II.

Requerimientos para la Implementación de una VLAN

2.1 Protocolos aplicados a una VLAN

Como toda tecnología, las VLANs deben seguir ciertas reglas que controlen y permitan la conexión, comunicación y transferencia de datos de una manera adecuada. En el caso de las redes virtuales, el principal estándar que existe para la implementación de las mismas es el 802.1Q desarrollado por la IEEE, en conjunto con la norma 802.1P.

Antes de la introducción del IEEE 802.1Q existían ya algunos otros protocolos como el ISL (*Inter Switch Link – Enlace entre Conmutadores*) de Cisco, el cual es una variante del IEEE 802.1Q, el VTP (*VLAN Trunk Protocol – Protocolo de Enlace Troncal de VLAN*) y el VLT (*Virtual LAN Trunk*) de 3Com.

A continuación se explica en qué consiste cada uno de los protocolos que rigen el mundo de las VLANs.

a) IEEE 802.1Q

El estándar IEEE 802.1Q fue publicado en 1998 por el organismo IEEE para resolver el problema que se presenta cuando diversas redes se encuentran compartiendo el mismo medio físico y por lo tanto consumiendo un mayor ancho de banda del necesario, generando tráfico broadcast y multicast.

Este protocolo interconecta VLANs entre varios switches, routers y servidores, proporcionando a su vez un mayor nivel de seguridad entre los segmentos de redes internas. Los switches Cisco soportan dicho estándar para las interfaces FastEthernet y GigabitEthernet.

Para poder identificar a una VLAN en específico, el IEEE 802.1Q inserta un campo en el frame, es decir, incluye una etiqueta de cuatro octetos (32 bits) en cada trama Ethernet entre la dirección fuente y el campo de longitud, como puede observarse en la **Figura II.1.**

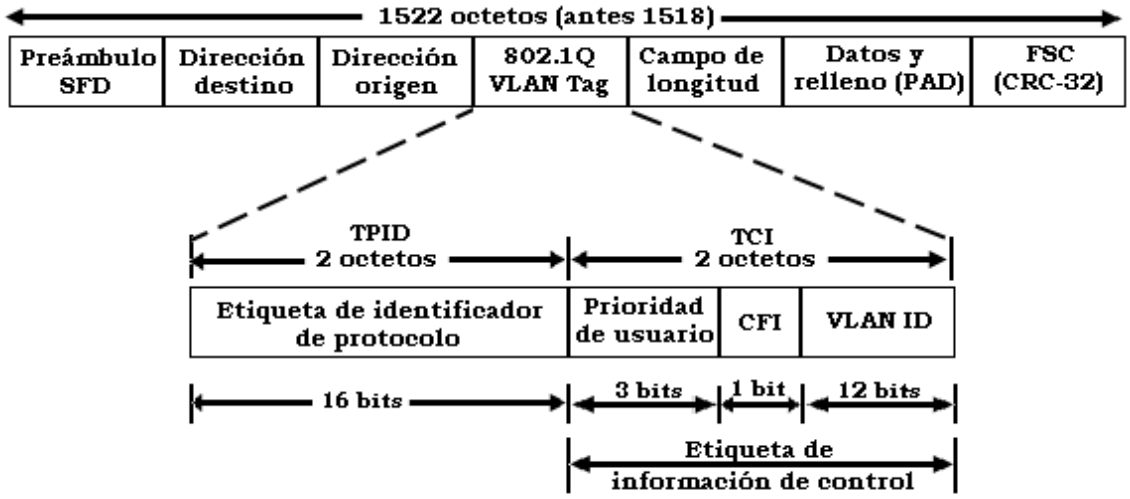

Figura II.1 Trama de la norma 802.1 Q

La etiqueta agregada a la trama Ethernet está compuesta por dos campos de información:

- La etiqueta de información de control (*Tag Control Information – TCI*) y el
- Campo de etiqueta de identificador de protocolo (*Tag Protocol IDentifier field – TPID*)

El campo TCI es constituido a su vez por tres sub-campos que suman 16 bits, es decir, dos octetos:

1. *VLAN ID* que consta de 12 bits, este campo indica el grupo de VLAN y permite acceder hasta 4096 VLANs. Todos los switches en la red usan este VLAN ID para enlazar las membrecías de redes virtuales entre sí. Los números de identificación VLAN ID deben asignarse de forma centralizada e informarse en su totalidad a los diferentes switches y nodos que conformen la red, de no ser así, un mismo VLAN ID podría repetirse varias veces. Para evitar esta situación, se recurre al Protocolo Genérico de Registro de Atributos (*Generic Attribute Registration Protocol – GARP*) que es la norma original 802.1P, este protocolo es utilizado como base para la comunicación de la membrecía de las redes VLAN entre los diferentes switches. Más adelante se explica con más detalle en qué consiste dicha norma.

2. *Prioridad de usuario* de 3 bits, este campo permite hasta ocho niveles de prioridad.

3. *CFI* (*Canonical Identifier Format – Indicador de Formato Canónico*) consta de un bit que se utiliza únicamente para comunicaciones Token Ring, indicando si el paquete encapsulado es una trama Token Ring en un formato de trama Ethernet.

El campo TPID consta también de 16 bits (2 octetos) y se usa para las transmisiones de datos de Token Ring, FDDI y codificadas en SNAP.

La membrecía de redes VLAN puede darse a conocer de dos formas:

- Implícita
- Explícita

La comunicación implícita supone que indirectamente el o los switches saben a qué VLAN en específico pertenece un paquete. Por otro lado, la comunicación explícita implica que cada paquete o trama debe ser como su nombre lo indica, explícitamente marcada para indicar su pertenencia a una VLAN en particular, por ejemplo, el tráfico de una VLAN basada en direcciones MAC debe marcarse con un identificador propio de esa red virtual.

En general las VLANs que se encuentran basadas en puertos y direcciones MAC usan comunicaciones explícitas, mientras que las VLANs con atributo de capa 3 como las basadas en protocolo o dirección IP pueden usar etiquetado implícito.

b) IEEE 802.1P

Una de las características del protocolo ATM (*Asynchronous Transfer Mode – Modo de Transferencia Asíncrona*) es su capacidad para dar prioridad al tráfico dentro de diferentes clases, sin embargo, dicho protocolo ha sido criticado debido a su falta de capacidad para distinguir entre datos cruciales y datos de menor importancia.

La norma 802.1P utiliza el concepto de clases de tráfico, en donde existen 8 tipos de ellas, conocidas también como prioridades de usuario (*pritority user*) por cada puerto de un conmutador. Para lograr el cumplimiento de dicha norma es necesario aumentar el formato básico de Ethernet, caso que se da con la aplicación de la norma 802.1Q en el subcampo prioridad de usuario perteneciente al campo TCI. En la **Tabla 2.1** se pueden observar los valores de prioridad de usuario así como el rango asignado de acuerdo al nivel de prioridad.

Tabla 2.1. Valores de prioridad

Prioridad de usuario	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

El concepto de colas en cada puerto también es importante, ya que una vez que las tramas se encuentran en las colas de los puertos, éstas se asocian con el tipo de tráfico; con lo cual se asegura que los paquetes se coloquen en los grupos correspondientes de acuerdo a su importancia. Un ejemplo de clasificación de tráfico es el mostrado en la **Tabla 2.2.**

Tabla 2.2. Relación tipo de tráfico/prioridad de usuario

Tipo de tráfico	Prioridad de usuario
Función de respaldo	2
Función de control de la red	7
Voz: Retardo < 10 ms.	6
Video: Retardo < 10 ms.	5
Carga controlada (algunas aplicaciones importantes)	4
Excelente esfuerzo	0
Mejor esfuerzo	3
Background	1

Como ya se mencionó, el estándar 802.1Q contiene un campo que permite 8 niveles de prioridad; algunas veces la norma de prioridad de tráfico 802.1P es mencionada como 802.1Q/P debido a que mientras que la prioridad tanto de tráfico como de protocolos asociados son parte de la especificación 802.1P, el campo de prioridad de una trama Ethernet se encuentra definido dentro de la norma 802.1Q, que contiene al identificador de la VLAN de 12 bits. Por lo tanto la prioridad es realmente una combinación de ambas normas.

802.1Q/P permite actualmente a los fabricantes construir switches y tarjetas NIC con la capacidad de priorizar el tráfico de datos susceptibles, tales como la voz y el video.

En la **Figura II.2** se muestra un prototipo de cómo es que funciona la prioridad de tráfico, aplicando la norma IEEE 802.1Q. En el ejemplo se presenta un servidor de archivos el cual se usa para transmitir grandes cantidades de tráfico a un solo cliente, esto se encuentra simbolizado por los paquetes *FS*, se presenta también un servidor de video que transmite tramas *VS* las cuales contienen video comprimido hacia un grupo de estaciones ubicadas en el switch; ambos servidores están conectados mediante un dispositivo basado en la norma 802.1Q/P.

Los switches generalmente trabajan con el algoritmo FIFO (*First In First Out – Primero en entrar, Primero en salir*). El problema surge cuando son enviados pequeños paquetes de video y a su vez grandes paquetes de datos, que implican la transferencia de grandes archivos. Los paquetes de video tendrían que esperar a que primero sean transmitidos los grandes paquetes de datos, acción que provocaría una variación en la imagen de video (*video jitter*).

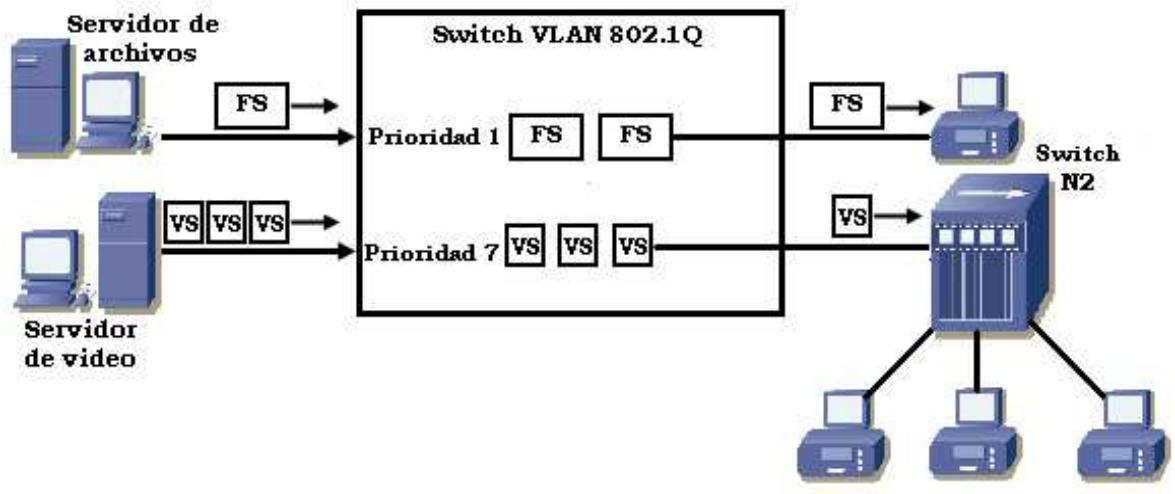

Figura II.2 Aplicación de la norma 802.1 Q

La combinación de una tarjeta NIC de servidor con la norma 802.1Q/P implementada entregará el video a tiempo, dando así prioridad a sus tramas sobre las tramas de los archivos. Esto se consigue otorgando una prioridad de 1 a las tramas de los archivos y una prioridad alta igual a 7 a las tramas de video.

