ Reducción al mínimo de los servicios TCP/IP ofrecidos por cada sistema.
- ✓ Reducción al mínimo de los usuarios en cada uno de los sistemas.
- ✓ Uso extensivo de tcp-wrappers[1] en los servicios necesarios.
- ✓ Monitorización de routers en alerta de tráfico sospechoso.
- ✓ Escaneos periódicos de todo el perímetro en busca de posibles problemas.
- ✓ Sincronización de relojes en todos los sistemas para poder hacer un seguimiento fiable de logs en el caso de posibles incidentes.

[1] **TCP-Wrappers**.- son programas que permiten monitorizar, controlar y difundir listas de acceso para las conexiones de los servicios de red (Systat, FInger, FTP, Telnet, Rlogin, RSh, Exec, Tftp, Talk,etc).

2.12.5- Seguridad en profundidad en la red interna

En cuanto a la red interna se puede clasificar los problemas provocados por usuarios internos o por intrusiones realizadas desde puntos no controlados de nuestra una red.

Contra este tipo de problemas, se debe aplicar medidas parecidas a las del perímetro externo, añadiendo el uso de programas de chequeo de la seguridad de las contraseñas elegidas por los usuarios.

Otra medida fundamental para prevenir accesos desde el exterior por puntos no controlados de una red, es establecer la prohibición del uso de modems con capacidad de llamada entrante. Si este uso fuese inevitable, como norma, debe utilizarse para ello, sistemas no conectados físicamente a la red o realizarse bajo la estricta vigilancia del administrador de red responsable.

2.13- Procedimientos generales de seguridad

Las normas dictadas en la elaboración de la política de seguridad, en algunos casos de forma concreta y en otros de forma más abstracta, pero igualmente concluyentes, deben materializarse en una serie de procedimientos y normas a seguir en la operación y mantenimiento de las tareas diarias, sobretodo en cuanto a lo relacionado con las actividades que de una forma u otra tienen que ver con uso del Internet.

2.13.1- Restricciones en el Firewall

La parte más importante de estas tareas se realiza en el firewall, conjuntamente con la tarea de permitir o denegar determinados servicios en

función de los distintos usuarios y su ubicación. Se definen tres grupos de usuarios:

1. Usuarios internos con permiso de salida para servicios restringidos
2. Resto de usuarios internos con permiso de salida para servicios no restringidos.
3. Usuarios externos con permiso de entrada desde el exterior

Las prioridades asignadas a cada grupo deben al igual que las políticas de seguridad de la empresa, iniciarse analizando esencialmente el nivel de prioridad que corresponde a cada grupo acorde a las necesidades de los usuarios. Sin embargo existen se pueden definir algunas políticas generales para la seguridad de cualquier firewall. La política de seguridad debe basarse en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación de la organización. Si no se dispone de la información detallada de la política a seguir, aunque sea un firewall esmeradamente desarrollado y armado, se estará exponiendo la red privada a un posible atentado.

2.13.2- Limitaciones del firewall

Un firewall no puede protegerse contra los ataques que se efectúen fuera de su punto de operación o fuera de su área de alcance.

El firewall no puede protegerse ante amenazas a las que esta sometidas debido a usuarios inconscientes. No puede prohibir, por ejemplo, que los usuarios copien datos importantes en medios magnéticos o tarjetas PCMCIA y substraigan estas de la organización.

El firewall no se puede proteger contra los ataques de la "Ingeniería Social", por ejemplo los comúnmente llamados hackers. Es por ello que los empleados deben ser informados acerca de los varios tipos de ataque social que pueden suceder, así como de sanciones en caso de la situación lo amerite. En base a esto la organización debe crear políticas en cuanto al uso de nombre de usuario y contraseñas.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, esto debido a que el firewall de no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el. La solución consiste en la utilización de software anti-viral en cada uno de los equipos.

Además, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

La seguridad que provea un firewall debe ser completada con políticas de seguridad generales para todos los grupos de usuarios y sus respectivos equipos.

2.14- Metodología para el Diseño de Redes de Área Local

El actual proyecto se basará en la metodología de diseño de redes área local descrita por Cisco Systems (CCNA 2005). Esta plantea una serie planificada de procesos para alcanzar una red LAN diseñada en óptimas condiciones.

2.14.1- Objetivos del Diseño de una LAN

Antes de diseñar una red de área local es esencial determinar inicialmente que es lo que se desea lograr mediante el diseño de la red.

Evidentemente estos objetivos no son fijos pues dependen de las necesidades de los usuarios así como de la infraestructura física de la organización. Sin embargo existen algunas directrices generales puesto que son básicas para el diseño de la mayoría de redes locales, y primordialmente por su importancia al diseñar una red local.

Funcionalidad

La red debe funcionar, satisfaciendo las necesidades de conectividad básicas para los usuarios de manera confiable y efectiva.

Escalabilidad

La red debe tener la capacidad de aumentar su tamaño sin que esto exija nuevos cambios en el diseño de la LAN.

Adaptabilidad

La red debe manejar un diseño que le permita adecuarse a los futuros cambios tecnológicos.

