



UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

IMPLEMENTACION DE VLAN EN UNA RED
ACADEMICA (UPIITA).

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICISTA

P R E S E N T A:
OSCAR HERNANDEZ FAJARDO

DIRECTOR DE TESIS:
ING. BENITO BARRANCO CASTELLANOS



FES Aragón

BOSQUES DE ARAGÓN, EDO. DE MÉXICO,

2005

0351068



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS:

Agradezco a Dios el haberme dado la oportunidad de realizar una de mis metas, poniendo en mi camino a cada una de las personas que me ayudaron a llegar a ella.

Laura y Katy

Son mi ilusión, la fuente de mi fuerza, y el motor que me impulsa a seguir adelante, con su amor, comprensión y paciencia

¡¡Las Amo!!

Gracias a mis padres

Ing. Arturo Hernández Márquez e Irma Fajardo Gómez

Y mi hermano **Edgardo**, con mucho cariño, ya que con su constante interés y apoyo, me dan ánimos siempre para salir adelante. ¡Este logro también es suyo!

Adolfo y Viky

Gracias por Darnos la mano como familia, amigos y hermanos en los momentos más difíciles y sin esperar nada a cambio,

¡Dios los Bendiga!

Augusto Vite Arontes

Gracias por tu amistad, enseñanzas y ejemplos, además de tu tiempo y paciencia, sabes que te admiro mucho como amigo, persona y maestro.

¡¡ERES UNA GRAN PERSONA!!

Ing. Benito Barranco Castellanos e

Ing. Luís N. Galván Flores

Por su apoyo constante y su amistad,
Su ayuda es invaluable para mí y mi familia.

Por ultimo, Agradezco a la **UNAM - FES Aragón**, mi escuela y mi casa, que me dio la formación académica.

Índice

aplicacion de una vlan en una red academica (UPIITA)

Introducción

i

Capítulo I. Generalidades de las redes

1. Generalidades de las redes	1
1.1. Uso de las redes de computadoras	1
1.2. Hardware de red	1
1.2.1. Redes de área local	1
1.2.2. Redes de área metropolitana	3
1.2.3. Redes de área amplia	4
1.3. Software de red	5
1.3.1. Modelos OSI	5
1.3.1.1. Capa 7: la capa de aplicación	7
1.3.1.2. Capa 6: la capa de presentación	8
1.3.1.3. Capa 5: la capa de sesión	8
1.3.1.4. Capa 4: la capa de transporte	8
1.3.1.5. Capa 3: la capa de red	9
1.3.1.6. Capa 2: la capa de enlace	9
1.3.1.7. Capa 1: la capa física	9
1.3.2. Interacción entre las capas e Intercambio de información	10
1.3.2.1. El modelo de referencia TCP/IP	12
1.3.2.1.1. La capa de Interred	12
1.3.2.1.2. La capa de transporte	13
1.3.2.1.3. La capa de aplicación	13
1.3.2.1.4. La capa de nodo de la red	13
1.3.2.2. Comparación de los modelos de referencia OSI y TCP	14
1.4. Los puentes y los Switches	15
1.4.1. Dispositivos de la capa de enlace	16
1.4.2. Los switches	16
1.5. Los Routers	17
1.5.1. Componentes Físicos	17
1.5.2. Funciones de un router	18
1.5.2.1. Interconectividad física.	19
1.5.2.2. Interconectividad lógica.	19
1.5.2.3. Cálculo y mantenimiento de la ruta	19
1.6. Ejemplos de Tecnologías de Red	21
1.6.1. Tecnologías de Ethernet	21
1.6.2. Tecnologías de Token ring	22

Capítulo II. Redes Virtuales de Área Local (VLAN)

2. Redes Virtuales de Área Local (VLAN)	25
2.1. Introducción	25
2.2. IEEE 802.1Q-1998	25
2.3. Arquitectura de VLAN	26
2.4. Soporte del Servicio MAC en VLANs	28
2.5. Principios de Operación	31
2.6. Formato de trama etiquetada	44
2.7. Uso de GMRP en VLANs	51
2.8. Administración de topología VLAN	53
2.9. Administración de Switch VLAN	57

Capítulo III. Implementación de una VLAN, en el edificio sur y centro de la UPIITA

3. Implementación de una VLAN	80
3.1. Planteamiento del Problema	80
3.2. Formulación de hipótesis	81
3.3. Levantamiento de Información.	81
3.3.1. Características del Producto	82
3.3.2. Panel Frontal	83
3.3.3. Módulos opcionales	84
3.3.4. Panel Trasero	85
3.3.5. Sumario de características	85
3.3.5.1. IEEE 802.1D Puente	85
3.3.5.2. Protocolo de Spanning Tree	86
3.3.5.3. Virtual LANs (VLANs)	87
3.3.5.3.1. VLAN por Puerto	87
3.3.5.3.2. VLAN por MAC	88
3.3.5.3.3. VLAN por Protocolo	88
3.3.5.3.4. VLAN por subredes de IP o IPX	88
3.3.5.3.5. VLAN por direcciones IP multicast	88
3.3.5.3.6. VLAN definidas por el usuario	88
3.3.5.3.7. VLAN Binding	88
3.3.5.3.8. VLAN por DHCP	89
3.4. Análisis e interpretación de los datos	89
3.4.1. Resultados	94
3.5. Comprobación de la hipótesis	95

Conclusiones

Índice de Tablas y figuras

Glosario

Bibliografía

Introducción

La finalidad para la creación de esta tesis fue la de consolidar los conocimientos obtenidos en el seminario y aplicarlos a un caso práctico, La Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas, del Instituto Politécnico Nacional. En esta unidad se encuentran equipos Enterasys muy parecidos a los que se utilizaron para las prácticas en el seminario consecuentemente, el desarrollo será conforme a las prácticas que se realizaron.

La aplicación como caso real, hace caso a las necesidades por parte del departamento de cómputo para solucionar un problema latente, al hacer la propuesta de VLANs pretendemos dar solución a la administración de la red, específicamente la administración de direcciones IP.

De esto se deriva el objetivo general de la tesis: Dar una visión General de las VLANs y hacer una implementación real mediante 4 equipos Enterasys ya instalados.

El capítulo 1 hace referencia general a las redes de computadoras, a lo largo del desarrollo encontraremos, uso de las computadoras, software y hardware de red, modelos de referencia, switch's y router's, y ejemplos de tecnologías, Ethernet y Token ring, que son los precursores de todas las tecnologías actuales, con esto se pretende adentrar a lector en el marco teórico.

El tema principal y al que esta enfocado el trabajo presentado son las VLANs que son Redes Virtuales de Área Local, son agrupamientos lógicos de dispositivos o usuarios que se pueden agrupar por función, departamento, aplicación, etc., independientemente de su ubicación física en un segmento. El punto más importante de este tipo de agrupación ya sea de manera estática y/o dinámica; es que esto se hace directamente en un Switch Administrable de Capa 2 del Modelo de referencia OSI (Capa de Enlace de Datos) realizando segmentación de dominios de colisión, por lo que la comunicación será más eficiente debido a que la carga en el Router (capa 3 del modelo de referencia OSI) es menor y más rápida.

Además permite una fácil escalabilidad debido a su fácil administración que permite adicionar puertos como miembros a una VLAN dada.

El capítulo 2 se refiere básicamente a cómo están compuestas las tramas basadas en el estándar IEEE 802.1Q, referente a la conformación de VLANs desde su forma de identificarse y diferenciarse de otros tipos de tramas, debido al filtro de la base de datos, al agrupado de los usuarios y en base a las direcciones MAC del Switch, o el tipo de protocolo de la capa de red, así como de la información que se le adiciona en la Capa de Enlace de Datos que esta conformada por la dirección MAC destino y fuente.

También nos muestra de cuantos bits se conforma la trama y de que elementos se conforma. Cuales bits cambian identificándose como una trama que forma parte de una VLAN, así como también la forma en que se transmite y se recibe. Los elementos esenciales de configuración, y su administración de acuerdo con el estándar.

Esta red se decidió implementar en la UPIITA, porque los equipos ya existían y no se explotaban sus capacidades, en conjunción con el departamento de cómputo, se decidió configurar en esta escuela varias VLAN's para solucionar problemas con las direcciones IP, en el capítulo 3 se describen los pasos a seguir para configurar las VLAN's sobre el VH-2402S, accediendo desde la consola, y mediante los menús del equipo.

Como metodología de investigación utilizamos el método científico general para el planteamiento del problema, levantamiento de información, resultados y conclusiones. En los primeros capítulos utilizamos la investigación documental.

Capitulo I. Generalidades de las redes

1.1 Uso de las redes de computadoras

El uso de las redes de computadoras en la actualidad, es tan difundido que se encuentran en los sistemas centrales que controlan todas las funciones de las ciudades, agilizan las transacciones de monetarias, prácticamente puedes encontrar cualquier parte

1.2 Hardware de red

Para la clasificación del hardware de red no existe una clasificación específica pero dos dimensiones sobresalen como importantes: la tecnología de transmisión y la escala. Por eso se examinarán cada una de ellas, en términos generales hay dos tipos de tecnologías de transmisión:

- Redes de difusión
- Redes punto a punto

Las redes de difusión tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes cortos (llamados paquetes) que envía una máquina son recibidos por los demás. Un campo de dirección dentro del paquete especifica quien se dirige. Al recibir un paquete, una máquina verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a alguna otra máquina, lo ignora.

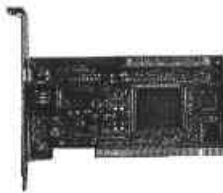


Fig 1.1 Tarjeta de red para puerto PCI

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando un paquete con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama difusión (broadcasting). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo conocido como multidifusión. Un esquema posible consiste en reservar un bit para indicar multidifusión. Los restantes $n-1$ bits de dirección pueden contener un número de grupo. Cada máquina se puede suscribir a cualquier grupo o a todos. Cuando se envía un paquete a cierto grupo, se entrega a todas las máquinas que se suscribieron a ese grupo.

En contraste las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo desempeñan un papel importante

1.2.1 Redes de área local

Las redes de área local, generalmente llamadas LAN (local area networks), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información. Las LAN se distinguen de otro tipo de redes por tres características: (1) su tamaño, (2) su tecnología de transmisión, y (3) su topología.

Las LAN están restringidas en tamaño, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano. Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos, y también simplifica la administración de la red.

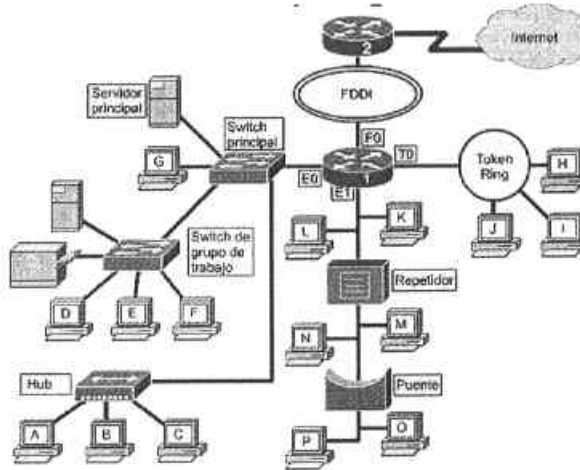


Fig 1.2 Ejemplo de interconexión entre redes LAN

Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas, como las líneas compartidas de la compañía telefónica que solían usarse en áreas rurales. Las LAN tradicionales operan a velocidades de 10 a 100 Mbps, tienen bajo retardo (décimas de microsegundos) y experimentan muy pocos errores. Las LAN más nuevas pueden operar a velocidades muy altas, de hasta cientos de megabits/seg.

Las LAN de transmisión pueden tener diversas topologías. En una red de bus (esto es, un cable lineal), en cualquier instante una computadora es la máquina maestra y puede transmitir; se pide a las otras máquinas que se abstengan de enviar mensajes. Es necesario un mecanismo de arbitraje para resolver conflictos cuando dos o más máquinas quieren transmitir simultáneamente. El mecanismo de arbitraje puede ser centralizado o distribuido. Por ejemplo, la IEEE 802.3, popularmente llamada Ethernet, es una red de transmisión basada en bus con control de operación descentralizado a 10 o 100 Mbps. Las computadoras de una Ethernet pueden transmitir cuando quieran; si dos o más paquetes chocan, cada computadora sólo espera un tiempo al azar y lo vuelve a intentar.

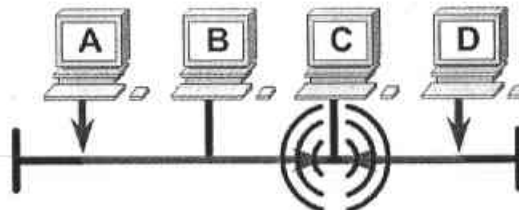


Fig 1.3 Ejemplo de una colisión en Ethernet

Un segundo tipo de sistema de difusión es el anillo. En un anillo, cada bit se propaga por sí mismo, sin esperar al resto del paquete al cual pertenece. Típicamente, cada bit recorre el anillo entero en el tiempo que toma transmitir unos pocos bits, a veces antes de que el paquete completo se haya transmitido. Como en todos los sistemas de difusión, se necesitan reglas para arbitrar el acceso simultáneo al anillo. Se emplean varios métodos que se analizarán más adelante en este libro. La IEEE 802.5 (el token ring de IBM), es una popular LAN basada en anillo que opera a 4 y 16 Mbps.



Fig 1.4 Ejemplo de red Token Ring

Las redes de difusión se pueden dividir también en estáticas y dinámicas, dependiendo de cómo se asigna el canal. Una asignación estática típica divide el tiempo en intervalos discretos y ejecuta un algoritmo de asignación cíclica, permitiendo a cada máquina transmitir únicamente cuando le llega su turno. La asignación estática desperdicia la capacidad del canal cuando una máquina no tiene nada que decir durante su segmento asignado, por lo que muchos sistemas intentan asignar el canal dinámicamente (es decir, por demanda).

Los métodos de asignación dinámica para un canal común son centralizados o descentralizados. En el método de asignación de canal centralizado hay una sola entidad, por ejemplo una unidad de arbitraje del bus, la cual determina quién es el siguiente. Podría hacer esto aceptando peticiones y tomando una decisión de acuerdo con un algoritmo interno. En el método de asignación de canal descentralizado no hay una entidad central; cada máquina debe decidir por sí misma si transmite o no. Podríamos pensar que esto siempre conduce al caos, pero no es así. Más adelante estudiaremos muchos algoritmos diseñados para poner orden en el caos potencial.

El otro tipo de LAN se construye con líneas punto a punto. Las líneas individuales conectan una máquina específica a otra. Una LAN así es realmente una red de área amplia en miniatura. Veremos esto posteriormente.

1.2.2 Redes de área metropolitana

Una red de área metropolitana, o MAN (metropolitan area network) es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o pública. Una MAN puede manejar datos y voz, e incluso podría estar relacionada con la red de televisión por cable local. Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Al no tener que conmutar, se simplifica el diseño.

La principal razón para distinguir las MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este estándar ya se está implementando: se llama DQDB (distributed queue dual bus, o bus dual de cola distribuida) o, para la gente que prefiere números a letras, 802.6 (el número de la norma IEEE que lo define). El DQDB consiste en dos buses

(cables) unidireccionales, a los cuales están conectadas todas las computadoras. Cada bus tiene una cabeza terminal (head-end), un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior. El tráfico hacia la izquierda usa el de abajo.

Un aspecto clave de las MAN es que hay un medio de difusión (dos cables, en el caso de la 802.6) al cual se conectan todas las computadoras. Esto simplifica mucho el diseño comparado con otros tipos de redes.

1.2.3 Redes de área amplia

Una red de área amplia, o WAN (wide area network), se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (es decir, de aplicación). Seguiremos el uso tradicional y llamaremos a estas máquinas hosts. El término sistema terminal (end system) se utiliza también ocasionalmente en la literatura. Las hosts están conectadas por una subred de comunicación, o simplemente subred. El trabajo de la subred es conducir mensajes de una host a otra, así como el sistema telefónico conduce palabras del que habla al que escucha. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (las hosts), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la sub red tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos, canales o troncales) mueven bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. Desafortunadamente, no hay una terminología estándar para designar estas computadoras; se les denomina nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos, entre otras cosas. Como término genérico para las computadoras de conmutación, usaremos la palabra router, pero conviene que el lector quede advertido de que no hay consenso sobre la terminología. En este modelo, cada host generalmente está conectada a una LAN en la cual está presente un router, aunque en algunos casos una host puede estar conectada directamente a un router. La colección de líneas de comunicación y routers (pero no las hosts) forman la subred.

Es pertinente un comentario al margen acerca del término "subred". Originalmente, sólo significaba la colección de routers y líneas de comunicación que movían los paquetes de la host de origen a la host de destino. Sin embargo, algunos años después surgió un segundo significado en relación con la identificación de direcciones en la red. Así, el término tiene cierta ambigüedad. Desafortunadamente, no existen opciones ampliamente aceptadas para su significado inicial, de modo que muy a pesar nuestro lo usaremos en ambos sentidos. Por el contexto, siempre quedará claro lo que significa la palabra.

En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas, cada una conectada a un par de routers. Si dos routers que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros routers. Cuando se envía un paquete de un router a otro a través de uno o más routers intermedios, el paquete se recibe completo en cada router intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, de punto a punto, de almacenar y reenviar, o de paquete conmutado. Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse celdas.

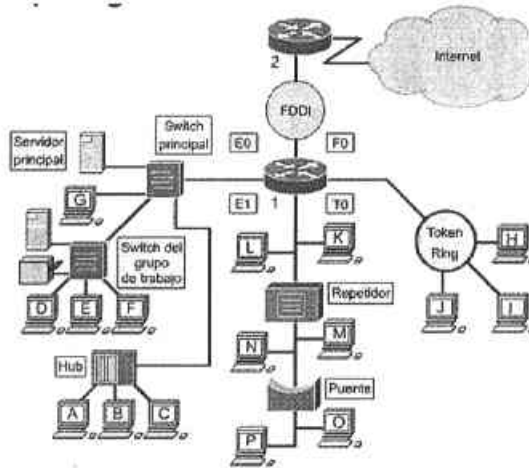


Fig. 1.5 Configuración de una red WAN

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión del router. Las redes locales que fueron diseñadas como tales usualmente tienen una topología simétrica. En contraste, las redes de área amplia típicamente tienen topologías irregulares.

Una segunda posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada router tiene una antena por medio de la cual puede enviar y recibir. Todos los routers pueden oír las salidas enviadas desde el satélite y en algunos casos pueden también oír la transmisión ascendente de los otros routers hacia el satélite. Algunas veces los routers están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza, las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

1.3 Software de red

1.3.1. Modelo OSI

La Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) elaborando así el modelo de referencia OSI en 1984.

Para enfrentar el problema de incompatibilidad de las redes y su imposibilidad de comunicarse entre sí, la *Organización Internacional para la Normalización (ISO)* estudió esquemas de red como DECNET, SNA y TCP/IP a fin de encontrar un conjunto de reglas. Como resultado de esta investigación, la ISO desarrolló un modelo de red que ayudaría a los fabricantes a crear redes que fueran compatibles y que pudieran operar con otras redes.

El proceso de dividir comunicaciones complejas en tareas más pequeñas y separadas se podría comparar con el proceso de construcción de un automóvil. Visto globalmente, el diseño, la fabricación y el ensamblaje de un automóvil es un proceso de gran complejidad. Es poco probable que una sola persona sepa cómo realizar todas las tareas requeridas para la construcción de un automóvil desde cero. Es por ello que los ingenieros mecánicos diseñan el

automóvil, los ingenieros de fabricación diseñan los moldes para fabricar las partes y los técnicos de ensamblaje ensamblan cada una una parte del auto.



Fig. 1.7 Las siete capas del modelo OSI

El *modelo de referencia OSI* (Nota: No debe confundirse con ISO.), lanzado en 1984, fue el esquema descriptivo que crearon. Este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje

La información que viaja a través de una red se conoce como *paquete*, *datos* o *paquete de datos*. Un paquete de datos es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación. Incluye la información de origen junto con otros elementos necesarios para hacer que la comunicación sea factible y confiable en relación con los dispositivos de destino. La dirección origen de un paquete especifica la identidad del computador que envía el paquete. La dirección destino especifica la identidad del computador que finalmente recibe el paquete.

En networking, un medio es el material a través del cual viajan los paquetes de datos. Puede ser cualquiera de los siguientes materiales:

- Cables telefónicos
- UTP de categoría 5 (se utiliza para Ethernet 10BASE-T)
- Cable coaxial (se utiliza para la TV por cable)
- Fibra óptica (delgadas fibras de vidrio que transportan luz)

Existen otros dos tipos de medios que son menos evidentes, pero que no obstante se deben tener en cuenta en la comunicación por redes. En primer lugar, está la atmósfera (en su mayor parte formada por oxígeno, nitrógeno y agua) que transporta ondas de radio, microondas y luz.

La comunicación sin ningún tipo de alambres o cables se denomina inalámbrica o comunicación de espacio abierto, usando ondas electromagnéticas (EM). Entre las ondas EM, que en el vacío viajan a velocidad de la luz, se incluyen las ondas de energía, ondas de radio, microondas, luz infrarroja, luz visible, luz ultravioleta, rayos x y rayos gama. Las ondas EM viajan a través de la atmósfera (principalmente compuesta de oxígeno, nitrógeno y agua), pero también viajan a través del vacío del espacio exterior (donde no existe prácticamente materia, ni moléculas ni átomos).

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o *protocolo*. Un *protocolo* es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente.

Las siete capas del modelo de referencia OSI son:

- Capa 7: La capa de aplicación
- Capa 6: La capa de presentación
- Capa 5: La capa de sesión
- Capa 4: La capa de transporte
- Capa 3: La capa de red
- Capa 2: La capa de enlace de datos
- Capa 1: La capa física



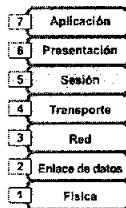
1.3.1.1. Capa 7: La capa de aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.



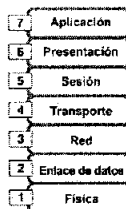
1.3.1.2. Capa 6: La capa de presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.



1.3.1.3. Capa 5: La capa de sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.



1.3.1.4. Capa 4: La capa de transporte

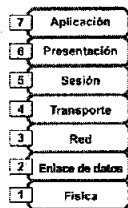
La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.



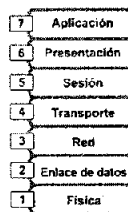
1.3.1.5. Capa 3: La capa de red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Se encarga mas que nada de selección de ruta, direccionamiento y enrutamiento.



1.3.1.6 Capa 2: La capa de enlace de datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico) , la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Se basa en tramas y control de acceso al medio.



1.3.1.7. Capa 1: La capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física.

Las capas del modelo OSI pueden ser divididas en dos categorías: capas superiores y capas inferiores. Las capas superiores se implementan únicamente para las aplicaciones en software y son las que se encuentran más cerca del usuario, por lo que respecta de las capas inferiores es que la capa física y la de enlace, se aplican principalmente en hardware y software, las demás capas se implementan únicamente en software, la capa más baja, la capa física, se enfoca principalmente en el medio de transmisión, como el cable por ejemplo, y es responsable de colocar la información en el medio.

1.3.2. Interacción entre las capas e Intercambio de información

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como comunicaciones de par-a-par. Durante este proceso, cada protocolo de capa intercambia información, que se conoce como unidades de datos de protocolo (PDU), entre capas iguales. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales. Después de que las Capas 7, 6 y 5 han agregado la información, la Capa 4 agrega más información. Este agrupamiento de datos, la PDU de Capa 4, se denomina segmento.

Por ejemplo, la capa de red presta un servicio a la capa de transporte y la capa de transporte presenta datos al subsistema de internetwork. La tarea de la capa de red consiste en trasladar esos datos a través de la internetwork. Ejecuta esta tarea encapsulando los datos y agregando un encabezado, con lo que crea un paquete (PDU de Capa 3). Este encabezado contiene la información necesaria para completar la transferencia, como por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red en una trama (la PDU de Capa 2); el encabezado de la trama contiene información (por Ej., direcciones físicas) que es necesaria para completar las funciones de enlace de datos. La capa de enlace de datos suministra un servicio a la capa de red encapsulando la información de la capa de red en una trama.

La capa física también suministra un servicio a la capa de enlace de datos. La capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros (bits) para su transmisión a través del medio (generalmente un cable) en la Capa 1.

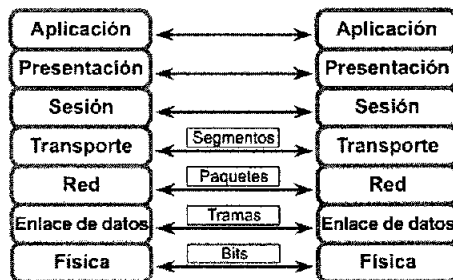


Fig. 1.8 Comunicación par a par

Capa de Aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran

fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Capa de Presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa de Sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Capa de Transporte

La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

Capa de Red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Se encarga más que nada de selección de ruta, direccionamiento y enrutamiento.

Capa de Enlace

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Se basa en tramas y control de acceso al medio.

Capa Física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física.

1.3.2.1. El modelo de referencia TCP/IP

Pasemos ahora del modelo de referencia OSI al modelo que se usa en la abuela de todas las redes de computadoras, la ARPANET, y su sucesora, la Internet mundial. Aunque más adelante presentaremos una breve historia de la ARPANET, es de utilidad mencionar ahora algunos de sus aspectos. La ARPANET era una red de investigación patrocinada por el DoD (Departamento de Defensa de Estados Unidos). Al final conectó a cientos de universidades e instalaciones del gobierno usando líneas telefónicas rentadas. Cuando más tarde se añadieron redes de satélite y radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una arquitectura de referencia nueva. Así, la capacidad de conectar entre sí múltiples redes de manera inconsútil fue uno de los principales objetivos de diseño desde el principio. Esta arquitectura se popularizó después como el modelo de referencia TCP/IP, por las iniciales de sus dos protocolos primarios.

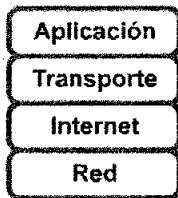


Fig. 1.9 Modelos de referencia TCP/IP

Debido a la preocupación del DoD por que alguno de sus costosos nodos, enrutadores o pasarelas de interredes pudiera ser objeto de un atentado en cualquier momento, otro de los objetivos principales fue que la red fuera capaz de sobrevivir a la pérdida del *hardware* de subred sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones permanecieran intactas mientras las máquinas de origen y destino estuvieran funcionando, aun si alguna de las máquinas o de las líneas de transmisión en el trayecto dejara de funcionar en forma repentina. Es más, se necesitaba una arquitectura flexible, pues se tenía la visión de aplicaciones con requerimientos divergentes, abarcando desde la transferencia de archivos hasta la transmisión de discursos en tiempo real.

1.3.2.1.1. La capa de interred

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred carente de conexiones. Esta capa, llamada capa de interred, es el eje que mantiene unida toda la arquitectura. La misión de esta capa es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino (que podría estar en una red diferente). Los paquetes pueden llegar incluso en un orden diferente a aquel en que se enviaron, en cuyo caso corresponde a las capas superiores reacomodarlos, si se desea la entrega ordenada. Nótese que aquí se usa "interred" en un sentido genérico, aunque esta capa esté presente en la Internet.

Aquí la analogía es con el sistema de correos (lento). Una persona puede depositar una secuencia de cartas internacionales en un buzón en un país, y con un poco de suerte, casi todas se entregarán en la dirección correcta en el país de destino. Es probable que las cartas viajen a través de una o más pasarelas internacionales de correo en el camino, pero esto es transparente para los usuarios. Más aún, los usuarios no necesitan saber que cada país (esto es, cada red),

tiene sus propias estampillas, tamaños preferidos de sobres y reglas de entrega.

La capa de interred define un formato de paquete y protocolo oficial llamado IP (*Internet protocol*, protocolo de interred). El trabajo de la capa de interred es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el ruteo de los paquetes, y también evitar la congestión. Por lo anterior es razonable decir que la capa de interred TCP/IP es muy parecida en funcionalidad a la capa de red OSI

1.3.2.1.2. La capa de transporte

La capa que está sobre la capa de interredes en el modelo TCP/IP se llama usualmente ahora capa de transporte. Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, TCP (*transmission control protocol*, protocolo de control de la transmisión) es un protocolo confiable orientado a la conexión que permite que una corriente de bytes originada en una máquina se entregue sin errores en cualquier otra máquina de la interred. Este protocolo fragmenta la corriente entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga del control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo de esta capa, el UDP (*user datagram protocol*, protocolo de datagrama de usuario), es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa, como las transmisiones de voz o vídeo.

1.3.2.1.3. La capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias, así que no se incluyeron. La experiencia con el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayor parte de las aplicaciones.

Encima de la capa de transporte está la capa de aplicación, que contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de terminal virtual (TELNET), el de transferencia de archivos (FTP) y el de correo electrónico (SMTP). El protocolo de terminal virtual permite que un usuario en una máquina ingrese en una máquina distante y trabaje ahí. El protocolo de transferencia de archivos ofrece un mecanismo para mover datos de una máquina a otra en forma eficiente. El correo electrónico fue en sus orígenes sólo una clase de transferencia de archivos, pero más adelante se desarrolló para él un protocolo especializado; con los años, se le han añadido muchos otros protocolos, como el servicio de nombres de dominio (DNS) para relacionar los nombres de los nodos con sus direcciones de la red; NNTP, el protocolo que se usa para transferir artículos noticiosos; HTTP, el protocolo que se usa para recuperar páginas en la *World Wide Web* y muchos otros.

1.3.2.1.4. La capa del nodo a la red

Bajo la capa de interred está un gran vacío. El modelo de referencia TCP/IP realmente no dice mucho de lo que aquí sucede, fuera de indicar que el nodo se ha de conectar a la red

haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes de IP. Este protocolo no está definido y varía de un nodo a otro y de red a red. Los libros y artículos sobre el modelo TCP/IP rara vez hablan de él.

1.3.2.2. Comparación de los modelos de referencia OSI y TCP/IP

Los modelos de referencia OSI y TCP/IP tienen mucho en común. Ambos se basan en el concepto de un gran número de protocolos independientes. También la funcionalidad de las capas es muy similar. Por ejemplo, en ambos modelos las capas por encima de la de transporte, incluida ésta, están ahí para prestar un servicio de transporte de extremo a extremo, independiente de la red, a los procesos que deseen comunicarse. Estas capas forman el proveedor de transporte. También en ambos modelos, las capas encima de la de transporte son usuarios del servicio de transporte orientados a aplicaciones.

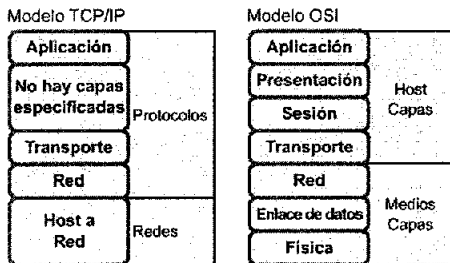


Fig. 1.10 Comparación entre OSI y TCP/IP

A pesar de estas similitudes fundamentales, los dos modelos tienen también muchas diferencias. Es importante notar que aquí estamos comparando los *modelos de referencia*, no las *pilas de protocolos* correspondientes. En el modelo OSI, tres conceptos son fundamentales:

1. Servicios.
2. Interfaces.
3. Protocolos.

Es probable que la contribución más importante del modelo OSI sea hacer explícita la distinción entre estos tres conceptos. Cada capa presta algunos servicios a la capa que se encuentra sobre ella. La definición de *servicio* dice lo que la capa hace, no cómo es que las entidades superiores tienen acceso a ella o cómo funciona la capa.

La *interfaz* de una capa les dice a los procesos de arriba cómo acceder a ella; especifica cuáles son los parámetros y qué resultados esperar; nada dice tampoco sobre cómo trabaja la capa por dentro.

Finalmente, los *protocolos* puros que se usan en una capa son asunto de la capa. Ésta puede usar los protocolos que quiera, siempre que consiga que se realice el trabajo (esto es, que provea los servicios que ofrece). La capa también puede cambiar los protocolos a voluntad sin afectar el *software* de las capas superiores.

Estas ideas ajustan muy bien con las ideas modernas acerca de la programación orientada a objetos. Al igual que una capa, un objeto tiene un conjunto de métodos (operaciones) que los procesos pueden invocar desde fuera del objeto. La semántica de estos métodos define

el conjunto de servicios que ofrece el objeto. Los parámetros y resultados de los métodos forman la interfaz del objeto. El código interno del objeto es su protocolo y no está visible ni es de la incumbencia de las entidades externas al objeto. "

El modelo TCP/IP originalmente no distinguía en forma clara entre servicio, interfaz y protocolo, aunque se ha tratado de reajustarlo después a fin de hacerlo más parecido a OSI. Por ejemplo, los únicos servicios reales que ofrece la capa de interred son SENT IP PACKET Y RECIVE IP PACKET para enviar y recibir paquetes de IP, respectivamente.

Como consecuencia, en el modelo OSI se ocultan mejor los protocolos que en el modelo TCP/IP y se pueden reemplazar con relativa facilidad al cambiar la tecnología. La capacidad de efectuar tales cambios es uno de los principales propósitos de tener protocolos por capas en primer lugar.

El modelo de referencia OSI se desarrolló *antes* de que se inventaran los protocolos. Este orden significa que el modelo no se orientó hacia un conjunto específico de protocolos, lo cual lo convirtió en algo muy general. El lado malo de este orden es que los diseñadores no tenían mucha experiencia con el asunto y no supieron bien cuál funcionalidad poner en cuál capa.

Por ejemplo, la capa de enlace de datos originalmente tenía que ver sólo con redes de punto a punto. Cuando llegaron las redes de difusión, se tuvo que insertar una nueva subcapa en el modelo. Cuando la gente empezó a construir redes reales haciendo uso del modelo OSI y de los protocolos existentes, descubrió que no cuadraban con las especificaciones de servicio requeridas, de modo que se tuvieron que injertar en el modelo subcapas de convergencia que permitieran "tapar" las diferencias. Por último, el comité esperaba originalmente que cada país tuviera una red controlada por el gobierno que usara los protocolos OSI, de manera que no se pensó en la interconexión de redes.

Lo contrario sucedió con TCP/IP: primero llegaron los protocolos, y el modelo fue en realidad sólo una descripción de los protocolos existentes. No hubo el problema de ajustar los protocolos al modelo; se ajustaban a la perfección. El único problema fue que el *modelo* no se ajustaba a ninguna otra pila de protocolos; en consecuencia, no fue de mucha utilidad para describir otras redes que no fueran del tipo TCP/IP.

Una diferencia obvia entre los dos modelos es la cantidad de capas: el modelo OSI tiene siete capas y el TCP/IP cuatro. Ambos tienen capas de (inter)red, de transporte y de aplicación, pero las otras capas son diferentes.

Otra diferencia se tiene en el área de la comunicación sin conexión frente a la orientada a la conexión. El modelo OSI apoya la comunicación tanto sin conexión como la orientada a la conexión en la capa de red, pero en la capa de transporte donde es más importante (porque el servicio de transporte es visible a los usuarios) lo hace únicamente con la comunicación orientada a la conexión. El modelo TCP/IP sólo tiene un modo en la capa de red (sin conexión) pero apoya ambos modos en la capa de transporte, con lo que ofrece una alternativa a los usuarios. Esta elección es importante sobre todo para los protocolos simples de petición y respuesta.

1.4. Puentes y los Switches

Los puentes y los switches son dispositivos de comunicación de datos que operan

principalmente en la capa dos del modelo OSI, son ampliamente conocidos como dispositivos de la capa de enlace. Los puentes se encontraron disponible por primera vez en los 80's al inicio los puentes conectaban y enviaban paquetes a través de dos redes homogéneas, actualmente los puentes entre diferentes redes se han definido y estandarizado. Hoy en día surge una nueva tecnología switches basado principalmente en soluciones de internetworking, con mayor flexibilidad a menor costo por puerto.

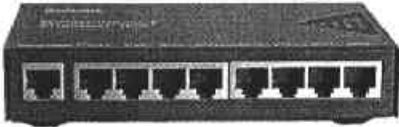


Fig. 1.11 Switch de 8 puertos

1.4.1. Dispositivos de la capa de enlace

Los puentes y switches funcionan en la capa de enlace, los cuales controlan el flujo de información, provee direccionamientos físicos y administran los accesos al medio físico, los puentes provee estas funciones por medio de los protocolos de enlace que especifican algoritmos de flujo de información, de direccionamiento y de acceso al medio ejemplos de protocolos populares incluye Ethernet, FDDI, y Token Ring.

La transparencia de los protocolos de las capas superiores es una ventaja principal tanto de los puentes como de los switches. Porque ambos dispositivos funcionan en la capa de enlace, no necesitan examinar la información de las capas superiores. Esto quiere decir que estos dispositivos pueden enviar rápidamente el tráfico representado por un protocolo de red.

Puente: dispositivo de capa 2 diseñado para conectar dos segmentos LAN. El propósito de un puente es filtrar el tráfico de una LAN, para que el tráfico local siga siendo local, pero permitiendo la conectividad a otras partes (segmentos) de la LAN para enviar el tráfico dirigido a esas otras partes. La forma en que se verifica la dirección local. Cada dispositivo de networking tiene una dirección MAC exclusiva en la NIC, el puente rastrea cuáles son las direcciones MAC que están ubicadas a cada lado del puente y toma sus decisiones basándose en esta lista de direcciones MAC.

Los puentes no son dispositivos complejos. Analizan las tramas entrantes, toman decisiones de envío basándose en la información que contienen las tramas y envían las tramas a su destino. Los puentes sólo se ocupan de pasar los paquetes, o de no pasarlos, basándose en las direcciones MAC destino. Los puentes a menudo pasan paquetes entre redes que operan bajo distintos protocolos de Capa 2.



1.4.2. Los switches

Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC destino, los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

La conmutación Ethernet aumenta el ancho de banda disponible en una red. Esto se hace creando segmentos de red dedicados, o conexiones punto a punto, y conectando estos segmentos en una red virtual dentro del switch. Este circuito de red virtual existe sólo cuando se

deben comunicar dos nodos. Esto se denomina *circuito virtual* ya que existe sólo cuando es necesario y se establece dentro del switch.

Aunque el switch de LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch se encuentran todavía en el mismo dominio de broadcast, por lo tanto, un broadcast desde un nodo será visto por todos los demás nodos conectados a través del switch de LAN.

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuerto; este proceso se denomina *microsegmentación*. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host.



1.5. Los routers

Los routers están diseñados para interconectar múltiples redes. Esta interconexión permite que las máquinas de diferentes redes se comuniquen entre sí. Las redes interconectadas pueden estar colocadas o dispersas geográficamente. Las redes que están geográficamente dispersas están habitualmente interconectadas mediante una WAN. Las WAN están formadas por muchas tecnologías distintas, incluyendo los routers, los servicios de transmisión y los controladores de línea. Lo que hace indispensable al router es su capacidad para interconectar redes en una WAN.

Un router es un dispositivo de red inteligente que funciona predominantemente en las tres primeras capas del modelo de referencia OSI. Los routers, al igual que los hosts, son en realidad capaces de actuar en las siete capas del modelo de referencia OSI. Dependiendo de su configuración particular, puede utilizar o no las siete capas de funcionalidad. Sin embargo, las necesidades de las tres primeras capas es virtualmente universal. La comunicación a través de las dos primeras capas permite que los routers se comuniquen directamente con las LAN (construcción de la capa de enlace de datos). Más importante aún es que los routers pueden identificar rutas a través de redes basándose en las direcciones de la Capa 3. Esto permite que los routers interconecten múltiples redes utilizando el direccionamiento de la capa de red, sin tener en cuenta lo cerca o lejos que puedan estar unos de otros.

Entender los routers y el enrutamiento necesita examinar un router desde dos perspectivas distintas: la física y la lógica. Desde una perspectiva física, los routers contienen miríadas de partes, cada una de las cuales tiene una función específica. Desde una perspectiva lógica, los routers realizan muchas funciones, incluyendo encontrar otros routers en la red, conocer las redes de destino potenciales y los hosts, descubrir y seguir rutas potenciales y enviar datagramas hacia un destino especificado. Juntos, estos componentes físicos y funciones lógicas le permiten construir y utilizar internetworks, incluidas las WAN.