Todos los switches usan un sistema de colas para poder analizar y posteriormente retransmitir el tráfico. El switch del ejemplo mostrado, inmediatamente coloca las tramas con prioridad 7 delante de las tramas con prioridad 1, asegurando una transmisión de video confiable.

c) Protocolo ISL

ISL es un protocolo propietario de Cisco que opera en ambientes punto a punto y permite interconectar múltiples switches.

Algunas características de este protocolo son las siguientes:

- ISL puede transportar cualquier protocolo de enlace de datos (Ethernet, Token Ring, FDDI, ATM, etc.).
- Soporta PVST (*Per VLAN Spanning Tree – Árbol de Expansión por VLAN*).
- No usa una VLAN nativa, solo encapsula cada trama.
- El proceso de encapsulación deja las tramas originales sin modificación.

ISL funciona a nivel de capa 2 del modelo OSI, encapsulando una trama de datos con una nueva cabecera (ISL) de 26 bytes que contiene una identificador de la VLAN a la que pertenece y al final se adiciona también un campo de verificación por redundancia cíclica (*CRC – Cyclic Redundancy Check*) de 4 bytes. El encapsulamiento ISL puede apreciarse en la **Figura II.3.**

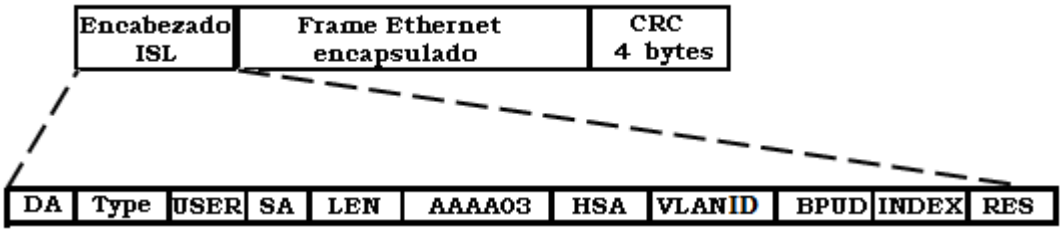

Figura II.3 Encapsulamiento ISL

A continuación se presenta una breve explicación de cada uno de los subcampos que conforman el encabezado ISL.

- *DA* (*Destination Address – Dirección destino*): La dirección destino es una dirección multicast que consta de 40 bits. Este primer campo es el que indica que la trama se encuentra encapsulada con el protocolo ISL.
- *Type:* Consiste en un código de 4 bits, el cual representa el tipo de trama: Ethernet (0000), Token Ring (0001), FDDI (0010) y ATM (0011).
- *USER:* Este campo es considerado una extensión del campo Type, ya que consiste en 4 bits que indican el nivel de prioridad Ethernet: prioridad más baja (0000), prioridad 1 (0001), prioridad 2 (0010) y prioridad 3 (0011).
- *SA* (*Source Address – Dirección fuente*): Indica la dirección de la cual proviene el paquete ISL y consta de un valor de 48 bits.
- *LEN* (*Length – Longitud*): Presenta el tamaño real del paquete original como un valor de 16 bits representados en octetos, exceptuando los campos DA, Type, USER, SA, LEN y campos de FCS. La longitud total de los campos excluidos es de 18 octetos, por lo que el campo LEN es la longitud total de la trama menos 18 octetos.
- *AAAA03* SNAP (*Subnetwork Access Protocol – Protocolo de Acceso a Subredes*): Es un campo con un valor constante de 24 bits.

- *HSA* (*High Bits of Source Address – Bits Altos de la Dirección Fuente*): Cuenta con un valor de 24 bits, los 3 primeros bytes representan el ID de fabricante o el ID único organizacional.
- *VLAN ID:* Consta de 15 bits y se utiliza para conocer a que VLAN pertenece cada trama, llegando a soportar hasta 1024 VLANs.
- *BPDU* (*Bridge Protocol Data Uniques – Unidades de Datos del Protocolo Puente*): Consta exclusivamente de 1 bit que identifica si la trama es spanning tree, para de esta forma determinar la información sobre la topología de la red.
- *INDEX:* Se emplea únicamente para objetivos de diagnóstico y puede ser puesto a cualquier valor de 16 bits por otros dispositivos.
- *RES*: Campo de reserva de 16 bits usado para información adicional.

El protocolo ISL utiliza un mecanismo llamado ISL tagging, que permite multiplexar el tráfico desde diversas VLANs en una sola trayectoria física.

ISL tagging está diseñado para implementarse en gran variedad de dispositivos (switches, routers, tarjetas de red de servidores, etc.), los cuales deben de estar configurados para soportar ISL ya que los equipos que no sean capaces de soportar dicha tecnología, pueden tomar como errores las tramas que excedan el tamaño de MTU (Maximum *Transmission Unit - Unidad Máxima de Transmisión*).

En la **Figura II.4** se encuentra representada la forma en que opera el ISL Tagging. Cuando se conectan dos switches con un enlace troncal y éste debe mover tramas de varias VLANs, tiene que ser configurado para realizar dicha función, en caso contrario llevará únicamente tramas de la VLAN1 o default.

Los enlaces troncales se configuran en puertos de 100 ó 1000 Mbps. Se establecen entre dos switches, entre un switch y un router o entre un switch y un servidor. Un enlace troncal puede llevar información de hasta 1005 VLANs.

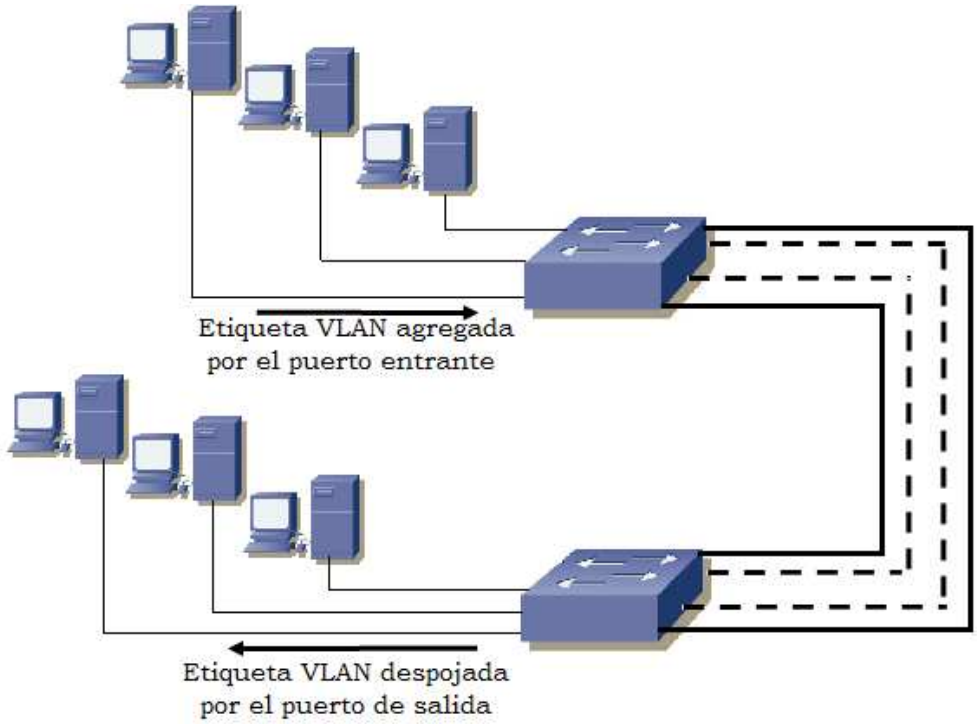

Figura II.4 ISL Tagging

d) Protocolo VTP

VTP es un protocolo usado para distribuir y sincronizar información de identificación acerca de las VLANs configuradas a través de una red switcheada. También es considerado como un estándar de mensajería de capa 2 que mantiene la consistencia de la configuración VLAN mediante el manejo de adiciones, borrado y cambio de nombres de las VLANs a través de las redes. Un dominio VTP es un switch o varios switches interconectados compartiendo el mismo ambiente VTP.

VTP opera en uno de tres modos posibles, los cuales se pueden observar en la **Figura II.5**; el modo VTP por default de un switch es el modo servidor, pero las VLANs no son propagadas sobre la red hasta que el nombre de un dominio de administración es especificado o aprendido.

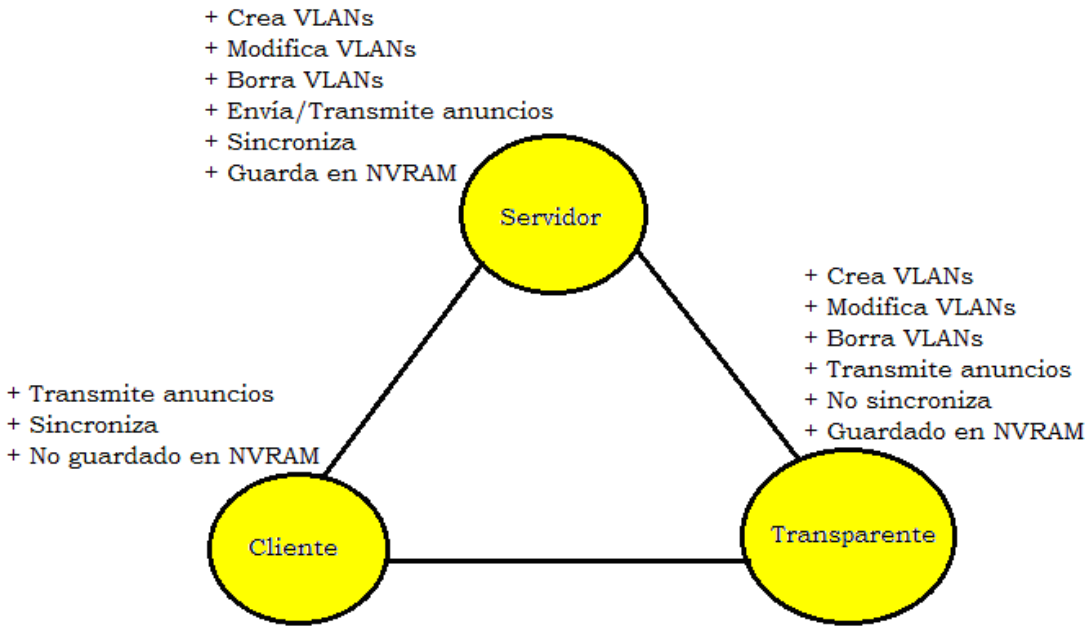

Figura II.5 Modos VTP

Cuando un cambio ocurre en la configuración de una VLAN con VTP en modo *Servidor*, el cambio es propagado a todos los switches que se encuentren en el dominio VTP.