Facilidad de Administración

El diseño debe permitir la administración y monitoreo de la red, garantizando el funcionamiento correcto de la misma.

2.14.2- Consideraciones para el diseño de una LAN

Las principales consideraciones que se deben tomar en cuenta antes de diseñar una LAN son:

Función y ubicación de los servidores

Los servidores empresariales deben colocarse en el servicio de distribución principal (MDF)[1]. Es recomendable que el tráfico hacia los servidores sólo viaje hacia el MDF y no se transmita a través de otras redes, aunque en ciertas ocasiones es inevitable debido a la existencia de un núcleo enrutado. Es ideal que los servidores de los grupos de trabajos se coloquen en el servicio de distribución intermedia (IDF)[2] más cercano a los usuarios que acceden a las aplicaciones en estos servidores. Esto permite al tráfico viajar por la infraestructura de red hacia un IDF y no afecta a los demás usuarios en ese segmento de red. Los switchs de Capa 2 ubicados en el MDF y los IDF deben tener 100 Mbps o más asignados para estos servidores.

Temas relacionados con los dominios de colisión

Las colisiones excesivas, provocadas por acceder al medio compartido o al dominio de colisión al mismo tiempo, pueden reducir el ancho de banda disponible de un segmento de red a treinta y cinco o cuarenta por ciento del ancho de banda disponible.

[1]**MDF(Main Distribution Frame):** Instalación principal de distribución. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión.

[2]**IDF(Intermedia Distribution Frame):** Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

Temas de segmentación

La segmentación se ejecuta cuando un sólo “dominio de colisión” [1] se divide en dominios de colisión más pequeños. Estos dominios de colisión más pequeños reducen la cantidad de colisiones en un segmento de LAN, permitiendo mayor utilización del ancho de banda.

Los dispositivos de la Capa 2 como por ejemplo puentes y switchs se pueden utilizar para segmentar una LAN. Los routers pueden lograr esto a nivel de la Capa 3.

Temas relacionados con los dominios de broadcast

Un dominio de broadcast se refiere al conjunto de dispositivos que reciben una trama de datos de broadcast desde cualquier dispositivo dentro de este conjunto. La trama de datos de broadcast debe ser procesado por todos los usuarios que la reciben, sin embargo este proceso consume recursos y el ancho de banda disponible.

Los dispositivos de Capa 2 como los puentes y switchs reducen el tamaño de un dominio de colisión pero no reducen el tamaño del dominio de broadcast, mientras los routers reducen el tamaño del dominio de colisión y el tamaño del dominio de colisión o de broadcast en la Capa 3.

[1] **Dominio de colisión**: es un segmento lógico de una red de ordenadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

2.14.3- Pasos Sistemáticos

Con el objetivo de alcanzar una LAN efectiva, capaz de satisfacer las necesidades de una organización y por tanto de sus usuarios, es esencial cumplir con una serie planificada de pasos sistemáticos, estos son:

2.14.3.1- Reunir requisitos y expectativas

Este proceso pretende identificar claramente cualquier inconveniente existente en la red, el estado actual de la red, los requerimientos de los usuarios, el crecimiento proyectado de la red y la disponibilidad de la red.

Esta información es identificada en base a:

- ✓ Historial de la organización y su estado actual
- ✓ Las proyecciones de la organización
- ✓ Políticas operativas
- ✓ Procedimientos de administración y procedimientos de los sistemas
- ✓ Procedimientos de oficina
- ✓ Las opiniones de quienes utilizan la LAN.

La documentación de los requisitos brinda una estimación de los costos para la implementación de diseño de LAN. Es esencial entender los problemas de rendimiento de cualquier red.

2.14.3.2- Analizar requisitos y datos

Este proceso consiste en analizar los requisitos de la red y de sus usuarios. Debido a nuevas aplicaciones introducidas en la red (por ejemplo voz y vídeo),

las necesidades del usuario de la red cambian constantemente, requiriendo inevitablemente el aumento de ancho de banda para cada uno de ellos. Una LAN no es efectiva si no puede brindar información rápida y precisa a los usuarios. Es necesario entonces asegurar que se cumplan los requisitos de información de la organización y de sus empleados.

2.14.3.3- Diseñar la estructura o topología de las Capas 1, 2 y 3 de la LAN

Este proceso consiste en decidir la topología LAN de la organización que satisfaga los requisitos del usuario. El diseño de una topología LAN se puede dividir en las tres siguientes categorías únicas del modelo de referencia OSI:

- ✓ Capa de red
- ✓ Capa de enlace de datos
- ✓ Capa física

2.14.3.4- Documentar la implementación física y lógica de la red

Este proceso consiste en la documentación, tanto de la topología física de la red así como de la topología lógica de la misma. La topología física es el modo en el que se conectan entre sí los dispositivos de una LAN, mientras el diseño lógico de la red se refiere al flujo de datos que hay dentro de una red.

Además se debe documentar los esquemas de nombre y dirección que se utilizan en la implementación de la solución de diseño LAN.