1.5.1. Componentes físicos

Un router es un dispositivo extraordinariamente complejo. Su complejidad yace en su máquina de enrutamiento (la lógica que permite que el dispositivo físico realice varias funciones de enrutamiento). La complejidad de la lógica de enrutamiento está oculta por la relativa simplicidad de la forma física del router. El tipo más común de routers actualmente un tipo de computadora altamente especializada; contiene los mismos componentes básicos que otras computadoras. Entre estos componentes se incluyen los siguientes:

- . Una unidad central de procesamiento (CPU).
- . Memoria de acceso aleatorio (RAM)

- . Un sistema básico de entrada / salida (810S).
- . Un sistema operativo (OS).
- . Una placa madre.
- . Puertos físicos de entrada / salida (E/S).
- . Una fuente de energía, un chasis y una "cubierta metálica".

La gran mayoría de los componentes de un router permanecen siempre ocultos a los ojos de los administradores de redes por la cubierta metálica del chasis. Estos componentes son extremadamente fiables y, en condiciones normales de funcionamiento, no deberían ver la luz del día. Las excepciones obvias a esta visión general se están expandiendo. En el momento en que necesite añadir más recursos al router, tendrá que quitar esta cubierta. Normalmente, dichos recursos incluyen memoria o puertos de E/S.

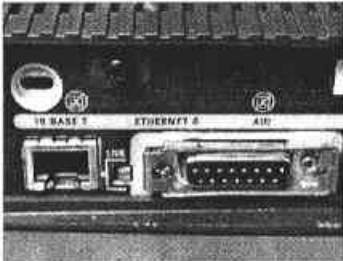


Fig. 1.12 Parte posterior de un Router

Los componentes con los que más frecuentemente se encontrará un administrador de redes son el sistema operativo y los puertos de E/S. El sistema operativo de un router es el software que controla los distintos componentes hardware y los hace utilizables. La mayoría de los administradores de redes utilizan una interfaz de línea de comandos para desarrollar una configuración lógica. La configuración es un perfil del sistema: los números, las posiciones, los tipos de cada puerto E/S, y detalles tales como la información de direccionamiento y de ancho de banda. La configuración de un router también puede incluir información de seguridad como a qué usuarios les está permitido acceder a puertos de E/S específicos y modos de configuración.

Los puertos de E/S son el único componente físico del router que los administradores de redes ven en su rutina. Los puertos confirman la capacidad única del router para interconectar aparentemente combinaciones infinitas de tecnologías de transmisión LAN y WAN. Cada una de éstas, LAN o WAN, debe tener su propio puerto de E/S en el router. Estos puertos funcionan como una tarjeta de interfaz de red (NIC) en una computadora conectada a una LAN; están relacionados con el medio y los mecanismos de entramado esperados y proporcionan las interfaces físicas apropiadas. Muchas de estas interfaces físicas se parecen bastante entre sí. Este parecido físico contradice las diferencias entre las funciones de capa superior de estas tecnologías. Por tanto, es más útil examinar las tecnologías de transmisión que examinar las interfaces físicas específicas.

1.5.2. Funciones de un router.

Igual de importantes que proporcionar Interconectividad física para múltiples redes son las funciones lógicas que realiza un router. Estas funciones hacen que las interconexiones físicas se puedan utilizar. Por ejemplo, las comunicaciones entre redes necesitan que al menos una ruta física interconecte las computadoras de origen y destino. Sin embargo, tener y utilizar una ruta física son dos cosas muy diferentes. Específicamente, las computadoras de origen y destino deben hablar un lenguaje común (un protocolo enrutado), También ayuda el hecho de si los routers que están entre ellas también hablan un lenguaje común (un protocolo de enrutamiento) y coinciden en cuál es la mejor ruta física. Además, algunas de las funciones más sobresalientes que puede proporcionar un router son éstas:

- Interconectividad física.
- Interconectividad lógica.
- Cálculo y mantenimiento de una ruta.
- Seguridad.

1.5.2.1. Interconectividad física

Un router tiene un mínimo de dos (y frecuentemente muchos más) puertos de E/S físicos. Los puertos de E/S, o interfaces, como son más conocidos, se utilizan para conectar físicamente servicios de transmisión de red a un router. Cada puerto se conecta a una placa de circuitos que está conectada a la placa madre del router. Por tanto, la placa madre en realidad proporciona Interconectividad entre múltiple redes.

El administrador de la red debe configurar cada interfaz mediante la consola del router. La configuración incluye la definición del número de puertos de la interfaz del router, la tecnología de transmisión específica y el ancho de banda disponible en la red conectada a esa interfaz, y los tipos de protocolos que se utilizarán a través de esa interfaz. Los parámetros que se deben definir varían según el tipo de interfaz de red.

1.5.2.2. Interconectividad lógica

Una interfaz de routers se puede activar tan pronto como sea configurada. La configuración de la interfaz identifica el tipo de servicio de transmisión al que está conectada, la dirección IP de la interfaz y la dirección de la red a la que está conectada. A partir de la activación de un puerto, el router comienza a controlar inmediatamente todos los paquetes que se están transmitiendo por la red conectada al nuevo puerto activado. Esto le permite "conocer" las direcciones IP de la redes y los hosts que residen en la redes que se pueden alcanzar mediante ese puerto. Estas direcciones están almacenadas en tablas llamadas tablas de enrutamiento. Las tablas de enrutamiento correlacionan el número de puerto de cada interfaz del router con las direcciones de capa de red que se pueden alcanzar (directa o indirectamente) mediante ese puerto.

También se puede configurar un router con una ruta predeterminada. Una ruta predeterminada asocia una interfaz de router específica con una dirección de destino desconocida. Esto permite que un router envíe un datagrama a destinos que todavía no conoce. Las rutas predeterminadas también se pueden utilizar de otras formas. Por ejemplo, se pueden utilizar para minimizar el crecimiento de las tablas de enrutamiento, o para reducir la cantidad de tráfico generado entre routers mientras éstos intercambian información de enrutamiento.

1.5.2.3. Cálculo y mantenimiento de una ruta

Los routers se comunican entre sí utilizando un protocolo predeterminado, un protocolo de enrutamiento. Los protocolos de enrutamiento permiten que los routers hagan lo siguiente:

- Identificar rutas potenciales a redes de destino específicas.
- Realizar un cálculo matemático, basado en el algoritmo del protocolo de enrutamiento, para determinar la ruta óptima a cada destino.
- Controlar continuamente la red para detectar cualquier cambio en la topología que pueda representar rutas conocidas no válidas.

Existen muchos tipos distintos de protocolos de enrutamiento. Algunos, como el Protocolo de información de enrutamiento (RIP), son bastante sencillos. Otros, como el protocolo

Primero la ruta libre más corta (OSFP), son extremadamente potentes y ricos en elementos, pero complicados. En general, los protocolos de enrutamiento pueden optar por dos planteamientos para tomar decisiones de enrutamiento: vectores de distancia y estados de enlace. Un protocolo de enrutamiento por vector de distancia toma decisiones basándose en algunas medidas de la distancia entre las computadoras de origen y destino. Un protocolo de estado de enlace basa sus decisiones en varios estados de los enlaces, o servicios de transmisión, que interconectan las computadoras de origen y destino. Ninguna es correcta o errónea: sólo son formas distintas de tomar decisiones. Sin embargo, ofrecen diferentes niveles de rendimiento, incluyendo los tiempos de convergencia.

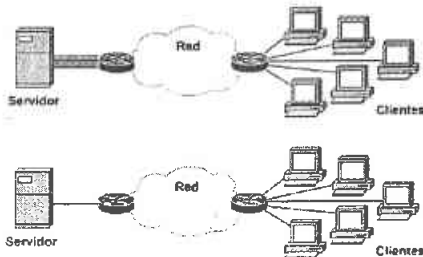


Fig. 1.13 Rutas en Internet

Puede evaluar los protocolos de enrutamiento empleando varios criterios más específicos que sólo los planteamientos que utilizan. Algunos de los criterios con más sentido son los siguientes:

- **Punto óptimo.** Describe la capacidad de un protocolo de enrutamiento para seleccionar la mejor ruta disponible. Por desgracia, la palabra "mejor" es ambigua. Existen distintas formas de evaluar rutas diferentes para un destino dado. Cada forma podría dar como resultado la selección de una ruta "mejor" diferente dependiendo de los criterios empleados. Los criterios que utilizan los protocolos de enrutamiento para calcular y evaluar las rutas se llaman métricas de enrutamiento. Se utiliza una amplia variedad de métricas, y varían ampliamente según el protocolo de enrutamiento. Una métrica sencilla es el número de saltos, es decir el número de saltos, o routers, que hay entre las computadoras de origen y destino.
- **Eficiencia.** Otro criterio a considerar cuando se evalúan protocolos de enrutamiento es su eficiencia operacional. La eficiencia operacional se puede medir examinando los recursos físicos, incluyendo la RAM del router y el tiempo de CPU; y el ancho de banda de la red necesario para un cierto protocolo de enrutamiento. Puede que necesite consultar al fabricante o vendedor del router para determinar las eficiencias relativas de los protocolos que va a considerar.
- **Resistencia.** Un protocolo de enrutamiento debería actuar de forma fiable en todo momento, no sólo cuando la red sea estable. Las condiciones de error, incluidos los fallos del hardware o de los servicios de transmisión, errores de configuración del router y cargas fuertes de tráfico, afectan adversa mente a la red. Por tanto, es primordial que un protocolo de enrutamiento funcione correctamente durante los periodos de fallos o inestabilidad de la red.
- **Convergencia.** Debido a que son dispositivos inteligentes, los routers pueden detectar automáticamente cambios en la internetwork. Cuando se detecta un cambio, todos los routers implicados deben converger en un nuevo acuerdo sobre la topología de la red y volver a calcular las rutas a los destinos conocidos de acuerdo a este cambio. Este proceso de alcanzar un acuerdo mutuo se llama convergencia. Cada protocolo de enrutamiento emplea mecanismos distintos para detectar y comunicar cambios en la red. Por tanto, cada uno converge a una

velocidad diferente. En general cuanto más lentamente converge un protocolo de enrutamiento, mayor es la posibilidad de que se interrumpa el servicio a través de la internetwork.

- Escalabilidad. La escalabilidad de una red es su capacidad para crecer. Aunque el crecimiento no sea un requisito en las organizaciones, el protocolo de enrutamiento que seleccione debería poder escalarse para cumplir el crecimiento proyectado para la red.

1.6. Ejemplos de Tecnologías de red

1.6.1. Tecnologías de Ethernet

El término Ethernet se refiere a la familia de red de área local (LAN), estas tienen aplicaciones que incluyen tres categorías principales.

- Ethernet y IEEE 802.3—LAN especificaciones que operan a 10 Mbps encima del cable coaxial.
- 100-Mbps Ethernet— especificación de LAN, también conocida como Fast Ethernet que opera, 100 Mbps encima del cable del par trenzado.
- 1000-Mbps Ethernet—especificación de LAN, también conocida como Gigabit Ethernet que opera, a 1000 Mbps (1 Gbps) encima de fibra y cables de par trenzado.

La arquitectura de red Ethernet se originó en la Universidad de Hawai durante los años setenta, donde se desarrolló el método de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD), utilizado actualmente por Ethernet. El centro de investigaciones PARC (Palo Alto Research Center) de la Xerox Corporation desarrolló el primer sistema Ethernet experimental a principios del decenio 1970-80. Este sistema sirvió como base de la especificación 802.3 publicada en 1980 por el Institute of Electrical and Electronic Engineers (IEEE).

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m	Estrella	Bus
1000Base-T	UTP Cat 5	1000 Mbps	100 m	Estrella	Bus

Tabla 1.1 Cronología de Ethernet

Poco después de la publicación de la especificación IEEE 802.3 en 1980, Digital Equipment Corporation, Intel Corporation y Xerox Corporation desarrollaron y publicaron conjuntamente una especificación Ethernet denominada "Versión 2.0" que era sustancialmente compatible con la IEEE 802.3. En la actualidad, Ethernet e IEEE 802.3 retienen en conjunto la mayor parte del mercado de protocolos de LAN. Hoy en día, el término Ethernet a menudo se usa para referirse a todas las LAN de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD), que generalmente cumplen con las especificaciones Ethernet, incluyendo IEEE 802.3.

Ethernet e IEEE 802.3 especifican tecnologías similares; ambas son LAN de tipo CSMA/CD. Las estaciones de una LAN de tipo CSMA/CD pueden acceder a la red en cualquier

momento. Antes de enviar datos, las estaciones CSMA/CD escuchan a la red para determinar si se encuentra en uso. Si lo está, entonces esperan. Si la red no se encuentra en uso, las estaciones comienzan a transmitir. Una colisión se produce cuando dos estaciones escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde. Los algoritmos de postergación determinan el momento en que las estaciones que han tenido una colisión pueden volver a transmitir. Las estaciones CSMA/CD pueden detectar colisiones, de modo que saben en qué momento pueden volver a transmitir.

Tanto las LAN Ethernet como las LAN IEEE 802.3 son redes de broadcast. Esto significa que cada estación puede ver todas las tramas, aunque una estación determinada no sea el destino propuesto para esos datos. Cada estación debe examinar las tramas que recibe para determinar si corresponden al destino. De ser así, la trama pasa a una capa de protocolo superior dentro de la estación para su adecuado procesamiento.

7	1	6	2	46-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección Destino	Dirección Origen	Tipo	Datos
					Secuencia de verificación de trama

7	1	6	2	46-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección Destino	Dirección Origen	Longitud	Embalaje de datos IEEE 802.3
					Secuencia de verificación de trama

Fig. 1.14 Formato de trama Ethernet y IEEE 802.3

Existen diferencias sutiles entre las LAN Ethernet e IEEE 802.3. Ethernet proporciona servicios correspondientes a la Capa 1 y a la Capa 2 del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física, o sea la Capa 1, y la porción de acceso al canal de la Capa 2 (de enlace), pero no define ningún protocolo de Control de Enlace Lógico. Tanto Ethernet como IEEE 802.3 se implementan a través del hardware. Normalmente, el componente físico de estos protocolos es una tarjeta de interfaz en un computador host o son circuitos de una placa de circuito impreso dentro de un host. Ethernet ha sobrevivido como una tecnología de los medios de comunicación esencial debido a su tremenda flexibilidad y su simplicidad relativa para llevar a cabo y entender. Aunque otras tecnologías se han aclamado como reemplazos probables, gerentes de la red se han vuelto a Ethernet y sus derivados como eficaces soluciones para un rango los requisitos de aplicación de campus. Para resolverse las limitaciones de Ethernet, innovadores (y cuerpos de las normas) ha creado cañerías de Ethernet progresivamente más grandes. Los críticos pueden despedir a Ethernet como una tecnología que no puede descansar, pero su esquema de la transmisión subyacente continúa para ser uno de los medios principales para transportar datos de las aplicaciones del campus.

1.6.2. Tecnologías de Token ring

IBM desarrolló la primera red Token Ring en los años setenta. Todavía sigue siendo la tecnología de LAN principal de IBM, y desde el punto de vista de implementación de LAN ocupa el segundo lugar después de Ethernet (IEEE 802.3).

La especificación IEEE 802.5 es prácticamente idéntica a la red Token Ring de IBM, y absolutamente compatible con ella. La especificación IEEE 802.5 se basó en el Token Ring de IBM y se ha venido evolucionando en paralelo con este estándar. El término Token Ring se refiere tanto al Token Ring de IBM como a la especificación 802.5 del IEEE. En el gráfico principal se destacan las similitudes y diferencias principales entre los dos estándares.

Los datos en Token-Ring se transmiten a 4 ó 16mbps, depende de la implementación que se haga. Todas las estaciones se deben de configurar con la misma velocidad para que

funcione la red. Cada computadora se conecta a través de cable Par Trenzado ya sea blindado o no a un concentrador llamado MSAU y aunque la red queda físicamente en forma de estrella, lógicamente funciona en forma de anillo por el cual da vueltas el Token. En realidad es el MSAU es que contiene internamente el anillo y si falla una conexión automáticamente la ignora para mantener cerrado el anillo.



Fig. 1.15 Transmisión de Tokens de Token Ring

Tokens

Los tokens tienen una longitud de 3 bytes y están formados por un delimitador de inicio, un byte de control de acceso y un delimitador de fin. El delimitador de inicio alerta a cada estación ante la llegada de un token o de una trama de datos/comandos. Este campo también incluye señales que distinguen al byte del resto de la trama al violar el esquema de codificación que se usa en otras partes de la trama.

Byte de control de acceso.

El byte de control de acceso contiene los campos de prioridad y de reserva, así como un bit de token y uno de monitor. El bit de token distingue un token de una trama de datos/comandos y un bit de monitor determina si una trama gira continuamente alrededor del anillo. El delimitador de fin señala el fin del token o de una trama de datos/comandos. Contiene bits que indican si hay una trama defectuosa y una trama que es la última de una secuencia lógica.

Tramas de datos/comandos.

El tamaño de las tramas de datos/comandos varía según el tamaño del campo de información. Las tramas de datos transportan información para los protocolos de capa superior; las tramas de instrucciones contienen información de control y no poseen datos para los protocolos de capa superior.

En las tramas de datos o instrucciones hay un byte de control de trama a continuación del byte de control de acceso. El byte de control de trama indica si la trama contiene datos o información de control. En las tramas de control, este byte especifica el tipo de información de control.

A continuación del byte de control de trama hay dos campos de dirección que identifican las estaciones destino y origen. Como en el caso de IEEE 802.5, la longitud de las direcciones es de 6 bytes. El campo de datos está ubicado a continuación del campo de dirección. La longitud de este campo está limitada por el token de anillo que mantiene el tiempo, definiendo de este modo el tiempo máximo durante el cual una estación puede retener al token.

A continuación del campo de datos se ubica el campo de secuencia de verificación de trama (FCS). La estación origen completa este campo con un valor calculado según el contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado mientras estaba en tránsito. Si la trama está dañada se descarta. Como en el caso del token, el delimitador de fin completa la trama de datos/comandos

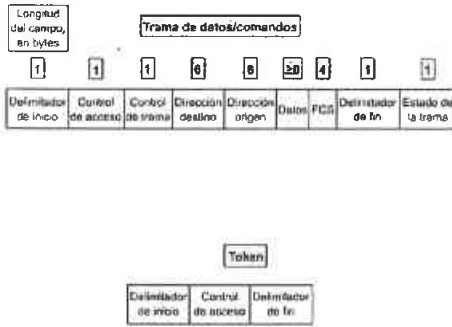


Fig. 1.16 Formato Token Ring

Prioridad de sistema

La red Token Ring usa un sistema de prioridad la cual se puede decir que usuarios tienen más prioridad, esto es cuando una máquina tiene prioridad, no importa donde está el token, sino que automáticamente el token pasa a él y puede transmitir, cuando dos o más dispositivos tienen la misma prioridad entonces entre los dispositivos, nuevamente, funciona el token entre ellos.

Transmisión de tokens.

Token Ring e IEEE 802.5 son los principales ejemplos de redes de transmisión de tokens. Las redes de transmisión de tokens transportan una pequeña trama, denominada token, a través de la red. La posesión del token otorga el derecho a transmitir datos. Si un nodo que recibe un token no tiene información para enviar, transfiere el token a la siguiente estación terminal. Cada estación puede mantener al token durante un período de tiempo máximo determinado, según la tecnología específica que se haya implementado.

Cuando una estación que transfiere un token tiene información para transmitir, toma el token y le modifica 1 bit. El token se transforma en una secuencia de inicio de trama. A continuación, la estación agrega la información para transmitir al token y envía estos datos a la siguiente estación del anillo. No hay ningún token en la red mientras la trama de información gira alrededor del anillo, a menos que el anillo acepte envíos anticipados del token. En este momento, las otras estaciones del anillo no pueden realizar transmisiones. Deben esperar a que el token esté disponible. Las redes Token Ring no tienen colisiones. Si el anillo acepta el envío anticipado del token, se puede emitir un nuevo token cuando se haya completado la transmisión de la trama.

La trama de información gira alrededor del anillo hasta que llega a la estación destino establecida, que copia la información para su procesamiento. La trama de información gira alrededor del anillo hasta que llega a la estación emisora y entonces se elimina. La estación emisora puede verificar si la trama se recibió y se copió en el destino.

A diferencia de las redes CSMA/CD (acceso múltiple con detección de portadora y detección de colisiones), como Ethernet, las redes de transmisión de tokens son determinísticas. Esto significa que se puede calcular el tiempo máximo que transcurrirá antes de que cualquier estación terminal pueda realizar una transmisión. Esta característica, y varias características de confiabilidad, hacen que las redes Token Ring sean ideales para las aplicaciones en las que cualquier demora deba ser predecible y en las que el funcionamiento sólido de la red sea importante. Los entornos de automatización de fábricas son ejemplos de operaciones de red que deben ser sólidas y predecibles.

2. REDES VIRTUALES DE AREA LOCAL (VLAN)

2.1. Introducción

En el anterior capítulo se dio una visión general de lo son las redes LAN, MAN y WAN, para poder comprender ahora el funcionamiento de las VLANs (Redes Virtuales de Área Local). Este capítulo proporciona una visión acerca del funcionamiento, configuración y administración de las VLANs visto a manera específica de estándar como tal, el IEEE 802.1 Q.

Mostrando de manera teórica las ventajas que una VLAN ofrece realizadas en la capa de *Enlace de Datos* del modelo de referencia OSI; realizando segmentación de dominios de colisión, por lo que la comunicación será más eficiente debido a que la carga en el Router (capa 3 del modelo de referencia OSI) es menor y por consiguiente más rápida.

Una VLAN es un agrupamiento lógico de dispositivos o usuarios. Estos dispositivos o usuarios se pueden agrupar por función, departamento, aplicación, etc., independientemente de su ubicación física en un segmento como se muestra en la figura 2.1. La configuración VLAN se hace en el switch a través de software.

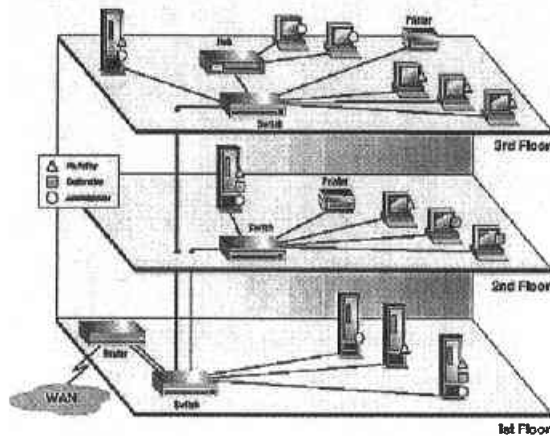


Fig. 2.1 Una VLAN es un agrupamiento independientemente de su ubicación física

A lo largo de este capítulo se mostrara mas a grandes rasgos la forma en que se conforma una VLAN.

2.2. IEEE 802.1Q-1998

Las actividades de estandarización de la capa de enlace de datos es donde se encuentran el direccionamiento físico (MAC) que fue diseñado por la ISO/IEC introduciendo el concepto de servicios de filtrado en LAN, con mecanismos de filtrado de direcciones y de bases de datos.

ISO/IEC 15802-3, la revisión de ISO/IEC 10038, extendieron el concepto de Servicio de Filtrado en Switchs LAN adicionando capacidades a los puentes y/o switches:

1. El de facilitar la capacidad de tráfico, para soportar la transmisión de información en tiempo crítico en la LAN
2. El uso de señalamientos de prioridad de información con identificaciones básicos de acuerdo a las clases de tráfico;
3. El servicio de filtrado que pueda soportar la definición dinámica y establecimiento de grupos de trabajo, y el filtrado de tramas por switches de acuerdo a las direcciones de los participantes del grupo y solo estas tendrán acceso a los segmentos de LAN de acuerdo al orden y alcance de los miembros de cada grupo.
4. El uso del Protocolo Genérico de Registro de Atributos (GARP) para soporte de los mecanismos que proveen la capacidad de filtrado de grupos, y solo esta hecho para usar otro atributo de registro en las aplicaciones.

Este estándar hace uso de los conceptos y mecanismos de *LAN Switching* que fue introducido por la ISO/IEC 15802-3, además define los mecanismos que se usan en la implementación de "*Switching LAN Virtual*" o *LAN Virtuales*; y son las siguientes:

5. Servicios Virtuales en LAN Switching;
6. La operación del *Proceso de Envío* que es requerido para dar soporte a *Switching LAN Virtual*;
7. La estructura del filtrado de la Base de Datos para soportar *LAN Virtuales*;
8. La naturaleza de los protocolos y procesos en el orden en que son requeridos para dar soporte a los servicios de VLANs, incluyendo la definición del formato de tramas para representar la información de identificación de VLANs, y los procesos usados en orden para insertar y borrar identificadores y encabezados de VLANs cada vez que son transportados;
9. La habilidad para soportar señalamiento de fin-a-fin con prioridad de información de usuario indiferentemente de la dirección MAC, con los protocolos de señalamiento de prioridad de información;
10. El *Protocolo de Registro de VLAN GARP* (GVRP) que permite la distribución y registro de información de miembros de la VLAN (ISO/IEC 15802-3);
11. La administración y operación de servicios para configurar y administrar *Switching LAN Virtual*.

El Estándar IEEE 802 referente a Redes de Área Local (LAN) de todos tipos pueden ser conectadas junto con los Switches con Control de Acceso al Medio (MAC), especificada en ISO/IEC 15802-3. Este estándar define la operación de las Redes de Área Local Virtuales (VLANs) Puentes que permiten la definición, operación y administración de topologías VLAN con infraestructura Switch LAN.

2.3. Arquitectura de VLAN

- La arquitectura de toda la trama de VLAN esta basada en un modelo de tres capas:
 - *Configuración*;
 - *Distribución de información de configuración*;
 - *Transmisión*.

2.3.1. *Configuración*: la configuración se interesa por los siguientes problemas:

- a) La configuración usa diferentes medios en los que se puede archivar vía local y/o remota por administración, vía servidores, vía protocolos de distribución, o vía otros medios. El almacenamiento de la configuración esta fuera del alcance de este estándar por lo que no será tocado.
- b) Asignación de parámetros de configuración VLAN.

2.3.2. *Distribución de información de configuración*: este proceso permite la distribución de la información para los Switchs, para ser capaz de determinar cual trama VLAN debería ser clasificada.

2.3.3. *Transmisión*: contiene los siguientes mecanismos de:

- a) Clasificación de cada trama recibida como perteneciendo a una y solo a una VLAN. Este aspecto de transmisión esta determinada por la configuración de las *reglas de ingreso* de un Switch MAC;
- b) Decisiones relacionadas a las tramas recibidas que deben ser enviadas. Este aspecto de la transmisión está determinado de acuerdo a la configuración de las *reglas de envío* del Switch MAC;
- c) Mapeando tramas para transmisión a través del puerto de salida apropiado, y un apropiado formato ya sea VLAN etiquetada o sin etiqueta. Estos aspectos de transmisión son determinados por la configuración de las *reglas de salida* de un Switch MAC;
- d) Los procesos usados para agregar, modificar y remover los encabezados de etiqueta, cuando transmiten tramas seguidas de segmentos LAN, de acuerdo con los detalles de los formatos de la trama VLAN usados para *VIDs* (referido a las etiquetas VLAN).

Las reglas de ingreso, envío y salida permite al Switch a:

- e) Clasificar cualquier trama recibida ya sea con *etiqueta de prioridad* o *sin etiqueta de prioridad* sometidas al "Proceso de Envío" como si perteneciera a una VLAN en particular, como esta definido en el PVID para el puerto receptor.
- f) Clasifica cualquier trama de "VLAN etiquetada" que son sometidas a el "Proceso de Envío" como si perteneciera a la VLAN identificada por el VID llevado en el encabezado de etiqueta;
- g) Hace uso de la clasificación de la VLAN de esta manera lo asocia con la trama recibida en orden para tomar la decisión apropiada de envío/filtrado;
- h) Transmite tramas de formato *VLAN etiquetado* o *sin etiqueta*, definido para dar aparear al Puerto a la VLAN.

2.3.4. Arquitectura del Filtrado de la Base de Datos

La arquitectura del "Filtrado de la Base de Datos" definida en el estándar reconoce que

- a) Para algunas configuraciones, es necesario permitir que las direcciones aprendan información en una VLAN para compartir entre un número de VLANs. Esto es conocido como *Aprendizaje Compartido de VLAN*;
- b) Para algunas configuraciones, esto es deseable para asegurar que la información de dirección sea aprendida en una VLAN y no sea compartida con otras VLANs. Esto es conocida como *Aprendizaje Independiente de VLAN*;
- c) Para algunas configuraciones, esto es indiferente si la información aprendida es compartida entre VLANs o no.

Compartir lo aprendido en una VLAN es archivado para incluir la información aprendida de un número de VLANs en la Base de Datos; *Aprendizaje Independiente de VLAN* es archivado para incluir información de cada VLAN en distintos *Filtros de Bases de Datos*.

Dentro de un LAN con VLAN Switchheada, puede haber una combinación de requisitos de configuración, para que los Switches de VLAN individuales puedan ser llamadas para compartir la información conocida, o no, según los requisitos de VLANs particulares o grupos de VLANs. La estructura de Base de Datos de Filtración en que está definida esta norma permite a la *VLAN-compartida* y la *VLAN de Aprendizaje Independiente* a ser llevado a cabo dentro del mismo Switch VLAN; es decir, permite compartir la información conocida entre estas VLANs pero solo usando la información necesaria para el direccionamiento de cada una. Los requisitos precisos para cada VLAN con respecto a compartir o independizar la información conocida es dada a conocer a los Switches VLAN por medio de la configuración de *Aprendizaje de VLAN*, que puede configurarse en los Switches por medio del funcionamiento de la dirección. Analizando las configuraciones que deben realizar las VLANs que están actualmente activas, el switch puede determinar:

- d) Cuántos "Filtros de la Base de Datos" independientes se exigen para encontrarse las ordenes que debe realizar;
- e) Por cada VLAN, en que los *Filtros de la Base de Datos* cargan cualquier información aprendida dentro (y usa la información aprendida).

El resultado es que cada VLAN es asociada con exactamente un Filtro de Base de Datos. Generalmente la mayoría de las aplicaciones del Filtro de Base de Datos que pueden soportar "m" independientes Filtros de Base de Datos, y pueden mapear "n" VLANs sobre cada Filtro de Base de Datos. Semejante a un switch es conocido como un Switch SVL/IVL.

De acuerdo a los requerimientos en este estándar reconoce que el Switch VLAN pueda ser implementado por diferentes capacidades en orden para encontrarse un amplio rango que necesita la aplicación, y que generalmente lleno el SVL/IVL próximo estos ambos no siempre son necesarios o deseables. El espectro completo de acuerdo a la implementación del Filtro de la Base de Datos es como sigue:

- f) El SVL/IVL Switch, como se describió anteriormente, tal switch provee soporte para M Filtros de Base de Datos, con la habilidad de mapear "n" VLANs en cada una;
- g) Soporte para un único Filtro de Base de Datos. La información de dirección MAC es aprendida en una VLAN pudiendo ser usadas en las decisiones de filtrado relativamente en

todas las otras VLANs soportadas por el Switch. Los switches que soportan un solo Filtro de Base de Datos son conocidos como SVL Switches.

- h) Soporte para múltiples Filtros de Bases de Datos, pero solo una VLAN puede ser mapeada sobre cada Filtro. La información de la dirección MAC es aprendida en una VLAN y no puede ser usada para filtrar decisiones tomadas relativamente para alguna otra VLAN. Los switches que soportan este modo de operación son conocidas como Switches IVL.

2.3.5. Clasificación de VLAN

La tecnología de VLAN introduce los tres tipos básicos de tramas:

- a) *Tramas sin etiqueta;*
- b) *Tramas con prioridad de etiqueta;* y
- c) *Tramas VLAN-etiquetadas.*

Una trama sin etiqueta o tramas con prioridad de etiqueta no carga alguna identificación de la VLAN a la cual pertenece. Semejantes tramas son clasificadas como pertenecientes a una VLAN en particular basada en parámetros asociados con el puerto receptor, o, a través de una extensión propietaria del estándar, basada en el contenido de dato en la trama (dirección MAC, ID de capa 3, etc.).

Una trama VLAN etiquetada carga una identificación explícita de la VLAN a la cual pertenece; carga una etiqueta en el encabezado que lleva un VID no nulo. Tal trama es clasificada a una VLAN en particular basándose en el valor del VID que esta incluido en el encabezado de la trama. La presencia del encabezado de la trama transporta un VID no nulo mediante algún otro dispositivo, cualquier creador de la trama o de un Switch VLAN-enterada, hace mapeo dentro de esta trama VLAN e inserta el VID apropiado.

2.3.6. Reglas para marcar Tramas

Para marcar una VLAN, todas las tramas transmiten en un segmento de VLAN dada por una VLAN enterada Switch debe marcar el mismo camino del segmento. Estas deben ser cualquiera:

- a) Todas desetiquetadas; o
- b) Todas las VLAN etiquetadas con el mismo VID.

2.3.7. Spanning Tree

Este estándar define en entorno en donde una VLAN opera en un sencillo "Spanning Tree". Todos los switches dentro de la infraestructura de un Switch LAN participa un "Spanning Tree" sencillo, como lo define la ISO/IEC 15802-3, donde múltiples VLAN pueden coexistir. Como una consecuencia, los switches implementados de acuerdo con ISO/IEC 15802-3 pueden estar integrados en la infraestructura de una VLAN basada en la especificación que contiene este estándar.

El objetivo primario del "Spanning Tree" es:

- a) Eliminación de bucles en la infraestructura de un Switch;
- b) Mejorar escalabilidad a lo largo de una red;
- c) Proveer de rutas redundantes, con las que puede ser activado en caso de falla.

Aquí están dos importantes elementos con respecto a la topología de Spanning Tree; Primero, el Spanning Tree formado en un ambiente VLAN necesita no ser idéntico a la topología de las VLANs. Todas las VLANs son alineadas a lo largo del Spanning Tree con el que estas son formadas; una VLAN dada esta definida por una subconfiguración de la topología del Spanning Tree en el cual este opera.

Segundo, la topología de una VLAN dinámica. La estructura de una VLAN puede cambiar debido a nuevos dispositivos-solicitados o descargados los servicios avalados por la VLAN. El carácter dinámico de VLANs tiene la ventaja de flexibilidad y conservación de ancho de banda, en el costo de administrar la complejidad de la red.

2.4. Soporte del Servicio MAC en VLANs

2.4.1. El Reforzamiento Interno de la Subcapa de Servicio (E-ISS)

Es derivado de una *Subcapa Interna de Servicio (ISS)* para argumentar la especificación con elementos necesarios para la operación de etiquetado y desetiquetado funciones del Switch MAC. Dentro de la estación final adjuntada, estos elementos pueden ser considerados para estar cualquiera bajo el límite del servicio MAC, y pertinentemente solo la operación del proveedor de servicio; o el local importante formando parte del par-a- par del servicio natural de la MAC.

Los switches que soportan estas funciones son conocidas como switches VLAN-enterados. El E-ISS define el Servicio MAC proveído para la función de retardo en switches VLAN-enterado. La unidad de datos primitivos que definen el servicio son:

```
Indicación EM_UNITDATA: {
    frame_type,
    mac_action,
    destination_address,
    source_address,
    mac_service_data_unit,
    user_priority,
    frame_check_sequence,
    canonical_format_indicator,
    vlan_identifier,
    rif_information (opcional)
}
```

Cada dato indica su primitiva correspondiente a la recepción de un *M_UNITDATA* indicando la primitiva de la *Subcapa Interna de servicio*, como lo define en la ISO/IEC 15802-3. Los parámetros "*frame_type*, *mac_action*, *destination_address*, *source_address*, *mac_service_data_unit*, *user_priority* y la *frame_check_séquence*" están definidos por el *M_UNITDATA* indicando la primitiva de la *Subcapa Interna de servicio*.

El parámetro "*canonical_format_indicator*" indica si incluye la dirección MAC transportada en el parámetro "*mac_service_data_unit*" son en formato Canónico o formato No-Canónico. El valor falso indica formato No-Canónico. El valor verdadero indica formato Canónico.

El parámetro "*vlan_identifier*" lleva el identificador VLAN asociado con el indicador. El parámetro "*rif_information*" se presenta si una etiqueta de encabezado esta presentado en el indicador, y si la etiqueta del encabezado contiene Campo de Información de Ruteo (Routing Information Field RIF). Este valor es igual al valor de RIF.

```
EM_UNITDATA.request (petición) {
    frame_type,
    mac_action,
    destination_address,
    source_address,
    mac_service_data_unit,
    user_priority,
    access_priority,
    frame_check_sequence,
    canonical_format_indicator,
    vlan_classification,
    rif_information (optional),
    include_tag
}
```

Una petición de datos primitiva se invocada para generar un "*M_UNITDATA. Request*" primitiva, como lo define la *Subcapa Interna de Servicio*, ISO/IEC 15802-3. Los parámetros "*frame_type*, *mac_action*, *destination_address*, *source_address*, *mac_service_data_unit*, *user_priority*, *access_priority*, y la *frame_check_séquence*" están definidos por el "*M_UNITDATA. Request*" primitiva de la *Subcapa Interna de servicio*. La definición del parámetro "*canonical_format_indicator*" esta definido por "*EM_UNITDATA. Indication*".

El parámetro "*vlan_classification*" lleva la clasificación VLAN asignada para la trama por la reglas de ingreso.

El parámetro "*rif_information*", si se presenta, lleva el valor de alguna información RIF para ser asignada con la petición.

El parámetro "*incluye_tag*" lleva un valor Booleano. Verdadero indica para el proveedor de servicio que el parámetro "*mac_service_data_unit*" del dato de petición debe incluir una etiqueta en el encabezado. Falso indica que la etiqueta del encabezado no debe ser incluido.

Soporte del E-ISS en Switch VLAN-enterado

- Indicación de Datos primitivos: En la recepción de un indicador de datos de la Subcapa Interna de Servicio, un "*EM_UNITDATA.indication*" primitivo es invocado, con los valores del parámetro como sigue:

Los parámetros "*frame_type*, *mac_action*, *destination_address*, *source_address*, y *frame_check_séquense*" llevan valores iguales al parámetro correspondiente en la recepción del indicador de datos.

El valor del parámetro "*mac_service_data_unit*" es determinado como:

- a) Si el parámetro recibido "*mac_service_data_unit*" contenido en un encabezado etiquetado, cuando el valor usado es igual al valor recibido del "*mac_service_data_unit*" acto seguido quita el encabezado etiquetado. Por otra parte;
- b) El valor usado es igual al valor de "*mac_service_data_unit*" recibido.

El valor del parámetro es determinado como "*user_priority*":

- c) Si el parámetro "*mac_service_data_unit*" recibido contiene un encabezado etiquetado, cuando el valor contenido en el campo "*user_priority*" del encabezado etiquetado es usado. Por otra parte;
- d) El valor del parámetro recibido "*user-priority*", regenerado y usado.

El valor del parámetro es determinado como "*canonical_format_indicator*":

- e) Si el parámetro recibido "*mac_service_data_unit*" contuviera un encabezado etiquetado, entonces el valor(es) contenido en el *Indicador del Formato Canónico* (CFI) (y el Indicador del Formato No-canónico [NCFI], si el presente campo del encabezado etiquetado determinan este valor del parámetro se usan, de acuerdo con la definición del CFI y el campo *NCFI*. Por otra parte;
- f) Si la entidad de MAC que recibió la indicación de los datos fuera un ISO/IEC 8802-5 Token Ring MAC, entonces, el parámetro lleva el valor Falso. Por otra parte;
- g) El parámetro lleva el valor verdadero.

El valor del parámetro es determinado como "*vlan_identifier*":

- h) Si los octetos iniciales del parámetro recibido "*mac_service_data_unit*" contuvieran un título de la etiqueta, entonces el valor contenido en el campo VID del encabezado etiquetado se usa. Por otra parte;
- i) Un valor igual al VLAN ID nulo es usado.