En los modos VTP *Servidor* y *Cliente*, los switches sincronizan sus configuraciones de VLAN con la última información recibida desde los otros switches en el dominio administrado.

Un switch operando en modo VTP *Transparente* no crea anuncios VTP o sincroniza su configuración VLAN con la información recibida de otros switches. Este protocolo trabaja de la siguiente manera:

- Los anuncios VTP son enviados como frames multicast.
- Los servidores y clientes VTP son sincronizados al último número de revisión.
- Los anuncios de VTP son enviados cada cinco minutos o cada vez que hay un cambio.

Los pasos anteriores pueden observarse en el ejemplo de la **Figura II.6**.

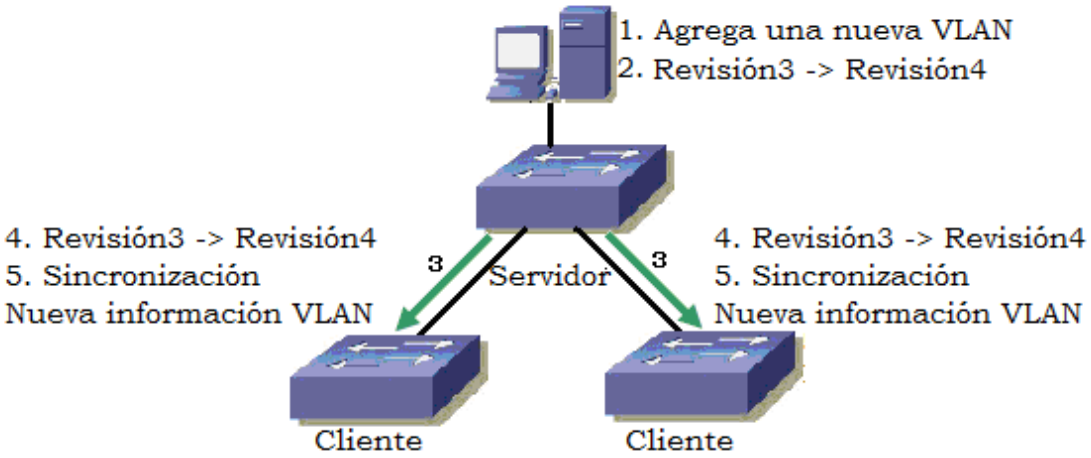

Figura II.6 Funcionamiento de VTP

Posteriormente un dispositivo que recibe anuncios VTP checa el nombre del dominio de administración y la contraseña en el anuncio, que debe ser igual a los configurados en el switch local antes de que la información pueda ser usada. El número de revisión de configuración es el parámetro crítico a revisar, cada vez que se modifica la configuración VLAN, el cambio incrementa el número de dicha revisión en uno. El dispositivo envía el anuncio VTP con el nuevo número y de esta manera los otros switches sobrescriben sus configuraciones VLAN con la nueva información que está siendo anunciada.

e) Protocolo VLT

VLT es una opción adicional proporcionada por los switches 3Com. Ambos puertos en un enlace deben de estar configurados para soportar el protocolo, ya que si uno de los puertos no se encuentra configurado para ello, será imposible agregar un enlace de este tipo y por lo tanto no se podrá llevar a cabo la transmisión de tráfico a todas las VLANs definidas en un switch 3Com. VLT es realmente muy similar al protocolo 802.1Q, sin embargo cuando la norma 802.1Q está siendo utilizada, no es posible aplicar VLT.

2.2 Tecnología necesaria para la implementación de una VLAN

Dentro del entorno de las VLANs existen tres aproximaciones diferentes que pueden ser empleadas como soluciones válidas para proporcionar redes virtuales:

- Conmutación de puertos
- Conmutación de segmentos con funciones bridging y
- Conmutación de segmentos con funciones bridging/routing

Estas soluciones se encuentran basadas en arquitecturas de red que emplean concentradores y/o conmutadores y por lo tanto, las tres cuentan con ciertas prestaciones de las VLANs, lo cual se explica más adelante.

Aunque las tres son soluciones válidas, únicamente la última de ellas ofrece todas las ventajas posibles ante la implementación de una VLAN.

a) Conmutación de puertos

Los conmutadores de puertos son concentradores que cuentan con diversos segmentos, cada uno de los cuales es capaz de proporcionar cierto ancho de banda disponible y de compartir el mismo entre todos los puertos existentes en dicho segmento, todo esto se realiza de acuerdo al tipo de red en el que se esté trabajando.

Los conmutadores de puertos se diferencian de los conmutadores tradicionales en que sus puertos pueden ser dinámicamente asociados, es decir, pueden ser usados por el sistema operativo cuando una aplicación tiene que conectarse a un servidor y por lo tanto necesita un puerto por donde salir.

Cada segmento se asocia a un “backplane”, el cual a su vez representa un grupo de trabajo. De esta manera las estaciones conectadas a los diversos puertos del conmutador pueden ser asignadas y reasignadas a diferentes grupos de trabajo o a diferentes VLANs.

Los conmutadores de puertos se definen también como "software patch panels" y una de sus ventajas fundamentales es que proporcionan una gran facilidad para la reconfiguración de los diferentes grupos de trabajo, sin embargo, como toda tecnología los conmutadores de puertos tienen también sus limitaciones, debido a que son dispositivos diseñados para compartir un mismo backplane físico; las reconfiguraciones que se quieran realizar en los grupos de trabajo están limitadas al entorno de un único concentrador, y por lo tanto todos los miembros del grupo en cuestión deben de encontrarse dentro de la misma ubicación física.

Las VLANs que cuentan con la tecnología de conmutación de puertos carecen de conectividad con el resto de la red, ya que al segmentar sus propios backplanes, no permiten proporcionar una conectividad íntegra entre los dispositivos que las conforman. Dicho problema implica no solo un aumento en los costos, sino también la necesidad de reconfigurar el bridge, switch o router, una vez que se presentan cambios en la red.

Por otro lado, un conmutador de puertos no resuelve el problema de saturación de ancho de banda, puesto que todos los nodos deben de conectarse al mismo segmento o backplane, lo que implica que compartan un ancho de banda en común, independientemente del número de nodos que existan.

b) Conmutación de segmentos con funciones de bridging

Una función bridging es aquella que permite unir dos redes físicamente separadas, es decir, que se tenga o aparente tener un único conjunto de equipos "físicamente agrupados".

Por ejemplo: Suponiendo que una red Ethernet cableada se quiere hacer crecer sin la necesidad de utilizar más cables, una opción para resolver dicho problema es la utilización de equipos wireless, como un Access Point en modo bridging para que los equipos que se conecten a él parezcan unidos a la red física Ethernet, y usen direcciones IP de la misma subred a la que se encuentran conectadas las demás máquinas que ya se tienen funcionando.

A diferencia de los conmutadores de puertos, los conmutadores de segmentos con funciones bridging suministran el ancho de banda de diversos segmentos de red manteniendo así la conectividad entre ellos.

Para poder lograr lo anterior se emplean los algoritmos tradicionales de los puentes (Bridges), o subconjuntos de los mismos. De esta forma es posible proveer conectividad a los múltiples segmentos con la velocidad máxima permitida de acuerdo a la topología de red y protocolos que esté empleando la VLAN en cuestión.

Mediante esta tecnología las VLANs no son únicamente grupos de trabajo que se encuentran conectados a un solo segmento o backplane, sino que son grupos lógicos de nodos que pueden ser conectados a cualquier cantidad de segmentos de red físicos, por lo tanto, dichas VLANs son consideradas como dominios de broadcast lógicos, es decir, conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que la conmutación por puertos, esta tecnología permite configurar y modificar las veces que sean necesarias la estructura de una VLAN mediante comandos de software, con la ventaja de que el ancho de banda disponible es repartido entre diversos segmentos físicos; lo cual es de gran ayuda, ya que para evitar la saturación de un grupo de trabajo conforme éste va creciendo, los usuarios del mismo pueden situarse en los diferentes segmentos, manteniendo el concepto de grupo de trabajo independiente al resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Sin embargo, la conmutación de segmentos con bridging, comparte el mismo problema que la conmutación de puertos en cuanto a su comunicación fuera del grupo de trabajo, al estar aislados del resto de la red, es necesaria la utilización de routers, lo cual a su vez implica mayores costos y reconfiguraciones en la red.

c) Conmutación de segmentos con funciones bridging/routing

En este punto se hace referencia al concepto "routing", así como la tecnología de conmutación de segmentos con funciones bridging/routing.

El funcionamiento de una red consiste en conectar las estaciones de trabajo y periféricos utilizando diferentes tipos de equipos, uno de ellos es el router, que permite a los dispositivos que están conectados a la red comunicarse unos con otros, así como con otras redes. Por ejemplo: un router se utiliza para conectar las máquinas de una red a Internet con el objetivo de compartir la conexión entre muchos usuarios. El router actuará como distribuidor, seleccionando la mejor ruta de desplazamiento de la información para que ésta llegue a su destino rápidamente.

Los routers analizan los datos que se van a enviar a través de la red, los empaquetan de forma diferente y los envían ya sea a la misma red o a una distinta, decidiendo qué equipos tienen prioridad sobre otros.

Dependiendo de los planes de conexión en red que tenga el Instituto los routers pueden incluir diferentes capacidades y funciones como:

- Cortafuegos: Software especializado que examina los datos entrantes y protege la red de posibles ataques.
- Red Privada Virtual (VPN): Método que permite a los empleados acceder remotamente a la red de forma segura.
- Red telefónica IP: Combina la red telefónica y la red de equipos del instituto utilizando la tecnología de voz y conferencia para simplificar y unificar las comunicaciones, etc.

El uso del routing permite a los miembros de una red, incluso a aquéllos que se encuentren en diferentes ubicaciones, obtener el mismo tipo de acceso a todas las aplicaciones empresariales, información y herramientas. Mantener a todos los integrantes de la red conectados a las mismas herramientas puede aumentar la productividad de los usuarios, además de que es posible proporcionar asistencia de aplicaciones avanzadas y activar servicios como voz

IP, videoconferencias y redes inalámbricas, aumentar la velocidad de acceso a la información, reduciendo costos y mejorando la seguridad en la red.

La conmutación de segmentos con bridging/routing es la tecnología ideal a aplicar en una VLAN. Los conmutadores que cuentan con dicha tecnología comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además con funciones añadidas de routing, lo que proporciona una fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expandan a través de diferentes segmentos de la red, y por otro lado, las funciones de routing facilitan también la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante el uso de las redes virtuales se pueden crear nuevos grupos de trabajo con tan solo una reconfiguración del software del conmutador, hecho que evita realizar cableado extra en la red o el cambio en direcciones de subredes; permitiendo así asignar el ancho de banda requerido por el o los nuevos grupos de trabajo sin afectar al resto de las aplicaciones de red existentes.

En las VLANs con funciones de routing, la comunicación con el resto de la red se puede llevar a cabo de dos formas:

- Permitiendo que algunos segmentos sean miembros de varios grupos de trabajo ó
- Mediante las funciones de routing multiprotocolo que facilitan el tráfico incluso entre varias VLANs.

Prestaciones de las VLANs

Los dispositivos con funciones VLAN ofrecen prestaciones de "valor añadido" suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLANs.

Al igual que en el caso de los grupos de trabajo físicos, las VLANs permiten a un grupo de trabajo lógico compartir un dominio de broadcast, lo que significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física, por lo cual las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales.

Al mismo tiempo, estos dominios de broadcast no son recibidos por estaciones situadas en otras VLANs.

Las VLANs no se limitan a un solo conmutador, sino que pueden extenderse a través de varios de estos dispositivos, estén o no físicamente en el mismo sitio. Además las VLANs pueden compartir determinados recursos como backbones de altas prestaciones o conexiones a servidores.

Uno de los mayores problemas a los que se enfrentan los responsables de las redes actuales es la administración de las mismas. Las VLANs tiene la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos sin tener que preocuparse por posibles colisiones.

Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred, por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico es capaz de soportar diversas subredes. Así mismo es importante tomar en cuenta que los modelos más avanzados de conmutadores con funciones VLAN soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, lo que permite definir con precisión las características del tráfico y seguridad que se desean en cada dominio, segmento, red o conjunto de redes.

Todo lo anterior se realiza en función de algoritmos de bridging y routing multiprotocolo.

2.3 Herramientas empleadas para la manipulación de VLANs

El manejo de VLANs requiere el uso de ciertas herramientas que permiten realizar fácilmente su administración y configuración.

Hoy en día, como ya se ha mencionado, las redes están conmutadas y segmentadas, aún más con la aparición de las VLANs.

Los conmutadores son rápidos, en muchas ocasiones, más rápidos de lo que se espera, además son fiables y permiten que cada dispositivo capture toda la capacidad de la red, aún si esto no es necesario.

Sin embargo, existe un inconveniente ante toda esta potencia y flexibilidad; puede resultar fácil resolver problemas en las redes conmutadas, por ejemplo, si una estación terminal o dispositivo de red en particular no está funcionando correctamente, es relativamente sencillo determinar y resolver ese inconveniente. El problema real ocurre cuando comienzan a surgir quejas por parte de los diversos usuarios en cuanto a una lentitud en la red. En este caso es importante definir si la red realmente está actuando de manera lenta, y si es así, analizar qué podría estarlo causando, de qué manera se podrían determinar y comprobar dichas causas y qué alternativas serían las más adecuadas a implementarse para de esta manera resolver dicha problemática.

Es muy difícil tener una buena idea del tráfico real que fluye a lo largo de una red conmutada, y más aún si existen numerosas conexiones que se encuentran trabajando en tiempo real.

Una posible solución es ver el interior de los conmutadores y de las VLANs. Idealmente el enfoque para resolver el problema en cuestión, debería de ser proactivo, esto quiere decir, que el administrador de la red debe tener una expectativa más amplia e integra de los procesos y actividades que pueden aplicarse para solucionar los inconvenientes que se presenten, y de esta forma ser capaz de llevar a cabo la planeación y la toma de decisiones con objeto de aumentar la efectividad, y de encontrar la verdadera causa de los problemas e incrementar la capacidad para el desarrollo que se espera que la red tenga.

De esta manera, los esfuerzos proactivos para evitar que los usuarios sean afectados por los problemas que una red enfrenta, incluyen verificar regularmente cada conmutador, y supervisar la calidad del tráfico, tal como se supervisaría cualquier otro segmento de manera regular.

La aplicación de técnicas tales cómo la supervisión y generación de tendencias de estadísticas de puertos de conmutación y la utilización de herramientas que permiten ver el interior de los conmutadores, hacen posible aplicar soluciones a los inconvenientes generados en la red y a un modo de prevención de los mismos.

A continuación se hace mención de diversas herramientas, tanto de hardware como de software que ayudan en la administración y manejo de las VLANs.

a) EtherScope™ Series II Network Assistant

EtherScope es un asistente rápido para la instalación y la solución de problemas de LAN y WiFi. En la **Figura II.7**, se muestra cómo es fisicamente esta herramienta. Entre las características más sencillas que puede desempeñar se encuentran las siguientes:

- Soluciones de problemas de LAN Gigabit e inalámbrica.
- Análisis de LAN para par trenzado 10/100/Gigabit y fibra óptica 100/Gigabit.
- Supervisar el tráfico de red y las interfaces de conmutación.
- Detección de dispositivos y configuraciones de infraestructura cableada e inalámbrica.
- Validación de disponibilidad y capacidad de respuesta de servicios LAN

Figura II.7 EtherScope™ Series II Network Assistant

Por otro lado EtherScope permite comprobar y solucionar problemas durante la instalación o durante la actualización, validar el funcionamiento de una LAN o una VLAN verificando los servicios de red y midiendo el rendimiento Ethernet después de la instalación.

El analizador EtherScope proporciona una visión instantánea de la red, con una completa pantalla principal de resultados de las pruebas e indicadores LED de tres colores. Se ejecutan varias pruebas a la vez para acelerar la detección de problemas. Si se selecciona una prueba concreta, se muestra información general en el panel de vista que aparece del lado izquierdo, como se aprecia en la **Figura II.8**.

Para obtener información detallada sobre alguna prueba en específico se selecciona la opción “Details” (Detalles).

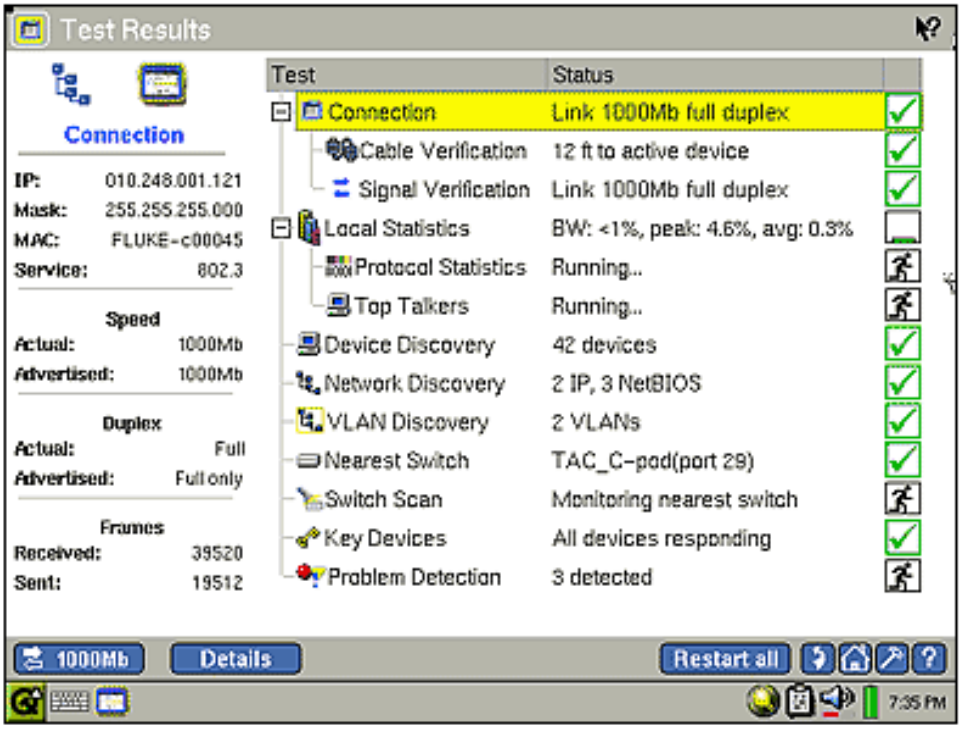

Figura II.8 Prueba automatizada en EtherScope

Los aspectos más importantes de la detección de problemas de redes automatizada del analizador EtherScope se muestran en la pantalla principal: identificando el switch más cercano, ranura y puerto a los que está conectado.

Determinar el punto de conexión a la red suele ser un problema importante cuando se trata de diagnosticar los problemas de los usuarios.

Una vez identificado el switch más cercano, como se aprecia en el ejemplo de la **Figura II.9** EtherScope permite lanzar un navegador Web o una sesión de Telnet para examinar su información y las estadísticas del puerto.

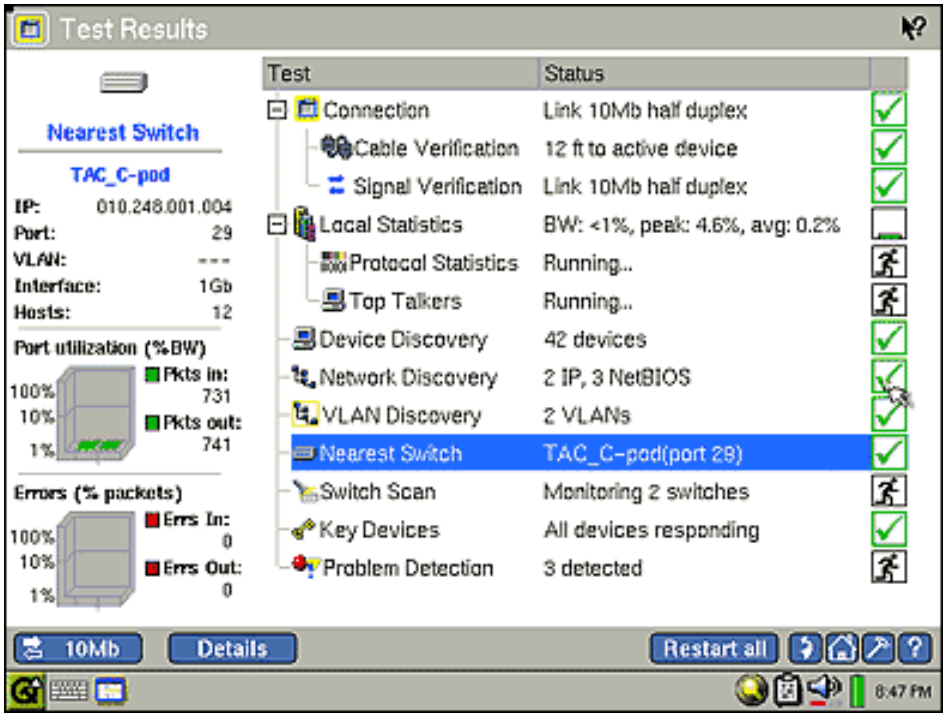

Figura II.9 Detección del switch más cercano

Puede llevarse a cabo un diagnóstico del puerto de un switch observando las redes VLANs que se encuentran disponibles, como en la **Figura II.10**; para así identificar problemas generales.