El valor del parámetro es determinado como "*rif_information*":

- j) Si los octetos iniciales del parámetro recibido "*mac_service_data_unit*" contuvieran un encabezado etiquetado, y este contuvo un campo de RIF en el cuál uno o más descripciones de la ruta estaban presentes, entonces, el valor contenido en el campo de RIF se usa. Por otra parte;
- k) El parámetro no esta presente.

Para la *Petición de datos primitivos* por un usuario de E-ISS, un "*M-UNITDATA.request*" primitivo es invocado, con el valor de los siguientes parámetros:

Los parámetros "*frame_type*, *mac_action*, *destination_address*, *source_address*, *user_priority*, y *access_priority*" llevan los valores igual a los parámetros correspondientes en la demanda de los datos recibidos.

Si el valor del parámetro del "*include_tag*" es Falso, el valor del parámetro "*mac_service_data_unit*" es determinado como sigue:

- a) Si el destino del método MAC está igual al método MAC en que los datos corresponden a la indicación recibida, entonces el valor usado es igual al valor del parámetro "*mac_service_data_unit*" recibido en la demanda de los datos. Por otra parte;

- b) El valor usado es igual al valor del parámetro "*mac_service_data_unit*" recibido en los datos pedidos, modificados, si necesario, de acuerdo con los procedimientos descritos en ISO/IEC 11802-5, IETF RFC 1042, e IETF RFC 1390.
- c) Si el parámetro "*canonical_format_indicator*" indica que el "*mac_service_data_unit*" puede contener la dirección de MAC incluida en un formato inapropiado al destino del método MAC, entonces el switch debe:
 - 1) Convertir cualquier dirección MAC incluido el "*mac_service_data_unit*" al formato apropiado al destino del método MAC; o
 - 2) Descartar los datos de EISS pedidos sin emitir una ISS correspondiente a los datos demandados.

Si el valor del parámetro "*incluye_tag*" es Verdad, entonces una etiqueta del encabezado, formateado como el requisito para el destino MAC, se inserta como los primeros "n" octetos del parámetro "*mac_service_data_unit*". Los valores "*user_priority*", "*canonical_format_indicator*", "*vlan_classification*", y "*rif_information*" (si está presente) se usan los parámetros para determinar el contenido de la etiqueta del encabezado. El valor insertado después de que la etiqueta del encabezado es determinada como sigue:

- d) Si el método de MAC destino está igual al método MAC en que los datos corresponden a la indicación recibida, entonces el valor usado es igual al valor del parámetro recibido "*mac_service_data_unit*" en la demanda de los datos. Por otra parte;
- e) El valor usado es igual al valor del parámetro recibido "*mac_service_data_unit*" en los datos pedidos, modificado, si necesario, de acuerdo con los procedimientos descritos en ISO/IEC 11802-5, IETF RFC 1042, e IETF RFC 1390.

El valor del parámetro es determinado como "*frame_check_séquence*":

- f) Si el parámetro recibido "*frame_check_séquence*" en la demanda de los datos es no especificado o inmóvil lleva un valor válido, entonces ese valor se usa. Por otra parte;
- g) El valor usado o se deriva de la información de FCS recibida por la modificación para tomar la cuenta de las condiciones que lo han causado para ponerse no válido, o el valor no especificado es usado.

2.4.2. Soporte del Servicio de Subcapa Interior por IEEE Std. 802.3 (CSMA/CD)

Además de las provisiones de ISO/IEC 15802-3, en el recibo de un "*M_UNITDATA.request*" primitivo representa una trama etiquetada, la implementación permite adoptar ambos los acercamientos siguientes con respecto al funcionamiento de Transmisión de Datos Encapsulados para tramas cuya longitud habría, mientras usando el procedimiento como descrito, esté menos de 68 octetos:

- a) Use el procedimiento como descrito en ISO/IEC 15802-3, 6.5.1. Esto puede producir tramas etiquetadas de menos que 68 octetos (pero por lo menos 64 octetos) transmitiéndose; o
- b) Incluya octetos adicionales antes del campo FCS en orden para la transmisión a lo largo de la trama para ser tramas de 68 octetos. Esto produce una mínima trama etiquetada con una longitud de 68 octetos.

Cuando una trama etiquetada de menos de 68 octetos de longitud se recibe en un segmento CSMA/CD de LAN, y se remite cuando una trama sin etiqueta, las provisiones de ISO/IEC 15802-3, producen octetos adicionales siendo incluido ante el campo FCS en la transmisión en orden que la trama transmitida se encuentre el mínimo los requisitos de tamaño de marco de IEEE Std 802.3, 1998 Edición.

2.5. Principios de Operación

Este punto establece los principios de funcionamiento de un Switch VLAN-enterado, por la referencia al modelo de funcionamiento, como sigue:

- a) Explica los elementos principales de funcionamiento del Switch y una lista de funciones que soportan éstos.
- b) Establece a un modelo arquitectónico para un Switch que gobierna la provisión de estas funciones.

- c) Proporciona un modelo de funcionamiento de un Switch en lo que se refiere a los procesos y entidades que soportan las funciones.
- d) Detalles de los direccionamientos requeridos en un LAN Switch y especifica el direccionamiento de entidades en un Switch.

Los aprovisionamientos de esta cláusula reemplazan los aprovisionamientos de ISO/IEC 15802-3, en un Switch VLAN-enterado.

2.5.1. Funcionamiento del Switch

Los elementos principales de funcionamiento del Switch son:

- a) Transmisión y filtrado de tramas.
- b) Mantenimiento de la información requerida para hacer filtración de tramas y las decisiones de transmisión.
- c) Administración de lo anterior.

2.5.1.1 Transmisión

Un Switch transmite los datos individuales del usuario entre las MACs separadas por el Switch LAN conectado a sus Puertos. Las funciones que apoyan la transmisión de tramas y mantienen la Calidad de Servicio son

- a) La recepción de trama.
- b) Descartar una trama recibida con ISO/IEC 15802-3.
- c) Trama descartada si el "frame_type" no es "user_data_frame"; o si su parámetro es "mac_activo" no es "request_with_no_response" (ISO/IEC 15802-3).
- d) Regeneración de prioridad del usuario, si es requerida (ISO/IEC 15802-3).
- e) Trama descartada siguiendo la aplicación de filtraje de información.
- f) Trama descartada en transmisión de servicio de unidad de datos con tamaño excedido.
- g) Reenvío de tramas recibidas a otros puertos del switch.
- h) Selección de clase de tráfico, siguiendo la aplicación de filtraje de información.
- i) Haciendo cola de tramas por la clase de tráfico.
- j) Descarte de tramas para asegurar que un retraso de tránsito máximo en el switch no se exceda.
- k) Selección de tramas hechos cola para la transmisión.
- l) Selección de prioridad de acceso a la salida.
- m) Mapeado de unidades de datos de servicio y re-cálculo de Verificación de Secuencia de Trama, si es requerido.
- n) Transmisión de trama.

2.5.1.2 Filtrando y Trasmisión de información

Un Switch filtra las tramas, es decir, no transmite tramas recibidas por un Puerto del Switch a otros Puertos en ese Switch, de tal forma que previene la duplicación de tramas. La función que soporta el uso y el mantenimiento de información para este propósito es:

- a) Calcular y configurar la topología de una LAN Switchheada.

Un Switch también filtra las tramas para reducir el tráfico en las partes de la LAN Switchheada que no esta en el camino entre la fuente y destino de ese tráfico. Las funciones que soportan el uso y mantenimiento de la información para este propósito es:

- b) La configuración permanente de direcciones reservadas.
- c) La configuración explícita de información de filtración estática.
- d) El aprendizaje automático de información de filtración dinámica para una dirección "unicast" destino que se dirige a través de la observación de direcciones fuente de tráfico de la LAN Switchheada.
- e) Información vieja fuera de la filtración dinámica que ya era conocida.
- f) La suma automática y removimiento de información de la filtración dinámica como resultado del protocolo de GMRP respecto a los intercambios.

Un Switch clasifica las tramas en clases de tráfico para apresurar la transmisión de tramas generada críticamente o los servicios dependientes del tiempo. La función que apoya el uso y mantenimiento de información para esto el propósito es:

- g) La configuración explícita de tráfico de clase de información asociada con los puertos del Switch.

Un Switch clasifica las tramas no etiquetadas y prioridad de tramas etiquetadas por pertenecer a un VLAN en particular de acuerdo con las reglas del ingreso. La función que apoya el uso y mantenimiento de información para este propósito es:

- h) La configuración explícita del Puerto VID (PVID) asociado con cada puerto del Switch.

Un Switch puede filtrar las tramas para prevenir la inyección de tramas sin etiqueta y tramas con prioridad de etiqueta en un puerto en que la recepción de tramas sin etiqueta y tramas con prioridad de etiqueta se desaprueba. La función que apoya el uso y mantenimiento de información para este propósito son:

- i) La configuración explícita del parámetro de Tipos de Trama Aceptable asociado con cada puerto del Switch.

Un Switch puede filtrar tramas en orden para prevenir la inyección de tráfico para una VLAN dada en un puerto en que esa VLAN es desaprobada. La función que apoya el uso y mantenimiento de información para este propósito es:

- j) La configuración explícita del parámetro de Filtro de Ingreso Habilitado que es el asociado con cada puerto del Switch.

Un Switch filtra las tramas para confinar tráfico destinado para un VLAN dada a segmentos de LAN que forman un camino de la fuente del tráfico a destinatarios que son miembros de esta VLAN. Las funciones que apoyan el uso y mantenimiento de información para este propósito son el:

- k) La configuración automática del Registro de Entradas Dinámicas a la VLAN por medio de GVRP;
- l) La configuración explícita de administración de controles asociados con el funcionamiento de GVRP por medio del Registro de Entradas estáticas a la VLAN;
- m) El aprendizaje Automático de direcciones MAC en VLANs asociadas a través de la observación del tráfico de red.

Un Switch adiciona y remueve etiquetas en los encabezados de las tramas, y hace la asociación de traslado que pueda ser requerida de acuerdo a las reglas de egreso que será explicada mas adelante.

2.5.2. Arquitectura del Switch

En la arquitectura de un switch LAN los componentes están interconectados mediante los puentes MAC, cada puerto de un Switch tiene una MAC y esta conectada a una LAN como se muestra en la figura 2.2. El modelo de un switch consiste de:

- a) Una MAC identidad que interconecta los puertos del switch: cada puerto del switch hace las funciones de transmisión, filtrado de tramas y aprendizaje de información de filtraje usando la subcapa de servicio interna para cada puerto y así las tramas son enviadas a diferentes puertos para diferentes LANs.
- b) Por lo menos dos puertos: cada puerto transmite y recibe tramas de diferentes LANs, una MAC identidad permanece asociada con los puertos de la Subcapa Interna de Servicio usada para transmisión y recepción de tramas.
- c) Altas entidades de capas, incluyendo por lo menos un protocolo de identidad de switch: que regularmente es GARP que hace uso de los procesos de la capa LLC (Control de Acceso Lógico); servicios que son proveídos por cada puerto usando el servicio MAC individualmente cada uno.

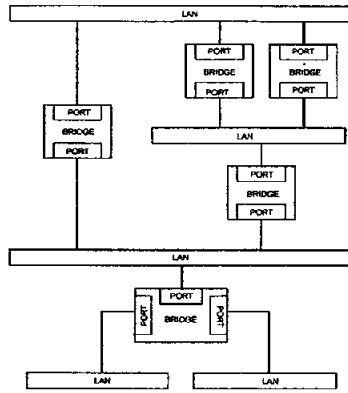


Fig.2.2 Ejemplo de un Switch LAN

2.5.3. Modelo de Operación.

Este describe el funcionamiento básico de un switch ya que sus funciones suelen variar de acuerdo a los diferentes fabricantes, en la figura 2.3 se muestra la arquitectura de un Switch con VLAN:

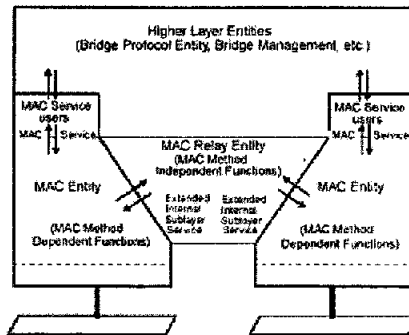


Fig.2.3 Arquitectura de un Switch VLAN

Las tramas son aceptadas para transmitir y entregar al receptor y para el proceso de identidad del modelo de operación de la Transmisión MAC Entidad en un Switch. Estos son:

- Las reglas de ingreso con la clasificación de las tramas recibida de acuerdo a los miembros de la VLAN, podrían filtrar tramas basadas en el VID de la trama recibida o también basadas en el identificador de la VLAN.
- El proceso de reenvío de tramas recibidas que vienen de otro puerto del switch, filtrando tramas basándose en la información contenida en la base de datos del filtro y en el estado de los puertos del switch.
- Las reglas de egreso donde se determina a que puerto serán enviadas las tramas y en que formato.
- Aprendiendo el proceso en el que se observa la dirección MAC fuente y los VIDs de las tramas clasificadas por las reglas de ingreso, actualizando la base de datos del filtro condicionadas en el estado del puerto.
- La base de datos del filtro con el que se puede filtrar la información y soporta preguntas por el proceso de reenvío de tramas de acuerdo a los valores del campo de la dirección MAC y VID puede ser reenviado al puerto dado.

También cada puerto del switch hace funciones de estaciones finales dando servicio MAC al LLC, con el que se soporta la operación del Protocolo de Entidad y de otros posibles usuarios de LLC, como protocolos proveídos para administración del Switch.

2.5.4. Estado de Puertos, Parámetro de Puertos, Puertos Activos y la topología activa.

El estado de la información esta asociada con cada puerto del switch, un puerto puede ser deshabilitado por el administrador sino forma parte de la operación del switch LAN, un puerto no puede ser deshabilitado dinámicamente excluyéndose si participa en el algoritmo de Spanning Tree.

Aprendiendo estados: la incorporación de la información de ubicación de estaciones finales en la base de datos del filtro pasa por un proceso de aprendizaje que depende de la topología activa. Si la información asociada con las tramas recibidas en un puerto son incorporadas en la base de datos del filtro para el proceso de aprendizaje, cuando el puerto es descrito como sigue en un estado de aprendizaje; de otra forma esto esta dentro de un proceso de no aprendizaje.

Tipos de Tramas Aceptadas: asociadas con cada puerto de un Switch VLAN el parámetro de Tipos de Tramas Aceptadas que controla la recepción de la trama etiquetada de la VLAN y de la trama no etiquetada de VLAN en el puerto. Los valores para este parámetro son:

- a) *Admite solo tramas etiquetadas de VLAN:* en la configuración de este parámetro cualquier trama recibida que no lleva VID es descartada por las reglas de ingreso. Las tramas que no son descartadas como resultado del valor de este parámetro son clasificadas y procesadas de acuerdo a las reglas de ingreso aplicadas para el Puerto.
- b) *Admitir Todas las Tramas.*

Cada Puerto del Switch debe soportar por lo menos uno de estos valores, y poder soportar ambos. Donde los dos valores son soportados.

- c) La implementación debe soportar el poder configurar el valor del parámetro por medio de operación del administrador; y
- d) El valor del parámetro por defecto debe *admitir todas las tramas.*

Identificador de puerto VLAN: en un puerto basado en la clasificación VLAN dentro de un Switch, el VID asociado con una trama sin etiqueta o prioridad de etiqueta se determina, basándose en el puerto de donde arriba la tramas dentro del Switch. Este mecanismo de clasificación requiere ser asociado a la especificación del VLAN ID, el *Identificador de puerto VLAN*, o *PVID*, con cada puerto del Switch. El PVID por cada puerto debe contener un valor valido de VID, y debe no contener el valor de VLAN ID nulo, este debe ser configurado por el administrador, si la operación de administración es soportada para la implementación, sino es así el PVID debe asumir el valor de PVID de defecto.

Habilitar el Filtro de Ingreso: este parámetro esta asociado con cada puerto y debe descartar cualquier trama recibida en el Puerto donde la clasificación VLAN no incluye en que configuración es miembro. Si el parámetro de restablecer para el puerto, las reglas de ingreso no debe descartar las tramas recibidas en el puerto basadas en su clasificación VLAN básica. El valor por defecto es *restablecer* es decir esta Deshabilitado el Filtro de Ingreso en todos los puertos y este puede ser configurado por medio de las operaciones de administración.

2.5.5. Recepción de trama

La MAC Entidad asociada con cada puerto del Switch examina todas las tramas recibidas en la LAN que es adjuntada. Todas las tramas recibidas libre de errores dan pie a la indicación "EM_UNITDATA" primitiva la cual debe ser tomada para ser adjuntada. Todas las tramas recibidas libres de errores dan cabida a la indicación para "EM_UNITDATA" primitiva.

Las tramas con "frame_type" de "user_data_frame" y direccionamiento para el Puerto del Switch como una estación final serán sometidas al usuario para Servicio MAC. Tramas semejantes llevan ambas la dirección de MAC individual del Puerto o un grupo de direcciones asociadas con el Puerto en el campo de dirección destino. Las tramas sometieron al servicio MAC el usuario también puede someterse a las reglas del ingreso.

El direccionamiento de tramas a un puerto del Switch como una estación del final, y transmitida a ese puerto del Switch el mismo Switch por el Proceso de Envío, también se someterá al Servicio MAC de usuario.

Ningún otra trama se someterá al Servicio MAC de usuario.

- a) Regenerando la prioridad de usuario: la recepción de la trama de prioridad de usuario es regenerada usando prioridad de información que contiene la trama y Regenerando la Tabla de Prioridad de Usuario por el puerto receptor. Por cada puerto receptor la regeneración de la tabla tiene ocho entradas, correspondientes a ocho posibles valores de "user_priority" (entre 0-7) (ver tabla 2.1). Cada entrada específica, por dar un valor de recepción de "user_priority", que corresponde al valor regenerado de "user_priority".

Prioridad de Usuario	Regeneración de prioridad de usuario por defecto	Rango
0	0	0-7
1	1	0-7
2	2	0-7
3	3	0-7
4	4	0-7
5	5	0-7
6	6	0-7
7	7	0-7

Tabla 2.1. Regeneración de usuario prioridad

2.5.6. Reglas de Ingreso

Cuando el parámetro que soporta el identificador VLAN en una indicación de datos recibida es igual al VLAN ID nulo y el parámetro de los Tipos de Tramas Aceptables por el puerto en el que la trama fue recibida se establece al valor *Admitir Solamente tramas etiquetadas VLAN*, entonces la trama será descartada. Cada trama que se recibe de un Switch VLAN es clasificada como perteneciente a una VLAN asociando un valor VID con la trama recibida.

- a) Si el parámetro que contiene el identificador VLAN en una indicación de datos recibidos es el VLAN ID nulo, entonces:
 - Cuando los soportes de implementación sean más lejanos a las reglas de clasificación del VLAN así como la clasificación Puerto-basado, y si la aplicación de estas reglas asocian el valor de un VID que no es nulo con la trama, el valor de aquel VID será usado.
 - Cuando la implementación mantenga solamente clasificación Puerto-basado, o alguna otra regla adicional de clasificación no sean capaces de ser asociadas con el VID que no es nulo con la trama, entonces será usado el valor del PVID asociado con el puerto por el cual fue recibida la trama.
- b) Cuando el parámetro que contiene el identificador VLAN en una indicación de datos recibida no es el VLAN ID nulo, entonces será utilizado el valor del parámetro del identificador VLAN.

El valor del VID que así sea identificado, conocido como la *clasificación VLAN* de la trama, será utilizado como el valor del parámetro de cualquier solicitud de datos correspondiente. Todas las tramas que no sean descartadas como resultado de la aplicación de las reglas de ingreso serán sometidas al Proceso de Envío.

2.5.7. Proceso de Envío (Forwarding Process)

Las tramas que son sometidas a el *Proceso de Envío* después de ser recibidas por cualquier puerto de Switch dado será enviado a través de otros puertos del Switch sujetos a las funciones componentes del *Proceso de Envío*. Estas funciones hacen cumplir restricciones topológicas, utilizando información de *Filtering Database* para filtrar tramas, poner en filas de espera las tramas, seleccionar las tramas en fila de espera para la transmisión, prioridades de mapa, y volver a calcular el FCS si se necesita.

- a) Cumpliendo con la restricción topológica: se selecciona a cada puerto como un Puerto de transmisión potencial, solamente si se cumplen los siguientes puntos:

- El puerto en el que se recibió la trama se encontraba en estado de expedición,
 - El puerto considerado para la transmisión está en estado de expedición,
 - El puerto considerado para la transmisión no es el mismo Puerto que recibió la trama.
 - El tamaño del "mac_service_data_unit" transportado por la trama no excede el tamaño del "mac_service_data_unit" apoyado por el LAN con un Puerto considerado para transmitir está adjunto.
- b) Filtrando tramas: las decisiones de filtrado son tomadas por el *Proceso de Envío* en base a:
- A la dirección MAC destino llevado en una trama recibida
 - El VID asociado con la trama recibida
 - La información contenida en el Filtro de la Base de Datos para aquélla dirección MAC y VID
 - El defecto del comportamiento del Grupo de filtrado para el Puerto de transmisión potencial
- c) Poniendo tramas en fila de espera: el *Proceso de Expedición* puede dar almacenaje a las tramas que se encuentran en estado de espera, las que en cualquier oportunidad para someterse a la transmisión de Entidades MAC individuales asociadas con cada puerto del Switch; el orden de tramas recibidas en un mismo puerto del Switch se mantiene de acuerdo a dos clasificaciones, las tramas sin un "user_priority" dado para una combinación dada de la dirección destino y una dirección de origen, y las tramas agrupadas en direcciones con un "user_priority" dado para la dirección destino que se de.
- El *Proceso de Expedición* puede otorgar más de una transmisión para una fila de espera de acuerdo al puerto del Switch dado, y para organizar las tramas en las filas de espera se utiliza una tabla que contiene información sobre el tipo de tráfico y esta es asociada con la información de cada puerto.
- d) Elijiendo tramas para transmisión: se utiliza un algoritmo que es apoyado por todos los puentes para seleccionar las tramas para transmitir, y esta determinado como sigue:
- Las tramas son elegidas para transmisión de acuerdo a las bases del tipo de clases que pueda soportar el Puerto, que irá administrando las tramas de acuerdo a sus valores.
 - Cuando las tramas sean elegidas en una fila de espera deberán mantener el orden requerido de acuerdo con la tabla 2. 2.
- e) Prioridad de Mapeo: el mapeo de prioridad de usuario que lleva la prioridad de acceso de salida se realiza de una manera constante. El parámetro de prioridad de acceso en un "EM_UNITDATA" pedido se determina de la prioridad de usuario de acuerdo con los valores que se encuentran en la tabla 2.2, los cuales no pueden ser modificados bajo ninguna circunstancia.

Prioridad de usuario	Prioridad de Acceso de Salida por método MAC								
	802.3	8802-4	8802-5 Predet.	8802-5 alternativa	8802-6	802.9a	8802.11	8802-12	FDDI
0	0	0	0	4	0	0	0	0	0
1	0	1	1	4	1	0	0	0	1
2	0	2	2	4	2	0	0	0	2
3	0	3	3	4	3	0	0	0	3
4	0	4	4	4	4	0	0	4	4
5	0	5	5	5	5	0	0	4	5
6	0	6	6	6	6	0	0	4	6
7	0	7	6	6	7	0	0	4	6

Tabla 2.2. Prioridad de acceso de Salida

f) R e c á l

culo de FCS: Donde la trama es remitida entre dos Entidades individuales MAC del mismo tipo de IEEE 802 LAN y la retransmisión de la trama implica que no haya cambios en los datos dentro de la cobertura del FCS, el FCS recibido a través de la indicación "EM_UNITDATA" puede ser abastecido en la petición "EM_UNITDATA" correspondiente y no es recalculable.

Donde la trama este siendo remitida, el calculo repetido de FCS es necesario si las diferencias entre los métodos LAN MAC son tales que un FCS calculado de acuerdo a las precedencias MAC para el método del destino del MAC puede diferenciar del FCS llevado por la trama recibida, o si al retransmitir la trama implique cambios en los datos que se encuentran dentro de la cobertura del FCS.

2.5.8. Reglas de Egreso

Las tramas pueden ser filtradas o descartadas en los siguientes casos:

- El puerto de transmisión no se encuentra presente en el sistema de Miembro para el VID de la trama como lo establecen las reglas de ingreso
- El valor del parámetro de la etiqueta incluida es falso, cómo se muestra más adelante, y el Puente no soporta la habilidad de traducir información de la dirección MAC introducida para el formato indicado por el parámetro del *"canonical_format_indicator"* a el formato apropiado para el método MAC el cual soportará los datos requeridos.

El valor del parámetro *"include_tag"* en los datos requeridos se determina como sigue:

- En caso de que la transmisión del Puerto está presente en el sistema sin etiqueta para el VID de la trama, como lo determinan las reglas de ingreso, el valor será Falso. En caso de que no se cumpla esto:
- El valor será Verdadero.

2.5.9. Transmisión de la Trama

La Entidad MAC individual asociada con cada puerto del Switch transmite tramas sometidas a esta por la Entidad de Retransmisión MAC. Las tramas que son retransmitidas están sometidas para ser transmitidas por medio del *Proceso de Expedición*. El requisito primitivo *"EM_UNTIDATA"* asociado con tales tramas transporta los valores de campo de la dirección de origen y de la dirección del destino en la indicación primitiva *"EM_UNITDATA"* correspondiente. Las tramas transmitidas para transportar Unidades de los Datos del Protocolo LLC llevan la dirección individual MAC del puerto en el campo de donde proviene la dirección. Cada trama es transmitida sujeta a la procedencia MAC para ser observada por la tecnología del IEE 802 LAN. Los valores de los parámetros del tipo de trama y de la acción MAC del requisito primitivo *"EM_UNITDATA"* podrían ser datos del usuario de la trama y requisitos sin respuesta. Las tramas que al ser transmitidas siguen una petición por el usuario LLC del servicio MAC puede ser sometido a la Entidad de Retransmisión MAC.

2.5.10. Proceso de Aprendizaje

Este Proceso observa la fuente de las Direcciones MAC de las tramas que recibe cada Puerto y actualiza la Base de Datos para el Filtrado (Filtering Database) de acuerdo con el estado del Puerto receptor, se utiliza la VID asociada con la trama para asegurar la información dada de la dirección de la trama de la VLAN. El Proceso puede deducir el Puerto por el que se pueden alcanzar estaciones extremas del Switch LAN de acuerdo a la Dirección MAC y el VID de la trama recibida. Se puede crear o actualizar una Entrada de Filtrado Dinámico asociando el VID de la Trama y la Dirección MAC del Puerto en caso de que:

- El Puerto receptor de la trama se encuentre en un estado que permita aprendizaje,
- El campo originario de la dirección de la trama denote una estación extrema,
- El total del número de entradas no exceda la capacidad de la Base de Datos para el Filtrado,
- El sistema de Miembro para el VID de la trama incluya al menos un Puerto.

2.5.11. La Base de Datos de Filtración

La Base de Datos de Filtración apoya preguntas por el Proceso de Expedición si las tramas recibidas por el Proceso de Expedición, con valores de destinación MAC y VID, son remitidas a través de un Puerto de transmisión potencial, el cuál contiene información de filtrado de manera que las entradas de filtración puedan ser cualquiera de las siguientes:

- Estáticas, y explícitamente configurada por acciones de la gerencia,
- Dinámicas y automáticamente incluidas dentro de la Base de Datos de Filtración por la operación normal del puente y los protocolos que maneja

Para poder representar la información de filtrado estático para las direcciones MAC utilizamos dos tipos de entradas:

- Expedición de tramas con un destinatario en particular,
- Incluir información dinámica de filtrado asociada con Servicios de Filtrado Extendido, y el uso de esta

La Entrada de Registro de una VLAN Estática representa toda la información estática en la Base de Datos de Filtrado para las VLANs, y permite el control sobre:

- Expedición de tramas con VIDs particulares
- Incluir y/o retirar etiquetas principales en tramas remitidas
- Incluir información sobre la membresía de VLANs dinámicas y utilizarla en la Base de Datos de Filtrado

Para representar información de filtrado dinámico se utilizan tres tipos de entradas, las cuales son:

- Entradas de Filtrado Estático y Entradas de Registro de Grupo, las cuales hacen un registro de acuerdo a las Direcciones MAC de un grupo, las cuales están incluidas al igual que las VID, administradas por el protocolo GMRP
- Entradas de Filtrado Dinámico, utilizadas para especificar el Puerto en donde la Dirección MAC ha sido aprendida, sujetas a un envejecimiento y retiro por parte de la Base de Datos, además de que incluye un Identificador de Filtrado
- Entradas Estáticas y de Registro Dinámico de VLAN, utilizadas para especificar el Puerto de acuerdo con la Membresía VLAN que ha sido registrada de manera dinámica, incluyendo un identificador de VLAN, administradas por el protocolo GVRP

Los Servicios de Filtrado que ofrece un Puente determinan el comportamiento del mismo con respecto a la expedición de tramas destinadas por un grupo de Direcciones MAC. En los Puertos que manejan Servicios de Filtrado Extendido, el comportamiento de expedición por un grupo de Direcciones MAC por cada puerto y por cada VID puede ser configurada de manera estática y dinámica por medios de Entradas de Filtrado Estático y/o Entradas de Registro de Grupo que acceden a las siguientes especificaciones de Direcciones MAC:

- Todas las Direcciones de Grupo, para las que no existe una Entrada específica de Filtrado Estático,
- Todos los Grupos de Direcciones No Registradas, para las cuales no existe más Entrada específica de Filtrado Estático

No hay retiros estandarizados en el tamaño de la Base de Datos de Filtrado en una implementación para la cual se conforme con la petición de este estándar. EL PICS necesita de lo siguiente para ser especificado por una implementación dada:

- El número total de entradas que la Base de Datos de Filtrado puede soportar,
- De acuerdo a esa cifra total obtenida, el total de las Entradas de Registro de VLAN (estáticas y dinámicas) que la Base de Datos de Filtrado pueda soportar.

2.5.12. Entidad del Protocolo del Puente y Entidad de Protocolo GARP

La Entidad del Protocolo del Puente opera el Árbol que Atraviesa el Algoritmo y Protocolo. Estas Entidades cuando pertenecen a un Puente adjunto a una LAN individual en una Switch LAN se comunican intercambiando BPDUs.

Las Entidades de Protocolo GARP operan los Algoritmos y Protocolos asociados con Aplicaciones GARP apoyadas por el Puente, y consiste en el sistema de Participantes GARP para aquellas Aplicaciones GARP. Las Entidades de Protocolo GARP de Puentes adjuntos a una LAN individual en una Switch LAN se comunican intercambiando GARP PDUs.

2.5.13. Administración

Las Instalaciones Remotas de la Administración pueden ser proporcionadas por el Puente. La Administración es modelada al ser realizada por medios de la Entidad de la Administración. Los protocolos de la Administración utilizan el servicio MAC proporcionado por el Switch LAN.

2.5.14. Dirección

Todas las Entidades MAC que comunican a través de una Switch LAN usarán direcciones de 48-bits, las cuales pueden ser Direcciones Universalmente Administradas, Direcciones Localmente Administradas, o una combinación de ambas.

- Estaciones Límite. Transmiten tramas que utilizan el servicio MAC por un Switch LAN transportando la información del origen y el destino de una estación Límite, pero no transporta la dirección de un Switch.
- Puertos del Switch. Las Entidades individuales MAC asociadas con cada puerto tienen una dirección individual MAC por separado.
- Entidades del Protocolo del Switch y Entidades de Protocolo GARP. Solo reciben y transmiten BPDUs desde otra Entidad de Protocolo del Switch; las Entidades de Protocolo GARP solo transmiten y reciben GARP PDUs que están formateados de acuerdo con los requerimientos de las Aplicaciones GARP, y solo son recibidas y transmitidas desde otras Entidades de Protocolo GARP.
- Entidades de Administración. Transmiten y reciben unidades de datos de protocolo utilizando el Servicio que brindan las Entidades individuales LLC asociadas con cada Puerto, y cada uno utiliza el Servicio MAC; como miembro de dicho Servicio la Entidad de Administración es adjunta a cualquier punto del LAN en el Puente. Cuidan que las tramas no sean duplicadas utilizando una LAN sencilla que asocie una dirección única. A las Entidades de Administración se les asigna una dirección por una o más Direcciones individuales MAC en conjunto con la mayor capa identificadora de protocolos e información de dirección; lo cual identifica la Dirección de un grupo estándar MAC para un uso público el cual sirve para transportar pedidos administrativos a Entidades Administrativas asociadas con todos los Puertos adjuntos a el LAN. Esta dirección sacará múltiples respuestas de un solo Puente.
- Identificación Única de Puente. Una Dirección MAC Universalmente Administrada de 48 – bit, conocida también como Dirección del Puente, será asignada a cada puente. Esta puede ser la Dirección Individual MAC de un Puerto, en el cual el uso de la dirección de menor número es recomendado.
- Direcciones Reservadas. Aquellas tramas que contengan cualquiera de las Direcciones MAC del grupo que se muestra en la tabla 2.3, en su área de destino no sean retransmitidas por el Switch, serán configuradas por la Base de Datos Permanente, la Administración no será capaz de modificar estas entradas desde el Filtro de la Base de Datos, estos cumplen con trabajos de protocolos estándar.
- Los puntos de unión y conectividad de las entidades de las capas altas (ver figura 2.4). Las entidades de la capas altas son modeladas al ser conectadas directamente al Switch LAN a través de uno o más puntos adjuntos. De acuerdo a el punto de vista de su unión con el Switch LAN, las Entidades de las Capas Altas asociadas con un Switch pueden ser vistas como si fuesen terminales distintas, directamente conectadas a segmentos LAN atendidos por los puertos del Switch. Las Entidades de las Capas Altas, en la mayoría de los casos, compartirán los mismos puntos físicos donde se efectúa la unión utilizada por la función del Switch. El comportamiento puede ser similar a como si hubieran estado ubicados en distintas terminales con puntos de unión fuera de los puertos, de acuerdo con el punto de vista de la transmisión y recepción de tramas.

Table 8-10—Reserved addresses

Assignment	Value
Bridge Group Address	01-80-C2-00-00-00
IEEE Std 802.3, 1998 Edition, Full Duplex PAUSE operation	01-80-C2-00-00-01
Reserved for future standardization	01-80-C2-00-00-02
Reserved for future standardization	01-80-C2-00-00-03
Reserved for future standardization	01-80-C2-00-00-04
Reserved for future standardization	01-80-C2-00-00-05
Reserved for future standardization	01-80-C2-00-00-06
Reserved for future standardization	01-80-C2-00-00-07
Reserved for future standardization	01-80-C2-00-00-08
Reserved for future standardization	01-80-C2-00-00-09
Reserved for future standardization	01-80-C2-00-00-0A
Reserved for future standardization	01-80-C2-00-00-0B
Reserved for future standardization	01-80-C2-00-00-0C
Reserved for future standardization	01-80-C2-00-00-0D
Reserved for future standardization	01-80-C2-00-00-0E
Reserved for future standardization	01-80-C2-00-00-0F

Tabla 2.3. Direcciones reservadas

Las Entidades de las Capas Altas pueden tener dos clasificaciones:

- Aquellas entidades que requieren solamente de un punto de unión a el Switch LAN
- Aquellas entidades que requieren de un punto de unión por Puerto de Puente

En esta última clasificación existen otras dos categorías, que es esencial para la operación de la entidad involucrada que es capaz de asociar tramas recibidas con el segmento LAN en el cual las tramas son vistas originalmente por el Puente, con la habilidad de transmitir tramas por entidad conectadas directamente a el segmento LAN. Por lo cual se considera esencial los siguientes puntos:

- No reciben tramas por un punto de unión asociado con un puerto que ha sido retransmitidos por el Puente desde otros Puertos;
- Tramas las que sus transmisiones las envía por un punto de unión sin ser retransmitidos por el Puente a otros Puertos.

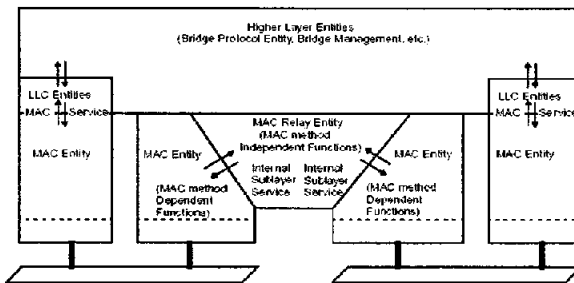


Fig 2.4. Separación lógica de puntos de unión usados por capas de entidades altas y la transmisión e MAC-entidad

Por esta razón las direcciones MAC que suelen alcanzar entidades de este tipo son configuradas de manera permanente en el Filtro de Base de Datos para evitar que el Puente vuelva a transmitir estas tramas recibidas por medio de cualquier Puerto a cualquier otro Puerto del Puente.

La Entidad de Retransmisión MAC remite una trama recibida en un Puerto a través de otro Puerto de el Puente, seguido de la información de control la cual permite este proceso:

- El estado de información del Puerto asociado con el Puerto que recibió la trama;
- La información sostenida en la Base de Datos de Filtrado;
- El estado de información del Puerto asociado con el Puerto en el cual la trama es potencialmente transmitida.

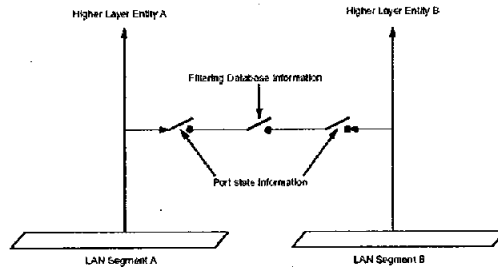


Fig. 2.5 Efecto de control de información en la ruta enviada

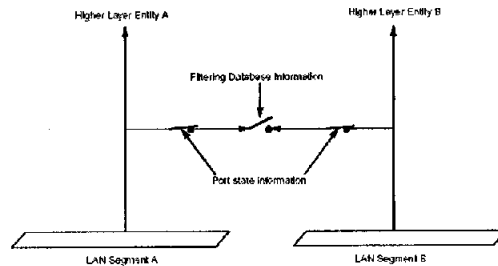


Fig. 2.6 Puntos de unión por puerto

En la figura 2.5 vemos como se ilustra lo que mencionaba de manera que el estado de Puerto representa la información control y la información de Base de Datos de Filtrado es representada por la serie de switches.

En la figura 2.4 se ilustra el estado de la trayectoria a largo plazo con respecto a las tramas destinadas por las Higher Layer Entities que necesitan por-puntos de unión con lo cual indica como un hecho que las Base de Datos de Filtrado son configuradas en todos los puertos para evitar que las tramas sean retransmitidas.

En la figura 2.5 ilustra el estado en el que la trayectoria de expedición con respecto a las tramas destinadas por las Higher Layer Entities que requieren únicamente un solo punto de unión, para el caso en el que el estado del Puerto y la Base de Datos de Filtrado permitan retransmitir las tramas.

En la figura 2.6 ilustra el estado en el que la trayectoria de expedición con respecto a las tramas destinadas por las Higher Layer Entities donde necesita únicamente de un solo punto de unión, para el caso en el que uno de los estados del Puerto no permita la retransmisión de tramas.

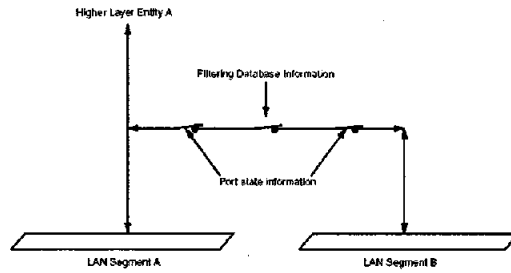
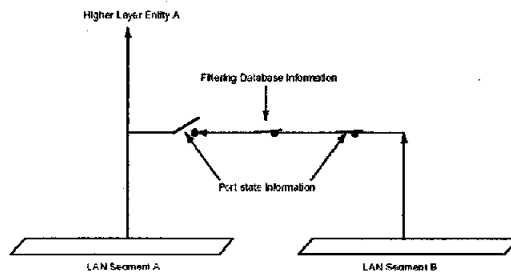
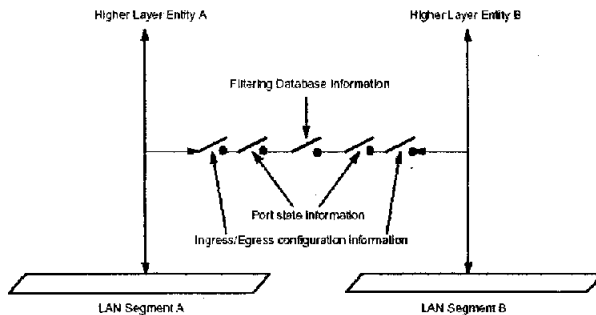


Fig. 2.5 Un solo punto de unión- transmisión permitida



2.6 Un solo punto de unión- transmisión no permitida

En el VLAN-aware Bridges, dos switches más aparecen en la trayectoria de expedición, corresponde a las reglas al ingreso y egreso mostrada en la figura 2.6.