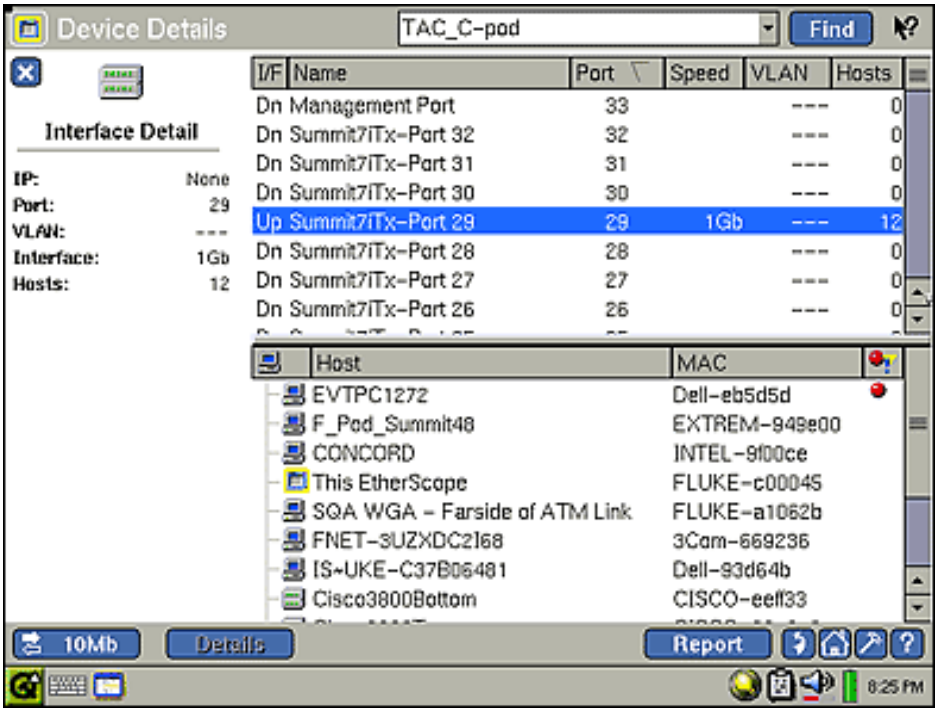

Figura II.10 Diagnóstico del puerto de un switch

Este dispositivo permite también detectar redes LAN y VLAN. En la **Figura II.11** se observa la detección de redes LAN.

EtherScope organiza los dispositivos descubiertos por subred IP y dominios NetBios, la información de subred incluye rangos de direcciones y máscaras, mientras que la información de dominio identifica los navegadores maestros y los controladores de dominio; buscando rápidamente en todas las redes los dispositivos que utilizan nombres totales o parciales y direcciones IP o MAC.

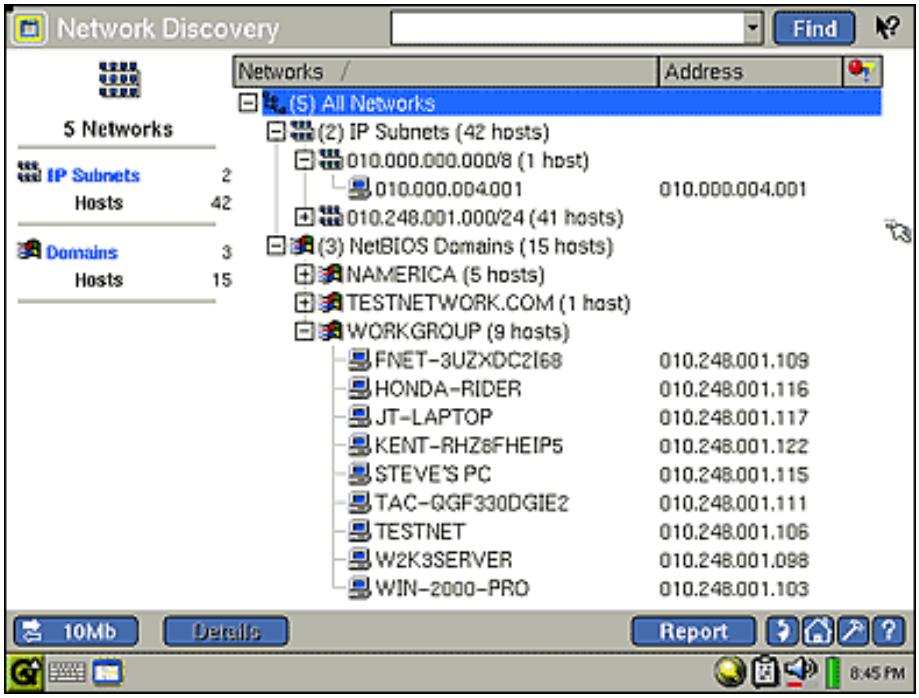

Figura II.11 Detección de redes LAN

La identificación de VLANs configuradas en las interfaces del o los switches, como se presenta en la **Figura II.12**, permite explorar hasta ver el estado de la interfaz, la información del host conectado y los datos de tendencia.

Para obtener una imagen o perspectiva completa de una VLAN en EtherScope basta con añadir los switches como dispositivos definidos por el usuario, facilitando la solución de problemas y el seguimiento de los cambios en la configuración.

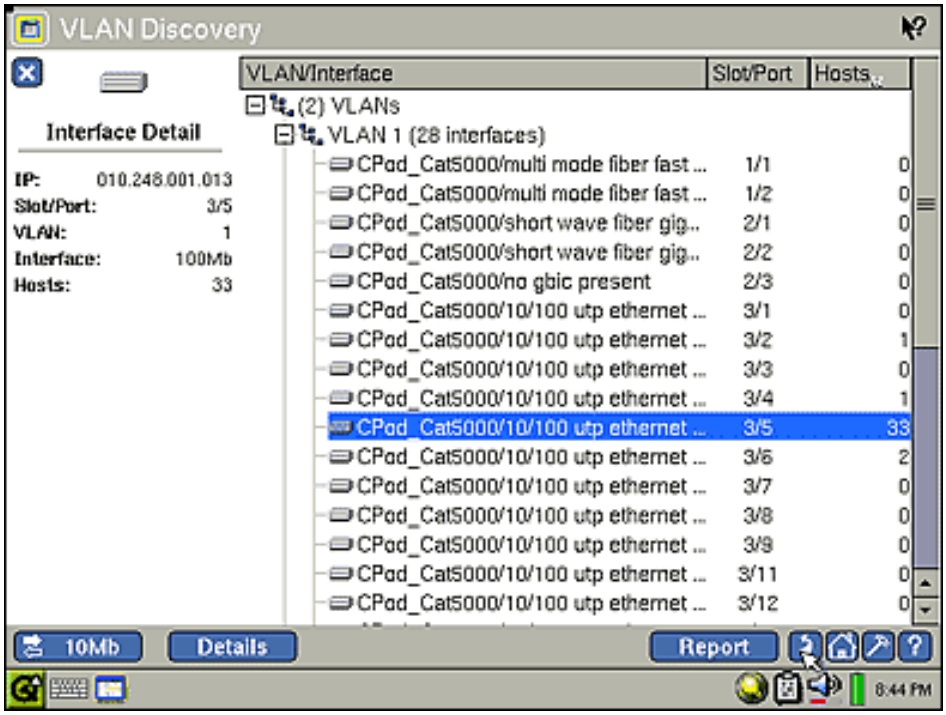

Figura II.12 Identificación de una VLAN

EtherScope es capaz de realizar muchas más funciones que ayudan a llevar a cabo un mejor manejo de la red, entre ellas se encuentran:

- Detección de dispositivos de redes.
- Comprobación del estado de una red.
- Analizar el tráfico de una red.
- Comprobar el cableado.
- Medición del rendimiento de una red.
- Probar redes de forma remota.
- Detección de redes inalámbricas.
- Identificación de Access Point.
- Detección de dispositivos no autorizados.
- Documentación de redes.
- Validación de servicios, etc.

b) Herramienta de Windows HyperTerminal

HyperTerminal es un software que se puede utilizar para llevar a cabo la conexión con otros equipos, sitios Telnet, sistemas de boletines electrónicos,

servicios en línea y equipos host, mediante un módem, un cable de módem nulo o Ethernet.

Aunque utilizar HyperTerminal con un servicio de boletín electrónico para tener acceso a información de equipos remotos es una práctica que está dejando de ser habitual gracias al World Wide Web, HyperTerminal sigue siendo un medio útil para configurar y probar switches y routers, o para examinar la conexión con otros sitios.

HyperTerminal graba los mensajes enviados o recibidos por servicios o equipos situados al otro extremo de la conexión. Por esta razón, es una herramienta útil para resolver problemas de configuración y pruebas.

Esta herramienta viene generalmente integrada en los sistemas Windows, como puede observarse en la **Figura II.13**.