2.6 Control de información de ingreso / egreso en la ruta de envío

Así como con el estado de información del Puerto, la configuración de las reglas de ingreso y egreso no afectan a la recepción de tramas en el mismo segmento LAN como con un punto de unión de una capa de entidad alta.

En caso de que las tramas transmitidas por capa de entidad alta sean VLAN-etiquetada o sin etiqueta la decisión dependerá sobre la capa de entidad alta en cuestión, y la relación que esta requiere

- El *Spanning Tree BPDUs* transmitido por la Protocolo de Entidad del Switch no esta expedida por Puentes, y debe ser visible a todos los demás BPEs adjuntos al mismo segmento LAN

- La definición de la aplicación GVRP convoca a todas las tramas GVRP a ser transmitidas sin etiqueta por razones similares
- La definición de la aplicación GMRP convoca a todas las tramas de su tipo originadas por dispositivos de VLAN enterada par ser transmitidos VLAN etiquetada, de manera que el VID en la etiqueta sirva para identificar el contexto VLAN
- Puede ser necesario para los PDUs transmitidos por la Administración al VLAN etiquetada de manera que alcance la conexión necesaria para administrar en un Switch VLAN, de manera que cuando se accese a la entidad Administrativa localizada en una red que esta hospedada por un sistema de VLANs, podrá ser necesario que se comunique con aquella entidad utilizando tramas VLAN etiquetada con uno de los VID involucrados, a menos que uno de estos VIDs sea un PVID para el puerto que atiende la estación de administración.

2.6. Formato de trama etiquetada

La trama Etiquetada se ha realizado para los propósitos siguientes:

- a) Para permitir que a la información de "user_priority" sean agregada las tramas llevadas en LAN IEEE 802 los tipos de MAC que no tienen ninguna habilidad inherente de señalar la información de prioridad del nivel de protocolo MAC;
- b) Para permitir una trama que lleva un VID;
- c) Para permitir una trama para indicar el formato de dirección MAC, información llevada en los datos del usuario MAC;
- d) Para permitirle a las VLANs ser soportado por los diferentes tipos de MAC.

Esta sección describe el formato de la trama usado para etiquetar las tramas, como sigue:

- e) Subcláusula 9.1 da una apreciación global de etiquetado
- f) Subcláusula 9.2 define las representaciones de los datos que se usan en las descripciones de los formatos de campo de etiqueta;
- g) Subcláusula 9.3 describe la estructura del encabezado de la etiqueta.

Más allá del análisis del formato de trama, las traducciones del formato que pueden ocurrir cuando se etiquetan las tramas o las sin etiqueta cuando se transmitió diferentes MAC.

La descripción de la estructura de la trama etiquetada, esta basado en dos formatos de tramas genéricas:

- h) El formato de tramas MACs usadas en IEEE Std 802.3, y qué se usa con variaciones menores de la Capa de Enlace de Datos basado en una opción entre la interpretación del Tipo e interpretación de Longitud del Campo de Extensión /Tipo. El Tipo de interpretación es usado donde un valor de Tipo proporciona la identificación de protocolo; la interpretación de Longitud se usa donde la dirección LLC proporciona la identificación de protocolo. Los métodos de LAN MAC que hacen uso de este formato de trama se envía al estándar como métodos MAC 802.3/Ethernet;
- i) El formato de trama usado en ISO/IEC 8802-5 y MAC FDDI, usado con las variaciones menores en otra MAC dónde el protocolo de identificación de la Capa de Enlace esta basado en LLC, y donde la tramas también puede poder llevar información de ruta-fuente. Los métodos de LAN MAC que haga uso de este formato de tramas se envía a este estándar como Token Ring/FDDI.

Para MACs de otra forma que 802.3, 8802-5, y FDDI, se aplican éstos formatos de tramas, con la modificación apropiada a la estructura de la trama. Por ejemplo:

- j) MACs como 8802-4 y 8802-6 que usa LLC como protocolo de identificación de la Capa de Enlace adoptando el formato i). Si ellos no mantienen el soporte de ruteo fuente, la variante de esto, formato que se usa en las Redes de área local de FDDI transparentes se usarían;
- k) MACs como 8802-12 eso puede apoyar la compatibilidad con MACs 802.3 y 8802-5 adoptaría cualquier formato h) o formato i), dependiendo en que modo de compatibilidad estaba operando.

2.6.1 Apreciación Global

Etiquetado de tramas requerido

- a) La suma de un encabezado etiquetado a la trama. Este encabezado es insertado inmediatamente seguido de la dirección MAC destino y la dirección fuente MAC, campos de la trama será transmitida;
- b) Si los métodos de la MAC fuente y destino difieren, mientras la trama es etiquetada puede involucrar la traducción o la encapsulación del resto de la trama;
- c) Recuento de la Verificación de Secuencia de la Trama (FCS).

En una trama etiquetada en un Switch MAC por 802.3/Ethernet, ajusta el campo PAD con un tamaño mínimo de trama etiquetada transmitida de 68 octetos. El encabezado de la etiqueta lleva la siguiente información:

- d) El Protocolo Identificador de Trama (TPID), este protocolo identifica la trama como etiquetada, conformando al formato de etiquetado descrito en esta norma. Conformado de 16 bits.
- e) Información de Control de Etiqueta (TCI): conformado de 16 bits; consiste de los elementos siguientes:
 - 1) Prioridad de usuario. Este campo permite a la trama etiquetada llevar en la prioridad de usuario la información para redes LAN conectadas en donde segmentos de LAN individuales pueden ser incapaces de leer la información de prioridad.
 - 2) Indicador de Formato Canónico (CFI). Este campo se usa en
 - i) En métodos Token Ring / fuente-ruteada FDDI MAC, para señalar el orden del bit de información de dirección llevado en la trama encapsulada; y
 - ii) En 802.3/Ethernet y FDDI MAC, para señalar la presencia o ausencia, de un campo de RIF, y, en combinación con el Indicador del Formato No-canónico (NCFI) llevado en RIF, para señalar el orden del bit de información de dirección llevado en la trama encapsulada.
 - 3) Identificador de VLAN (VID). Este campo único identifica la trama a la que la VLAN pertenece; esta conformada de 12 bits.
- f) En 802.3/Ethernet y FDDI MAC, un Campo de Información Integrada en la Fuente-Ruteada (ERIF) es incluida, si requirió por el estado de la bandera de CFI en el TCI. Si el presente, además de proporcionar, la habilidad de llevar la información fuente-ruteada, este campo incluye una bandera extensa, el NCFI que señala el orden del bit de información de dirección llevado en la trama encapsulada.

La estructura de la trama etiquetada permite identificar los siguientes tipos de información y llevar en tramas etiquetadas todos los métodos de MAC:

- g) Ethernet Tipo-codificado (E) y LLC-codificada (L) la información;
- h) Tramas en que cualquier Dirección MAC incluido en los datos MAC son llevados en formato Canónico (C) o No-canónico (N);
- i) Fuente-ruteada (R) y tramas transparente (T).

Transmitiendo una trama etiquetada requerida

- j) Si los formatos de trama usados en la fuente y destino MAC difieren, traduce el encabezado de la etiqueta al formato apropiado para el destino MAC;
- k) Si la fuente y destino MAC difieren, la trama puede requerir la traducción del resto de la trama, definido en ISO/IEC 11802-5, IETF RFC 1042, e IETF RFC 1390;
- l) Inclusión/ajuste del campo PAD, si es necesario, donde el destino MAC es 802.3 / Ethernet;
- m) Re-cómputo de la Verificación de Secuencia de la Trama (FCS) si necesario.

Desetiquetando tramas etiquetadas requiere

- n) Removiendo el encabezado de la etiqueta, reteniendo el RIF en la posición apropiada al final del desetiquetado de la trama si necesario;
- o) Si los formatos de trama usados en la fuente y destino MAC difieren, el desetiquetado de trama requiere la traducción del resto de la trama, definido en ISO/IEC 11802-5, IETF RFC 1042, e IETF RFC 1390;
- p) Ajuste del campo PAD, si es necesario, dónde el destino MAC es 802.3/Ethernet;
- q) Re-cómputo de la Verificación de Secuencia de la Trama (FCS).

Las traducciones de la trama definida en ISO/IEC 11802-5, IETF RFC 1042, e IETF RFC 1390 son aplicados, como necesarios, para todas las tramas que llevan información tipo Ethernet por los Switches VLAN-enterados. El uso de la bandera de CFI en la trama etiquetada permite

- r) El formato de información de dirección MAC con señalización fin-a-fin por una VLAN sin la necesidad de traducir el formato de dirección MAC por los Switches VLAN-enterados cuando la trama esta en formato etiquetado, sin tener en cuenta los métodos de MAC involucrados llevando la trama etiquetada de la fuente al destino;
- s) Fuente-enrutada información a ser llevado vía fin-a-fin por una VLAN, sin tener en cuenta los métodos MAC, llevando la trama etiquetada fuente al destino.

El propósito primario permitiendo la distinción entre la información Canónica y No-canónica a ser representada en la trama etiquetada es permitir que tal información sea llevada por una VLAN sin la necesidad de que las VLAN-enteradas traduzcan el formato de dirección MAC incluido en el ruteo; sin embargo, las tramas de los Switchs sin etiquetar todavía pueden necesitar tener el formato de dirección en la cuenta, y realizar la traducción apropiada si es necesario, y si el Switch soporta tal traducción.

La habilidad de soportar la traducción de direcciones MAC incluido entre los formatos Canónicos y No-canónicos (y viceversa) cuando transmiten tramas sin etiquetadas no se requiere por este estándar. En Switchs que no soportan la traducción en un puerto que sale, las tramas pueden requerir la traducción antes de que se envíen como tramas sin etiquetada o el puerto desechará esta.

El etiquetado de tramas ocurre cuando una trama sin etiquetada se transmite por un Switch hacia un segmento de LAN será requerido aplicar las reglas de la salida para ser transmitido en el formato etiquetado.

El desetiquetado de tramas ocurre cuando una trama etiquetada se transmite por un Switch hacia un segmento de LAN requiriendo aplicar las reglas de la salida para ser transmitido en el formato sin etiquetada.

2.6.2 Transmisión y representación de octetos

Los octetos en una PDU (o un campo de PDU) se numera el arranque en 1 y aumentando en el orden en que se ponen en un Servicio de Datos de Unidad MAC (MSDU). Se numeran los bits en un octeto de 1 a 8, dónde 1 es el menos significante.

Donde se usan los octetos consecutivos para representar un número binario, el número más bajo del octeto lleva el valor más significante.

Donde el valor de un campo se representa en notación hexadecimal, como una secuencia de dos-dígitos con valores hexadecimal separados por los guiones (por ejemplo, A1-5B-03), el valor mas a la izquierda (A1 en este ejemplo) aparece en el campo como el número más bajo y el valor mas a la derecha (03 en este ejemplo) aparece in el campo como el número más alto del octeto.

Cuando los términos de inicio (set) y reinicio (reset) se usa para indicar los valores de campos de solo-bit, el inicio se pone en código binario como un 1 y reinicio como 0 binario.

Cuando la codificación de un PDU (o un campo dentro de un PDU) es representado usando un diagrama, se usan las siguientes representaciones:

- a) Los Octetos se muestran con el octeto más bajo numerado más cercano al encabezado de la página, la enumeración del octeto incrementa para profundizar; o
- b) Los Octetos se muestran con el octeto numerado más bajo más cercano la izquierda de la página, la enumeración del octeto aumentando de izquierda a derecha;
- c) Dentro de un octeto, los bits se muestran con 8 bits a la izquierda y 1 a la derecha.

2.6.3 Estructura del encabezado de la etiqueta

El encabezado de la etiqueta consiste de los siguientes componentes:

- a) La Etiqueta Identificadota del Protocolo (TPID);
- b) La Información de Control de Etiqueta (TCI);
- c) En 802.3/Ethernet y trama fuente-no-Ruteada FDDI (es decir, tramas FDDI en la que el bit RII es restablecido), si el E-RIF es requerido por el estado del CFI.

Hay tres formas del encabezado de etiqueta, depende del tipo de codificación usado por el TPID y el tipo de MAC subyacente. La estructura global de las tres formas de encabezado se muestra en la figura 2.7.

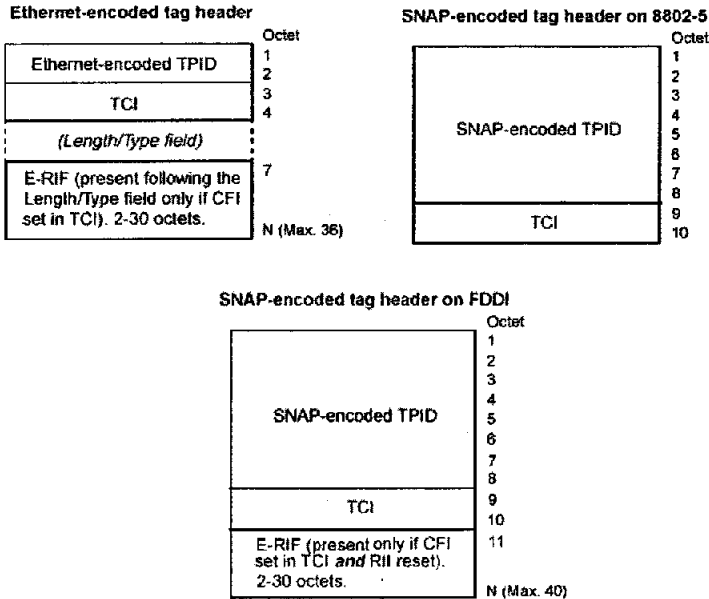


Fig. 2.7. Formato de encabezado de etiquetas

La forma de Ethernet-codificado del encabezado de etiqueta es usado donde la trama etiquetada será transmitida usando métodos de MAC 802.3/Ethernet.

Las dos formas de SNAP-codificado del encabezado de etiqueta será transmitido en métodos MAC: Token Ring y FDDI:

- d) En MACs 8802-5, cualquier información RIF, si presenta, aparece en la posición normal en la trama, es decir, directamente envía el campo de dirección MAC destino, y no es una parte del encabezado de etiqueta.
- e) En MAC FDDI, la información RIF, puede llevarse en la posición normal en la trama (es decir, directamente enviada al campo de dirección MAC destino), o dentro del campo E-RIF en el encabezado de etiqueta.

2.6.3.1 Formato de la Etiqueta del Identificador de Protocolo (TPID)

La estructura del campo TPID toma dos formas, dependiendo en que campo es Ethernet codificada o el SNAP codificado. El TPID lleva un valor de Tipo Ethernet (Tipo de Etiqueta 802.1Q), que identifica la trama como una trama etiquetada (ver tabla 2.4). El valor del Tipo de Etiqueta 802.1Q es:

Nombre	Valor
Etiqueta del Tipo de Protocolo 802.1Q(Tipo de Etiqueta 802.1Q)	81-00

Tabla 2.4 .Asignación de tipo 802.1 Q Ethernet

2.6.3.1.1 TPID Ethernet-codificada

El campo TPID Ethernet-codificada (ETPID) es de longitud de dos octetos. El valor lleva ETPID el valor de tipo de etiqueta 802.1Q, como se muestra en la tabla 2.5:

1	802.1Q TagType
2	

Tabla 2.5. Formato de TPID Ethernet-codificada

2.6.3.1.2 TPID de SNAP-codificado

El TPID de SNAP-codificado (STPID) es de una longitud de ocho octetos, codificado en formato SNAP, como sigue:

- a) Octetos numerados de 1 a 3 llevando el estándar SNAP en el encabezado, consistiendo del valor hexadecimal, AA-AA-03;
- b) Octetos numerados de 4 a 6 llevando el PID SNAP, consistiendo del valor hexadecimal 00-00-00;
- c) Octetos de 7 y 8 llevando las Etiquetas Tipo 802.1Q, como se muestra a continuación figura 2.8 ilustrando la estructura del STPID.

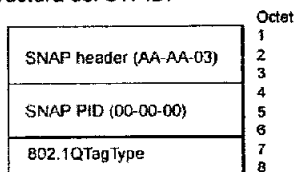


Fig.2.8. Formato de TPID de SNAP-codificado

2.6.3.2 Formato de etiqueta de Información de Control (TCI)

El campo de TCI es dos octetos de longitud, y contiene *user_priority*, los campos CFI y VID (el Identificador VLAN). Como lo ilustra la estructura del campo de TCI (figura 2.9).

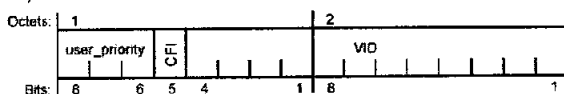


Fig. 2.9. Formato de etiqueta de Información de Control

2.6.3.2.1 Prioridad de usuario (User_priority)

El campo de prioridad de usuario tiene longitud de tres bits, interpretado como un número binario. La prioridad de usuario es capaz de representar ocho niveles de prioridad, de 0 a 7. El uso e interpretación de este campo está definido en ISO/IEC 15802-3.

2.6.3.2.2 Formato de CFI

El Indicador del Formato Canónico (CFI) es un solo valor de bit de bandera. La reinicialización de CFI indica que toda la información de dirección MAC que puede estar presente en los datos de MAC llevada por la trama está en formato Canónico.

El significado de CFI cuando la configuración depende en la variante del encabezado de etiqueta en que aparece.

- a) En un encabezado de etiqueta SNAP-codificado, transmitió usando métodos MAC 802-5, CFI tiene los siguientes significados:
 - 1) Cuando inicializa, indica que toda la información de dirección MAC que puede estar presente en los datos de MAC llevada por la trama en formato No-canónico (N);
 - 2) Cuando reinicializa, indica que toda la información de dirección MAC que puede estar presente en los datos de MAC llevada por la trama en formato Canónico (C).
- b) En un encabezado de etiqueta Ethernet-codificada, se transmitió usando métodos MAC 802.3/Ethernet, CFI teniendo los siguientes significados:
 - 1) Cuando inicializa, indica que el campo de E-RIF está presente en el encabezado de etiqueta, y que el bit NCFI en el RIF determina si la información de la dirección MAC puede estar presente en los datos de MAC llevada por la trama en formato Canónico (C) o No-canónico (N);
 - 2) Cuando reinicializa, indica que el campo de E-RIF no está presente en el encabezado de etiqueta, y que toda la información dirigida a la dirección MAC puede estar presente en los datos de MAC llevada por la trama en formato Canónico (C).
- c) En un título de la etiqueta SNAP-inicializado en código se transmitió usando FDDI los métodos de MAC, CFI tiene los significados siguientes:

- 1) Cuando la trama toma la forma fuente-ruteada (es decir, el bit RII es configurado en la trama fuente del campo de dirección MAC y un RIF sigue la dirección MAC fuente), la interpretación del bit CFI es definido para los encabezados de etiqueta SNAP-codificados transmitidos usando 802-5. El campo ERIF el campo no está presente en esta forma;
- 2) Cuando la trama toma la forma transparente (es decir, el bit RII es configurado en la trama fuente del campo de dirección MAC y hay ningún RIF que sigue la dirección MAC fuente), la interpretación del bit CFI y la presencia o ausencia del E-RIF son como se definen en b) para los encabezados de etiqueta de Ethernet-codificado se transmitieron usando 802.3/Ethernet.

2.6.3.2.3 Formato de VID

El bit-doce es el Identificador de VLAN (VID) este campo identifica que la trama pertenece a una VLAN en particular. El VID se pone en código como un número binario sin firmar. Como se muestra en la siguiente tabla 2.6 que identifica los valores del campo de VID que tiene significados específicos y/o usos; los valores restantes de VID están disponibles para el uso general como identificadores VLAN.

Una etiqueta-prioridad es una trama etiquetada cuyo encabezado de etiqueta el título contiene un valor VID igual a la VLANID nula. Un trama VLAN-etiquetada es una trama etiquetada cuyo encabezado de etiqueta contiene un valor de VID de otra manera será una VLANID nula.

Valor VID (hexadecimal)	Significado/Usos
0	El VLAN ID nulo. Indica que el encabezado de etiqueta contiene información solo de prioridad de usuario; en la trama no es presentado el identificador VLAN. Este valor de VID no debe ser configurado como un PVID, configurado en la entrada de Filtrado de Base de datos, o usado en alguna operación de Administración.
1	El valor de PVID por defecto es usado para clasificar tramas o a través de un Puerto de Switch. El valor de PVID puede cambiarse por medio de administración en un puerto-base.
FFF	Reservado para implementaciones. Este valor de VID no debería de ser configurado como un PVID, configurado en la entrada de Filtrado de Base de Datos, usado en alguna operación de Administración, o transmitido en un encabezado de etiqueta.

Tabla 2.6. Valores VID reservados

Un Switch puede llevar a cabo la habilidad de soportar menos del rango completo de valores de VID; es decir, para una implementación dada, un límite superior, N, es definido por valores VID soportados, donde N es menor o igual a 4094. Todas las aplicaciones apoyarán que el uso de todo el VID valora en el rango 0 a través de su máximo definido VID, N.,

2.6.3.3 Formato de RIF incluido

El E-RIF que puede aparecer en los encabezados de la etiqueta Ethernet-codificada, y en la forma transparente de encabezados de la etiqueta SNAP-codificada en FDDI, es una modificación del RIF definido en ISO/IEC 15802-3. Cuando presenta, sigue inmediatamente los siguientes campos Tipo/Longitud en la trama etiquetada 802.3/Ethernet, o inmediatamente sigue el campo TCI en una trama FDDI. Consiste en dos componentes:

- a) Un Campo de Ruteo de Control (RC) de dos-octetos;
- b) Descripción de Ruta de cero o más octetos (a un máximo de 28 octetos), como lo define RC.

La estructura y semántica asociada con la Descripción de Ruta definida en ISO/IEC 15802-3. La figura 2.10 ilustra el formato del componente de RC, usado en el E-RIF. Los campos del RC, y su uso, está definido en los puntos siguientes.

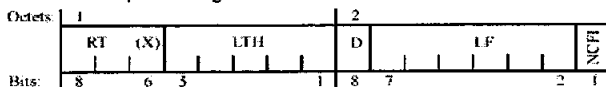


Fig. 2.10. Campo de Control de Ruteo (RC) E-RIF

2.6.3.3.1 Definición del campo de Tipo de Ruteo (RT) en el E-RIF

La definición de este campo es definido en ISO/IEC 15802-3, con la suma que un valor RT de 01X indica una trama. El valor del bit más a la derecha, X, se ignora; es decir, el valor es binario 01 en 8 y 7 que es usado para señalar tramas transparentes.

El valor de la trama transparente indica que, con la excepción del NCFI, el resto del ERIF se desechará si en la trama que envía usa 8802-5. Un E-RIF que contiene un valor de RT que indica una trama transparente no contiene ninguna descripción de ruta, y es por consiguiente exactamente de 2 octetos de longitud (sin embargo, el valor del campo de LTH se configura en cero en este caso).

El bit menos significativo del campo de RT, marcado (X) es reservado, como definido en ISO/IEC 15802-3. Las reglas siguientes aseguran que la interpretación y uso del campo de RT por los dispositivos de VLAN-enterada son inequívocos, y no choca con el uso por los dispositivos VLAN-no enterada:

- a) Donde una trama des Etiquetada, fuente-ruteada se recibe de Token Ring/FDDI LAN y se releva como una trama etiquetada o en 802.3/Ethernet o en Token Ring/FDDI, si el valor recibido del campo RT era el 0XX, entonces el valor del campo de RT en el E-RIF o RIF en la trama etiquetada se transmitirá como 000 (es decir, algún 01X es convertido a 000);
- b) Donde una trama des Etiquetada transparente se recibe de una LAN Token Ring y se releva como una trama etiquetada en 802.3/Ethernet o en FDDI, el encabezado de la etiqueta llevará un E-RIF en el que el valor del campo de RT será 010;
- c) Donde una estación final en una VLAN-consciente en Token Ring/FDDI genera una fuente-ruteada, las tramas etiquetadas no transmitirá valores de RT de 010 o 011 en el RIF;
- d) Donde una estación final VLAN-consciente en 802.3/Ethernet o FDDI genera fuente-ruteada, etiquetó las tramas en forma transparente entonces no usará valores de RT de 010 o 011 en el E-RIF;
- e) "X" en estas reglas se toma para significar "Ignoró en el recibo, transmitió como cero."

2.6.3.3.2 Definición de la Longitud (LTH) en el campo E-RIF

Este campo está definido en ISO/IEC 15802-3, con la excepción que si el valor del campo de RT en el E-RIF tiene 01X, indicando una trama transparente, entonces el campo de LTH llevará un valor de 0.

2.6.3.3.3 Definición de la Dirección del Bit (D) en el campo E-RIF

Este campo está definido en ISO/IEC 15802-3.

2.6.3.3.4 Definición de la Trama más Grande (LF) en el campo E-RIF

Este campo está definido en ISO/IEC 15802-3, y se usa de acuerdo con todas las tramas etiquetadas transmitidas usando 802.3/Ethernet o FDDI que llevan un E-RIF, si fuente-rutea o es transparente.

Para tramas transmitidas usando 802.3/Ethernet, el valor de este campo indicará un tamaño de trama más grande de 1470 octetos o menos.

2.6.3.3.5 Definición del campo de NCFI en el E-RIF

El campo de Indicador de Formato No-canónico del E-RIF tiene los significados siguientes:

- a) Cuando se restablece, indica que toda la información de dirección MAC que puede estar presente en los datos de MAC llevó por la trama el formato No-canónico (N);
- b) Cuando se inicia, indica que toda la información de dirección MAC que puede estar presente en los datos de MAC llevó por la trama el formato Canónico (C).

En la trama de fuente-ruteada en Token Ring / FDDI, este bit en el RIF es reservado, y su valor se conserva por los Switchs; su valor normalmente se restablece.

Donde una trama de fuente ruteada es recibida de una LAN Token Ring / FDDI y transmitida como una trama etiquetada conteniendo un E-RIF en 802.3/Ethernet o FDDI (es decir, donde la información RIF llevada en la posición normal de una trama de fuente-ruteada es incluida en E-RIF), el valor recibido de este campo es remplazado por el valor apropiado N o C.

Donde una trama etiquetada contiene un E-RIF se releva de una LAN 802.3/Ethernet o FDDI hacia una LAN Token Ring o FDDI como una trama fuente-ruteada (es decir, cuando la información RIF llevada en el E-RIF es restaurada a su posición normal en la trama), este bit en RIF es restaurada en la trama transmitida en la LAN destino.

2.6.3.3.6 Uso de E-RIF en las tramas etiquetadas en 802.3/Ethernet y FDDI

Hay tres casos donde una trama etiquetada llevará un E-RIF:

- a) En una trama transparente que lleva información E-N o L-N;
- b) Es una trama fuente-ruteada que lleva información E-N o L-N;
- c) Es una trama fuente-ruteada que lleva la información del L-C.

Caso a) ocurre si

- d) Una trama desetiquetada que contiene datos E-N o L-N, y sin RIF (RIF restablecido), se recibe de una LAN 8802-5 y se transmite como una trama VLAN-etiquetada en 802.3/Ethernet o FDDI; o
- e) Una trama etiquetada con CFI configurada, y sin RIF (RIF restablecido), se recibe de una LAN 8802-5 y es transmitido como una trama VLAN-etiquetada en 802.3/Ethernet o FDDI.

El caso b) ocurre si

- f) Una trama desetiquetada contiene datos E-N o L-N, y con un RIF (RIF configurado), se recibe de una LAN Token Ring / FDDI y se transmite como una trama VLAN-etiquetada en una VLAN 802.3/Ethernet, o FDDI que no soporta la fuente ruteadora; o
- g) Una trama etiquetada con CFI configurada, y con un RIF (RIF configurado), se recibe de una LAN Token Ring / FDDI y se transmite como una trama VLAN-etiquetada en una LAN 802.3/Ethernet, o en un FDDI que no apoya la asignación de ruta de la fuente.

El caso c) ocurre si

- h) Una trama desetiquetada contiene los datos del L-C, y con un RIF (RIF configurado), se recibe de una LAN Token Ring / FDDI y se transmite como una trama VLAN-etiquetada en una LAN 802.3/Ethernet, o FDDI que no soporte fuente-ruteada; o
- i) Una trama etiquetada con CFI restableció, y con un RIF (RIF configurado), se recibe de una LAN Token Ring / FDDI y se transmite como una trama VLAN-etiquetada en una LAN 802.3/Ethernet, o FDDI que no soporta la asignación de ruta de la fuente.

Las otras posibles representaciones de la trama Token Ring / FDDI, a saber, el transporte de la información de tramas transparentes L-C o E-C, se representa en medios de comunicación 802.3/Ethernet como tramas VLAN-etiquetadas con CFI restablecido (es decir, RIF no esta presente).

En caso de que a), el RIF es creado desde el principio como parte de la traducción de la trama. El RIF en este caso consiste de sólo 2 octetos, con los valores del campo como sigue:

- j) RT se configura a un valor binario 010, para indicar una trama transparente,
- k) LTH se configura a 0;
- l) Se configura D y campos de LF a 0;
- m) NCFI se restablece para indicar que el formato es No-canónico.

En los casos b) y c), el RIF contuvo la trama a ser traducida se usa el des-modificador, con las dos excepciones que

- n) Recibido los valores RT de 0XX son cambiados a 000 en el campo de RT del E-RIF;
- o) El campo de NCFI es apropiadamente configurado para indicar el formato (Canónico o No-canónico) de los datos llevados en la trama.

2.7. Uso de GMRP en VLANs

El GARP Protocolo de Registro de Multicast (GMRP), definido en la cláusula 10 de ISO/IEC 15802-3 permiten la declaración y diseminación de información del numero de miembro de Grupo, en orden para permitir GMRP-consiente los switches filtran tramas destinadas por grupo a las direcciones MAC en puertos a través del cuál semejantes tramas no pueden ser rechazadas, esto, también es conocido como la base del Spanning Tree.

En el ambiente de switches LAN que soportan la definición y administración de VLANs de acuerdo con este estándar, la operación de GMRP esta definida en ISO/IEC 15802-3 permitiendo operar en diferentes contextos de GIP, y estos son activados en el Switch.

2.7.1. Definiendo el contexto de una VLAN.

La configuración de Puertos de un Switch definido como parte de la topología activa para dar el contexto de VLAN debe ser igual a la configuración de Puertos que siguen siendo ciertos:

- a) El puerto es un miembro de la configuración Miembro de la VLAN; y
- b) El Puerto es uno de los Puertos del Switch que son parte de la topología activa del Spanning Tree que soporta esa VLAN, donde un solo Spanning Tree es usado para soportar todas las VLANs cada que una VLAN es definida.

2.7.2. Participantes de GMRP y Contextos GIP

Por cada Puerto del Switch, una diferente instancia del Participante GMRP puede existir por cada Contexto VLAN soportada por cada Switch. Cada GMRP Participante mantiene su propia configuración de GARP Aspirante y Registrador del estado de las maquinas, y su propia Salida del estado de la maquina. Este no es un Participante GMRP asociado con la Base del Contexto de Spanning Tree.

Un Participante GARP dado, opera en un Contexto GIP dado, manipulando solo el Modo de Filtraje de Puerto y el Grupo de Registro de Entrada información concerniente al contexto. En el caso del Registro de Grupo de Entradas, el Contexto GIP Identificador valor correspondiente para el valor del campo VID de entrada.

2.7.3. Identificación del Contexto GMRP en PDUs

Las implementaciones de GMRP conformada para la especificación de GMRP en ISO/IEC 15802-3 intercambio PDUs en el Contexto de la Base de Spanning Tree, tal PDUs son transmitidas y recibidas por Participantes GMRP como tramas desetiquetadas.

Las implementaciones de GMRP en Switches VLAN aplican la misma regla de ingreso (8.6) para recibir PDUs GMRP que son definidas por el Puerto receptor. Por lo tanto

- a) Las tramas GMRP sin clasificación VLAN son descartadas si el parámetro de Tipo de Tramas Aceptables por el Puerto esta configurado para Admitir Solo tramas VLAN-tagged (etiquetadas). Por otra parte están clasificados de acuerdo al PVID para el Puerto;
- b) Las tramas VLAN-tagged GMRP son clasificadas de acuerdo al VID llevado en el encabezado de la etiqueta.
- c) Si el Filtraje de Ingreso esta habilitado, y el Puerto no es un Miembro de la configuración para la trama GMRP de la clasificación VLAN, cuando la trama es descartada.

La clasificación VLAN así asociada con las PDUs GMRP recibidas establece el Contexto VLAN para recibir PDU, e identifica el GARP Participante en caso que la PDU este dirigida.

Las PDUs GMRP son transmitidas por Participantes GMRP son las VLAN clasificadas de acuerdo al contexto VLAN asociado con este participante. Los Participantes en Switches VLAN aplican las mismas reglas de egreso que son definidas para el Puerto. Por lo tanto

- d) Las PDUs GMRP son transmitidas por medio de un solo Puerto dado si el valor del Miembro Fijo por el Puerto para la VLAN concerniente indica que VLAN esta registrada en que Puerto;
- e) Las PDUs GMRP son transmitidas como tramas VLAN-tagged o como tramas desetiquetadas de acuerdo con el estado de la Configuración Desetiquetada para que Puerto para la VLAN concerniente. Donde tramas VLAN-untagged son transmitidas, el campo VID de la etiqueta del encabezado lleva el valor del Contexto Identificador de VLAN.

2.7.4. Comportamiento del Filtraje del Grupo Predefinido y la propagación de GMRP.

La propagación de registros GMRP dentro de una VLAN tiene implicaciones respecto a la forma de escoger el comportamiento del filtraje de grupo predefinido dentro de un switch LAN. Como las tramas GMRP son transmitidas solo en Puertos de salida que son miembros de una VLAN, la propagación de registro de Grupos dada por un Switch sucede solo hacia regiones del Switch LAN donde tienen registro (estático o dinámico).

2.8. Administración de topología VLAN

Las reglas de egreso definidas por el Proceso de Envío de VLANs en Switches cuentan con una información de configuración existente por cada VLAN definida en los Puertos del Switch a

través de qué uno o más miembros sean alcanzados. Esta configuración de Puertos es conocida como Miembro Conjunto, y este número de miembro es determinado por la presencia o ausencia de información de configuración en el Filtrado de la Base de Datos, en la forma del Registro VLAN de Entrada Estática o Dinámica.

La operación confiable de la infraestructura de la VLAN requerida para la información del miembro de la VLAN en el Filtro de la Base de Datos para ser mantenida de constante manera a través de toda la VLAN-aware (enterada) en el Switch LAN, en orden para asegurarse que las tramas destinadas a la estación(es) final(es) sean correctamente entregadas dentro de la VLAN, independientemente de donde las tramas hayan sido generadas dentro del Switch. Manteniendo esta información para estaciones finales que son fuentes de tramas VLAN-etiquetadas permitiendo tales estaciones para suprimir transmisiones de tales tramas si no existen miembros de la VLAN concerniente.

Este estándar define los siguientes mecanismos que permiten a configurar la información de los miembros de la VLAN:

- a) Configuración dinámica y distribución de los miembros de la VLAN por medio de la GARP Registration Protocol (GVRP).
- b) Configuración estática de la información de los miembros de la VLAN por mecanismos de administración, que permiten la configuración del Registro de Entrada de VLAN Estática.

Estos mecanismos proveen información de la configuración de miembros de la VLAN como un resultado de:

- c) Registros dinámicos de acciones tomadas por estaciones finales o Switches;
- d) Acciones administrativas.

2.8.1. Configuración de VLANs Estáticas y Dinámicas.

La combinación de funcionalidad proveída para la habilidad para configurar el Registro VLAN de Entradas Estáticas en el Filtro de la Base de Datos, unido con la habilidad de GVRP para dinámicamente crear y actualizar el Registro VLAN de Entradas Dinámicas, ofrecen las siguientes posibilidades con respecto a como las VLANs son configuradas en un Puerto dado:

- a) Solo configuración estática: los medios de administración son usados para establecer precisamente que VLANs tienen este Puerto como miembro, y la administración de control de GVRP son usados para deshabilitar la operación del protocolo GVRP en el Puerto. Ahora, uso del algún del GVRP por dispositivos alcanzables vía el ignorado de Puerto, el de y el Miembro puso para todas las VLANs poder determinarse por consiguiente sólo por medio del estado de estáticas en el Filtro de la Base de Datos.
- b) Solo configuración dinámica: la operación de GVRP esta contado en establecer Entradas de Registro de VLAN Dinámicas que dinámicamente reflejaron que VLANs están registradas en el Puerto, estos contenidos cambian como la configuración de la red cambie. La administración de los controles GVRP están configurados para habilitar la operación del protocolo GVRP en el Puerto.
- c) Combinando configuración dinámica y estática: los mecanismos de configuración estática son usados en orden para configurar información de algunos miembros de la VLAN; por otras VLANs, GVRP estuvo contado en establecer la configuración. La administración de los controles GVRP son configurados para habilitar la operación del protocolo GVRP en el Puerto.

Todos los mencionados arriba son soportados por los mecanismos definidos en este estándar y cada uno se aplica en diferentes circunstancias. Por ejemplo:

- d) Uso de la configuración estática puede ser apropiada en Puertos donde la configuración adjunta del dispositivo esta fija, o donde el administrador de la red desea establecer una administración limitada fuera de algún registro de información GVRP esta sea ignorada. Por ejemplo, esto puede ser deseable para todos los Puerto sirviendo a los dispositivos finales que sean configurados estáticamente en orden para asegurarse que particularmente usuarios finales tengan acceso solo a VLANs en particular.
- e) Uso de configuración dinámica pueden ser apropiados en Puertos donde la configuración esta inherentemente dinámica; donde usuarios de una particular VLANs pueden conectarse a la red vía diferentes Puertos por un anuncio hoc base, o donde esto sea deseable para permitir una reconfiguración dinámica en los cambios de topología de

Spanning Tree. En particular, si el centro de la LAN Virtual del Switch, entonces esto es deseable para los Puertos Switches que forman el centro de la red para ser configurada dinámicamente.

- f) Uso de ambas configuraciones la estática y dinámica pueden ser apropiadas en Puertos donde esto es deseable para tomar lugar restricciones en la configuración de algunas VLANs, cuando mantienen la flexibilidad de registros dinámicos para otros. Por ejemplo, en Puertos sirviendo a dispositivos móviles, estos deberían mantener los beneficios de VLAN dinámica con registros del punto de vista de reducir tráfico, cuando aún permiten el control administrativo sobre algunas VLANs vía ese Puerto.

2.8.2. Protocolo de Registro VLAN GARP

El Protocolo de Registro VLAN GARP (GVRP) define una *aplicación GARP* que provee el registro de servicio VLAN. GVRP hace uso de la Declaración de Información GARP (GID) y la Información de Propagación (GIP), que provee la descripción del estado común de la máquina y la información común de los mecanismos de propagación definido para usarse en aplicaciones basadas en GARP. La arquitectura GARP, GID, y GIP están definidas en ISO/IEC 15802-3.

GVRP provee un mecanismo para mantenimiento dinámico de los contenidos de los Registros de Entradas de VLAN Dinámicas por cada VLAN, y para propagar la información que ellos contienen para otros Switches. Esta información permite GVRP-aware para dispositivos que se establecen dinámicamente y actualizan su conocimiento de la configuración de VLANs que actualmente tienen miembros activos, y a través de qué Puertos esos miembros pueden ser alcanzados.

2.8.2.1 Visión global de GVRP

La operación de GVRP esta encajonada similar a la operación de GMRP, que es usada para registrar la información de los miembros del Grupo. Las diferencias primarias son las siguientes:

- a) Los atributos de los valores llevados por el protocolo son de un valor de 12 bit del VID, más 48 bits de la dirección MAC y Grupo de servicio de información requerida;
- b) Los actos de registro/desregistro una VID afectan los contenidos de las Registros de Entradas de VLAN Dinámicas, más de los contenidos del Registro de Entradas del Grupo.

GVRP permite a las estaciones finales y Switches en un Switch LAN para publicar y revocar relaciones declaradas para miembros de VLANs. El efecto de publicar tal declaración es que cada GVRP Participante reciba las declaraciones que crearan o actualizaciones de los Registros de Entradas en el Filtro de la Base de Datos para indicar que la VLAN esta registrada en el Puerto receptor. Subsecuentemente, si todos los Participantes en un segmento que tiene un interés en obtener una declaración de revocación del VID, el Puerto adjunto para que el segmento este configurado para Desregistrar en el Registro de Entradas de la VLAN Dinámica para esa VLAN por cada GVRP Participante adjunto para ese segmento.

2.8.2.1.1 Comportamiento de las estaciones finales

La VLAN conoce que estaciones finales participan en la actividad del protocolo GVRP, como apropiadamente para la configuración de las VLANs de qué ellas son generalmente miembros. GVRP proporciona un camino para semejante en una estación final para asegurarse que la(s) VLAN(s) de qué esta es miembro están registradas por cada Puerto en algún segmento LAN para que las estación final este adjuntada. GVRP también provee por cada información para ser propagada por el Spanning Tree para otra VLAN concedora de los dispositivos, se describe en el siguiente punto.

La información entrante de los miembros de la VLAN (de todos los otros dispositivos en el mismo segmento LAN) permite que las estaciones finales sean una fuente recortada de algún tráfico destinado para las VLANs que generalmente no tienen otros miembros en el Switch LAN, así evitan la generación de tráfico innecesario en los segmentos de su LAN local.

2.8.2.1.2 Comportamiento de Switches

La VLAN conoce el registro de los Switches y propaga los miembros de la VLAN en todos los Puertos de los Switches que son parte de la topología activa del Spanning Tree fundamental. El registro VID entrante y de registro de información es usada para actualizar el Registro de Entrada

de la VLAN Dinámica asociada con cada VLAN. Algunos cambios en el estado de registros de un VID dado en un Puerto dado es propagada en Puertos que son parte de la topología activa del Spanning Tree, en orden para asegurarse que otro GVRP conoce los dispositivos en el Switch LAN actualizando sus Bases de Datos para filtrar apropiadamente. Se configuran así automáticamente las Bases de Datos del Filtro en todos los dispositivos GVRP-conscientes de tal manera que el Puerto Trace en el Registro de Entrada de la VLAN Dinámica para un VID dado que indica que un Puerto dado es registrado si uno o más miembros del VLAN correspondiente son alcanzables a través del Puerto.

2.8.2.1.3 Uso del PVID

El estado inicial de la Base de Datos contiene un Registro de Entrada de la VLAN Estática para el PVID Predefinido, en que el Mapa del Puerto indica el Registro Fijado en todos los Puertos. Esto asegura eso en el estado predefinido dónde el PVID en todos los Puertos es el PVID Predefinido, el número de miembros del PVID Predefinido se propaga por el Switch LAN a todos los otros dispositivos GVRP-conscientes. Subsecuente la acción administrativa puede cambiar la Base de datos Permanente y la Base de Datos del Filtro en orden para modificar o quitar esta configuración inicial, y puede cambiar el valor del PVID en cada Puerto del Switch.

2.8.2.2 Definición del servicio de registro VLAN

El servicio de registro VLAN les permite Servicio MAC a usuarios para indicar al proveedor de servicios MAC la configuración de VLANs en que ellos desean participar; es decir, que el Servicio MAC al usuario desea recibir tráfico destinado para los miembros de esta configuración de VLANs. Los servicios primitivos permiten al usuario de servicio a:

- a) El número de miembros del Registro de un VLAN;
- b) El número de miembros del Des-registro de un VLAN.

La provisión de estos servicios se logra por medio de GVRP y sus procedimientos asociados.

ES_REGISTER_VLAN_MEMBER (VID)

Indica al proveedor de servicios MAC que el Servicio MAC del usuario desea recibir las tramas destino para la VLAN identificada por el parámetro VID.

ES_DEREGISTER_VLAN_MEMBER (VID)

Indica al proveedor de servicios MAC que el Servicio MAC del usuario no desea ya recibir las tramas destino para el VLAN identificado por el parámetro VID.

El uso de estos servicios puede producir la propagación de información VID por el Spanning Tree, afectando los contenidos del Registro de Entrada de la VLAN Dinámica en los Switches y estaciones finales en la LAN conectada, y afectando la trama que reenvía la conducta de esos Switches Puentes y estaciones finales.

2.8.2.3 Definición de la Aplicación de GVRP

2.8.2.3.1 Definición de los elementos del protocolo GARP

2.8.2.3.1.1 GVRP Aplicación de dirección

La dirección MAC de grupo usada como la dirección de destino para PDUs GARP destinada para los Participantes de GVRP será la dirección de GVRP identificada en la siguiente tabla. Las PDUs recibidas que son construidas de acuerdo con el formato de PDU definido en ISO/IEC 15802-3, y que lleva una dirección MAC destino igual a la dirección de GVRP se procesa como sigue:

- a) En los Switches y estaciones finales que soportan el funcionamiento de GVRP, todas las PDUs se someterá a el GVRP Participante asociado con el Puerto receptor para más allá procesarlo;
- b) En Switches que no soportan el funcionamiento de GVRP, todas las PDUs se someterá al Proceso de Reenvío.

Assignment	Value
GVRP address	01-80-C2-00-00-21

Fig. 2.11. Dirección de la aplicación GVRP

2.8.2.3.1.2 Codificación de GVRP Tipos de Atributo

El funcionamiento de GVRP define un solo Tipo de Atributo (ISO/IEC 15802-3) eso se lleva en protocolo de intercambios GARP; el Tipo de Atributo VID. El Tipo de Atributo VID se usa para identificar los valores de los Identificadores VLAN (VIDs). El valor del Tipo del Atributo de Grupo llevado en GVRP PDUs será de 1.

2.8.2.3.1.3 Codificación de GVRP Tipos de Atributo

Valores de casos del Tipo de Atributo VID como los Valores del Atributo en PDUs GARP (ISO / IEC 15802-3) como dos octetos, tomado para representar un número binario sin firmar, e iguala al valor hexadecimal del identificador de VLAN que será puesto en código.

2.8.2.3.2 Provisión y soporte del registro de servicio de la VLAN

2.8.2.3.2.1 Sistema final de la declaración del número de miembros de la VLAN

El elemento de Aplicación GVRP de un Participante de GVRP proporciona el registro dinámico y los servicios de desregistro se definieron como sigue:

En la recepción de un servicio primitivo ES_REGISTER_VLAN_MEMBER, el Participante GVRP emite un servicio primitivo GID_Join.request (demanda de unión GID) (ISO/IEC 15802-3). El parámetro del attribute_value (tipo de atributo) de la demanda lleva el valor del Tipo de Atributo VID y el parámetro del attribute_value lleva el valor del parámetro de VID llevado en el ES_REGISTER_VLAN_MEMBER primitivo.

En la recepción de un servicio primitivo ES_DEREGISTER_VLAN_MEMBER, el GVRP Participante tiene problemas en el servicio primitivo GID_Leave.request (ISO/IEC 15802-3). El parámetro del attribute_type de la demanda lleva el valor del Tipo de Atributo VID y el parámetro del attribute_value lleva el valor del parámetro de VID llevado en el ES_REGISTER_VLAN_MEMBER primitivo.

En la recepción de un servicio primitivo ES_DEREGISTER_VLAN_MEMBER, el GVRP Participante emiten un servicio primitivo GID_Leave.request (ISO/IEC 15802-3). El parámetro del attribute_type de la petición lleva el valor del Atributo Tipo VID y el parámetro del attribute_value lleva el valor del parámetro de VID llevado en el ES_REGISTER_VLAN_MEMBER primitivo.

2.8.2.3.2.2 Registro del número de miembros VLAN

El elemento de la Aplicación GVRP de un Participante GVRP responde al registro y eventos del desregistro señalado por GID como sigue:

En la recepción de un GID_Join.indication (ISO/IEC 15802-3) cuyo attribute_type es igual al valor del Atributo Tipo VID, el elemento de la Aplicación GVRP indica el Puerto receptor como Registrado en el Mapa del Puerto del Registro de Entrada de la VLAN Dinámica para el VID indicado por el parámetro del attribute_value. Si ninguna tal entrada existe, y hay espacio suficiente en el Filtro de la Base de datos, una entrada se crea.

En la recepción de un GID_Leave.indication (ISO/IEC 15802-3) cuyo attribute_type es igual al valor del Atributo Tipo VID, el elemento de la Aplicación GVRP indica el Puerto receptor como No registrado en el Mapa del puerto del Registro de Entrada de la VLAN Dinámica para el VID indicado por el parámetro del attribute_value. Si marcando este Puerto como No registrados los resultados en un Mapa del puerto que no indica algún puerto como Registrado, la entrada es borrada.

2.8.2.3.2.3 Controles administrativos

La provisión de control estático sobre la declaración o estado de registro del estado de las máquinas asociadas con la Aplicación GVRP es archivada por medio del Archivero de control de parámetros administrativos proporcionados por GARP (ISO/IEC 15802-3). Estos parámetros de

control administrativos son representados como las Entradas de Registro de VLAN Estáticas en el Filtro de la Base de datos. Donde la capacidad de dirección se lleva a cabo, estos controles pueden manipularse por medio de la funcionalidad de administración.

La provisión de control estático encima de la habilidad del Solicitante del estado de las maquinas para participar en el intercambio de protocolo se logran por medio del Solicitante Administrativo de Control parámetros asociados con el funcionamiento de GARP (ISO/IEC 15802-3). Donde la capacidad de administración se lleva a cabo, el Solicitante Administrativo de Control de parámetros puede aplicarse y modificarse por medio de la funcionalidad de la administración.

2.8.2.3.3 Contexto de GIP para GVRP

GVRP como definido por esta norma opera en el Contexto del Spanning Tree Base (ISO/IEC 15802-3); es decir, GVRP sólo opera en el Spanning Tree Base definido por ISO/IEC 15802-3. Por consiguiente, todas las PDUs GVRP enviadas y recibidas por los Participantes de GVRP se transmiten como tramas desetiquetadas.

2.9. Administración de Switch VLAN

Este punto define la configuración de objetos administrados, y su funcionalidad que permite la configuración administrativa de VLANs.

Este punto:

- a) Introduce las funciones de administración para ayudar en la identificación de los requisitos situados en los Switches para soportar los medios de administración.
- b) Establece la correspondencia entre los Procesos usados para modelar el funcionamiento del Switch y la administración de objetos del Switch.
- c) Especifica las operaciones administrativas soportadas cada objeto manejado.

2.9.1 Funciones Administrativas

Las Funciones Administrativas relacionan a los usuarios que necesitan para medios soportar la planificación, organización, vigilancia, control, protección, y seguridad de los recursos de comunicación, y responde para su uso. Estos medios pueden ser categorizados como soportar las áreas funcionales de Configuración, Falta, Desempeño, Seguridad, y Administración de Cuenta.

2.9.1.1 Administración de la Configuración

La Administración de la configuración mantiene la identificación de recursos de comunicaciones, inicialización, reinicialización y cierre, el suministro de parámetros operacionales, y el establecimiento y descubrimiento de la relación entre los recursos. Los medios proporcionados por la Administración del Switch en esta área funcional son:

- a) La identificación de todos los Switches que juntos constituyen la LAN Conectada y sus ubicaciones respectivas y, como consecuencia de esa identificación, la ubicación específica de estaciones finales en una LAN individual en particular.
- b) La habilidad de restablecer remotamente, es decir, reinicializarse, los Switches especificados.
- c) La habilidad de controlar la prioridad con que un Puerto del Switch transmite las tramas.
- d) La habilidad de forzar una configuración específica del Spanning Tree.
- e) La habilidad de controlar la propagación de tramas especificando las Direcciones MAC del grupo para ciertas partes de la LAN configurada.
- f) La habilidad de identificar las VLANs en uso, y a través de que Puertos del Switch las tramas destinadas para un VLAN dada pueden recibirse y/o pueden retransmitirse.

2.9.1.2 Administración por defecto

La Administración por defecto mantiene prevención por defecto, detección, diagnóstico, y corrección. Los medios proporcionados por la Administración del Switch en esta área funcional son:

- a) La habilidad de identificar y corregir los funcionamientos defectuosos del Switch, incluso errores de registro e informantes.

2.9.1.3 Administración del Desempeño

La Administración del Desempeño se mantiene evaluando la conducta de recursos de comunicaciones y la efectividad de las actividades de comunicación. Los medios proporcionados por la Administración del Desempeño en esta área funcional son:

- a) La habilidad de recoger estadísticas relacionadas al desempeño y al análisis de tráfico. Especifica métricas incluyendo la utilización de la red, tramas enviadas, y cuentas de tramas desechadas por los Puertos individuales dentro de un Switch.

2.9.1.4 Administración de Seguridad

La Administración de seguridad proporciona para la protección de recursos. La Administración del Switch no proporciona algún medio específico en este área funcional.

2.9.1.5 Administración de Cuenta

La Administración de Cuenta mantiene la identificación y distribución de validación y la configuración de cargas. La Administración del Switch no proporciona ningún medio específico en esta área funcional.

2.9.2 Administración de Objetos

Los objetos administrados modelan la semántica de funcionamientos de la administración. La operación en un objeto suministra información involucrada, o facilita el control sobre, el Proceso o Entidad asociada con ese objeto.

Los recursos administrados de un Switch MAC son aquéllos de los Procesos y Entidades establecidas en ISO/IEC 15802-3. Específicamente,

- a) La Administración de la Entidad del Switch.
- b) Las Entidades MAC individuales asociadas con cada Puerto del Switch.
- c) El Proceso de Envío de la MAC Relay Entity.
- d) La Filtración de la Base de datos de la MAC Relay Entity.
- e) La Entidad del Protocolo del Switch (ISO/IEC 15802-3).
- f) Los Participantes de GARP (ISO/IEC 15802-3).

La administración de cada uno de estos recursos se describe en términos de administración de objetos y bajo operaciones.

2.9.3 Tipo de datos

Este subcláusula especifica la semántica de funcionamientos independiente de su codificación en el protocolo de administración. Los tipos de datos de los parámetros de operaciones sólo están definidos como es requerido para esa especificación.

Los siguientes tipos de datos son usados:

- a) Booleano.
- b) Enumeró, para una colección de valores nombrados.
- c) Sin firmar, para todos los parámetros especificados como "el número de" alguna cantidad, y por valores de prioridad de Spanning Tree que se comparan numéricamente. Cuando comparando la prioridad del valor de Spanning Tree, el más bajo número representa el valor de prioridad más alto.
- d) La dirección MAC.
- e) Latin1 String, definido por ANSI X3.159, para todos los cordones del texto.
- f) Intervalo de Tiempo, un valor sin firmar que representa un número de segundos positivos íntegro, para todos los parámetros de la interrupción del protocolo Spanning Tree;
- g) El Contador, para todos los parámetros especificados como una "cuenta" de alguna cantidad. Un contador incrementa y envuelve con un módulo de 2 al poder de 64.
- h) El Tiempo de Intervalo GARP, un valor Sin firmar que representa un número de centésimas de segundo íntegro positivo, para todos los parámetros del protocolo GARP fuera de tiempo.

2.9.4 Entidad de Administración de Switch

Los objetos que comprenden estos recursos administrados son

- a) La Configuración del Switch.
- b) La Configuración del puerto por cada puerto.

2.9.4.1 Configuración del Switch

La Configuración del Switch objeto forman los funcionamientos que modifican, o inquiera sobre, la configuración de los recursos del Switch. Hay un solo objeto de Configuración del Switch por Switch.

La administración de operaciones que pueden realizarse en la Configuración del Switch son

- a) Descubrir el Switch;
- b) Lea el Switch;
- c) Configurando el Nombre de Switch;
- d) Restablezca el Switch.

2.9.4.1.1 Descubrir el Switch

2.9.4.1.1.1 Propósito

Para solicitar la información de la configuración con respecto al Switch(s) en la LAN Conectada.

2.9.4.1.1.2 Entradas

a) El Rango de la Inclusión, una configuración de peticiones de Direcciones MAC específicas. Cada par especifica un rango de direcciones MAC. Un Switch responderá si y sólo si:

- 1) Para uno de los pares, la comparación numérica de la Dirección del Switch con cada dirección MAC de las muestras del par él para ser mayor que o igual a el primero, y
- 2) Menor que o igual a el segundo, y
- 3) Su Dirección del Switch no aparece en el parámetro de Lista de Exclusión.

La comparación numérica de una dirección MAC con otra, con el propósito de esta operación, se logra derivando un número de la dirección MAC según el procedimiento siguiente. Se toman los octetos consecutivos de la Dirección de MAC para representar un número binario; el primer octeto que se transmitiría en un medio de LAN cuando la Dirección MAC se usa en la fuente o campos del destino de una trama MAC tiene el valor más significativo, el próximo octeto es el próximo valor más significativo. Dentro de cada octeto el primer pedazo de cada octeto es el pedazo significativo.

b) La Lista de Exclusión, una lista de direcciones MAC específicas.

2.9.4.1.1.3 Salidas

- a) La dirección del Switch: la dirección MAC del Switch de que el Switch Identificador usado por el Algoritmo de Spanning Tree y el Protocolo es derivado (ISO/IEC 15802-3).
- b) El nombre del Switch: un texto de 32 caracteres, de importancia localmente determinada.
- c) Número de Puertos: el número de Puertos del Switch (Entidades MAC).
- d) Direcciones de Puerto: una lista especificando a lo siguiente para cada Puerto:
 - 1) El Número de Puerto—el numero del Puerto del Switch (ISO/IEC 15802-3).
 - 2) Direcciones de Puerto—la Dirección MAC específica la MAC Entidad individual asociada con el Puerto.
- e) Tiempo arriba—cuenta en segundos del tiempo transcurrido desde que el Switch fue restablecido en último lugar o inicializado (ISO/IEC 15802-3).

2.9.4.1.2 Lectura del Switch

2.9.4.1.2.1 Propósito

Para obtener la información general con respecto al Switch.

2.9.4.1.2.2 Entradas

Ninguno.

2.9.4.1.2.3 Salidas

- a) La Dirección del Switch—la Dirección MAC para el Switch de que el Identificador del Switch usado por el Algoritmo de Spanning Tree y el Protocolo se deriva (ISO/IEC 15802-3).

- b) Nombre del Switch—un texto de longitud de 32 caracteres, de importancia localmente determinada.
- c) Número de Puertos—el número de puertos del Switch (Entidades MAC).
- d) Direcciones de Puerto—una lista especificando el siguiente para cada puerto:
 - 1) El Número del puerto (ISO/IEC 15802-3).
 - 2) La Dirección de puerto—la dirección MAC específica de la MAC Entidad individual asociado con el puerto.
- e) Tiempo arriba—cuenta en segundos del tiempo transcurrido desde que el Switch fue restablecido o inicializó (ISO/IEC 15802-3).

2.9.4.1.3 Configuración del Nombre del Switch

2.9.4.1.3.1 Propósito

Para asociar una cadena de texto, legible para la operación de Lectura del Switch, con un Switch.

2.9.4.1.3.2 Entradas

- a) Nombre del Switch—una cadena de texto con 32 caracteres.

2.9.4.1.3.3 Salidas

Ninguno.

2.9.4.1.4 Reinicialización del Switch

2.9.4.1.4.1 Propósito

Para restablecer el Switch especificado. El Filtraje de la Base de Datos se limpia e inicializa con las entradas especificadas en la Base de Datos Permanente, y la Entidad del Protocolo del Switch es inicializado (ISO/IEC 15802-3).

2.9.4.1.4.2 Entradas

Ninguno.

2.9.4.1.4.3 Salidas

Ninguna.

2.9.4.2 Configuración del Puerto

La Configuración del puerto objeto modela las operaciones que modifica, o inquiriere sobre, la configuración de los puertos de un Switch. Hay una configuración fija de los puertos del Switch por Switch (una MAC para cada interfaz), y cada uno es identificado por un Número de puerto permanentemente asignado.

Los Números de puerto asignados no se exigen ser consecutivos. También, algunos Números del puerto pueden ser entradas mudas, sin el puerto de LAN real (por ejemplo, para permitir una expansión del Switch por adición más allá por la suma de MAC una en el futuro). Los puertos mudos apoyarán el funcionamiento de dirección de la Configuración de Puertos, y otros funcionamientos de puerto-dirección relacionados de una manera consistente con el puerto que es permanentemente inválido.

La información proporcionada por la Configuración del puerto consiste en datos sumados que indican su nombre y tipo. Especifica información contada que pertenece al número de paquetes enviados, filtrados, y en error se mantiene por el recurso del Proceso de Envío. Las operaciones de administración soportadas por la Entidad del Protocolo del Switch permiten controlar los estados de cada puerto.

Las operaciones de administración que pueden realizarse en la Configuración del puerto son

- a) Lectura de puerto;
- b) Configuración del Nombre de puerto.

2.9.4.2.1 Lectura del Puerto

2.9.4.2.1.1 Propósito

Para obtener la información general con respecto a un puerto del Switch específico.

2.9.4.2.1.2 Entradas

- a) Número de puerto—el número del puerto del Switch (ISO/IEC 15802-3).

2.9.4.2.1.3 Salidas

- a) Nombre del puerto—una cadena de texto de 32 caracteres, de importancia localmente determinada.
- b) Tipo de puerto—el tipo de MAC Entidad del Puerto (IEEE Std 802.3; ISO/IEC 8802-4; ISO/IEC 8802-5; ISO/IEC 8802-6; ISO/IEC 8802-9; IEEE Std 802.9a-1995; ISO/IEC 8802-12 (formato IEEE Std 802.3); ISO/IEC 8802-12 (formato ISO/IEC 8802-5); ISO 9314; otro).

2.9.4.2.2 Configuración del Nombre de puerto

2.9.4.2.2.1 Propósito

Para asociar un cadena de texto, legible por la operación de Lectura de Puerto, con un puerto del Switch.

2.9.4.2.2.2 Entradas

- a) Número de Puerto (ISO/IEC 15802-3).
- b) Nombre del Puerto—a cadena de texto de 32 caracteres.

2.9.4.2.2.3 Salidas

Ninguno.

2.9.5 Entidades MAC

La Administración de Operaciones y Medios proporcionados por las Entidades MAC son aquellos especificados en el estándar de la Capa de Administración de MACs individuales. Una MAC Entidad es asociada con cada Puerto del Switch.

2.9.6 Proceso de Envío

El Proceso de Envío contiene información relacionada al envío de tramas. Los contadores son mantenidos que proveen información sobre el número de tramas enviadas, filtradas, y dejó caer la deuda al error. La Configuración de datos, define cómo la trama prioridad es manipulada, es mantenido por el Proceso de Envío.

Los objetos que comprenden este recurso de administración son

- a) Los Contadores de Puerto.
- b) La Prioridad de Manipulación de objetos para cada Puerto;
- c) La Tabla de Clase de Tráfico por cada Puerto.

2.9.6.1 Los Contadores de Puerto

Los Contadores de Puerto a modelos de objeto las operaciones que pueden realizarse en los contadores de Puerto del recurso del Proceso de Envío. Hay casos múltiples (uno para cada VLAN para cada MAC Entidad) del objeto de Contadores de Puerto por Switch.

La operación de administración que puede realizarse en los Contadores del Puerto que Envía a los Contadores del Puerto de Lectura.

2.9.6.1.1 Lectura Enviada a los contadores del puerto

2.9.6.1.1.1 Propósito

Para leer los contadores enviados asociados con un puerto del Switch específico.

2.9.6.1.1.2 Entradas

- a) Número de Puerto (ISO/IEC 15802-3);
- b) Opcionalmente, Identificador de VLAN.

Si el parámetro Identificador de VLAN es soportado, entonces los contadores del puerto enviado se mantienen por VLAN de puerto. Si el parámetro no es soportado, entonces el envío de contadores del puerto sólo se mantienen por puerto.

2.9.6.1.1.3 Salidas

- a) Tramas Recibidas—suma de todas las tramas válidas recibidas (incluso BPDUs, tramas direccionadas al Switch como una estación final y tramas que están sometidas al Proceso de Envío).
- b) Opcionalmente, Octetos Recibidos—cuenta del número total de octetos en todas las tramas validas recibidas (incluyendo BPDUs, las tramas direccionadas al Switch como una estación final, y tramas que son sometidas al Proceso de Envío).
- c) Desecho Entrante—cuenta de tramas recibidas que son descartadas por el Proceso de Envío.
- d) Envío de Salida—cuenta de tramas enviadas para asociar la MAC Entidad.
- e) Desechando la Falta de Buffers—cuenta de tramas que fueron transmitidas a través del Puerto asociado pero será descartado debido a la falta de memoria intermedia.
- f) Retraso de Tránsito por Desecho Excedido—cuenta de tramas que serían transmitidas pero estaban descartadas debido al puente con máximo tránsito retrasado sería excedido (los buffers pueden haber estado disponibles).
- g) Desechando un Error—cuneta de tramas que serían enviadas a la MAC asociada pero no podría ser transmita (por ejemplo, la tramas habría sido larga, ISO/IEC 15802-3).
- h) Si el Ingreso Filtrante es soportado, Descartado por Ingreso Filtrante—cuenta de tramas que son descartadas como resultado de Ingreso Filtrante al ser habilitado.
- i) Opcionalmente, Desecho en Detalles de Error—una lista de 16 elementos, cada uno que contiene la dirección fuente de una trama y la razón por qué la trama estaba descartada (trama demasiado larga). La lista se mantiene como un buffer circular. Las razones para descartar un error, en la actualidad, son
 - 1) Servicio transmisible de unidad de datos de tamaño excedido; o
 - 2) Desecho debido a la Filtración de Ingreso. El VID asociada con la última trama es grabado.

2.9.6.2 Manejo de Prioridad

El Manejo de Prioridad de objetos modelan las operaciones que pueden realizarse, o inquiriere sobre, el parámetro de Prioridad de Usuario Predefinido, la Regeneración de la Tabla del parámetro del Usuario Prioridad, y la Tabla de parámetros de Prioridad de Acceso de Salida por cada puerto. Los funcionamientos que pueden realizarse en este objeto son

- a) Lectura de Puerto de Prioridad de Usuario Predefinido;
- b) Configuración de Puerto de Prioridad de Usuario Predefinida;
- c) Lectura de Puerto Usuario de Prioridad con Regeneración de Tabla;
- d) Configuración de Puerto Usuario de Prioridad con Regeneración de Tabla;
- e) Lectura de Acceso de salida de Prioridad de Tabla.

2.9.6.2.1 Lectura de puerto de Prioridad de Usuario Predefinido

2.9.6.2.1.1 Propósito

Para leer el estado actual del parámetro de Prioridad de Usuario Predefinido (ISO/IEC 15802-3) para un puerto de Switch específico.

2.9.6.2.1.2 Entradas

- a) Número de puerto.

2.9.6.2.1.3 Salidas

- a) El valor de Prioridad de Usuario Predefinido- Integra un rango de 0-7. _____

2.9.6.2.2 Configuración de puerto de Prioridad del Usuario Predefinida

2.9.6.2.2.1 Propósito

Para configurar el estado actual del parámetro de Prioridad de Usuario Predefinido (ISO/IEC 15802-3) para un puerto específico del Switch.

2.9.6.2.2.2 Entradas

- a) Número de Puerto;
- b) Valor de de Prioridad Usuario Predefinido—Integra un rango 0–7.

2.9.6.2.2.3 Salidas

Ninguno.

2.9.6.2.3 Lectura de Puerto Usuario Prioridad Regeneración de Tabla

2.9.6.2.3.1 Propósito

Para leer el estado actual del parámetro Usuario Prioridad Regeneración de Tabla para un puerto del Switch específico.

2.9.6.2.3.2 Entradas

- a) Número de puerto.

2.9.6.2.3.3 Salidas

- a) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 0—Integrado en un rango 0–7.
- b) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 1—Integrado en un rango 0–7.
- c) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 2—Integrado en un rango 0–7.
- d) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 3—Integrado en un rango 0–7.
- e) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 4—Integrado en un rango 0–7.
- f) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 5—Integrado en un rango 0–7.
- g) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 6—Integrado en un rango 0–7.
- h) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 7—Integrado en un rango 0–7.

2.9.6.2.4 Configuración Puerto Usuario Prioridad Regeneración de Tabla

2.9.6.2.4.1 Propósito

Para poner el estado actual del parámetro Usuario Prioridad Regeneración Tabla para un Puerto del Switch específico.

2.9.6.2.4.2 Entradas

- a) Número de puerto;
- b) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 0—Integrado en un rango 0–7.
- c) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 1—Integrado en un rango 0–7.
- d) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 2—Integrado en un rango 0–7.
- e) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 3—Integrado en un rango 0–7.
- f) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 4—Integrado en un rango 0–7.
- g) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 5—Integrado en un rango 0–7.
- h) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 6—Integrado en un rango 0–7.

- i) Regeneró el valor de Prioridad de Usuario por el Usuario Recibido Prioridad 7—Integrado en un rango 0–7.

2.9.6.2.4.3 Salidas

Ninguno.

2.9.6.2.5 Lectura de Acceso de Salida con Prioridad de Tabla

2.9.6.2.5.1 Propósito

Para leer el estado del parámetro de Acceso de Salida con Prioridad de Tabla para un puerto del Switch específico.

2.9.6.2.5.2 Entradas

- a) Número de Puerto.

2.9.6.2.5.3 Salidas

- a) Prioridad de Acceso valor para el Usuario Prioridad 0—Integrado en un rango 0–7.
- b) Prioridad de Acceso valor para el Usuario Prioridad 1— Integrado en un rango 0–7.
- c) Prioridad de Acceso valor para el Usuario Prioridad 2— Integrado en un rango 0–7.
- d) Prioridad de Acceso valor para el Usuario Prioridad 3— Integrado en un rango 0–7.
- e) Prioridad de Acceso valor para el Usuario Prioridad 4— Integrado en un rango 0–7.
- f) Prioridad de Acceso valor para el Usuario Prioridad 5— Integrado en un rango 0–7.
- g) Prioridad de Acceso valor para el Usuario Prioridad 6— Integrado en un rango 0–7.
- h) Prioridad de Acceso valor para el Usuario Prioridad 7— Integrado en un rango 0–7.

2.9.6.3 Tabla de Clase de tráfico

Los modelos de operación de la Tabla de Clase de Tráfico pueden realizarse, o inquiriere sobre, los contenidos actuales de la Tabla de Clase de Tráfico para un puerto dado. Las operaciones que pueden realizarse en este objeto son la Lectura de Clase de Tráfico y Configuración de la Tabla de Clase de Tráfico.

2.9.6.3.1 Lectura de la Tabla de Clase de Tráfico

2.9.6.3.1.1 Propósito

Para leer los contenidos de la Tabla de la Clase de Tráfico para un puerto dado.

2.9.6.3.1.2 Entradas

- a) Número de puerto.

2.9.6.3.1.3 Salidas

- a) El número de Clases de Tráfico, en el rango 1 a través de 8, soportado en el Puerto;
- b) Para cada valor de Clase de Tráfico apoyado en el puerto, el valor de la Clase de Tráfico en el rango 0 a 7, y la configuración del valor asignado de `user_priority` para que Clase de Tráfico.

2.9.6.3.2 Configuración de la Tabla de Clase de Tráfico

2.9.6.3.2.1 Propósito

Para configurar los contenidos de la Tabla de Clase de Tráfico para un puerto dado.

2.9.6.3.2.2 Entradas

- a) Número de Puerto;
- b) Para cada valor de Clase de Tráfico soportado en el puerto, el valor de la Clase de Tráfico en el rango 0 a 7, y la configuración del valor asignado de `"user_priority"` para que Clase de Tráfico.

2.9.6.3.2.3 Salidas

Ninguna.

2.9.7 Filtrando la Base de Datos

Contiene información de filtraje usada por el *Proceso de Envío* decidiendo a través de que puertos del Switch las tramas deben enviarse.

Los objetos que comprenden estos recursos de administración son

- a) La Filtración de la Base de Datos;
- b) Las Entradas de la Filtración Estática;
- c) Las Entradas de la Filtración Dinámica;
- d) Las Entradas del Registro de Grupo;
- e) Los Registros de Entradas de VLAN Estáticas;
- f) Los Registros de Entradas de VLAN Dinámicas;
- g) La Base de Datos Permanente.

2.9.7.1 La Filtración de la Base de Datos

La Filtración de la Base de Datos modelan las operaciones que pueden ser realizadas, o afecta, el Filtraje de la Base de Datos como un conjunto. Hay un solo objeto de Filtración de Base de Datos por el Switch.

La administración de operaciones que pueden realizarse en la Base de Datos son:

- a) Lectura de la Base de Datos Filtrada;
- b) Configuración del Tiempo de Envejecimiento del Filtraje de la Base de Datos;
- c) Lectura Permanente de la Base de Datos;
- d) Creando el Filtraje de Entrada;
- e) Borrando el Filtraje de Entrada;
- f) Leyendo el Filtraje de Entrada;
- g) Leyendo el Filtraje de Rango de Entrada.

2.9.7.1.1 Lectura del Filtraje de la Base de Datos

2.9.7.1.1.1 Propósito

Obtener la información general con respecto al Puente está Filtrándose la Base de datos.

2.9.7.1.1.2 Entradas

Ninguno.

2.9.7.1.1.3 Salidas

- a) Tamaño del Filtraje de la Base de Datos—el número máximo de entradas que pueden sostenerse en el Filtro de la Base de Datos.
- b) Número de Filtraje de la Entrada Estática—el número de Filtraje de Entradas Estáticas actualmente en la Base de datos Filtrándose;
- c) Número de Filtración de Entradas Dinámica—el número de Entradas del Filtraje Dinámico actualmente en el Filtro de la Base de Datos;
- d) Número de Registro de Entradas de VLAN Estática—el numero de Registro de Entradas de VLAN Estáticas actualmente Filtrando la Base de Datos;
- e) El Número de Registro de Entradas de VLAN Dinámicas—el número de Registro de Entradas de VLAN Dinámica actualmente en el Filtro de la Base de Datos.
- f) Tiempo de Envejecimiento—por envejecimiento fuera de las Entradas del Filtro Dinámicas cuando el Puerto asociado con la entrada es en el estado de Envío.
- g) Si los Servicios de Filtración Extendidos son soportados, el Número de Registro de Entradas de Grupos—numeran las Entradas de Registro de Grupo actualmente en la Base de datos del Filtro;

2.9.7.1.2 Configuración del Tiempo de Envejecimiento del Filtraje de la Base de Datos

2.9.7.1.2.1 Propósito

Para poner el tiempo viejo por las Entradas de la Filtración Dinámicas (8.11.3).

2.9.7.1.2.2 Entradas

- a) Tiempo de envejecimiento.

2.9.7.1.2.3 Salidas

Ninguno.

2.9.7.2 Una Entrada de la Filtración Estática

Una Entrada de la Filtración Estática objeto modelos que pueden realizarse en una sola Entrada de la Filtración Estática en la Base de Datos del Filtro. La configuración de la Entrada de la Filtración Estática dentro del Filtrado de la Base de Datos sólo cambia bajo control de administración.

Una Entrada de la Filtración Estática soporta las siguientes operaciones:

- a) Crear el Filtro de Entrada;
- b) Borrar el Filtro de Entrada;
- c) Lectura del Filtro de Entrada;
- d) Lectura del Filtro de Rango de Entrada.

2.9.7.3 Entrada del Filtrado Dinámico

Filtración de Entrada Dinámica modela las operaciones que pueden realizarse en una sola Entrada de la Filtración Dinámica (es decir, uno que se crea por el Proceso de Aprendizaje como resultado de la observación de tráfico de la red) en el Filtrado de la Base de Datos.

Un Filtrado de Entrada Dinámica soporta las siguientes operaciones:

- a) Borrar el Filtrado Entrante;
- b) Lectura del Filtrado Entrante;
- c) Lectura del Rango de Entrada del Filtro.

2.9.7.4 Registro de un Grupo Entrante

Un Registro de un Grupo de Entrada las operaciones que pueden realizarse en un simple Registro de Grupo Entrante en el Filtro de la Base de Datos. La configuración de Registro de Entrada de Grupo dentro del Filtro de la Base de Datos cambia solo con un resultado del intercambio del protocolo GARP.

Un Registro de Entrada de Grupo soporta las siguientes operaciones:

- a) Lectura del Filtrado Entrante;
- b) Lectura del Rango de Entrada del Filtro.

2.9.7.5 Registro Entrante de una VLAN

Un Registro Entrante de una VLAN las operaciones pueden realizarse en un solo Registro Entrante de una VLAN en el Filtro de la Base de Datos. La configuración del Registro Entrante de la VLAN dentro de los cambios del Filtro de la Base de Datos bajo la administración y también como un resultado de intercambio del protocolo GARP.

2.9.7.5.1 Objeto Registro Entrante de una VLAN Estática

Un Registro Entrante de una VLAN Estática soporta las siguientes operaciones:

- a) Crea el Filtrado Entrante;
- b) Borra el Filtrado Entrante;
- c) Lectura del Filtrado Entrante;
- d) Lectura del Rango de Filtrado de Entrada.

2.9.7.5.2 Objeto Registro Entrante de una VLAN Dinámica

Un Registro Entrante de una VLAN Dinámica soporta las siguientes operaciones:

- a) Lectura del Filtrado Entrante;
- b) Lectura del Rango de Filtrado de Entrada.

2.9.7.6 Base de Datos Permanente

La Base de Datos Permanente soporta las operaciones que pueden realizarse, o afecta, la Base de Datos Permanente. Hay una sola Base de Datos Permanente por Filtrado de Base de Datos.

La administración del funcionamiento que puede realizarse en la Base de Datos Permanente son

- a) Lectura de la Base de Datos Permanente;
- b) Crea la Entrada del Filtro;
- c) Borra la Entrada del Filtro;
- d) Lectura de la Entrada del Filtro;

- e) Lectura del Rango de Filtrado de Entrada.

2.9.7.6.1 Lectura la Base de datos Permanente

2.9.7.6.1.1 Propósito

Para obtener información general con respecto a la Base de datos Permanente.

2.9.7.6.1.2 Entradas

Ninguno.

2.9.7.6.1.3 Salidas

- a) Tamaño de la Base de Datos Permanente—número máximo de entradas que pueden sostenerse en la Base de Datos Permanente.
- b) Número de Entradas de Filtrado Estático—numero de Entradas de Filtrado Estático actualmente en la Base de Datos Permanente;
- c) Número de Entradas de Filtrado de VLAN Estática—numero de Registro de Entradas de VLAN Estática actualmente en la Base de datos Permanente.

2.9.7.7 Operación del Filtrado General de la Base de Datos

En estas operaciones del Filtrado de la Base de Datos, la operación de los parámetros hace uso de valores VID, incluso al operar una Entrada de Filtrado Dinámica de quien la estructura lleva un FID en lugar de un VID. En este caso, el valor usado en el parámetro de VID puede ser cualquier VID que se ha asignado al FID involucrado.

2.9.7.7.1 Crean la Entrada de la Filtrado

2.9.7.7.1.1 Propósito

Crear o actualizar una Entrada de la Filtrado Estática o el Registro Entrante de VLAN Estática en el Filtrado de la Base de Datos o de la Base de Datos Permanente. Pueden crearse sólo entradas estáticas en el Filtro de la Base de Datos o la Base de Datos Permanente.

2.9.7.7.1.2 Entradas

- a) Identificador—Filtrado de la Base de Datos o la Base de Datos Permanente.
- b) Dirección—la dirección MAC de la entrada (no el presente en el Registro de Entrada).
- c) VID— El Identificador de entrada de la VLAN.
- d) Mapeo de puerto—una configuración de los indicadores de control, uno para cada puerto.

2.9.7.7.1.3 Salidas

Ninguna.