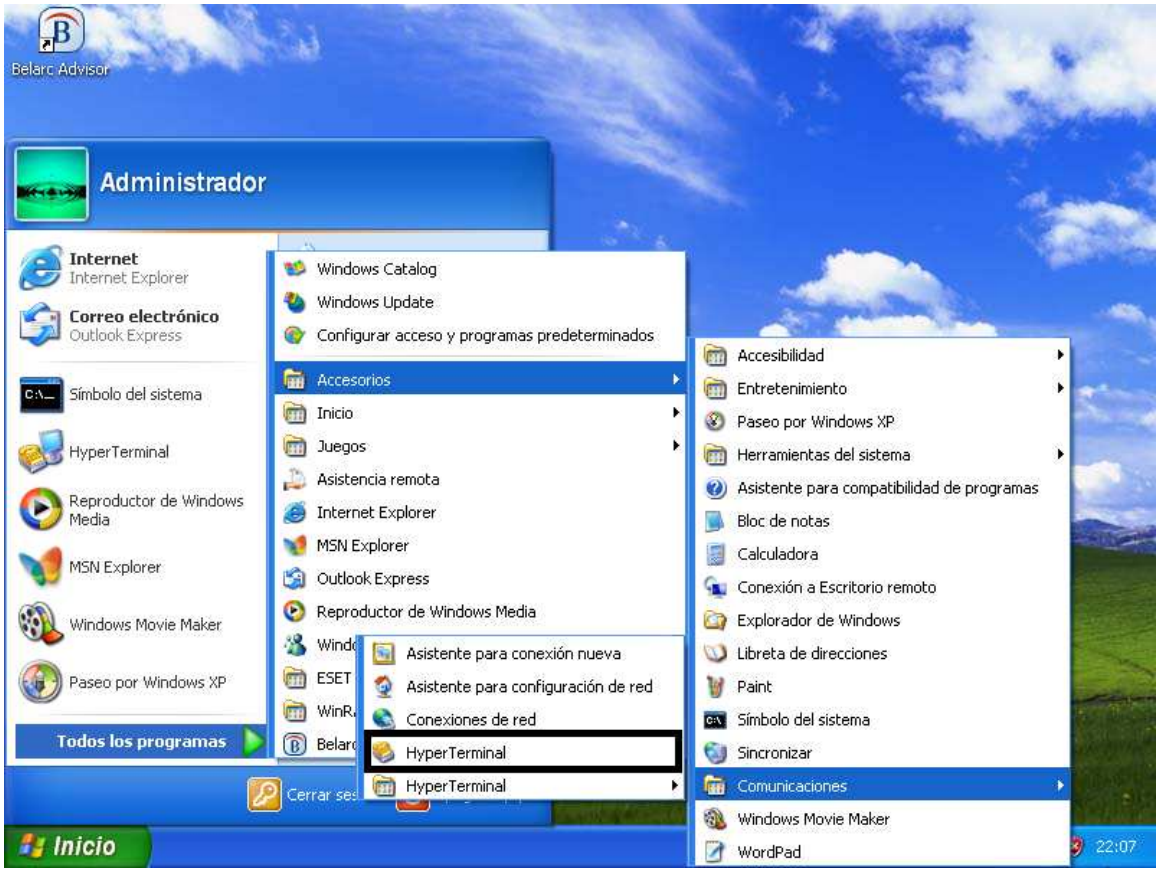

Figura II.13 Herramienta de Windows HyperTerminal

En caso de que el sistema no cuente con dicha herramienta, ésta también puede ser descargada libremente. HyperTerminal resulta ser muy útil en la administración y configuración de las VLANs, ya que permite llevar a cabo la configuración de los switches por los cuales pasan dichas redes, así como la configuración de sus puertos.

Con HyperTerminal es posible asignar un nombre exclusivo a un switch, así como contraseñas correspondientes. Para poder configurar la dirección IP a un switch es necesario hacerlo sobre una interfaz de VLAN, por defecto la VLAN 1 es la red virtual nativa del switch, al asignar un direccionamiento a la interfaz VLAN 1 se podrá administrar el dispositivo vía Telnet.

Si se lleva a cabo otra configuración de interfaz de VLAN automáticamente queda anulada la anterior configuración puesto que únicamente se admite una sola interfaz de VLAN.

Si el switch necesita enviar información a una red diferente a la de administración, HyperTerminal permite configurar el Gateway correspondiente. A pesar de que en esta herramienta existe la configuración de la NVRAM, las VLANs no se eliminan debido a que se guardan en un archivo de la memoria flash llamado VLAN.dat. Todo lo mencionado anteriormente es realizado mediante comandos, que se van introduciendo en la ventana de HyperTerminal como la que se observa en la **Figura II.14**.

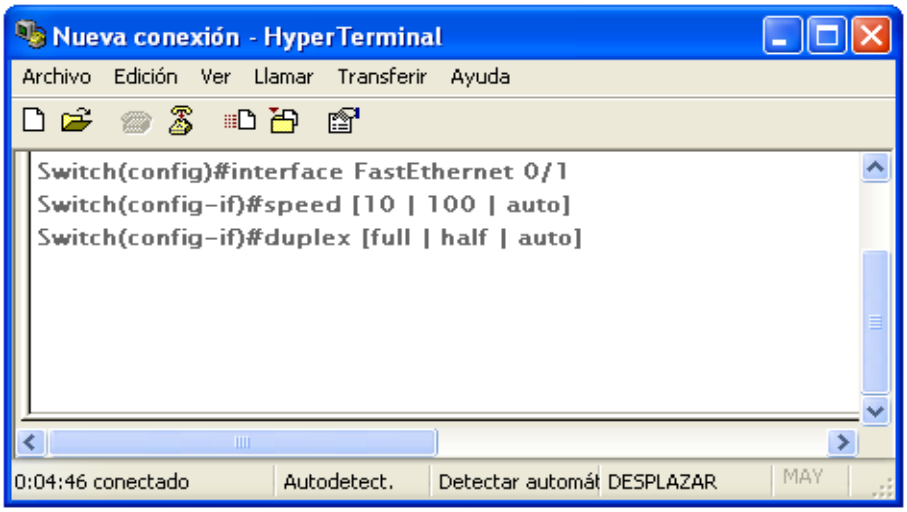

Figura II.14 Conexión HyperTerminal

c) Vía Web

Otra manera interesante de llevar a cabo el manejo de VLANs es hacerlo vía Web. Este proceso consta de la conexión física del switch a una estación de trabajo, siempre y cuando ésta cuente con el servicio de red para así poder realizar todo el desarrollo referente a la configuración de las redes virtuales a través de este medio.

Para realizar dicha configuración dentro de un switch, se necesita acceder a él vía consola, es decir, conectarse al dispositivo mediante una sesión que puede abrirse ya sea mediante HyperTerminal, o simplemente escribiendo en la barra de búsqueda de Internet, la dirección IP que identifique al switch por configurar. Una vez que se ha logrado entrar al switch, aparece la interfaz que permite observar sus características, como VLANs, asignación de puertos, dirección MAC, etc.

Generalmente en el Instituto se utilizan switches 3Com y Cisco. El ejemplo mostrado en la **Figura II.15** presenta la interfaz de un switch 3Com, donde pueden observarse las diversas VLANs que se encuentran configuradas en él.

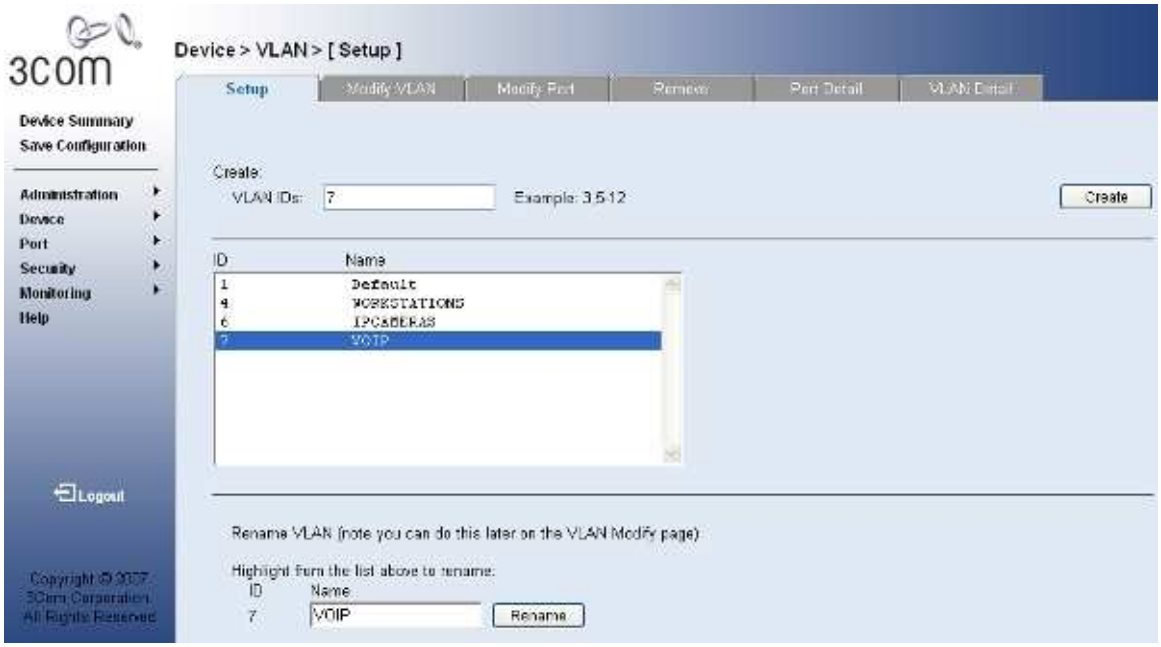

Figura II.15 VLANs configuradas en un switch 3Com

La administración vía Web permite también configurar los puertos del switch que van a pertenecer a cada VLAN, los cuales pueden configurarse de dos maneras: *tagged* y *untagged.*

El significado de esta configuración, se explica en el Capítulo 4, en el cual se ve a detalle en qué consiste la administración y la configuración de VLANs vía Web, así como diversas acciones que dicho método permite realizar.

Por lo pronto en la **Figura II.16** se muestra la interfaz del switch correspondiente a la figura anterior, sólo que en este caso pueden observarse los puertos pertenecientes a una VLAN definida dentro de dicho switch, su color de acuerdo a la configuración y el número que identifica a cada uno de ellos.