2.9.7.7.2 Borrando la Entrada de la Filtrado

2.9.7.7.2.1 Propósito

Para anular una Entrada de la Filtrado o el Registro de Entrada del Filtrado de la Base de Datos de la VLAN o la Base de Datos Permanente.

2.9.7.7.2.2 Entradas

- a) Identificador—Filtrado de la Base de Datos o la Base de Datos Permanente.
- b) Dirección—Dirección MAC de la entrada deseada (no el presente en el Registro de Entradas de la VLAN).
- c) VID— el Identificador de entrada de la VLAN.

2.9.7.7.2.3 Salidas

Ninguna.

2.9.7.7.3 Lectura de la Entrada de Filtración

2.9.7.7.3.1 Propósito

Para leer una Entrada de la Filtración, Registro de Entrada de Grupo, o Registro de Entrada de la VLAN o las Bases de Datos Permanente.

2.9.7.7.3.2 Entradas

- a) Identificador—Filtraje de la Base de Datos o la Base de Datos Permanente.
- b) Dirección—dirección MAC de la entrada deseada (no el presente en el Registro de Entradas de la VLAN).
- c) VID—el Identificador de entrada de la VLAN.
- d) Tipo—entrada Estática o Dinámica.

2.9.7.7.3.3 Salidas

- a) Dirección—dirección MAC de la entrada deseada (no el presente en el Registro de Entrada de la VLAN).
- b) VID—el Identificador de entrada de la VLAN.
- c) Tipo—entrada Estática o Dinámica.
- d) Mapeo de Puerto—una configuración de indicadores de control como apropiada para la entrada.

2.9.7.7.4 Lectura del Rango de Filtraje de Entrada

2.9.7.7.4.1 Propósito

Para leer un rango de Filtraje de las entradas de la Base de Datos (de cualquier tipo) de la Filtración o las Bases de Datos Permanentes.

Desde el número de valores para ser devueltos en el rango pedido pueden haber excedido la capacidad de servicio de la unidad de datos que lleva la respuesta de administración, el regreso del rango de entrada se identifica. El índice que define el rango tomado en valores de cero a Filtrarse el Tamaño de la Base de Datos menos uno.

2.9.7.7.4.2 Entradas

- a) Identificador—del Filtraje de la Base de Datos o la Base de Datos Permanente.
- b) Índice de Inicio—inclusive el índice de inicio del rango de entrada deseado.
- c) Índice de Parada—inclusive el índice de parada del rango deseado.

2.9.7.7.4.3 Salidas

- a) Índice de Inicio—inclusive el índice de inicio del rango de la entrada devuelto.
- b) Índice de Parada—inclusive el índice final del rango de la entrada devuelto.
- c) Por cada índice devuelto:
 - 1) Dirección—dirección MAC de la entrada deseada (no el presente en el Registro de Entradas de la VLAN).
 - 2) VID—identificador de la VLAN entrante.
 - 3) Tipo—entrada Estática o Dinámica.
 - 4) Mapeo de Puerto—una configuración de indicadores de control como apropiado para la entrada.

2.9.8 Protocolo Entidad del Switch

El Protocolo Entidad del Switch se describe en ISO/IEC 15802-3.

Los objetos que comprenden este recurso de administración son

- a) El propio Protocolo Entidad.
- b) Los Puertos bajo su control.

2.9.8.1 El Protocolo Entidad

El Protocolo Entidad muestra las operaciones que pueden realizarse, o inquiriere sobre, la operación del Algoritmo y Protocolo de *Spanning Tree*. Hay un solo Protocolo Entidad por Switch; puede, por consiguiente, ser identificado como un solo componente fijo del recurso del Protocolo Entidad.

Las operaciones administrativas que pueden realizarse en el Protocolo Entidad son

- a) Lectura de los Parámetros del Protocolo del Switch;
- b) Configuración de los Parámetros del Protocolo del Switch.

2.9.8.1.1 Lectura de los Parámetros del Protocolo del Switch

2.9.8.1.1.1 Propósito

Para obtener la información con respecto al Switch del Protocolo Entidad del Switch.

2.9.8.1.1.2 Entradas

Ninguna.

2.9.8.1.1.3 Salidas

- a) Identificador del Switch—definido en ISO/IEC 15802-3.
- b) Tiempo desde el Cambio de Topología—cuenta en segundos del tiempo pasado desde el parámetro bandera del Cambio de Topología (ISO/IEC 15802-3) será el último Verdadero.
- c) Cuenta del Cambio de Topología—cuenta de los tiempos del parámetro bandera del Cambio de Topología del Switch tiene que ser fijo (es decir, la transición de Falso a Verdadero) desde que el Switch fue apagado o inicializado.
- d) Cambio de Topología (ISO/IEC 15802-3).
- e) Raíz Designada (ISO/IEC 15802-3).
- f) Costo de Ruta Raíz (ISO/IEC 15802-3).
- g) Puerto Raíz (ISO/IEC 15802-3).
- h) Edad Máxima (ISO/IEC 15802-3).
- i) Tiempo de Saludo (Hello Time) (ISO/IEC 15802-3).
- j) Retraso de Envío (ISO/IEC 15802-3).
- k) Edad Máxima del Switch (ISO/IEC 15802-3).
- l) Tiempo de Saludo al Switch (ISO/IEC 15802-3).
- m) Retraso de Envío del Switch (ISO/IEC 15802-3).
- n) Tiempo de retención (hold time) (ISO/IEC 15802-3).

2.9.8.1.2 Configuración de los Parámetros de Protocolos del Switch

2.9.8.1.2.1 Propósito

Para modificar los parámetros en el Switch del *Protocolo Entidad del Switch* en orden para forzar una configuración del *Spanning Tree* y/o poner a punto el tiempo de reconfiguración para satisfacer una topología específica.

2.9.8.1.2.2 Entradas

- a) Edad Máxima del Switch—el nuevo valor (ISO/IEC 15802-3).
- b) Tiempo de Saludo del Switch—el nuevo valor (ISO/IEC 15802-3).
- c) Retraso de Envío del Switch—el nuevo valor (ISO/IEC 15802-3).
- d) Switch Prioridad—el nuevo valor de la parte de prioridad del Identificador del Switch (ISO/IEC 15802-3).

2.9.8.1.2.3 Salidas

Ninguna.

2.9.8.1.2.4 Procedimiento

Los valores de parámetro de entrada se verifican de acuerdo a ISO/IEC 15802-3. Si ellos no cumplen, o el valor de *Edad Máxima del Switch* o el *Retraso de Envío del Switch* es menor que el límite de rango mas bajo especificado en ISO/IEC 15802-3, entonces ninguna acción se tomará para cualquiera de los parámetros proporcionados. Si el valor cualquiera de *Edad Máxima del Switch*, *Retraso de Envío del Switch*, *Retraso de Envío del Switch*, o *Tiempo de Saludo del Switch* está fuera del rango especificado en ISO/IEC 15802-3, entonces la necesidad del Switch no toma acción.

El procedimiento de *Configuración de Prioridad del Switch (ISO/IEC 15802-3)* se usa para poner la parte de prioridad del valor proporcionado al Identificador del Switch.

2.9.8.2 Puerto del Switch

Es un puerto del Switch relacionado a un puerto individual del Switch en relación a la operación del algoritmo y protocolo de Spanning Tree, es una configuración fija de puertos en el Switch por el Switch; puede cada puerto ser identificado por un Número de puerto asignado permanentemente, como un componente fijo del recurso del Protocolo Entidad.

La administración de las operaciones que pueden realizarse en un puerto del Switch son

- a) Parámetros de Puerto de Lectura;
- b) Estado de Fuerza de Puerto;
- c) Configuración de Parámetros de Puerto.

2.9.8.2.1 Parámetros de Puerto de lectura

2.9.8.2.1.1 Propósito

Para obtener la información con respecto a un puerto en específico dentro del Switch en el Protocolo del Switch Entidad.

2.9.8.2.1.2 Entradas

- a) Número de Puerto—numeran el Puerto del Switch.

2.9.8.2.1.3 Salidas

- a) Tiempo activo—cuenta en segundos el tiempo que pasó desde que el puerto fue restablecido o inicializado (ISO/IEC 15802-3).
- b) Estado—el estado actual del puerto (es decir, deshabilitado, escuchando, aprendiendo, enviando, o bloqueando) (ISO/IEC 15802-3).
- c) Identificador de puerto—el único identificador de puerto que comprende dos partes, el Número del Puerto y el campo de Prioridad de puerto (ISO/IEC 15802-3).
- d) Costó de Ruta (ISO/IEC 15802-3).
- e) Raíz Designada (ISO/IEC 15802-3).
- f) Costo Designado (ISO/IEC 15802-3).
- g) Switch Designado (ISO/IEC 15802-3).
- h) Puerto Designado (ISO/IEC 15802-3).
- i) Cambio de Topología Reconocida (ISO/IEC 15802-3).

2.9.8.2.2 Estado de Fuerza de Puerto

2.9.8.2.2.1 Propósito

Para forzar el puerto especificado a Deshabilitarse (ISO/IEC 15802-3) o Bloquearse (ISO/IEC 15802-3).

2.9.8.2.2.2 Entradas

- a) Número de puerto—el número de puerto del Switch.
- b) Estado—cualquiera deshabilitado o bloqueando (ISO/IEC 15802-3).

2.9.8.2.2.3 Salidas

Ninguna.

2.9.8.2.2.4 Procedimiento

Si el estado seleccionado es deshabilitado, el puerto deshabilitado (ISO/IEC 15802-3) se usa para el puerto especificado. Si el estado seleccionado está Bloqueando, el puerto habilitado procede a ser usado (ISO/IEC 15802-3).

2.9.8.2.3 Configuración de parámetros de puerto

2.9.8.2.3.1 Propósito

Para modificar los parámetros para un puerto en el Switch del Protocolo de Entidad del Switch para forzar una configuración de *Spanning Tree*.

2.9.8.2.3.2 Entradas

- a) *Número de puerto*—enumeran el puerto del Switch.
- b) *Costo de Ruta*—el nuevo valor (ISO/IEC 15802-3).
- c) *Puerto Prioridad*—el nuevo valor del campo de prioridad para el Identificador de puerto (ISO/IEC 15802-3).

2.9.8.2.3.3 Salidas

Ninguna.

2.9.8.2.3.4 Procedimiento

El procedimiento de *Costo de Ruta Fija* (ISO/IEC 15802-3) se usa para configurar el parámetro *Costo de Ruta* para el puerto especificado. El procedimiento de *Prioridad de Puerto Fijo* (ISO/IEC 15802-3) se usa para poner la parte de prioridad del *Identificador del puerto* (ISO/IEC 15802-3) al valor proporcionado.

2.9.9 Entidades GARP

La operación de GARP se describe en ISO/IEC 15802-3. Los objetos que comprenden este recurso de administración es

- a) El Cronómetro de GARP;
- b) El Atributo Tipo GARP;
- c) El Estado de la Máquina GARP.

2.9.9.1 El Cronómetro de GARP

El *Cronómetro de GARP* muestra las operaciones que pueden realizarse, o inquiriere sobre, las escenas actuales de los cronómetros usadas por el protocolo de *GARP* en un puerto dado. Las operaciones de administración que pueden realizarse en el *GARP Participante* son

- a) Lectura de los *Cronómetros de GARP*;
- b) Configuración de los *Cronómetros de GARP*.

2.9.9.1.1 Lectura los Cronómetros de GARP

2.9.9.1.1.1 Propósito

Para leer los *Cronómetros de GARP* actuales para un puerto dado.

2.9.9.1.1.2 Entradas

- a) El identificador de puerto.

2.9.9.1.1.3 Salidas

- a) El valor Actual de "*JoinTime*"—Centésimas de segundos (ISO/IEC 15802-3);
- b) El valor Actual de "*LeaveTime*"— Centésimas de segundos (ISO/IEC 15802-3);
- c) El valor Actual de "*LeaveAllTime*"— Centésimas de segundos (ISO/IEC 15802-3).

2.9.9.1.2 Configuración de los Cronómetros de GARP

2.9.9.1.2.1 Propósito

Para poner los nuevos valores por los Cronómetros de GARP para un puerto dado.

2.9.9.1.2.2 Entradas

- a) El identificador de puerto;
- b) El nuevo valor de "*JoinTime*"— Centésimas de segundos (ISO/IEC 15802-3);
- c) El nuevo valor de "*LeaveTime*"— Centésimas de segundos (ISO/IEC 15802-3);
- d) El nuevo valor de "*LeaveAllTime*"— Centésimas de segundos (ISO/IEC 15802-3).

2.9.9.1.2.3 Salidas

Ninguna.

2.9.9.2 El Atributo Tipo GARP

El *Atributo Tipo GARP* muestra las operaciones que pueden realizarse, o inquiriere sobre, el funcionamiento de *GARP* para un *Tipo del Atributo* dado (ISO/IEC 15802-3). La administración de operaciones que pueden realizarse en un *Atributo Tipo GARP* son

- a) Lectura de Solicitante de Controles *GARP*;
- b) Configuración del Solicitante de Controles *GARP*.

2.9.9.2.1 Lectura de Solicitante de Controles *GARP*

2.9.9.2.1.1 Propósito

Para leer valores actuales de los parámetros del Solicitante Administrativo del control de parámetros *GARP* (ISO/IEC 15802-3) asociado con todos los Participantes *GARP* para un puerto dado, *Aplicación GARP* y *Tipo del Atributo*.

2.9.9.2.1.2 Entradas

- a) El identificador de puerto;
- b) La dirección de *Aplicación GARP* (ISO/IEC 15802-3);
- c) El *Tipo de Atributo* (ISO/IEC 15802-3).

2.9.9.2.1.3 Salidas

- a) El actual Solicitante al Valor de Control Administrativo (ISO/IEC 15802-3);
- b) Registros Fallidos—Cuenta del número de tiempos que esta *Aplicación GARP* no ha registrado un atributo de este tipo debido a la falta de espacio en la *Base de Datos de Filtrado*.

2.9.9.2.2 Configuración del Solicitante de Controles *GARP*

2.9.9.2.2.1 Propósito

Para poner los nuevos valores para los parámetros de control del Solicitante Administrativo *GARP* (ISO/IEC 15802-3) asociado con todos los Participantes *GARP* para un puerto dado, *Aplicación GARP* y *Tipo de Atributo*.

2.9.9.2.2.2 Entradas

- a) El identificador de puerto;
- b) La dirección de *Aplicación GARP* (ISO/IEC 15802-3);
- c) El *Tipo de Atributo* (ISO/IEC 15802-3) asociado con el estado de la máquina;
- d) El Solicitante deseado al *Valor de Control Administrativo* (ISO/IEC 15802-3).

2.9.9.2.2.3 Salidas

Ninguna.

2.9.9.3 El Estado de Máquina *GARP*

El Estado de la Máquina *GARP* modela las operaciones que pueden realizarse, o inquiriere sobre, el funcionamiento de *GARP* para el Estado de una Máquina dada.

La operación de administración que puede realizarse en un Estado de Máquina *GARP* se Lee el Estado de *GARP*.

2.9.9.3.1 Lectura del Estado de *GARP*

2.9.9.3.1.1 Propósito

Para leer el valor actual de un caso de un estado de una máquina *GARP*.

2.9.9.3.1.2 Entradas

- a) Identificador de puerto;
- b) La dirección de *Aplicación GARP* (ISO/IEC 15802-3);
- c) El Contexto de *GIP* (ISO/IEC 15802-3);
- d) El *Tipo de Atributo* (ISO/IEC 15802-3) asociado con el estado de máquina;
- e) El *Valor del Atributo* (ISO/IEC 15802-3) asociado con el estado de máquina.

2.9.9.3.1.3 Salidas

- a) El valor actual del Solicitante combinado y Registrador del estado de máquina para el atributo (ISO/IEC 15802-3);
- b) Opcionalmente, Creador de dirección—la dirección MAC del creador de la más reciente PDU GARP que será responsable para causar un cambio en el estado en este estado de máquina (ISO/IEC 15802-3).

2.9.10 Administrar el Switch VLAN

La siguiente administración define la semántica de los funcionamientos de administración que pueden realizarse en los aspectos de VLAN de un Switch:

- a) La administración de Configuración de un Switch VLAN;
- b) La administración de Configuración de una VLAN;
- c) La administración de Contención de Aprendizaje de la VLAN.

2.9.10.1 Configuración del Switch VLAN administrado

La Configuración del Switch VLAN administrado modela las operaciones que modifican, o inquiriere sobre, la configuración global de los recursos del Switch VLAN. Hay un solo Switch que Configura el manejo de VLAN por Switch.

Las operaciones de administración que pueden realizarse en la Configuración del Switch VLAN administrado son

- a) Lectura de la Configuración del Switch VLAN;
- b) Configurar valores PVID;
- c) Configurar los parámetros de Tipo de Tramas Aceptables;
- d) Configurar los parámetros de Filtrado de Ingreso Habilitado;
- e) Reinicialización del Switch VLAN;
- f) Notifique el registro de falla VLAN.

2.9.10.1.1 Puesto de la lectura la Configuración de VLAN

2.9.10.1.1.1 Propósito

Para obtener la información de VLAN general de un Switch.

2.9.10.1.1.2 Entradas

Ninguna.

2.9.10.1.1.3 Salidas

- a) El número de versión de VLAN 802.1Q. Informado como "1" por dispositivos que implementan la funcionalidad de VLAN según esta edición de la norma;
- b) Los rasgos de VLAN optativos apoyados por la aplicación:
 - 1) El número máximo de VLANs soportadas;
 - 2) Si la aplicación soporta la habilidad sustituir el PVID predefinido, y su estado de salida (*VLAN-etiquetada o desetiquetada*) en cada Puerto.
- c) Para cada puerto:
 - 1) El número de puerto;
 - 2) El valor PVID actualmente asignado a ese puerto;
 - 3) El estado del parámetro de Tipos de Tramas Aceptables. Los valores permisibles para este parámetro son:
 - i) Admita solo las tramas *VLAN-etiquetadas*;
 - ii) Admita todas las tramas.
 - 4) El estado del parámetro del *Filtro de Ingreso Habilitado*; Habilitado o Deshabilitado.

2.9.10.1.2 Configuran los valores de PVID

2.9.10.1.2.1 Propósito

Para configurar el(los) valor(es) de PVID asociado con uno o más puertos.

2.9.10.1.2.2 Entradas

- a) Para cada puerto a ser configurado, un número de puerto y el valor PVID a ser asociado con ese puerto.

2.9.10.1.2.3 Salidas

Ninguna

2.9.10.1.3 Configuración de parámetros de Tipo de Tramas Aceptables

2.9.10.1.3.1 Propósito

Para configurar el parámetro de *Tipos de Tramas Aceptables* asociadas con uno o más puertos.

2.9.10.1.3.2 Entradas

- a) Para ser configurado por cada puerto, un número de puerto y el valor del parámetro de *Tipos de Tramas Aceptables* para ser asociadas con ese puerto. Los valores permitidos de este parámetro son:
 - 1) Admitir solo tramas VLAN-etiquetadas;
 - 2) Admitir todas las tramas.

2.9.10.1.3.3 Salidas

Ninguna.

2.9.10.1.4 Configurar los parámetros del Filtro de Ingreso Habilitado

2.9.10.1.4.1 Propósito

Para configurar el(los) parámetro(s) de *Filtro de Ingreso Habilitado* asociado con uno o más puertos.

2.9.10.1.4.2 Entradas

- a) Para cada puerto para ser configurado, un número de puerto y el valor del parámetro del *Filtro de Ingreso Habilitado* para ser asociado con ese puerto. Los valores permitidos para el parámetro son:
 - 1) Habilitado;
 - 2) Deshabilitado.

2.9.10.1.4.3 Salidas

Ninguna.

2.9.10.1.5 Reinicio del Switch VLAN

2.9.10.1.5.1 Propósito

Restablecer la información de configuración estáticamente de la VLAN-relacionada en el Switch a su estado predefinido. Este funcionamiento

- a) Borra toda la Configuración de administración de la VLAN;
- b) Restablece el PVID asociado con cada puerto del Switch al valor de PVID Predefinido;
- c) Restablece los parámetros de *Tipos de Tramas Aceptables* asociadas con cada puerto al valor predefinido.

2.9.10.1.5.2 Entradas

Ninguna.

2.9.10.1.5.3 Salidas

Ninguna.

2.9.10.1.6 Notificación de registro fallido de la VLAN

2.9.10.1.6.1 Propósito

Para notificar a un administrador que GVRP no ha registrado una VLAN dado que deben faltar recursos en el Filtro de la Base de Datos para la creación de un Registro de Entrada de VLAN Dinámica.

2.9.10.1.6.2 Entradas

Ninguna.

2.9.10.1.6.3 Salidas

- a) El VID del VLAN que GVRP no registró;
- b) El número de puerto, del puerto en que la demanda de registro fue recibida.

2.9.10.2 Configuración de administración de la VLAN

La configuración de la VLAN modela la operación que modifica, o inquiriere sobre, la configuración de una VLAN en particular dentro de un Switch. Esta la configuración múltiple de VLAN por Switch; sólo una puede existir para un ID VLAN dado.

Las operaciones de administración que pueden realizarse en la configuración de VLAN son:

- a) Lectura de la Configuración de VLAN;
- b) Crea la Configuración de VLAN;
- c) Borra la Configuración de VLAN;

2.9.10.2.1 Lectura de la Configuración de VLAN

2.9.10.2.1.1 Propósito

Para obtener la información general con respecto a una Configuración de VLAN específica.

2.9.10.2.1.2 Entradas

- a) El Identificador de VLAN: un VID de 12-bits.

2.9.10.2.1.3 Salidas

- a) Nombre de la VLAN: una cadena de texto de 32 caracteres de importancia localmente determinada;
- b) Lista de puertos Sin etiqueta: la configuración de números de puerto para que este VLAN ID sea un miembro desetiquetado configurado para ese puerto;
- c) Lista de puertos de Salida: la configuración de números de puerto para que este VLAN ID sea un miembro de la configuración para ese puerto.

2.9.10.2.2 Crear la Configuración VLAN

2.9.10.2.2.1 Propósito

Crear o poner al día una Configuración de VLAN manejan el objeto.

2.9.10.2.2.2 Entradas

- a) Identificador VLAN: un VID de 12-bits;
- b) Nombre de la VLAN: una cadena de texto de 32 caracteres de importancia localmente determinada.

2.9.10.2.2.3 Salidas

Ninguna.

2.9.10.2.3 Borrando la Configuración VLAN

2.9.10.2.3.1 Propósito

Para anular una Configuración de VLAN administrada.

2.9.10.2.3.2 Entradas

- a) Identificador de VLAN: un VID de 12-bits;

2.9.10.2.3.3 Salidas

Ninguna.

2.9.10.3 Aprendiendo las Restricciones de la VLAN administrada

El *Aprendizaje de las Restricciones* de la VLAN administrada modela las operaciones que modifican, o inquiriere sobre, la configuración de *Restricciones de Aprendizaje* de la VLAN y VID a las asignaciones de FID eso aplica al funcionamiento del *Proceso de Aprendizaje* y la *Base de Datos del Filtro*. Hay un sola VLAN *Aprendiendo las Restricciones* administradas por el Switch. El objeto se planea como un par de tablas de longitud fija, como sigue:

- a) Una tabla de *Restricciones de Aprendizaje* en que cada entrada de la tabla define una sola

Restricción de Aprendizaje o es indefinido. Para algunos de los funcionamientos que pueden realizarse en la tabla, se usa un índice de la entrada; esto identifica el número de la entrada en la tabla dónde el número de índice 1 es el primero, y N es el último (donde la tabla contiene las entradas de N).

- b) Un *VID* para la asignación de tabla *FID* con una entrada por *VID* soportada por la aplicación. Cada entrada de la tabla indica, para la *VID* que esta actualmente
- 1) Ninguna asignación definida; o
 - 2) Una asignación fija *FID X*; o
 - 3) Una asignación dinámica *FID X*.

Las operaciones de administración que pueden realizarse en la administración de *Aprendizaje de Restricciones* son

- c) *Lectura de Restricciones de Aprendizaje* de la VLAN;
- d) *Lectura de Restricciones de Aprendizaje* de la VLAN para VID;
- e) Configuración de *Restricciones de Aprendizaje* de la VLAN;
- f) Borra las *Restricciones de Aprendizaje* de la VLAN;
- g) Lectura de las asignaciones VID para FID;
- h) Lectura de las asignaciones FID para VID;
- i) Lectura de las asignaciones VIDs para FID;
- j) Configuración de VID para las asignaciones de FID;
- k) Borrar VID para las asignaciones de FID;
- l) Notifique la Violación de *Restricciones de Aprendizaje*;

2.9.10.3.1 Lectura de Restricciones de Aprendizaje de la VLAN

2.9.10.3.1.1 Propósito

Para leer los contenidos de un rango de una o más entradas en la tabla de *Restricciones de Aprendizaje* de la VLAN.

2.9.10.3.1.2 Entradas

- a) Primer Entrada—Índice de la primera Entrada para ser leído;
- b) Últimos Entrada— Índice de la última Entrada para ser leído.

2.9.10.3.1.3 Salidas

- a) La lista de Entradas—por cada entrada que se leyó:
 - 1) Índice de Entrada;
 - 2) El tipo del *Restricciones de Aprendizaje*: Indefinido, S o I;
 - 3) El valor de las *Restricciones de Aprendizaje*, que es de uno:
 - i) Indefinido, indicando un elemento vacío en la tabla;
 - ii) Una *Restricción* de valor S, consistiendo en un par de VIDs;
 - iii) Una *Restricción* de valor I, consistiendo de un VID y un Identificador Fijo Independiente.

2.9.10.3.2 Lectura de Restricciones de Aprendizaje de la VLAN para VID

2.9.10.3.2.1 Propósito

Para leerle las *Restricciones de Aprendizaje* de la VLAN para un VID dado.

2.9.10.3.2.2 Entradas

- a) VID—El identificador de la VLAN para el cual la lectura aplica.

2.9.10.3.2.3 Salidas

- a) Todos los valores de aprendizaje de restricciones que identifican el VID pedido. Cada valor devuelto es cualquiera:
 - 1) Un valor S Restringido, consistiendo en un par de VIDs; o
 - 2) Un valor I Restringido, consistiendo en un VID y un Identificador Fijo Independiente.

2.9.10.3.3 Configuración de *Restricciones de Aprendizaje* de la VLAN

2.9.10.3.3.1 Propósito

Para modificar los contenidos de una de las entradas de la tabla de las *Restricciones de Aprendizaje* de la VLAN.

2.9.10.3.3.2 Entradas

- a) Índice de Entrada— Índice de Entrada de la entrada a ser configurada;
- b) El tipo de Restricciones de Aprendizaje: S o I;
- c) El valor de las Restricciones de Aprendizaje, que es cualquiera:
 - i) Un Restricción de valor S, consistiendo en un par de VIDs; o
 - ii) Una Restricción de valor I, consistiendo en un VID y un Identificador Fijo Independiente.

12.2.9.3.3.3 Salidas

- a) El estado de Operación. Esto toma uno de los valores siguientes:
 - 1) Operación rechazada debido a la especificación de las restricciones de aprendizaje—La configuración de operación requiere una configuración de restricción que es inconsistente con otra restricción ya definida en la tabla de restricciones. El funcionamiento devuelve el valor de restricción involucrado; o
 - 2) Operación rechazada debido al VID fijo incoherente a la asignación de FID—La Configuración de operación configura una restricción que es inconsistente con un VID fijo a la asignación de FID ya definido en la tabla de asignación. La operación devuelve el valor de la asignación fija involucrada; o
 - 3) La operación rechazada debido al índice de la entrada que excede el índice máximo soportado por la tabla de restricción; o
 - 4) Operación aceptada.

2.9.10.3.4 Borra las Restricciones de Aprendizaje de la VLAN

2.9.10.3.4.1 Propósito

Para borrar una de las entradas en la tabla de *Restricciones de Aprendizaje* de la VLAN. Esta operación tiene el efecto de poner el valor de la entrada de la tabla especificada a "Indefinido."

2.9.10.3.4.2 Entradas

- a) Índice de Entrada—índice de entrada de la entrada a ser borrada.

2.9.10.3.4.3 Salidas

- a) Estado de Operación. Esto toma uno de los valores siguientes:
 - 1) Operación rechazada debido al índice de entrada que excede el índice máximo soportado por la tabla de restricciones; o
 - 2) Operación aceptada.

2.9.10.3.5 Lectura VID para asignar a FID

2.9.10.3.5.1 Propósito

Para leer los contenidos de un rango de una o más entradas en el VID para asignar a la tabla FID.

2.9.10.3.5.2 Entradas

- a) Primera Entrada—VID de primera entrada para ser leída;
- b) Última Entrada—VID de última entrada para ser leída.

2.9.10.3.5.3 Salidas

- a) Lista de Entradas—Por cada entrada que se leyó:
 - 1) VID—Identificador VLAN para esta entrada;
 - 2) Tipo de Asignación—el tipo de asignación: Indefinida, Fija o Dinámica;
 - 3) FID—El FID al que el VID se asigna (si no de tipo Indefinido).

2.9.10.3.6 Lectura de las asignaciones FID para VID

2.9.10.3.6.1 Propósito

Para leer el FID a un VID especificado asignado actualmente.

2.9.10.3.6.2 Entradas

- a) VID—Identificador VLAN al que la operación de lectura aplica.

2.9.10.3.6.3 Salidas

- a) VID—Identificador VLAN al que la operación de lectura aplica;
- b) Tipo de Asignación—el tipo de asignación: Indefinida, Fija o Dinámica;
- c) FID—el FID a que el VID se asigna (si no de tipo Indefinido).

2.9.10.3.7 Lectura de las asignaciones VIDs para FID

2.9.10.3.7.1 Propósito

Leer todos los VIDs actualmente asignaron a un FID dado.

2.9.10.3.7.2 Entradas

- a) FID—el Filtro Identificador a que la operación de lectura aplica.

2.9.10.3.7.3 Salidas

- a) FID—el Filtro Identificador al que la operación de lectura aplica
- b) Lista de Asignación—una lista de asignaciones para este FID. Para cada elemento en la lista:
 - 1) Tipo de Asignación—el tipo de asignación: Fija o Dinámica;
 - 2) VID—el VID que es asignado.

2.9.10.3.8 Configuración de VID para las asignaciones de FID

2.9.10.3.8.1 Propósito

Para establecer una asignación fija de un VID a un FID.

2.9.10.3.8.2 Entradas

- a) VID—el VID de la entrada a ser configurada;
- b) FID—la FID a la que el VID será asignada.

2.9.10.3.8.3 Salidas

- a) Estado de Operación. Este toma uno de los valores siguientes:
 - 1) La operación rechazada debido a la especificación de aprendizaje inconsciente de restricción—la operación de configuración requerida a la configuración de asignación fija que es incoherente con el Aprendizaje de Restricciones VLAN. La operación regresa el valor de Aprendizaje de Restricciones VLAN involucrado; o
 - 2) Operación rechazada debido al VID que excede el VID máximo soportada por la tabla asignada; o

- 3) Operación rechazada debido a la FID que excede el ID máximo soportado por la aplicación; o
- 4) Operación aceptada.

2.9.10.3.9 Borrar el VID para las asignaciones de FID

2.9.10.3.9.1 Propósito

Para quitar un VID fijo a la asignación de FID del VID a la tabla asignada FID. Esta operación tiene el efecto de poner el valor de la entrada de la tabla especificada a "Indefinido."

2.9.10.3.9.2 Entradas

- a) VID—VID asignada a ser anulada.

2.9.10.3.9.3 Salidas

- a) Estado de Operación. Esto toma uno de los valores siguientes:
 - 1) Operación rechazada debido a que el VID excede el valor máximo soportado por la tabla asignada; o
 - 2) Operación aceptada.

2.9.10.3.10 Notifique la Violación de Restricciones de Aprendizaje

2.9.10.3.10.1 Propósito

Para alertar al Administrador de la existencia de una violación de Aprendizaje de Restricciones. Ésta es una notificación no solicitada de la administración entidad del Switch, emitido durante la detección de violación de restricciones.

2.9.10.3.10.2 Entradas

- a) Ninguna.

2.9.10.3.10.3 Salidas

- a) Violación de Tipo /Argumento—uno de
 - 1) VLAN compartida Aprendiendo no apoyadas. El argumento devuelto que indica al VIDs de un par de VLANs activas para una restricción S existente.

 - 2) VLAN independiente Aprendiendo no apoyada. El argumento devuelto que indica el VIDs de un par de VLANs activas para una restricción I existente que contenga el mismo identificador de la configuración independiente.

 - 3) Rango requerido FID no soportado. El argumento devuelto indica
 - i) El VID que el Switch es incapaz de asignar a un FID;
 - ii) El número máximo de FIDs soportado por el Switch.

La violación tipo *rango Requerido de FID no soportado* es detectado sólo por *IVL* o *Switches IVL/SVL* que soportan menos de 4094 FIDs.

Capitulo III Implementación de una VLAN, en el edificio sur y centro de la UPIITA

En este capitulo mostraremos los resultados de la aplicación teórica de los dos capítulos anteriores y su aplicación para el desarrollo real de VLAN's así como los resultados obtenidos, acorde a los estudios realizados primero explicaremos el método de investigación utilizado así como sus antecedentes.

El método de investigación, son procedimientos aprobados de investigación utilizados por los investigadores a fin de dar la objetividad y veracidad que se buscan en la observación y experimentación de fenómenos y hechos, para nuestra investigación utilizaremos el método científico.

El método científico (modelo general), es un conjunto de reglas que señalan el procedimiento para llevar a cabo una investigación cuyos resultados sean aceptados como validos. En forma concreta, el método científico se resume a la observancia de estas etapas:

- Etapa 1. Planteamiento del problema: es el inicio, cuando se hace el planteamiento general del problema a resolver por medio de la investigación
- Etapa 2. Formulación de hipótesis: Después de plantear el problema se presenta la propuesta que se pretende comprobar con la investigación
- Etapa 3. Levantamiento de información: Es la recopilación de antecedentes con los métodos e instrumentos diseñados para esta fase.
- Etapa 4. Análisis e interpretación de datos: una vez concluida la recopilación de los antecedentes se procede a la tabulación, análisis e interpretación.
- Etapa 5. Comprobación de la hipótesis: Con el análisis e interpretación de los antecedentes se comprueba o desaprueba la hipótesis planteada.
- Etapa 6. Difusión de resultados: es la presentación y divulgación de los resultados obtenidos con la investigación para hacer universal el conocimiento.

3. Implementación de una VLAN

3.1 Planteamiento del Problema.

El problema más grave desde el punto de vista de la administración de la red es la asignación de las direcciones ip, Porque?, existen computadoras cuya asignación es estática porque tienen que ser monitoreadas desde la Dirección de Informática, Dirección de Recursos humanos, Dirección Administrativa, Dirección de servicios escolares y Biblioteca Central, además estas direcciones no son consecutivas.

Por otra parte los laboratorios de computo cuentan con direcciones dinámicas para evitar que los usuarios pongan paginas de Internet y se puedan hacer accesibles desde sitios remotos como aplicaciones peer to peer, esto se hace mediante un servidor DHCP bajo la plataforma de Windows 2000 Server.

Esto al principio resolvió la situación pero en el momento en que el servidor DHCP estuvo arriba empezó a recibir una gran demanda por lo que en un tiempo muy corto de tiempo las direcciones ip se acabaron, esto se debía principalmente a las computadoras portátiles de los alumnos, computadoras de proyecto de los profesores y computadoras de las secretarías.

Ante esta situación se creo un rango alternativo de direcciones ip. En un servidor linux se configuro una clase c, con restricciones para servicios de mensajería instantánea, respuesta a servidores remotos, por mencionar algunos, esto para dar servicio a los laboratorios de computo, el problema de esta solución fue que las computadoras solo estaban separadas del resto de las demás por la asignación de la dirección ip, y no segmentadas físicamente en consecuencia cualquier persona que les cambiara la dirección ip tenia nuevamente acceso a todos los servicios.

Al principio la asignación de laboratorios a un rango alternativo de ip, parecía solucionar todo pero comenzó un nuevo problema el robo de direcciones por parte de los usuarios de computadoras portátiles que se les permitía el acceso a los nodos de los profesores, esto en conjunción con los hubs de 8 puertos que se empezaron a poner agotaron las direcciones ip nuevamente.

El robo de direcciones ip comenzó hacerse en cadena inclusive con las personas del soporte técnico puesto que la necesidad de hacer funcionar las computadoras de los usuarios los obligaba a buscar una dirección ip temporal que después se convertía en definitiva, lo que desencadeno un descontrol administrativo y técnico.

Básicamente el problema a resolver es controlar las computadoras que se conectan a Internet y tienen salida a las red institucional así como algunos de los servicios. La figura 3.1 es de cómo esta constituida la red de la escuela en un plano de conectividad.

3.2. Formulación de hipótesis

Si podemos controlar los accesos de las computadoras a la red a nivel físico o lógico de capa uno, dos o tres entonces lograremos que todos los usuarios se registren sus computadoras y podremos asignarles una dirección ip estática o dinámica según sea el caso.

3.3. Levantamiento de Información.

La conectividad de la unidad esta basada en un enlace E1 de fibra óptica que proviene del La dirección de Informática, en el interior de la escuela esta distribuida por un anillo de fibra óptica (que no esta terminado completamente), los tres site están conectados ala fibra pero los enlaces a los usuarios tienen convertidores a UTP cat 5.

Dentro de la estructura interna de se cuentan con un router principal y switches cabletron y enterasys en la estructura de cada uno de los edificios, existen también hubs que son instalados por parte de los usuarios pero esos se consideran fuera de norma por lo que no son tomados en cuenta para nuestro estudio.

En los sites sur y central están distribuidos cinco equipos enterasys (Switches) los cuales utilizaremos para implementar el proyecto, en él site central tenemos un arreglo en cascada de 4 switches alimentados desde él site sur.

En él site sur existe un switch enterasys únicamente, que es alimentado directamente del router del site norte por una línea de cable UTP cat 5, este es uno de los sites con menos concentración de nodos de red porque son las oficinas administrativas y salones de clases aquí no hay laboratorios de computo ni cubiculos de profesores.

Para completar un poco la información sobre los Switches Enterasys Vertical Horizont VH-2402S haremos un poco de análisis sobre la hoja de especificaciones.