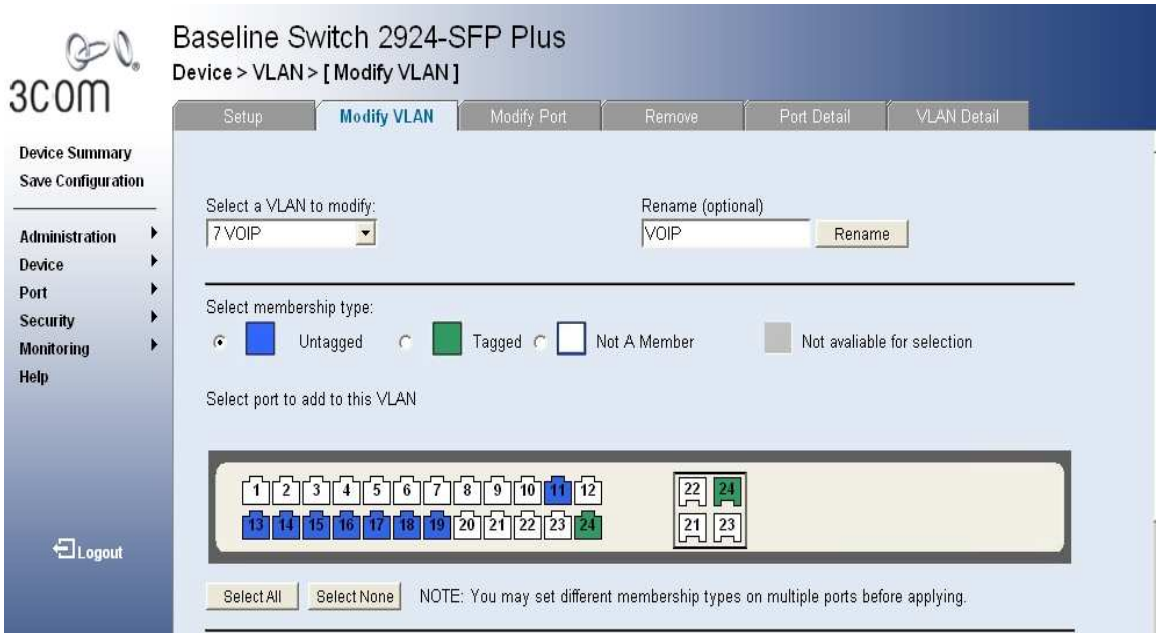

Figura II.16 Puertos asignados a una VLAN en un switch

d) Packet Tracer

Es una herramienta de aprendizaje y simulación de red que permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples presentaciones visuales. Sus principales funcionalidades son:

- Soporte para Windows (2000, XP, Vista) y Linux (Ubuntu y Fedora).
- Permite configuraciones multiusuario y colaborativas en tiempo real.
- Soporte para IPv6 y redistribución de rutas.
- Soporta diversos protocolos, entre ellos: HTTP, TELNET, SSH, DHCP y DNS.

Generalmente en el Instituto, esta herramienta se utiliza para realizar algunos ejercicios de simulación sobre pequeños cambios en la red, para posteriormente llevarlos a cabo con la seguridad de que no se presentarán inconvenientes.

Este software pertenece a Cisco y actualmente está teniendo un real impacto en su apoyo a las academias con recursos de redes limitados y también como apoyo a las tareas habituales de los estudiantes e instructores.

Packet Tracer utiliza la animación para mostrar a los usuarios qué ocurre en una red. Así se puede seguir la ruta de un paquete de datos a través de la red como si tuviera diferentes dispositivos, tanto paso a paso o como si fuera una película continua.

Por ejemplo, en la **Figura II.17** puede apreciarse la interfaz de Packet Tracer, donde es posible elegir entre diversos switches, routers, PCs y otros dispositivos, así como realizar conexiones entre ellos.

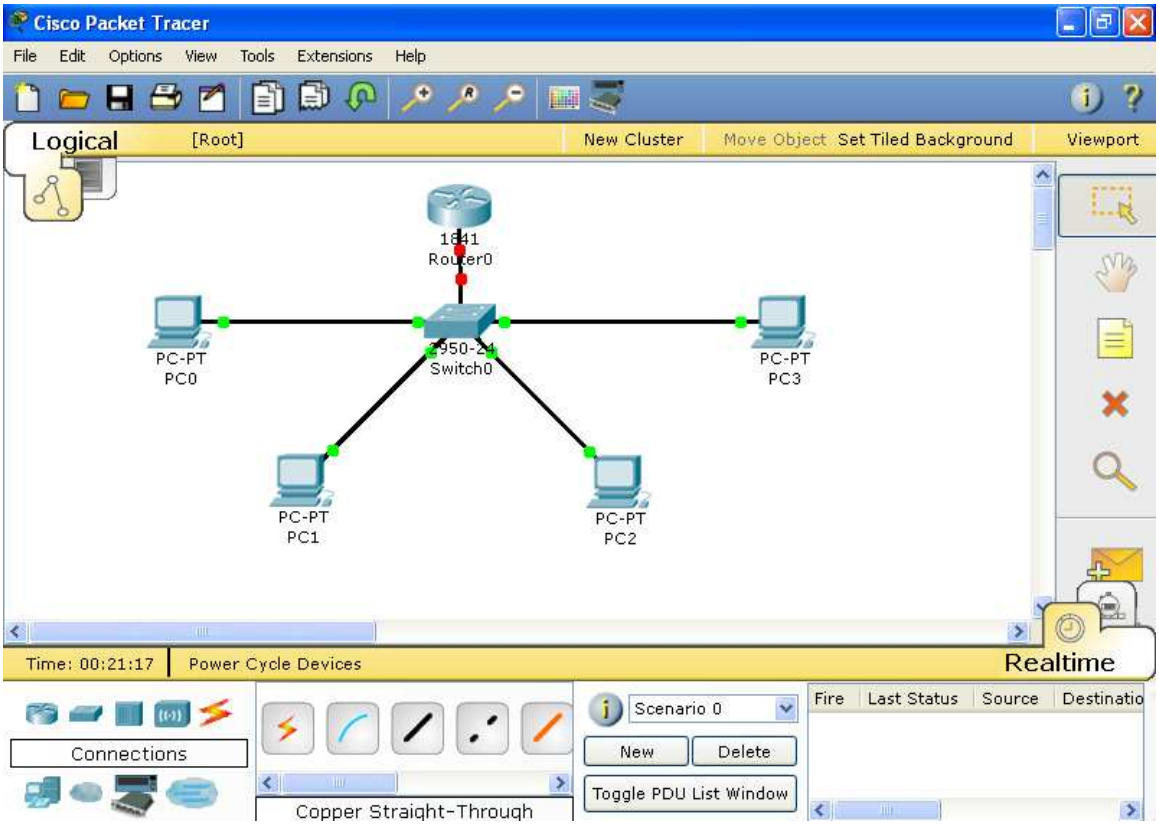

Figura II.17 Interfaz de Packet Tracer

Una gran ventaja que proporciona Packet Tracer, es la alternativa de poder configurar las características de cada uno de los dispositivos que se pretenden utilizar, por ejemplo, en una computadora puede llevarse a cabo la configuración de IP, un buscador de Internet, tecnología dial-up, es decir, acceso a servicio de Internet a través de una línea telefónica analógica y un módem, y algunas otras opciones que hacen posible la simulación de diversos proyectos.

El menú que esta herramienta proporciona para el caso de una PC se muestra en la **Figura II.18**. Sin embargo, cada dispositivo es diferente y por lo tanto las opciones a configurar en cada uno de ellos será distinta.

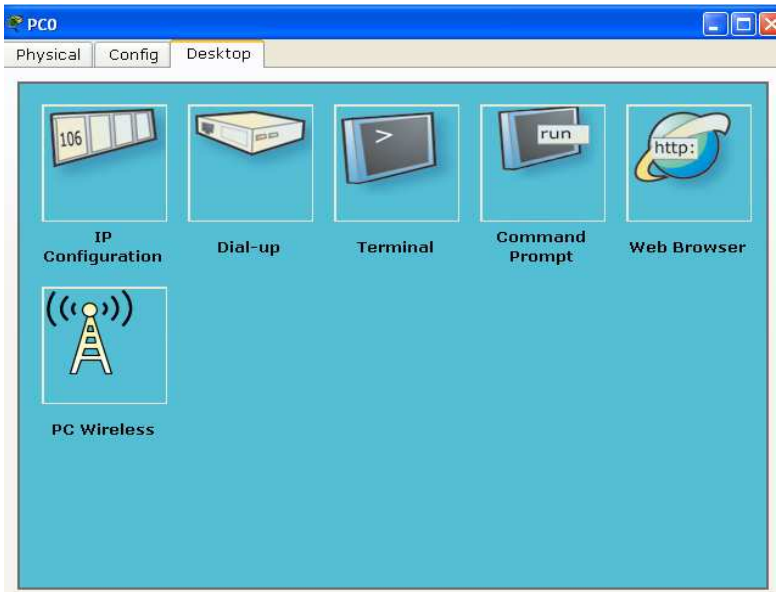

Figura II.18 Configuración de una PC en Packet Tracer

Dentro de la configuración de switches en Packet Tracer, es posible, la creación de VLANs, esto puede apreciarse en la **Figura II.19**, donde se presenta la configuración del switch que aparece en la **Figura II.17**.

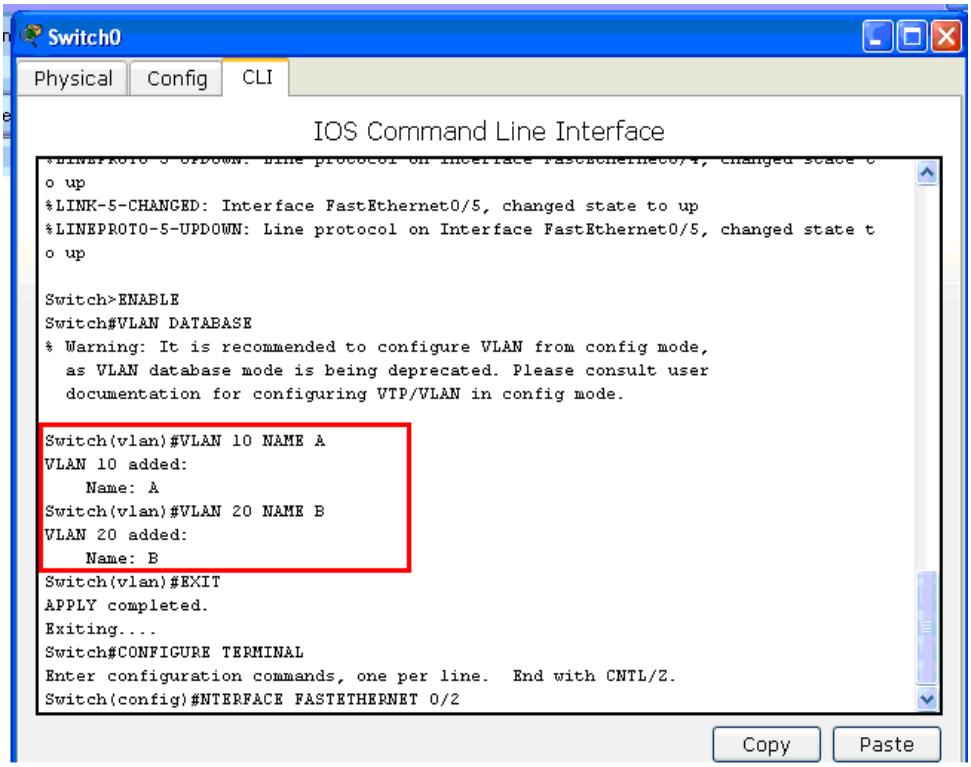

Figura II.19 Configuración de VLANs en Packet Tracer

Se puede observar en la **Figura II.20**, que dentro de la simulación de una VLAN es posible asignar los puertos de un switch, a una VLAN en específico.