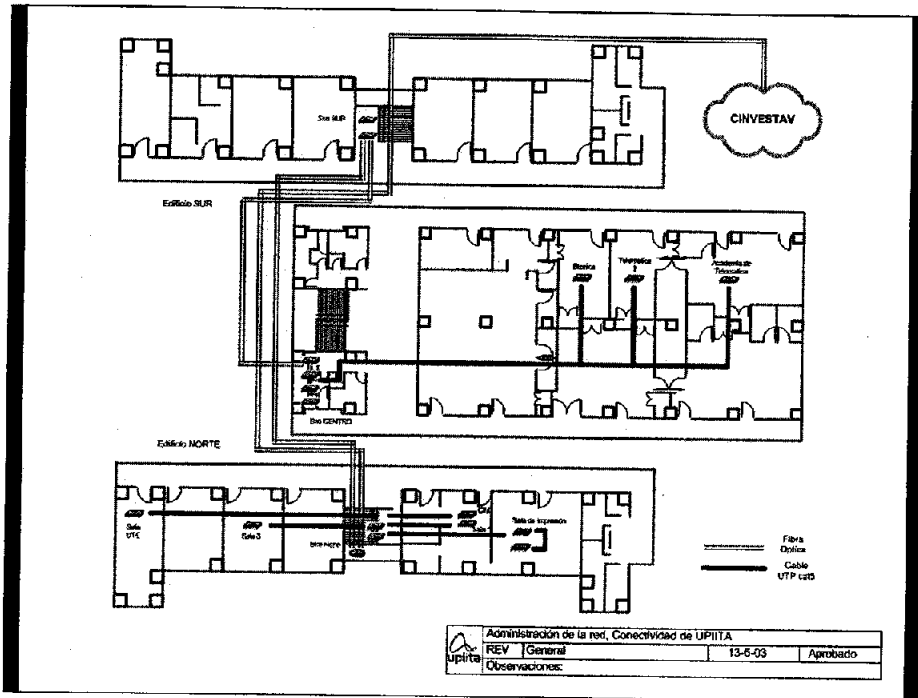


Fig. 3.1 Conexión lógica de UPIITA

3.3.1. Características del Producto

- Puertos:
 - 24 dual-speed 10Base-T/100Base-TX ports using RJ-45 connectors (MDI-X)
 - 3 slots for optional modules
 - 1 redundant power unit socket
- Módulos opcionales:
 - VH1000-S1SX: 1000Base-SX Modulo provisto de 1 SC Puerto de apilamiento para conectar a la pila de fibra óptica multimodo.
 - VH1000-S1LX: 1000Base-LX Modulo provisto de 1 SC Puerto de apilamiento para conectar a la pila de fibra óptica monomodo.
 - VH100-S2MFX: 100Base-FX Modulo provisto de 2 SC Puerto de apilamiento para conectar a la pila de fibra óptica multimodo.
 - VH100-S1SFX: 100Base-FX Modulo provisto de 1 SC Puerto de apilamiento para conectar a la pila de fibra óptica monomodo.
- Módulos opcionales de crecimiento:
 - VH-STACK: modulo para apilar provisto de 2 SCSI II conectores para apilamiento los switches incluyen uno.
- Cables opcionales para crecimiento:
 - 9380142: 32 cm cable de interconexión para apilar

- Modulo opcional de administracion RMON/SNMP/Web :
 - VH-SMGMT: Modulo de Administración provee SNMP, RMON, y soporte para administración Web para el apilamiento.
- Arquitectura del Switch:
 - 3 controles con 8 10/100 ports
 - IEEE 802.3u auto-negociación de half/full-duplex operación en todos los puertos RJ-45.
 - Arriba de 7 unidades switch pueden ser apiladas juntas soportando un total de 182 conexiones.
 - 128 KB de buffer para 10/100 ports, 2 MB de buffer de paquetes para 1000 puertos
 - Guardar y redirigir switching
 - 8K de tabla de ruteo
 - Ruteo: 14,880 paquetes por segundo (64 byte packets) @10 Mbps; 148,800 pps 100 Mbps; 1,488,000 pps @1000 Mbps
- Administracion de red
 - Agente SNMP: MIB II (RFC 1213); Bridge MIB (RFC 1493); Ethernet-like MIB (RFC 1643); RMON – Estadísticas, historial, alarmas y grupo de (RFC 1757); Interface, evolucion MIB (RFC 1573); Q-MIB (IEEE 802.1Q); privada MIB extensiones
 - Access via in-band, Internet browser, or Telnet
 - Puerto de consola (RS-232, macho DB-9 conector, null modem) soporta acceso via directa o conexión por modem
 - Configuración BootP para dirección IP
- Confiabilidad
 - Soporte para línea de poder redundante
- Software:
 - Diagnostico de producto para pruebas y resolución de problemas
 - Actualización de Firmware usando el puesto de consola o servidor TFTP
- LED indicadores:
 - Sistema: poder, RPU, administración.
 - 10Base-T/100Base-TX ports: Enlace/velocidad/deshabilitado/modo/actividad/control de flujo/full duplex
 - Modulo multimedia de estatus y actividad.

3.3.2. Panel Frontal

La figura 3.2 muestra el panel frontal de un Enterasys Networks Vertical Horizon VH-402S y la tabla 3.1 define los componentes del panel frontal del VH-2402S

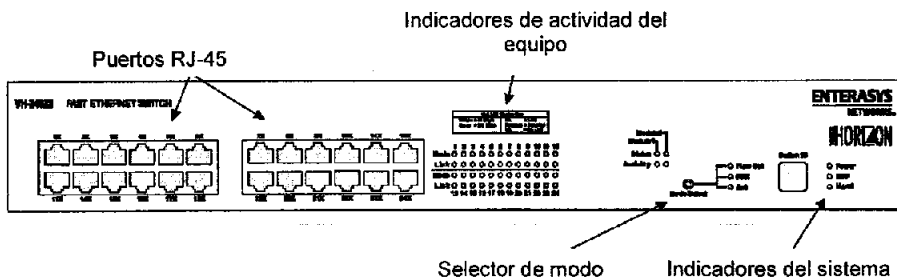


Fig. 3.2 Panel frontal de un VH-2402S

Nombre	Funcion
Power LED	Luces permanentes en verde indican que la línea de poder esta correcta y apagadas indican que la fuente de poder no esta conectada.
RDP LED	Luces permanentes para indicar que la unidad de poder redundante esta conectada en modo de respaldo o en modo activo.
Mgmt LED	Luces permanentes para indicar que el modulo de administración esta conectado y esta en modo operacional.
Link LEDs	En amarillo indican enlace a 10 Mbps en verde indican enlace a 100 Mbps, apagadas indican que no existe enlace y parpadeantes indican que el puerto ha sido deshabilitado manualmente.
Mode LEDs	El botón selector de modo, selecciona el foco indicador del modo.
Act:	Parpadeando indican actividad en el segmento de puertos.
FDX:	Amarillas permanentes indican operación full-duplex.
Flow Ctrl:	Luces permanentes para indicar que el control de flujo es habilitada para el puerto.
Module LEDs Status:	Indica que el modulo esta instalado en la ranura.
Activity:	Parpadeando indican actividad en el modulo.
Panel identificador del Switch despliega el numero de identificación que pertenece al switch. 10Base-T/100Base-TX y puertos RJ-45.	
Puertos de cobre que utilizan conectores RJ-45 y todos los puertos cableados con MDI-X.	

Tabla 3.1 Definición de los LED's del VH-2402S

3.3.3. Módulos opcionales

Las figuras 3.3 y 3.4 muestran los módulos opcionales que se le pueden poner al Enterasys Networks Vertical Horizon VH-2402S.

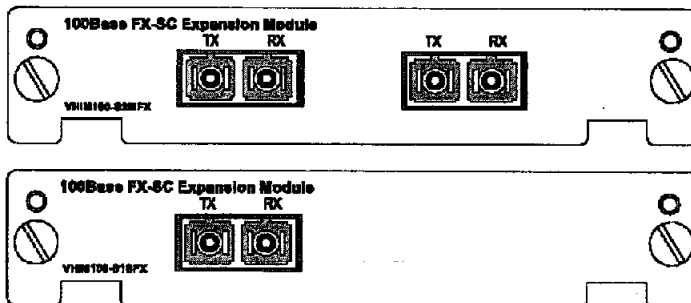


Fig. 3.3 Módulos opcionales

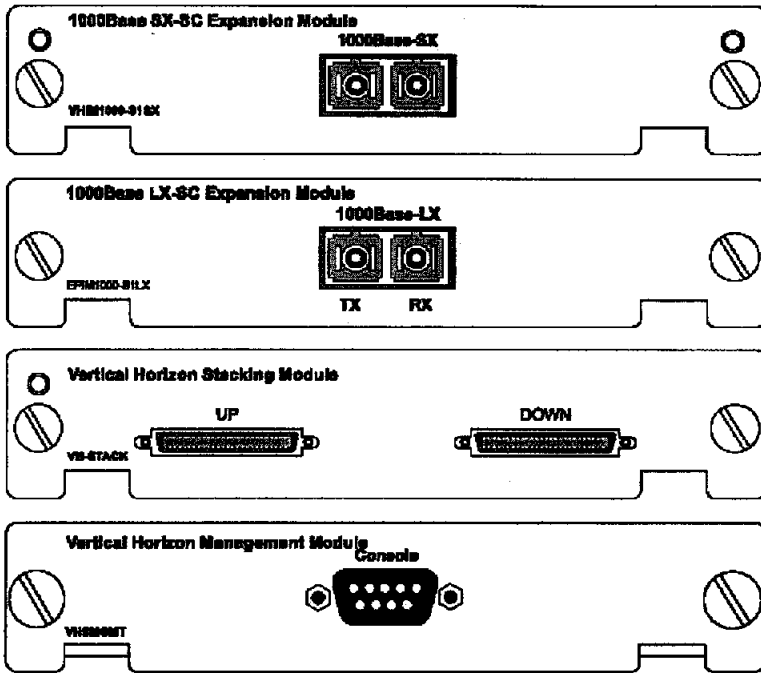


Fig. 3.4 Módulos opcionales

3.3.4. Panel Trasero

La figura 3.5 muestra la parte trasera de un Enterasys Networks Vertical Horizon VH-402S



Fig. 3.5 Parte trasera de un VH-2402S

3.3.5. Sumario de características

El siguiente es un sumario de las características del VH-2402S todas las características técnicas del equipo cumplen con los estándares, funcionalidad, desempeño y opciones

3.3.5.1. IEEE 802.1D Puente

El VH-2402S switch es completamente compatible con el estándar IEEE 802.1D especificaciones de puenteo transparente. Una dirección es provista para aprender, filtrar, y

enlutar. El Switch puede soportar como máximo mas de 8000 direcciones. Direcciones son automáticamente aprendidas por el Switch, y pueden ser asignadas individualmente a un procedimiento diseñado por el administrador de la red. La tabla de ruteo puede configurarse via remota por una consola o mediante una interfase SMTP o telnet ya sea para dirección estáticas o dinámicas. Una dirección estática es asignada por defecto a cada uno de los puertos por default. La dirección estática de unicast en la tabla de direccionamiento te permite darle un tratamiento individual con los menús de pantalla como sea requerido

3.3.5.2. Protocolo de Spanning Tree

El VH-2402S switch soporta el IEEE 802.1D Protocolo de Spanning Tree. Este protocolo permite la redundancia de conexiones para ser creados diferentes segmentos de LAN para este propósito con tolerancia a fallos, Dos o mas conexiones físicas entre diferentes segmentos pueden ser creadas a lo largo del switch, con el protocolo de Spanning Tree escoger una ruta sencilla que sea dada en cualquier tiempo puede ser desviada a una alternativa cuando esta este activa, de la misma forma mantener la conexión. Esto previene el trafico de la red en los puntos circulantes y en los extremos evitando loop's formados por múltiples conexiones en el mismo segmento de LAN

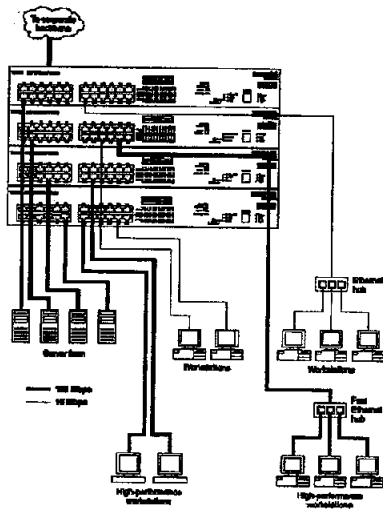


Fig. 3.6 Ejemplo de configuración de una red con Switches Enterasys

Los parámetros de Spanning Tree son configurables usando el menú de configuración en la consola o el menú, o los accesos Web o la comunidad SNMP. También se puede usar la latencia en el Switch ya que es un dispositivo de guardar y seguir. Cada trama que es copiada a la memoria del switch antes de ser enviada a otro puerto. Este método asegura que toda las tramas enviadas conforme al estándar de Ethernet de tamaño tengan correcto chequeo de redundancia cíclica (CRC) para la integridad de la información. El método de este switch previene las tramas erróneas a través de la red y usando un valor de ancho de banda, como el cut-through switching technology.

Para minimizar la posibilidad de desechar tramas en puertos congestionados. El switch VH-2402S provee 128 KB de buffer de trama por puerto. Este espacio de buffer es usado en la cola de transmisión de los paquetes en redes congestionadas. Esta es una ventaja adicional sobre la tecnología cut-through switching technology, la cual desechar paquetes inmediatamente cuando experimenta colisiones.

3.3.5.3. Virtual LANs (VLANs)

Las VLANs permiten conectar a usuarios a un segmento específico de LAN de acuerdo a su localización física. El VH-2402S switch soporta tagged VLANs de acuerdo al estándar IEEE 802.1Q. Con la trama tag un pequeño identificador es puesto en cada uno de los paquetes que viajan en la red. Este tag le dice a los switch's a que VLAN pertenece la trama direccionandolos correctamente.

Estas son unas de las características principales otras que además se describen como soportadas por el equipos son:

- Class of Service
- Port Trunking
- Flow Control
- Full Duplex Mode
- LEDs
- BootP
- Auto-negotiation
- Port Mirroring
- RMON
- Configuration and Management Interfaces
- Non-Volatile Parameter Storage
- Software Download
- Frame Buffering and Frame Latency

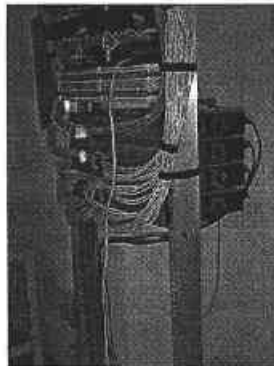


Foto 3.1 Rack del edificio central

Otra información que es necesaria y que se debe de tener en cuenta es el tipo de VLAN's que podemos hacer para tomar una decisión correcta, de las VLAN's que podemos utilizar están las siguientes

3.3.5.3.1. VLAN por Puerto

Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN - , el problema se presenta cuando se quieren hacer MAC ya que la tarea es compleja.

Aquí el puerto del switch pertenece a una VLAN , por tanto, ahí alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla , el servidor estará en la VLAN amarilla.

3.3.5.3.2. VLAN por MAC

Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación. Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

3.3.5.3.3. VLAN por Protocolo

Lo que pertenezca a IP se enrutara a la VLAN de IP e IPX se dirigirá a la VLAN de IPX, es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectara automáticamente a la VLAN correspondiente.

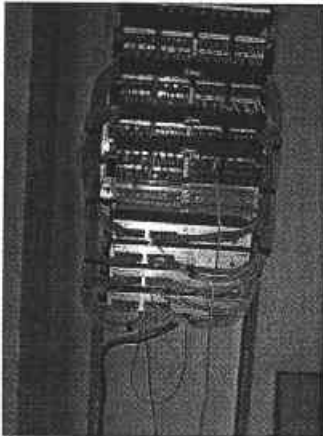


Foto 3.2 Arreglo de 4 equipos Enterasys

3.3.5.3.4. VLAN por subredes de IP o IPX

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de este para que el usuario – aunque este conectado a la VLAN del protocolo IP – sea asignado en otra VLAN -subred- que pertenecerá al grupo 10 o 20 dentro del protocolo.

3.3.5.3.5. VLAN por direcciones IP multicast

Generalmente son las direcciones de clase D las que ayudan a formular la VLAN. El mapeo o la asignación a la VLAN se basa o referencia en la dirección multicast.

3.3.5.3.6. VLAN definidas por el usuario

En esta política de VLAN se puede generar un patrón de bits, para cuando llegue el frame. Si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario – protocolo, dirección MAC y puerto.

Si el usuario manifiesta otro patrón de bits, entonces se trasladara a la VLAN que le corresponda; aquí el usuario define las VLAN.

3.3.5.3.7. VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es del puerto x, entonces se le asignara una VLAN correspondiente.

También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se

coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

3.3.5.3.8. VLAN por DHCP

Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente. Esta política de VLAN es de las últimas generaciones.

3.4. Análisis e interpretación de los datos

El tipo de VLAN que se va a configurar es Binding casando las computadoras con su dirección MAC y el número de puerto para que de esta forma, en primera instancia solo tendremos un número exacto y controlado de computadoras conectadas, también controlaremos los lugares en los que pueden ser colocados hubs para compartir conexión y por último definiremos los lugares en que los alumnos pueden conectar sus computadoras portátiles.

Debido a que los puertos de conexión de fibra óptica son limitados no podemos utilizar las capacidades de Smart Trunk por lo que en las primeras implementaciones que hagamos las VLAN's deben de pertenecer a un mismo switch algo que no afecta de manera sustancial nuestra solución.

Otro detalle importante de hacer notar es que los switch's que se configuraron son los pertenecientes al edificio central y edificio sur. Por lo tanto estas son las propuestas de VLAN's basadas en la ubicación de los nodos existentes en la escuela:

Los planos son para indicar cuáles nodos van a integrar a cada una de las VLAN's se describirán por pisos y por edificios, los nodos que no se señalen es por que no tienen privilegio de salida a Internet o porque no pertenecen a ninguna VLAN, por ser servidores. figuras 3.7, 3.8, 3.9 y 3.10, con la asignación de nodos a VLAN y su identificación.

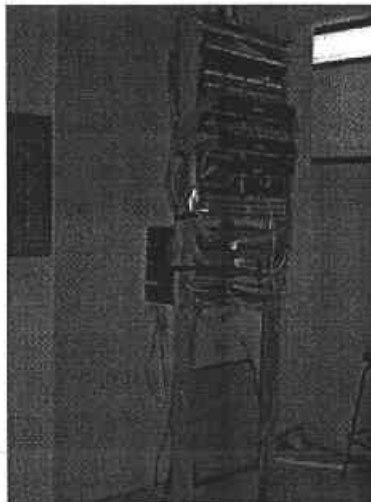
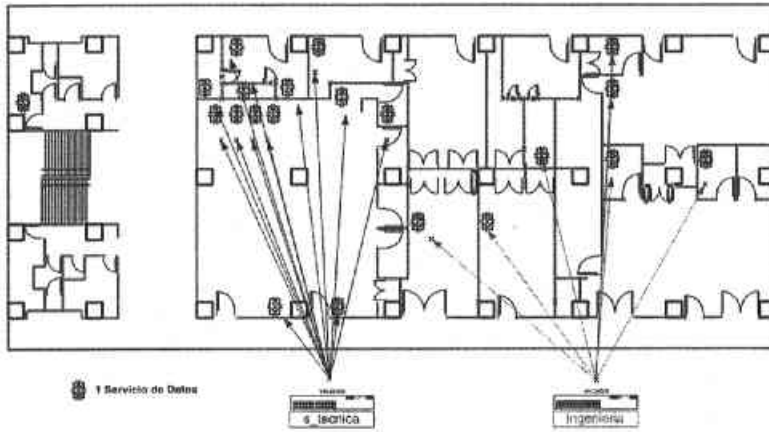

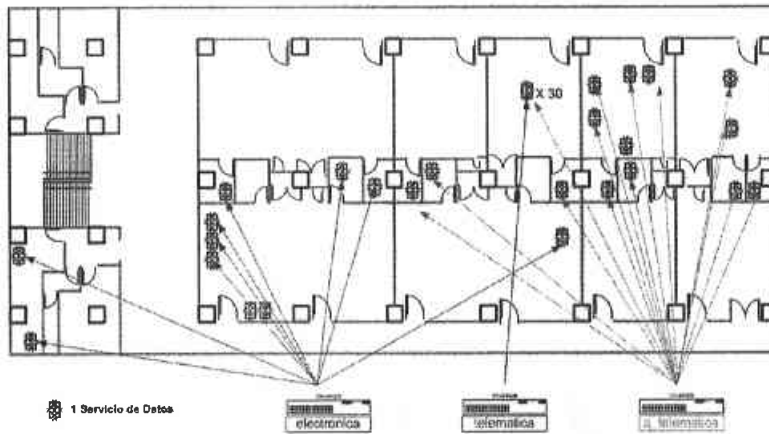



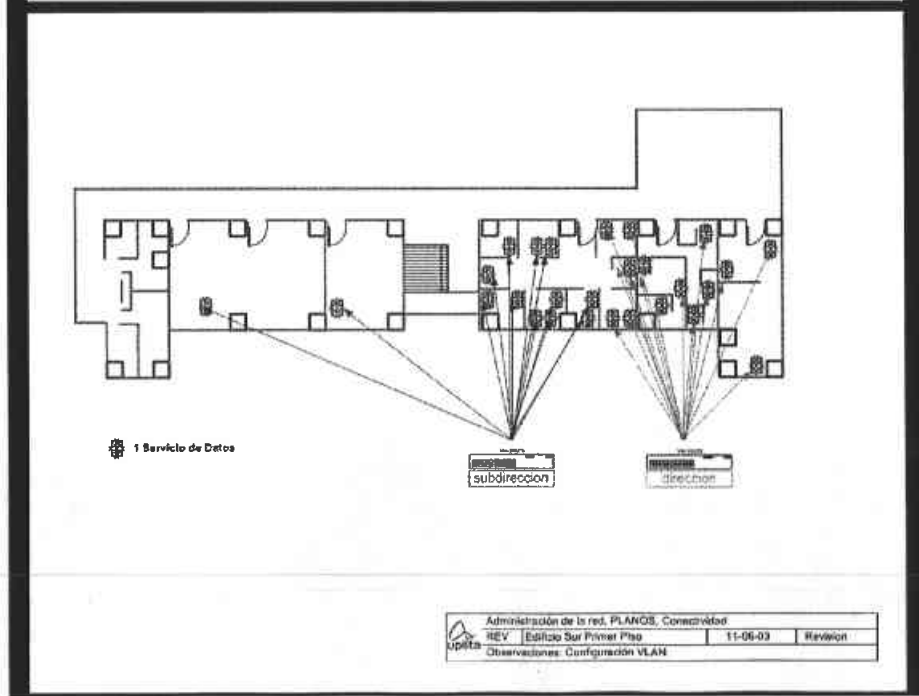
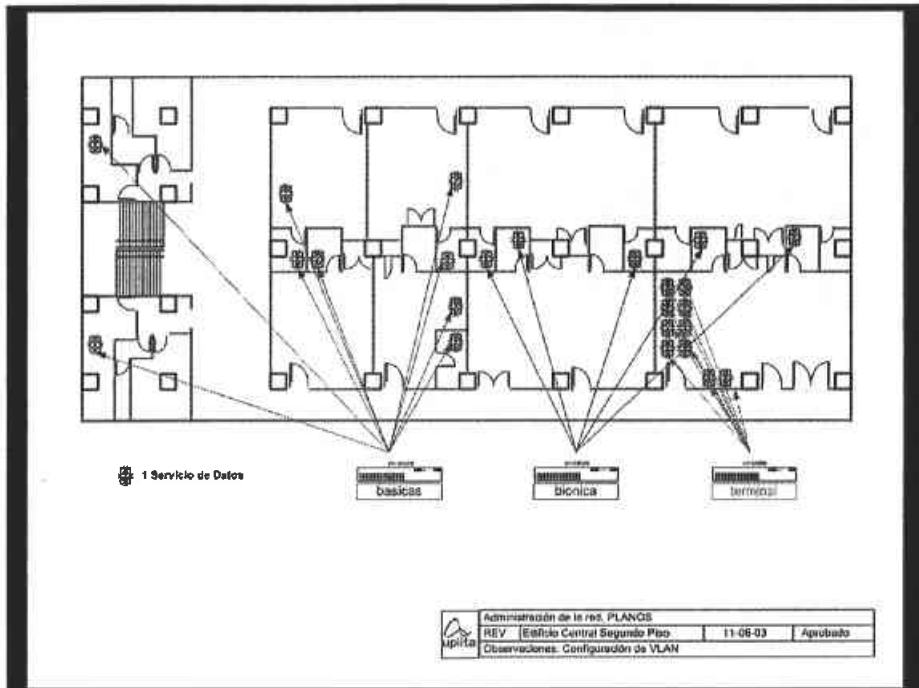
Foto 3.3 Rack con servicios de voz, datos y equipo activo



	Administración de la red, PLANOS		
	REV	Edificio Central Planta Baja	11-06-03
	Aprobado		
Observaciones: Configuración de VLAN			



	Administración de la red, PLANOS		
	REV	Edificio Central Primer Piso	11-06-03
	Aprobado		
Observaciones: Configuración de VLAN			



Para la configuración de las VLAN se utilizó la terminal de consola con un cable de red directamente conectado al equipo, las pantallas que se muestran a continuación son las de configuración del VH-2402S, así como el procedimiento estándar para la creación de VLAN's y asignación de puertos.

Para configurar VLAN's se deben de seguir los siguientes pasos:

1. Seleccionar del menú principal. "Device Control Menu."
2. Seleccionar " 802.1Q VLAN Static Table Configuration Menu."
3. En el nombre de campo "VID y VLAN", Configura el número de ID (1-2048) y un nombre alfanumérico de más de 8 caracteres para identificar la VLAN
4. Ajusta el estado del campo para activar y entonces seleccionar, aplicar y salvar los cambios en las configuraciones
5. Desde al "Device Control Menu", seleccionamos "Port Assigment VLAN Configuration."
6. Para cada puerto miembro de VLAN se asigna PVID a la identificación de VLAN
7. Se selecciona aplicar los cambios, se salvan y regresamos a la pantalla de "802.1Q VLAN Static Table Configuration"
8. Para configurar otras VLAN selecciona "New" y presionamos "ENTER"

```

Vertical Horizon Local Management -- VH-2402S

Global VLAN Configuration

VLAN Version Number           : 1
MAX VLAN ID                   : 2048
MAX Supported VLANs           : 256
Current Number of 802.1Q VLANs Configured: 10

VLAN ID                       : 1
VLAN Name                     : bionica
Status                        : Enabled
Selected by                   : VID [Show]

<APPLY>                       <OK>                       <CANCEL>
Use <TAB> or arrow keys to move. <Enter> to select
    
```

Fig. 3.11 Menú de Configuración Global VLAN

```

Vertical Horizon Local Management -- VH-2402S

      Port Assignment VLAN Configuration

      Unit Port PVID 802.1Q Trunk Ingress Filter
-----
      1   1   2   NO      FALSE
      1   2   1   NO      FALSE
      1   3   1   NO      FALSE
      1   4   1   NO      FALSE
      1   5   1   NO      FALSE
      1   6   1   NO      FALSE
      1   7   1   NO      FALSE
      1   8   1   NO      FALSE
      1   9   1   NO      FALSE
      1  10   1   NO      FALSE

Unit ID      : 1          [Show]
Port ID     : 1          [More]

      <APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
    
```

Fig 3.12 Configuración y asignación de puerto VLAN

```

Vertical Horizon Local Management -- VH-2402S

      802.1Q VLAN Base Information

VLAN Version Number           : 1
MAX VLAN ID                   : 2048
MAX Supported VLANs           : 256
Current Number of 802.1Q VLANs Configured: 10

      <OK>
      <Enter> to select.
    
```

Fig. 3.13 Información de 802.1Q VLAN Base

3.4.1. Resultados

Las VLAN que se crearon y configuraron son:

No.	VLAN ID	Numero de puertos asignados
1	ingeniería	7
2	s_tecnica	13
3	electronica	9
4	telematica	24
5	a telematica	14
6	basicas	9
7	bionica	5
8	terminal	10
9	subdirección	13
10	direccion	11 + un switch de 8 puertos

Tabla 3.2 VLAN's Configuradas

Un beneficio inesperado que descubrimos en este equipo es, el de configurar la seguridad de los puertos. Por medio de este menú de configuración podemos decirle a los puertos que solo acepten una dirección o direcciones determinadas, así que esto, en conjunto con la contención de los dominios de broadcast del switch y la seguridad de las VLANs le podemos añadir la seguridad en autenticación de los puertos para que los usuarios encuentren una primera barrera para entrar a servicios de red.

```

Vertical Horizon Local Management -- VH-2402S

Port Security Configuration

MAC Address MAC Address
-----

Secure address count : 0      Secure address count for port : 0
Unit : 1      Port : 1      MAC : 00-00-00-00-00-00
[Show]      [More]      [Add]      [Delete]
Mode:DISABLE [Apply]      [Clear]

<OK>
Use <TAB> or arrow keys to move. <Enter> to select
    
```

Fig. 3.14 Configuración de seguridad de puerto

3.5. Comprobación de la hipótesis

Las bases para formular nuestra hipótesis son: control de los usuarios a nivel físico o lógico, asignación de una dirección IP. Mas adelante en el planteamiento de la problemática aclaramos que es imperativo detener la modificación de direcciones IP por parte de los usuarios y que nos es viable utilizar un control a nivel de los equipos porque estos no están controlados ni regulados.

De las propuestas que se hicieron, varias desencadenaron en soluciones de las cuales mencionamos a continuación:

- Se logró la implementación de VLAN's en el edificio central con buenos resultados todas las computadoras de laboratorios como los de telemática se lograron aislar del resto de las computadoras, las computadoras del área de telemática donde se levantan servidores DHCP, DNS, servidores de Web y de bases de datos se encuentran en una VLAN específica que permite que trabajen a mayor velocidad en ese laboratorio y evita que computadoras como las de bionica que son contiguas respondan a peticiones falsas.
- Con las características de seguridad de los Switch's se implementaron medidas de autenticación en cada uno de los puertos de los equipos, esto se traduce en que cada una de las computadoras tiene que estar dadas de alta en una base de datos del arreglo si no es así no pueden acceder a la red, además de esto la dirección MAC debe de pertenecer a un puerto específico.

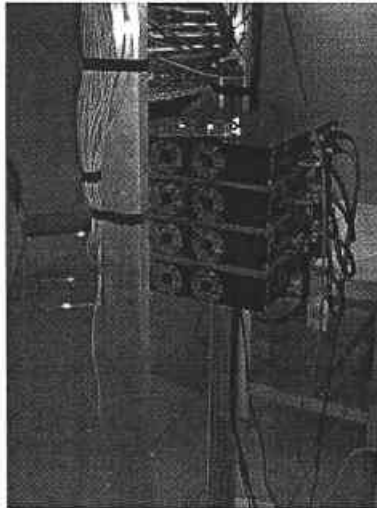


Foto 3.4 Arreglo de switch's y acometida de fibra óptica

Por esta razón la hipótesis se cumplió cabalmente y se lograron además autenticación de los puertos, pero es también razonable mencionar que las VLAN's que se configuraron son del tipo estático por lo que los usuarios solo se pueden conectar en el puerto que tienen asignado y en otro puerto no van a tener acceso a su VLAN ni se les va a permitir la conexión debido a la autenticación, lo ideal es que las VLAN fueran dinámicas para que en cualquier lugar que se conecten puedan acceder a todos los privilegios.

Conclusiones

De las experiencias personales mas importantes que me dejo el trabajar con equipos de comunicaciones de alto rendimiento es que, se deben de estudiar bien todas las especificaciones del producto para tener siempre presente con que se esta trabajando, porque muchas veces nos sucedió que nos perdimos con las configuraciones, pensando o tratando de buscar errores de programación y al revisar nuevamente nuestro trabajo, el error se centraba en especificaciones no soportadas por el equipo.

Por otro lado al trabajar bajo presión por que la conectividad de la escuela estaba fuera, recomendamos ampliamente el uso de una bitácora, ya que esto nos soluciono el problema inicial de probar dos o tres veces una configuración en específico.

La configuración primariamente la realizamos por el puerto de consola, directamente del equipo, porque al tratar de usar las interfaces Web del Vertical Horizont, encontramos dificultades del tiempo de vida de la sesión, además de la autenticación por Web es muy lenta y no muestra bien los resultados. Por esto recomendamos que las sesiones de trabajo inicial o de configuración de muchos parámetros se realicen directamente en el equipo y las actualizaciones o modificaciones menores se realicen por la interfase Web.

Un detalle importante que encuentre al estar configurando el equipo, fue un menú de configuración de seguridad el cual me permitió adicionar seguridad por medio de autenticación a cada uno de los puestos del equipo. Esto se conjunto con las VLAN's creadas para cumplir cabalmente con los requerimientos del departamento de computo y comunicaciones de la escuela de la siguiente forma:

- Las direcciones IP pertenecen a una VLAN para evitar servicios de red en colisión
- Las direcciones IP especifican a cada uno de los equipos al que pertenecen y se lleva un registro de los mismos
- La autenticación de puertos controla la cantidad de equipos a los que se les puede dar servicio
- La autenticación de equipos evita la entrada de computadoras a la red sin un registro previo.
- Las VLAN's dan libertad a los usuarios de levantar servicios de prueba, sin que entren en conflicto con otras áreas de la unidad.

Hablando del proyecto de la UPIITA, podemos decir que se alcanzaron y superaron los requerimientos iniciales y todo esto con transparencia para los usuarios puesto que los servicios de red nunca estuvieron fuera de línea, porque los trabajos se llevaron acabo los fines de semana y desde la consola Web en horario nocturno.

De la parte de entregables que se realizaron para la escuela están los inventarios de las direcciones IP que tienen configurados los equipos, los mapas de localización de los nodos y su pertenencia a VLAN's, y por ultimo las contraseñas de todos los equipos.

Me parece interesante que esta tesis sea tomada en cuenta como una base para la configuración de estos equipos en el IPN, porque la utilización que se tiene de ellos en este momento es por debajo de sus características y en base a la observación de los resultados del proyecto de UPIITA podemos afirmar que administrar y filtrar las redes de forma local puede solucionar problemas de ancho de banda para el IPN.

Índice de Tablas y Figuras

- Índice de imágenes

Capítulo 1

- Fig 1.1 Tarjeta de red para puerto PCI
- Fig 1.2 Ejemplo de interconexión entre redes LAN
- Fig 1.3 Ejemplo de una colisión en Ethernet
- Fig 1.4 Ejemplo de red Token Ring
- Fig. 1.5 Configuración de una red WAN
- Fig. 1.7 Las siete capas del modelo OSI
- Fig. 1.8 Comunicación par a par
- Fig. 1.9 Modelos de referencia TCP/IP
- Fig. 1.10 Comparación entre OSI y TCP/IP
- Fig. 1.11 Switch de 8 puertos
- Fig. 1.12 Parte posterior de un Router
- Fig. 1.13 Rutas en Internet
- Fig. 1.14 Formato de trama Ethernet y IEEE 802.3
- Fig. 1.15 Transmisión de Tokens de Token Ring
- Fig. 1.16 Formato Token Ring

Capítulo 2

- Fig. 2.1 Una VLAN es un agrupamiento independientemente de su ubicación física
- Fig. 2.2 Ejemplo de un Switch LAN
- Fig.2.3 Arquitectura de un Switch VLAN
- Fig 2.4. Separación lógica de puntos de unión usados por capas de entidades altas y la transmisión e MAC entidad
- Fig. 2.5. Efecto de control de información en la ruta enviada
- Fig. 2.6 Puntos de unión por puerto
- Fig. 2.7. Formato de encabezado de etiquetas
- Fig.2.8. Formato de TPID de SNAP-codificado
- Fig. 2.9. Formato de etiqueta de Información de Control
- Fig. 2.10. Campo de Control de Ruteo (RC) E-RIF
- Fig. 2.11. Dirección de la aplicación GVRP

Capítulo 3

- Fig. 3.1 Conexión lógica de UPIITA
- Fig. 3.2 Panel frontal de un VH-2402S
- Fig. 3.3 Módulos opcionales
- Fig. 3.4 Módulos opcionales
- Fig. 3.5 Parte trasera de un VH-2402S
- Fig. 3.6 Ejemplo de configuración de una red con Switches Enterasys
- Figuras 3.7, 3.8, 3.9 y 3.10 la asignación de nodos a VLAN y su identificación.
- Fig. 3.11 Menú de Configuración Global VLAN
- Fig 3.12 Configuración y asignación de puerto VLAN
- Fig. 3.13 Información de 802.1Q VLAN Base
- Fig. 3.14 Configuración de seguridad de puerto

- **Índice de Tablas**

Capítulo 1

Tabla 1.1 Cronología de Ethernet

Capítulo 2

Tabla 2.1. Regeneración de usuario prioridad

Tabla 2.2. Prioridad de acceso de Salida

Tabla 2.3. Direcciones reservadas

Tabla 2.4. Asignación de tipo 802.1 Q Ethernet

Tabla 2.5. Formato de TPID Ethernet-codificada

Tabla 2.6. Valores VID reservados

Capítulo 3

Tabla 3.1 Definición de los LED's del VH-2402S

Tabla 3.2 VLAN's Configuradas

- **Índice de Fotos**

Capítulo 1

Capítulo 2

Capítulo 3

Foto 3.1 Rack del edificio central

Foto 3.2 Arreglo de 4 equipos Entereasys

Foto 3.3 Rack con servicios de voz, datos y equipo activo

Foto 3.4 Arreglo de switch's y llegada de fibra óptica

Glosario de términos

A

AI Artificial Intelligence. Inteligencia Artificial. Parte de la informática que estudia la simulación de la inteligencia.

Access Provider Proveedor de Acceso Centro servidor que da acceso lógico a Internet, es decir sirve de pasarela (Gateway) entre el usuario final e Internet.

ACK Acknowledgment. Reconocimiento. Señal de respuesta.

ADSL Asymmetric Digital Subscriber Line. Línea Digital Asimétrica de Abonado. Sistema asimétrico de transmisión de datos sobre líneas telefónicas convencionales. Existen sistemas en funcionamiento que alcanzan velocidades de 1,5 y 6 Megabits por segundo en un sentido y entre 16 y 576 Kilobits en el otro.

ANSI American National Standard Institute. Instituto Nacional Americano de Estándar.

API Application Program Interface. Interfaz de Aplicación del Programa. Es el conjunto de rutinas del sistema que se pueden usar en un programa para la gestión de entrada/salida, gestión de ficheros etc.

APPLET Aplicación escrita en JAVA y compilada.

Archie Software utilizado para localizar archivos en servidores FTP. A partir de 1994 ha caído en desuso debido a la aparición del WWW, o Web.

ARPA Advanced Research Projects Agency. Agencia de Proyectos de Investigación Avanzada.

ARPANET Advanced Research Projects Agency Network. Red de la Agencia de Proyectos de Investigación Avanzada. Red militar Norteamericana a través de líneas telefónicas de la que posteriormente derivó Internet.

ASAP As Soon As Possible. Tan Pronto Como Sea Posible. Mandato u opción en una red o programa que determina la prioridad de una tarea.

ASCII. American Standard Code for Information Interchange. Estándar Americano para Intercambio de Información. La tabla básica de caracteres ASCII esta compuesta por 128 caracteres incluyendo símbolos y caracteres de control. Existe una versión extendida de 256

ASN Autonomous System Number. Número de sistema autónomo. Grupo de Routers y redes controlados por una única autoridad administrativa.

ATM Asynchronous Transmission Mode. Modo de Transmisión Asíncrona. Sistema de transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea. Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1,2

Aplicación de VLAN en una red academica

Gbps. Implementación normalizada (por ITU) de Cell Relay, técnica de conmutación de paquetes que utiliza celdas de longitud fija.

AUI Asociación de usuarios de Internet.

Avatar Identidad representada gráficamente que adopta un usuario que se conecta a un CHAT con capacidades gráficas.

B

Backbone Estructura de transmisión de datos de una red o conjunto de ellas en Internet. Literalmente: "columna vertebral"

Bandwith Ancho de Banda. Capacidad de un medio de transmisión.

BBS Bulletin Board System. Tablero de Anuncios Electrónico. Servidor de comunicaciones que proporciona a los usuarios servicios variados como e-mail o transferencia de ficheros. Originalmente funcionaban a través de líneas telefónicas normales, en la actualidad se pueden encontrar también en Internet.

Ban Prohibir. Usado normalmente en IRC. Acto de prohibir la entrada de un usuario "NICK" a un canal.

Baud Baudio. Unidad de medida. Número de cambios de estado de una señal por segundo.

BIOS Basic Input Output System. Sistema Básico de Entrada/Salida. Programa residente normalmente en Eprom que controla la iteraciones básicas entre el hardware y el Software.

BIT Binary Digit. Dígito Binario. Unidad mínima de información, puede tener dos estados "0" o "1".

BITNET Because It's Time NETWORK. Porque es tiempo de red. Red internacional de computadoras de instituciones educativas. Esta red está conectada a Internet y algunas de las herramientas más comunes hoy en día, como los servidores de correo Listservs, se originaron en ella. Actualmente está en proceso de desaparición conforme sus miembros se integran a Internet.

Bookmark Marca. Anotación normalmente de una dirección WWW o URL que queda archivada para su posterior uso.

BOOTP Bootstrap Protocol. Protocolo de Arranque-Asignación. Proporciona a una máquina una dirección IP, Gateway y Netmask. Usado en comunicaciones a través de línea telefónica.

BOT Automatismo, programa o script que realiza funciones que de otra manera habría que hacer de forma manual.

Bounce Rebote. Devolución de un mensaje de correo electrónico debido a problemas para entregarlo a su destinatario.

BPDU: Bridge Protocol Data Unit (ISO/IEC 15802-3)

BPS Bits per second. Bits por segundo. Medida de la velocidad de transmisión de datos en la transmisión en serie.

Bridge. Puente. Dispositivo que interconecta redes de área local (LAN) en la capa de enlace de datos OSI. Filtra y retransmite tramas según las direcciones a Nivel MAC.