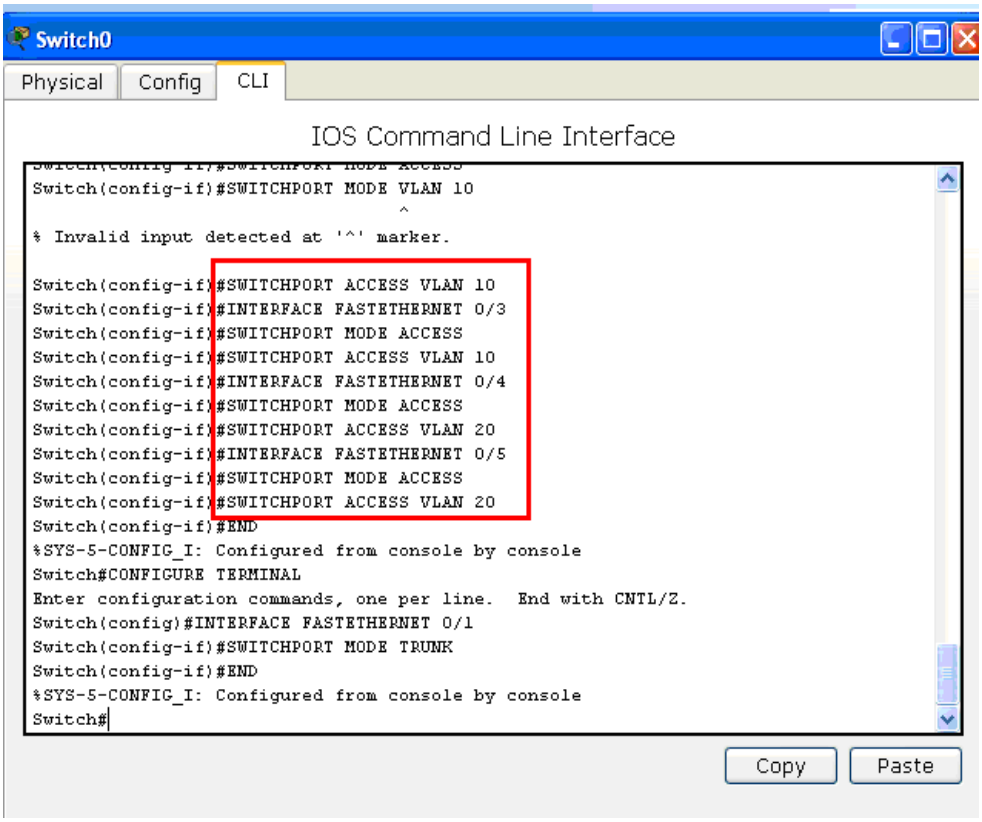

Figura II.20 Asignación de puertos a una VLAN en Packet Tracer

Al hacer la simulación de una VLAN se pueden realizar pruebas para el envío de paquetes entre los diferentes miembros, la simulación mostrará si la configuración de dicha VLAN resulta exitosa o fallida como se muestra en la **Figura II.21.**

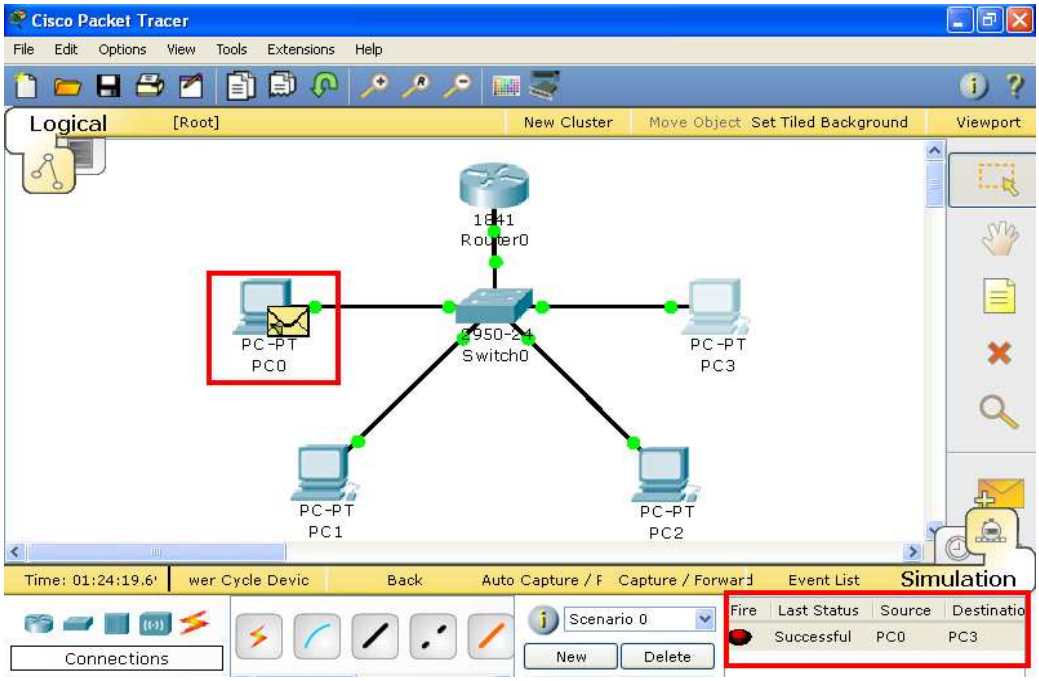

Figura II.21 Simulación del envío de paquetes a través de una VLAN

Hoy en día existen numerosas herramientas que ayudan a tener un mejor manejo de la red de una institución. En este capítulo se presentó la descripción de algunas de las cuales son utilizadas en el Instituto Hospitalario así como sus características generales.

2.4 Variables que determinan la implementación de una VLAN en el Instituto Hospitalario.

Generalmente la implementación de una VLAN requiere de equipo que pueda soportar dicha tecnología, sin embargo, como ya se ha indicado, una VLAN es una red lógica creada dentro de una red física, esto significa que los equipos y dispositivos que permitan realizar la creación de estas redes deben ser contemplados dentro de la implementación de la red LAN del Instituto, a partir de la cual se llevan a cabo el desarrollo, configuración y administración de las redes virtuales.

Por lo tanto, en este punto se habla un poco de las variables que se consideraron para la implementación de la LAN del Instituto Hospitalario y

que en general deben tomarse en cuenta para cualquier institución, puesto que hoy en día, las redes LAN son las más comunes y accesibles.

Para que una red de este tipo pudiera ser implementada en el Instituto fue necesario tomar en cuenta el número de usuarios que realmente necesitaban el acceso a la red, sin embargo, toda institución a lo largo del tiempo sufre diversos cambios, entre ellos se encuentra al crecimiento, y por lo tanto no solo se requieren cambios en la red, sino también en todos los servicios que el instituto es capaz de proveer. En el caso del crecimiento de la red, inicialmente un número limitado de personas dentro del Hospital contaban con dicho servicio, aproximadamente entre 200 y 300 usuarios.

El avance de la tecnología, el incremento de personal, así como el crecimiento y necesidad del Internet han generado que actualmente en el Instituto alrededor de 1400 usuarios cuenten con este recurso. Dicha cantidad puede ir en aumento, de acuerdo a las necesidades que se vayan generando dentro del Hospital.

La instalación de una red LAN puede considerar tantos elementos como necesite el Instituto. La cantidad de computadoras se encuentra determinada por el número de estaciones de trabajo disponibles, y lo mismo sucede con la cantidad y tipo de impresoras. Si el flujo de impresión es importante, quizá resulte más conveniente el uso de servidores de impresión, (Print Servers), que permiten conectar la impresora, directamente a la red sin necesidad de usar una estación de trabajo como intermediaria.

También es necesario disponer de concentradores de terminales, (switches, hubs, routers, conmutadores, servidores, etc.), que soporten la red, de tal manera que los equipos conectados a ellos puedan compartir recursos entre sí. El costo de instalar una red LAN depende de las siguientes variables:

- Cantidad de estaciones de trabajo que se necesitan (computadoras disponibles)
- Distancia entre las estaciones de trabajo, (Cable UTP, fibra óptica y conectores RJ-45).

- Routers (Necesarios para compartir Internet a las estaciones de trabajo).
- Switches (Necesarios para conectar en red los equipos).
- Accesorios de instalación, (Canaleta, módulos, terminaciones, racks, paneles de parcheo, etc.).
- Servicio de Internet de banda ancha, (Contrato con empresas locales), etc.

Los precios de estos requerimientos varían de una marca a otra, y es el jefe del departamento quien decide cuales son los más convenientes dejándose guiar no solamente por el precio, sino por la calidad y efectividad que puede proporcionar cada uno de los elementos por adquirirse.

Por otro lado los aspectos tecnológicos que determinan la naturaleza de una red LAN son:

- Topología
- Medio de transmisión
- Técnicas de control de acceso al medio

La implementación en cuanto a cableado, enlaces, e instalación de la red LAN es llevada a cabo por empresas y proveedores independientes a las personas que se encargan de administrar la red.

Sin embargo, los administradores son quienes deciden qué tipo de equipo es necesario para realizar cambios dentro de la red, dónde deben de estar ubicados los enlaces, por dónde es más conveniente realizar el cableado, qué tipo de dispositivos son los que se requieren etc. Por lo tanto los proveedores solo se encargan de realizar dicha infraestructura.

Los administradores de la red, conocen qué tipo de dispositivos son capaces de soportar la tecnología para la implementación de VLANs, pues son ellos los que llevan a cabo la configuración de dichas redes.

Por ejemplo, para que una red VLAN pueda ser implementada, generalmente es necesario utilizar switches administrables, ya que éstos permiten soportar una cantidad alta de usuarios, y porque como su nombre lo dice, permiten una mejor administración, puesto que pueden mostrar qué es lo que está pasando en la red.

El implementar una VLAN en este tipo de switches ayuda a optimizar el tráfico, mejorando la seguridad y la flexibilidad para reaccionar ante el crecimiento de la red, y aumentar la confiabilidad y disponibilidad de la misma.

De la misma manera en que se requiere de cierto tipo de switches para poder hacer uso de las VLANs, es inidspensable que los administradores de la red hagan un análisis de los requerimientos tanto de hardware como de software que son necesarios para realizar una mejora en la red.

No se considera únicamente la cantidad de usuarios a los que se les tiene que brindar un servicio, también es importante considerar que exista el espacio suficiente para ubicar los equipos que se van adquiriendo, el presupuesto con el que se cuenta durante cada determinado tiempo, así como tener una apreciación de qué cambios y recursos son realmente indispensable para generar un manejo más adecuado de la red; y por supuesto contar con la visión de planeación a futuro.