Browser. Navegador. Término aplicado normalmente a los programas que permiten acceder al servicio WWW.

BUS. Vía o canal de Transmisión. Típicamente un BUS es una conexión eléctrica de uno o más conductores, en el cual todos los dispositivos ligados reciben simultáneamente todo lo que se transmite

C

Callback Sistema muy empleado en EE.UU. para llamadas internacionales consistente en (previo abono) llamar a un Tlf. indicar el número con el que queremos contactar y colgar. Posteriormente se recibe una llamada que nos comunica con el número deseado.

Carrier Operator de Telefonía que proporciona conexión a Internet a alto nivel.

Caudal Cantidad de ocupación en un ancho de banda. Ejp. En una línea de 1Mbps. puede haber un caudal de 256Kbps. con lo que los 768Kbps. restantes de el ancho de banda permanecen desocupados.

CCITT. International Consultative Committee on Telegraphy and Telephony. Comité Consultivo de Telegrafía y Telefonía. Organización que establece estándares internacionales sobre telecomunicaciones.

CD. Compact Disc. Disco Compacto. Disco Optico de 12 cm de diámetro para almacenamiento binario. Su capacidad "formateado" es de 660 Mb. Usado en principio para almacenar audio. Cuando se usa para almacenamiento de datos genéricos es llamado CD-ROM.

CDA. Communications Decency Act. Acta de decencia en las Telecomunicaciones. Proyecto de ley americano que pretendía ejercer una especie de censura sobre Internet. Por el momento ha sido declarado anticonstitucional.

CERN. Conseil Europeen pour la Recherche Nucleaire. Consejo Europeo para la Investigación Nuclear. Institución europea que desarrolló, para sus necesidades internas, el primer navegador y el primer servidor WWW. Y por tanto el HTTP. Ha contribuido decisivamente a la difusión de esta tecnología y es uno de los rectores del W3 Consortium

CERT. Computer Emergency Response Team. Equipo de Respuesta a Emergencias Informáticas.

CFI: Canonical Format Indicator

CG. Computer Graphics. Gráficos de Computador.

CGI Common Gateway Interface. Interfaz de Acceso Común. Programas usados para hacer llamadas a rutinas o controlar otros programas o bases de datos desde una página Web. También pueden generar directamente HTML.

CHAT Charla. Ver IRC.

CIR Committed Information Rate. Es el Caudal mínimo de información que garantiza el operador telefónico al cliente (normalmente el proveedor de acceso) el resto del ancho de banda esta pues sujeto al estado de la red y las necesidades del operador telefónico.

CIX Commercial Internet Exchange. Intercambio Comercial Internet.

Codificación del Control Lógico de Control (LLC) usado del direccionamiento LLC de la trama como un protocolo asociado con el Servicio de la trama de transporte de datos de la MAC.

Connection Provider Proveedor de Conexión Entidad que proporciona y gestiona enlace físico a Internet

COOKIE Pequeño trozo de datos que entrega el programa servidor de HTTP al navegador WWW para que este lo guarde. Normalmente se trata de información sobre la conexión o los datos requeridos, de esta manera puede saber que hizo el usuario en la ultima visita.

Cracker Individuo con amplios conocimientos informáticos que desprotege/piratea programas o produce daños en sistemas o redes.

CSLIP Compressed Serial Line Protocol. Protocolo de Línea Serie Comprimido. Es una versión mejorada del SLIP desarrollada por Van Jacobson. Principalmente se trata de en lugar de enviar las cabeceras completas de los paquetes enviar solo las diferencias.

CSMA Carrier Sense Multiple Access. Acceso Múltiple por Detección de Portadora. Protocolo de Red para compartir un canal. Antes de transmitir la estación emisora comprueba si el canal esta libre.

CSMA/CD Carrier Sense Multiple Access / Collision Detection. Detección de portadora de acceso múltiple / colisión. En este protocolo las estaciones escucha al bus y sólo transmiten cuando el bus está desocupado. Si se produce una colisión el paquete es transmitido tras un intervalo (time-out) aleatorio.

D

DATAGRAM Datagràma. Usualmente se refiere a la estructura interna de un paquete de datos.

DCD Data Carrier Detected. Detectada Portadora de Datos.

DCE Data Communication Equipment. Equipo de Comunicación de Datos

decir, con calidad para ser emitido en cualquiera de los sistemas de televisión existentes.

DVD Digital Video Disk. Nuevo estándar en dispositivos de almacenamiento masivo con formato de CD pero que llega a 14 GB de capacidad.

E

EBCDIC Extended Binary Coded Decimal Interchange Code. Código Extendido de Binario Codificado Decimal. Sistema mejorado de empaquetamiento de números decimales en sistema binario.

ECC Error Checking and Correction. Chequeo y Corrección de errores.

EFF Electronic Frontier Foundation. Fundación Frontera Electrónica. Organización para la defensa de los derechos en el Cyberespacio.

EIA Electronics Industry Association. Organismo responsable de publicar normas RS (Recommended Standards), relacionadas con la comunicación entre computadoras y terminales. (Ej: RS-232)

E-ISS: Enhanced Internal Sublayer Service

E-mail Electronic Mail. Correo Electrónico. Sistema de mensajería informática similar en muchos aspectos al correo ordinario pero muchísimo más rápido.

EPROM. Erasable Programmable Read Only Memory. Memoria borrable programable sólo de lectura.

Ethernet. Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus Coaxial. Método de acceso es CSMA/CD.

ETSI European Telecommunication Standards Institute. Instituto Europeo de Estándares en Telecomunicaciones.

E-ZINE Electronic Magazine. Revista Electrónica. Cualquier revista producida para su difusión por medios informáticos, principalmente por Internet.

F

FAQ Frequent Asked Question. Preguntas Formuladas Frecuentemente. Las "faqs" de un sistema son archivos con las preguntas y respuestas más habituales sobre el mismo.

FAT File Allocation Table. Tabla de Localización de Ficheros. Sistema de organización de ficheros en discos duros. Muy usado en PC.

FCS: Frame Check Sequence

FDDI Fiber Digital Device Interface. Dispositivo Interface de Fibra (óptica) Digital.

Finger. Literalmente "dedo". Facilidad que permite averiguar información básica sobre usuarios de Internet o Unix.

FID: Filter Identifier

DDE Dynamic Data Exchange. Intercambio Dinámico de Datos. Conjunto de especificaciones de Microsoft para el intercambio de datos y control de flujo entre aplicaciones.

DES Data Encryption Standard. Algoritmo de Encriptación de Estándar. Algoritmo desarrollado por IBM, utiliza bloques de datos de 64 bits y una clave de 56 bits. Es utilizado por el gobierno americano.

Dialup Marcar. Establecer una conexión de datos a traves de una línea telefónica.

DNS Domain Name System. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

Domain Dominio. Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. ejp: mercadeo.com

Download Literalmente "Bajar Carga". Se refiere al acto de transferir un fichero/s desde un servidor a nuestro computador. En español: " bajarse un programa "

Downsizing. El concepto de "downsizing" en computación, cuya traducción mas lógica podría ser la de "integración hacia micros", es la interconexión de redes de microcomputadoras con mini computadoras y computadoras de orden principal.

DownStream Flujo de datos de un computador remoto al nuestro.

DS-3. Digital Signal 3. Señal Digital Jerarquía 3 (45 Mbps para un T3).

DSP Digital Signal Processor. Procesador Digital de Señal.

DSR Data Set Ready (MODEM).

DTE Data Terminal Equipment. Equipo Terminal de Datos. Se refiere por ejemplo al computador conectado a un modem que recibe datos de este.

DTMF Dual Tone Multifrequency. Multi frecuencia de doble tono. Son los tonos que se utilizan en telefonía para marcar un número telefónico.

DTR Data Transfer Ready. Preparado para Transmitir Datos (MODEM).

DUPLEX Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/transmitir. Existen dos modalidades HALF-DUPLEX: Cuando puede recibir y transmitir alternativamente y FULL-DUPLEX cuando puede hacer ambas cosas simultáneamente.

DVB Digital Video Broadcast. video Digital para Emisión. Formato de video digital que cumple los requisitos para ser considerado Broadcast, es

FIX. Federal Interagency eXchange. Interagencia Federal de Intercambio.

Firewall. Cortina de Fuego. Router diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

Frame. Estructura. También trama de datos. Grupo de bits transmitido de manera serial sobre un canal de comunicación. En Browsers de WWW como Netscape se refiere a una estructura de sub-ventanas dentro de un documento HTML.

Frame Relay. Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

Frame Relay la función de Forwarding Process que envía las tramas siguiendo los puertos de un Switch.

FTP. File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los protocolos de transferencia de ficheros mas usado en Internet.

Full Duplex. Circuito o dispositivo que permite la transmisión en ambos sentidos simultáneamente.

FXO. Foreign Exchange Office. Central Externa. Voz que emula una extensión de PABX tal como aparece ante la central telefónica para la conexión de una PABX a un multiplexor.

G

GARP: Generic Attribute Registration Protocol (ISO/IEC 15802-3)

Gateway. Pasarela. Puerta de Acceso.

Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

GID: GARP Information Declaration (ISO/IEC 15802-3)

GIF Graphics Interchange Format. Formato Grafico de Intercambio.

GIP: GARP Information Propagation (ISO/IEC 15802-3)

GIX Global Internet Exchange. Intercambio Global Internet.

GMRP: GARP Multicast Registration Protocol

GMT Greenwich Mean Time. Hora de Referencia de Greenwich. Equivalente a UT.

Gopher. Nombre dado en Internet al servicio de rastreo de información organizado en menús jerarquizados

GSM Global System Mobile communications. Sistema Global de Comunicaciones Móviles.

Sistema digital de telecomunicaciones principalmente usado para telefonía móvil. Existe compatibilidad entre redes por tanto un teléfono

GSM puede funcionar teóricamente en todo el mundo. En EE.UU. esta situado en la banda de los 1900MHZ y es llamado DCS-1900.

GT Global Time. Tiempo Global. Sistema horario de referencia en Internet.

GUI Graphic User Interface. Interfase Gráfico de Usuario.

GVRP: GARP VLAN Registration Protocol

H

Hacker Experto en informática capaz de de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

Hardware. A los componentes que es posible ver y tocar se les llama en jerga computacional "hardware", palabra inglesa cuyo significado es máquina o "cosa dura".

Half Duplex. Un circuito que permite de manera alternante la transmisión y la recepción de señales, pero no de manera simultánea.

Hayes. Norma desarrollada por el fabricante Hayes para el control de modems mediante comandos.

HDLC High-Level Data Link Control. Control de Enlace de Datos de Alto Nivel. Es un protocolo orientado al bit.

HDSL High bit rate Digital Subscriber Line. Línea Digital de Abonado de alta velocidad. Sistema de transmisión de datos de alta velocidad que utiliza dos pares trenzados. Se consiguen velocidades superiores al Megabit en ambos sentidos.

Header Cabecera. Primera parte de un paquete de datos que contiene información sobre las características de este.

Hit. Se usa para referirse a cada vez que un link es pulsado en una página WEB. Literalmente "golpe".

Homepage. Página principal o inicial de un sitio WEB.

Host. Anfitrión. Computador conectado a Internet. Computador en general.

HPFS High Performance File System. Sistema de Archivos de Alto Rendimiento. Sistema que utiliza el OS/2 opcionalmente para organizar el disco duro en lugar del habitual de FAT.

HTML HyperText Markup Language. Lenguaje de Marcas de Hipertexto. Lenguaje para elaborar paginas Web actualmente se encuentra en su versión 3. Fue desarrollado en el CERN.

HTTP HyperText Transfer Protocol. Protocolo de Transferencia de Hipertexto. Protocolo usado en WWW.

I

IANA Internet Assigned Number Authority. Autoridad de Asignación de Números en Internet. Se trata de la entidad que gestiona la asignación de direcciones IP en Internet.

ICMP Internet Control Message Protocol. Protocolo Internet de Control de Mensajes.

IEEE Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana. IEEE 802.3 Protocolo para la red LAN de la IEEE que especifica una implementación del nivel físico y de la subcapa MAC, en la capa de enlace de datos. El IEEE 802.3 utiliza CSMA/CD a una variedad de velocidades de acceso sobre una variedad de medios físicos. Extensiones del estándar IEEE 802.3 especifica implementaciones para Fast Ethernet.

IETF Internet Engineering Task Force. Grupo de Tareas de Ingeniería de Internet. Asociación de técnicos que organizan las tareas de ingeniería principalmente de telecomunicaciones en Internet. Por ejemplo: mejorar protocolos o declarar obsoletos otros.

INDEPENDENT VLAN LEARNING (IVL): configuración y operación del proceso de aprendizaje y filtraje de la Base de Datos semejante para una configuración de VLANs, si se da una dirección MAC individual es aprendida en una VLAN, esta información no es usada para encaminar o tomar decisiones de filtrado debido a que las direcciones están relativamente en otra VLAN configurada.

Independent VLAN Learning (IVL) Bridge un tipo de puenteo que solo soporta aprendizaje de VLAN Independiente.

INTERNET. Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

INTERNIC Entidad administrativa de Internet que se encarga de gestionar los nombres de dominio en EE.UU.

INTRANET Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW. IP Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de internet. También se refiere a las direcciones de red Internet.

IPI Intelligent Peripheral Interface. Interface Inteligente de Periféricos. En ATM: Initial Protocol Identifier. identificador Inicial de Protocolo.

IPX Internet Packet Exchange. Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

IRC Internet Relay Chat. Canal de Chat de Internet. Sistema para transmisión de texto multiusuario a través de un servidor IRC. Usado normalmente para conversar on-line también sirve para transmitir ficheros.

ISDN Integrated Services Digital Network. Red Digital de Servicios Integrados. Servicio provisto por una empresa de comunicaciones que permite transmitir simultáneamente diversos tipos de datos digitales conmutados y voz.

ISO International Standard Organization. Organización Internacional de Estándares.

ISP Internet Service Provider. Proveedor de Servicios Internet.

ISS Internet Security Scanner. Rastreador de Seguridad de Internet. Programa que busca puntos vulnerables de la red con relación a la seguridad.

ISS: Internal Sublayer Service (Clause 7, ISO/IEC 15802-3)

ITU International Telecommunications Union. Unión Internacional de Telecomunicaciones. Forma parte de la CCITT. Organización que desarrolla estándares a nivel mundial para la tecnología de las telecomunicaciones.

IVL: Independent VLAN Learning

J

JAVA Lenguaje de programación orientado a objeto parecido al C++. Usado en WWW para la tele carga y tele ejecución de programas en el computador cliente. Desarrollado por Sun microsystems.

JAVASCRIPT Programa escrito en el lenguaje script de Java que es interpretado por la aplicación cliente, normalmente un navegador (Browser).

JPEG Join Photograph Expert Group. Unión de Grupo de Expertos Fotográficos. Formato gráfico con pérdidas que consigue elevados ratios de compresión.

K

Kick "Patada". Usado normalmente en IRC. Acto de echar a un usuario de un canal.

Knowbot Robot de conocimiento o robot virtual. Se trata de un tipo de PDA.

L

LAN Local Area Network. Red de Área Local. Una red de área local es un sistema de comunicación de alta velocidad de transmisión. Estos sistemas están diseñados para permitir la comunicación y transmisión de datos entre estaciones de trabajo inteligentes, comúnmente conocidas como Computadoras Personales. Todas las PCs, conectadas a una red local, pueden enviar y recibir información. Como su mismo nombre lo indica, una red local es un sistema que cubre distancias cortas. Una red local se limita a una planta o un edificio.

LAPM Link Access Procedure for Modems. Procedimiento de Acceso a Enlace para Modems.

Layer Capa. En protocolos o en OSI se refiere a los distintos niveles de estructura de paquete o de enlace respectivamente.

LCP Link Control Protocol. Protocolo de Control de Enlace

Link Enlace. Unión. Se llama así a las partes de una página WEB que nos llevan a otra parte de la misma o nos enlaza con otro servidor.

Linux Versión Shareware del conocido sistema operativo Unix. Es un sistema multitarea multiusuario de 32 bits para PC.

Legacy region (región legal) la configuración de segmentos de LAN semejantes interconectados físicamente entre par de segmentos usando ISO/IEC 15802-3-adaptada, VLAN-inadvertida por los switches MAC.

LLC: Logical Link Control (ISO/IEC 8802-2)

LU Logic Unit. Unidad Lógica.

Lock Cerrado. Bloqueado.

LS: Least-significant

M

MAC Media Access Control. Control de Acceso a Medio. Protocolo que define las condiciones en las cuales las estaciones de trabajo acceden al medio. su uso está difundido en las LAN. en las LAN tipo IEEE la capa MAC es la subcapa más baja del protocolo de la capa de enlace de datos.

MAC: Medium Access Control (IEEE 802)

MAN Metropolitan Area Network. Red de Área Metropolitana.

MBONE Multicast Backbone. Red virtual que utiliza los mismos dispositivos físicos que la propia Internet con objeto de transmitir datos con protocolos Multicast.

MIB: Management Information Base (ISO/IEC 7498-4)

MIME Multipurpose Internet Mail Extensions. Extensiones Multi propósito de Correo Internet. Extensiones del protocolo de correo de Internet que permiten incluir información adicional al simple texto.

MMX Multi Media eXtensions. Extensiones Multimedia. Juego de instrucciones extra que incorporan los nuevos microprocesadores Pentium orientado a conseguir una mayor velocidad de ejecución de aplicaciones que procesan o mueven grandes bloques de datos.

MNP Microcom Networking Protocol. Protocolo de Redes de Microcom. Protocolo de corrección de errores desarrollado por Microcom muy usado en comunicaciones con MODEM. Existen varios niveles MNP2(asíncrono), MNP3(síncrono) y MNP4(síncrono).

MODEM Modulator/Demodulator.

Modulador/Demodulador. Dispositivo que adapta las señales digitales para su transmisión a través de una línea analógica. Normalmente telefónica.

MPEG Motion Pictures Expert Group. Grupo de Expertos en Imagen en Movimiento. Formato gráfico de almacenamiento de video. Utiliza como

Aplicación de VLAN en una red academica el JPEG compresión con perdidas alcanzando ratios muy altos.

MROUTER Multicast Router. Ruteador que soporta Protocolos Multicasting.

MRU Maximum Receive Unit. Unidad Máxima de Recepción. En algunos protocolos de Internet se refiere al máximo tamaño del paquete de datos.

MS: Most-significant

MS-DOS Microsoft Disk Operating System. Sistema Operativo en Disco de Microsoft. Sistema operativo muy extendido en PC del tipo de línea de comandos.

MSDU: MAC Service Data Unit (ISO/IEC 15802-1)

MTU Maximum Transmission Unit. Unidad Máxima de Transmisión. Tamaño máximo de paquete en protocolos IP como el SLIP.

MUD Multi User Dimension. Dimensión Multi Usuario. Sistemas de juegos multiusuario de Internet.

MULTICASTING Técnica de transmisión de datos a través de Internet en la que se envían paquetes desde un punto a varios simultáneamente.

N

NACR Network Announcement Request.

Petición de participación en la Red. Es la petición de alta en Internet para una sub red o dominio.

NAP Network Access Point. Punto de Acceso a la Red. Normalmente se refiere a los tres puntos principales por los que se accede a la red Internet en U.S.

NC Network Computer. Computador de Red. Computador concebido para funcionar conectado a Internet. Según muchos el futuro. Se trata de equipos de hardware muy reducido (algunos no tienen ni disco duro).

NCFI: Non-Canonical Format Indicator

NCP Network Control Protocol. Protocolo de Control de Red. Es un protocolo del Network Layer

NET Red

NETBIOS Network BIOS. Network Basic Input/Output System. Bios de una red, es decir, Sistema Básico de Entrada/Salida de red.

Netiquette Etiqueta de la RED. Formas y usos comunes para el uso de los servicios de Internet. Se podría llamar la "educación" de los usuarios de Internet.

Netizen Ciudadano de la Red.

NEWS Noticias. Servicio de Internet con una estructura de "tablón de anuncios" dividido en temas y países en los que los usuarios de determinados grupos de interés dejan o responden a mensajes relacionados con el mencionado grupo.

Nick Nombre o pseudónimo que utiliza un usuario de IRC.

Nodo Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red. Punto de interconexión a una RED.

NSA National Security Agency. Agencia Nacional de Seguridad. Organismo americano para la seguridad entre otras asuntos relacionados con la informática.

NSF National Science Fundation. Fundación Nacional de Ciencia. Fundación americana que gestiona gran parte de los recursos de Internet.

O

OEM Original Equipment Manufactured. Manufactura de Equipo Original. Empresa que compra un producto a un fabricante y lo integra en un producto propio. Todos los fabricantes por ejemplo, que incluyen un Pentium en su equipo actúan como OEM.

OS2 Operating System 2. Sistema operativo de 32 bits multitarea creado por IBM. Creado para PC con entorno gráfico de usuario. La versión actual es la 4 la cual soporta ordenes habladas y dictado.

OSI Open Systems Interconnection. Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO. Divide las tareas de la red en siete niveles.

P

Packet Driver Pequeño programa situado entre la tarjeta de red y el programa de TCP de manera que proporciona una interfaz estándar que los programas pueden usar como si de un driver se tratase.

Packet Paquete Cantidad mínima de datos que se transmite en una red o entre dispositivos. Tiene una estructura y longitud distinta según el protocolo al que pertenezca. También llamado TRAMA.

PAN Personal Area Network. Red de Área Personal. Sistema de red conectado directamente a la piel. La transmisión de datos se realiza por contacto físico.

PAP Password Authentication Protocol. Protocolo de Autenticación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante password.

PBX Private Branch Exchange. Central Privada

PDA Personal Digital Assistant. Asistente Personal Digital. Programa que se encarga de atender a un usuario concreto en tareas como búsquedas de información o selecciones atendiendo a criterios personales del mismo.

Suele tener tecnología de IA (Inteligencia Artificial).

PDU: Protocol Data Unit

PEER En una conexión punto a punto se refiere a cada uno de los extremos.

PEM Private Enhanced Mail. Correo Privado Mejorado. Sistema de correo con encriptamiento.

PERL Lenguaje para manipular textos, ficheros y procesos. Con estructura de script. Desarrollado por Larry Wall, es multiplataforma ya que funciona en Unix.

PGP Pretty Good Privacy. Excelente clave pública de seguridad desarrollada por Phil Zimmerman y mejorada por muchos otros incluyendo a Hal Finney, Branko Lankester, and Peter Gutmann.

Phracker Pirata informático que se vale de las redes telefónicas para acceder a otros sistemas o simplemente para no pagar teléfono.

PICS: Protocol Implementation Conformance Statement

PIN Personal Identification Number. Número Personal de Identificación. Número secreto asociado a una persona o usuario de un servicio mediante el cual se accede al mismo. Se podría decir que es una "Password" numérica.

PING Packet Internet Groper. Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible. Envía paquetes de control para comprobar si el anfitrión está activo y los devuelve.

PNG Portable Network Graphics. Gráficos Portables de Red. Formato gráfico muy completo especialmente pensado para redes.

POP Post Office Protocol. Protocolo de Oficina de Correos. Protocolo usado por computadores personales para manejar el correo sobre todo en recepción.

POST Power On Self Test. AutoTest de Encendido. Serie de comprobaciones que hace un computador de sus dispositivos al ser encendido.

POTS Plain Old Telephone Services. Servicios Telefónicos Planos Antiguos.

PPP Point to Point Protocol. Protocolo Punto a Punto. Un sucesor del SLIP. El PPP provee las conexiones sobre los circuitos síncronos o asíncronos, entre router y router, o entre host y la red. Protocolo Internet para establecer enlace entre dos puntos.

PPV. Pay Per View. Pagar Para Ver. Se refiere a las televisiones llamadas "interactivas" o "televisión a la carta" en las que hay que pagar por cada programa que se selecciona para ver.

Priority-tagged frame: esta trama esta en el encabezado transportando información de prioridad, pero no transporta información sin identificarse como parte de una VLAN.

PROXY. Servidor Caché. El Proxy es un servidor de que conectado normalmente al servidor de

acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

PU Physical Unit. Unidad Física.

PVID: Port VID

PVC Permanent Virtual Circuit. Circuito Virtual Permanente. Línea punto a punto virtual establecida normalmente mediante conmutaciones de carácter permanente. Es decir a través de un circuito establecido.

Q

QAM Quadrature Amplitude Modulation. Modulación de Amplitud en Cuadratura. Sistema de modulación para transmisión de datos y telecomunicaciones.

R

RARP Reverse Address Resolution Protocol. Protocolo de Resolución de Dirección de Retorno. Protocolo de bajo nivel para la asignación de direcciones IP a máquinas simples desde un servidor en una red física.

RAM Random Access Memory. Memoria de Acceso Aleatorio. Varios son los tipos de memoria que se usa en las computadoras. La más conocida son las RAM. Se les llama así porque es posible dirigirse directamente a la célula donde se encuentra almacenada la información. Su principal característica es que la información se almacena en ellas provisoriamente, pudiendo ser grabadas una y otra vez, al igual que un cassette de sonido. La memoria RAM se puede comparar a un escritorio, donde se coloca los papeles con que se va a trabajar. Mientras más grande el escritorio más papeles soporta simultáneamente para ser procesados.

RAS Remote Access Server. Servidor de Acceso Remoto.

Retrain Se llama así a la acción que ejecuta un modem para re establecer el sincronismo con el otro modem después de una pérdida de comunicación.

RDSI Red Digital de Servicios Integrados. Red de telefónica con anchos de banda desde 64Kbps. Similar a la red telefónica de voz en cuanto a necesidades de instalación de cara al abonado, pero digital. En inglés ISDN.

RFC Request For Comment. Petición de comentarios. Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet. Los RFC son elaborados por la comunidad Internet.

RIF: Routing Information Field (ISO/IEC 8802-5)

Aplicación de VLAN en una red academica

RIP Routing Information Protocol. Protocolo de Información de Routing.

ROM Read Only Memory. Memoria sólo de lectura. Las memorias ROM se usan para mantener instrucciones permanentes, que no deben borrarse nunca. Estas memorias vienen grabadas de fábrica. Son como los discos fonográficos, que sólo permiten reproducir el sonido. Tienen la ventaja de ser de alta velocidad y bajo costo.

ROOT Raíz. En sistemas de ficheros se refiere al directorio raíz. En Unix se refiere al usuario principal.

Router Dispositivo conectado a dos o mas redes que se encarga únicamente de tareas de comunicaciones

RS-232 Conjunto de estándares especificando varias características eléctricas y mecánicas para interfaces entre computadoras terminales y modems. Normalmente presenta 25 pines. Virtualmente idéntica a V.24

RS-422 Interfaz física más rápida que la RS-232 y para distancias de cableados mayores.

RSA Rivest, Shamir, Adelman [public key encryption algorithm]. Algoritmo de encriptación de clave pública desarrollado por Rivest, Shamir y Adelman.

RTC Red Telefónica Conmutada. Red Telefónica para la transmisión de voz.

RTP Real Time Protocol. Protocolo de Tiempo Real. Protocolo utilizado para la transmisión de información en tiempo real como por ejemplo audio y vídeo en una video-conferencia.

RWIN Receive Window. Ventana de recepción. Parámetro de TCP que determina la cantidad máxima de datos que puede recibir el computador que actúa como receptor.

RX Abreviatura de Recepción o Recibiendo.

S

SATAN Security Analysis Tool for Auditing Networks. Herramienta de Análisis de Seguridad para la Auditoría de Redes. Conjunto de programas escritos por Dan Farmer junto con Wietse Venema para la detección de problemas relacionados con la seguridad.

SDH Synchronous Digital Hierarchy. Estándar Europeo que define un grupo de formato que son transmitidos usando señalización óptica sobre fibra. El SDH es similar al SONET, con un rango básico de 155.52 Mbps, diseñado para viajar a STM-1.

SDLC Synchronous Data Link Controller. Controlador de Enlace de Datos Sincrono. También se trata de un protocolo para enlace sincrónico a través de línea telefónica. Protocolo propietario de IBM orientado al bit.

SDSL Symmetric Digital Subscriber Line. Línea Digital Simétrica de Abonado. Sistema de

transferencia de datos de alta velocidad en líneas telefónicas normales.

SEPP Secure Electronic Payment Protocol. Protocolo de Pago Electrónico Seguro. Sistema de pago a través de Internet desarrollado por Netscape y Mastercard.

SGML Standard Generalized Markup Language. Lenguaje de Anotaciones Generales. Lenguaje del que deriva el HTML.

S-HTTP Secure HTTP. HTTP seguro. Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

Shared Virtual Local Area Network (VLAN) Learning (SVL) Bridge: un tipo de puenteo que solo soporta Shared VLAN Learning.

Shared Virtual Local Area Network (VLAN) Learning (SVL): la configuración y operación de el proceso de aprendizaje y filtrado de Base de Datos semejante, dados por la configuración de VLAN, si una dirección MAC individual es aprendida en una VLAN, es usada la información para encaminar información tomando decisiones de las direcciones relativamente de todas las otras VLANs configuradas.

Shared Virtual Local Area Network (VLAN) Learning (SVL)/ Independent Virtual Local Area Network (VLAN) Learning (IVL) Bridge: este es un tipo de puenteo que simultáneamente soporta Shared VLAN Learning y Independent VLAN Learning.

SIM Single Identification Module. Módulo Simple de Identificación. Normalmente se refiere a una tarjeta: Tarjeta SIM. Que identifica y a través de ella da servicio a un usuario, su uso más común es el los teléfonos GSM.

SLIP Serial Line Internet Protocol. Protocolo Internet en Línea Serial. Protocolo, antecesor del PPP, que permite establecer conexiones TCP/IP a través de enlaces seriales.

SmartCard Tarjeta Inteligente. Tarjeta del formato estándar de crédito que incorpora un microchip (EEPROM o Microprocesador) que almacena información y/o la procesa. Por ejemplo las tarjetas telefónicas (EEPROM) o las tarjetas SIM de teléfonos móviles (Microprocesador).

SMTP Simple Mail Transfer Protocol. Protocolo de Transferencia Simple de Correo. Es el protocolo usado para transportar el correo a través de Internet.

SMS Short Message Service. Servicio de Mensajes Cortos. Servicio de mensajería electrónica de texto entre teléfonos GSM. Gracias a esta capacidad se puede enviar también e-mail desde un teléfono GSM y recibir mensajes desde Internet, aunque esta posibilidad parece ser que aún no funciona en España.

SNA System Network Architecture. Arquitectura de Sistemas de Redes. Arquitectura

Aplicación de VLAN en una red académica de red exclusiva de IBM. Principalmente orientada a Mainframes.

Sniffer Literalmente "Husmeador". Pequeño programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente su uso es ilegal.

Software. Esta palabra inglesa que significa "cosa suave", tiene dos significados: (a) uno amplio, de "procedimientos lógicos, para la cooperación armónica de un grupo de personas y máquinas, persiguiendo un objetivo común"; (b) el otro restringido, de "programas de computadora", o conjunto de instrucciones, que se pone en la memoria de una computadora para dirigir sus operaciones.

Spam / Spammer Se llama así al "bombardeo" con correo electrónico, es decir, mandar grandes cantidades de correo o mensajes muy largos.

Spider Robot-Web. Programa que automáticamente recorre la WWW recogiendo páginas Web y visitando los Links que estas contienen.

STPID: SNAP-encoded Tag Protocol Identifier

SQL Structured Query Language. Lenguaje de Petición Estructurada. Lenguaje para base de datos.

SSL Secure Sockets Layer. Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

STT Secure Transaction Technology. Tecnología de Transacción Segura. Sistema desarrollado por Microsoft y Visa para el comercio electrónico en Internet.

SVL: Shared VLAN Learning

T

Tagged frame: es una trama que contiene una etiqueta en el encabezado inmediatamente seguida de la dirección MAC fuente en el campo de la trama o, si la trama contiene un campo de información de ruteo, inmediatamente seguida de la información del campo de ruteo. Estas son dos tipos de etiquetas de trama: VLAN-tagged frames y priority-tagged frames.

T1 Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 1.54 Mbps a través de una red telefónica.

T3 Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 44.7 Mbps a través de una red telefónica.

TCM Trellis-Coded Modulation

TCI: Tag Control Information

TCP/IP Transmission Control Protocol / Internet Protocol. Protocolo de Control de Transmisión / Protocolo Internet. Nombre común para una serie de protocolos desarrollados por DARPA en los Estados Unidos en los años 70,

para dar soporte a la construcción de redes interconectadas a nivel mundial. TCP corresponde a la capa (layer) de transporte del model OSI y ofrece transmisión de datos. El IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal característica es comunicar sistemas diferentes. Fueron diseñados inicialmente para ambiente Unix por Victor G. Cerf y Robert E. Kahn. El TCP / IP son básicamente dos de los mejores protocolos conocidos.

TELNET Protocolo y aplicaciones que permiten conexión como terminal remota a una computadora anfitriona, en una localización remota.

Time-out Parámetro que indica a un programa el tiempo máximo de espera antes de abortar una tarea o función. También mensaje de error.

Tipo de Codificación Ethernet: el uso del tipo de interpretación de la IEEE 802.3 tipo/longitud en el campo de la trama como un protocolo que se asocia con el Servicio de la trama de transporte de datos de la MAC.

Throughput. Transferencia Real. Cantidad de datos que son transmitidos a algún punto de la red.

Trama (Frame) una unidad de transmisión de datos en una IEEE 802 LAN MAC que llevan un protocolo de unidad de datos (PDU) seguido de la dirección MAC. Están estos tres tipos de tramas: desetiquetar (untagged), etiquetado-VLAN (VLAN-tagged) y prioridad de etiquetado (priority-tagged).

TTD Telefónica Transmisión de Datos. División de Telefónica para la transmisión de datos.

TTL Time To Live.Tiempo de Vida. Contador interno que incorporan los paquetes Multicast y determinan su propagación.

TPID: Tag Protocol Identifier

Tunneling Transporte de paquetes Multicast a través de dispositivos y Routers unicast. Los paquetes multicast se encuentran encapsulados como paquetes normales de esta manera pueden viajar por Internet a través de dispositivos que solo soportan protocolos unicast.

TX Abreviatura de Transmisión o Transmitiendo.

U

UDP User Datagram Protocol. Protocolo de Datagrama de Usuario. Protocolo abierto en el que el usuario (programador) define su propio tipo de paquete.

UNICAST Se refiere a Protocolos o Dispositivos que transmiten los paquetes de datos de una dirección IP a otra dirección IP.

UNIX Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas mas conocidos como MS-DOS están basadas en este sistema muy extendido para

Aplicación de VLAN en una red academica grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

Untagged frame: es una trama que no contiene una etiqueta en el encabezado de la trama inmediatamente sigue la dirección fuente MAC al campo de la trama o, si la trama contiene un campo de información de ruteo, inmediatamente sigue la información del campo de ruteo.

URL Uniform Resource Locator. Localizador Uniforme de Recursos. Denominación que no solo representa una dirección de Internet sino que apunta aun recurso concreto dentro de esa dirección.

USB Universal Serial Bus. Bus Serie Universal.

UT Universal Time. Hora Universal. Ver GMT.

UUCP Unix to Unix Communication Protocol. Protocolo de Comunicaciones de Unix a Unix. Uno de los protocolos que utilizan los sistemas Unix para comunicarse entre si.

UUENCODE Unix to Unix Encoding. Codificador Unix a Unix. Método de transmitir archivos binarios en mensajes electrónicos ASCII.

V

VID: VLAN Identifier

VINES Virtual Integrated Network Service. Sistema Operativo para Red desarrollado y manufacturado por Sun Systems.

VR Virtual Reality. Realidad Virtual.

VRML Virtual Reality Modeling Language. Lenguaje para Modelado de Realidad Virtual. Lenguaje para crear mundos virtuales en la Web.

Virtual Bridged Local Area Network (LAN) es cuando existen una o más VLAN puenteadas dejando definir, crear y mantener VLANs.

Virtual Local Area Network (VLAN) una sub-configuración de la topología activa de un puente LAN, asociado con cada VLAN es un identificador (VID).

VLAN-aware: es una propiedad de puentes o de estaciones finales que reconocen y soportan VLAN con tramas etiquetadas.

VLAN-tagged frame: es una trama etiquetada cuyo encabezado transporta ambos: identificadores VLAN y prioridad de información.

VLAN-unaware: una propiedad de los puentes o estaciones finales que no reconocen VLAN-tagged frames.

W

WAIS Wide Area Information Server Servidores de Información de Área Amplia. Sistema de obtención de información patrocinado por Apple, Thinking Machines y Dow Jones.

WAN Wide Area Network. Red de Área Ancha. Wanderer. Robot-Web. Ver Spider.

Warez Software pirata que ha sido desprotegido.

Web Site. Sitio en el World Wide Web. Conjunto de páginas Web que forman una unidad de presentación, como una revista o libro. Un sitio está formado por una colección de páginas Web. RELI - Revista en Línea puede considerarse un sitio web. Una de las páginas del sitio es este glosario.

Webcam Cámara conectada a una página WEB a través de la cual los visitantes pueden ver imágenes normalmente en directo.

WINDOWS Pseudo sistema operativo, que funciona basado en el DOS. Más bien se trata de un entorno gráfico con algunas capacidades multitarea. La versión actual WINDOWS 95 funciona parcialmente a 32 bits.

WWW, WEB o W3 World Wide Web. Telaraña mundial. Sistema de arquitectura cliente-servidor para distribución y obtención de información en Internet, basado en hipertexto e hipermedia. Fue creado en el Laboratorio de Física de Energía Nuclear del CERN, en Suiza, en 1991 y ha sido el elemento clave en el desarrollo y masificación del uso de Internet.

X

X Window System. Sistema de Ventanas X. El sistema de Ventanas X permite que cada ventana se conecte con una computadora remota.

X.25 Protocolo de transmisión de datos. Establece circuitos virtuales, enlaces y canales. Es una tecnología antigua de red usado en Europa.

Z

ZIP Zone Information Protocol. Protocolo de Información de Zona.

Bibliografía

1. **Andrew S. Tanenbaum.**: "Redes de computadoras", Tercera Edición, Pearson Education, pp. 814, México 1997
2. **Douglas E. Comer.**: "Redes globales de información con Internet y TCP/IP", Tercera Edición, Prentice Hall, Vol. I, pp. 621, México 1995
3. **Merilee Ford, H. Kim Lew, Steve Spainer, Tim Stevenson.**: "Tecnologías de Interconectividad de redes", Pearson, pp. 736, Mexico 1998
4. **Carlos Muñoz Razo.**: "Cómo elaborar y asesorar una investigación de Tesis", Primera edición, Pearson Education, pp. 300, México 1998
5. **Cisco System, Inc.**: "Guía del segundo año", Segunda Edición, Cisco System, pp. 736, España 2001

Manuales de Enterasys Networkers

802.1 Q VLANS Course
Enterasys Specialist SmartSwitch Router Configuration Course
Vertical Horizon VH-2402s Fast Ethernet Switch Management Guide
Vertical Horizon VH-2402s Fast Ethernet Switch User Guide
802.1 Q VLAN User Guide Local Management Introduction
802.1 Q VLAN User's Guide
SmatTrunk User's Guide
802.1 Q VLAN User Guide Local Management Supplement

Paginas de Internet

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/confg_qd/vlans.htm, Tutorial de Configuración de vlans por cisco
<http://www.nwfusion.com/index.html>, Manual de configuración por nwfusion
<http://www.iol.unh.edu/training/vlan/sld002.htm>, Manual de entrenamiento por Hadriel Kaplan
http://www.intel.com/network/connectivity/resources/doc_library/tech_brief/virtual_lans.htm, Manual de intel para la configuración de vlans
<http://www.monografias.com/trabajos12/intrants/intrants.shtml>, articulo sobre implementación de seguridad sobre vlans
http://www.intel.com/network/connectivity/resources/doc_library/tech_brief/virtual_lans.pdf, como configurar vlans con equipos intel
<http://www.angelfire.com/al2/Comunicaciones/enlaces.html>, documentación técnica por la Universidad del Táchira
<http://www.consulintel.es/Html/Tutoriales/Articulos/smds.html>, articulo llamado Redes Virtuales: El primer paso hacia la ubicuidad geográfica.

Estándares

- 802.1V-2001 IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridge Local Area Networks - Amendment 2: VLAN Classification by Protocol and Port (Amendment to IEEE 802.1Q, 1998 Edition) 2001