UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

COMUNICACIÓN ENTRE VLANs DE UN INSTITUTO HOSPITALARIO

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA

VILLASECA RODRÍGUEZ IVONNE ALICIA

DIRECTORA DE TESIS

M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

AGRADECIMIENTOS

En primer lugar quiero darles las gracias a mis padres, por apoyarme a lo largo de toda mi vida y proporcionarme todas las herramientas necesarias para desarrollarme como ser humano y como profesionista. En especial a mi padre por no dejar sola a mi madre en su tarea de educarme y de guiarme en la vida, pues gracias a él puedo decir que soy en gran parte la persona que hoy soy.

A mi tía Verónica Sánchez, por ser para mí un ejemplo a seguir y por alentarme siempre a luchar por mis metas y objetivos.

A Fernando, por creer en mí y estar a mi lado siempre.

A toda mi familia y a mis amigos, por crecer junto a mí durante toda mi preparación y por compartir conmigo muy agradables momentos.

A la profesora Ma. Jaquelina López Barrientos, por guiarme durante todo este proceso.

A la Facultad de Ingeniería, por ayudarme a adquirir muchos de los conocimientos que hoy me permiten iniciar esta nueva etapa en mi vida.

Y por supuesto a la Universidad Nacional Autónoma de México, por permitirme formar parte de ella y de la historia que como la máxima casa de estudios del país va construyendo día a día.

ÍNDICE

INTRODUCCIÓN

Es evidente que el crecimiento y la evolución que ha tenido el Internet en la actualidad, y desde su aparición hace ya treinta años; es realmente sorprendente. No solo por el hecho de la gran cantidad de usuarios que emplean dicho recurso, sino por las numerosas actividades que pueden realizarse a través de la red, que van desde los servicios más sencillos, como son correos electrónicos, grupos de noticias, telefonía, etc.; hasta llegar a ser la fuente principal del crecimiento de la industria, comercio, turismo, y muchas otras actividades que implican la economía y el desarrollo de un país.

El uso del Internet, proporciona múltiples facilidades a grandes empresas e instituciones de todo tipo, en este caso, como ya se ha señalado en el índice, se abarcará lo referente a un Instituto Hospitalario. Un instituto como éste, entre muchos otros; requieren de conexiones a Internet para poder llevar a cabo las funciones y labores de trabajo correspondientes, sin embargo, cuando en una empresa surgen nuevas necesidades en cuanto a recursos y dispositivos de la red, el llevar a cabo la administración de dicho crecimiento resulta ser más complejo de lo habitual; ya que se requiere de un mayor análisis que permita un correcto desempeño y una máxima utilización de los recursos de la red en cuestión.

Para poder lograr lo anterior, se debe tomar en cuenta un factor muy importante, que es la forma en que la red de una institución se encuentra segmentada. Los segmentos que constituyan una red deben ser pequeños, ya que esto ayuda a tener una mayor velocidad en la transmisión de datos; lo que permite a su vez limitar las colisiones que se puedan presentar y por consecuencia tener un adecuado manejo en cuanto a flexibilidad, mantenimiento y seguridad de la misma.

No obstante, la segmentación de una red conlleva ciertos inconvenientes, y es aquí donde el uso de las Redes Virtuales, en este caso las VLANs, juega un papel muy importante.

Debido a las diversas actividades que se realizan en las instituciones y empresas, existen lo que son los grupos de trabajo, los cuales comparten recursos, y por lo tanto utilizan el mismo acceso a Internet. Estos grupos de trabajo generalmente son creados en un mismo segmento de red, al ocurrir esto, también se comparten el ancho de banda, los dominios de broadcast e incluso el área física o geográfica, entre otros recursos, de tal forma que los miembros de dichos grupos deben adaptarse a cierto tipo de conexiones dirigidas a un mismo concentrador o segmento de red. Los problemas aumentan cuando se producen cambios dentro de uno o varios grupos de trabajo, ya que las modificaciones que este tipo de situaciones generan, influyen en sí, en el funcionamiento y desempeño general de la red.

Es por eso que la mejor alternativa para solucionar la problemática planteada y que por supuesto ya se lleva a cabo en diversos lugares, es la implementación de VLANs. El uso de estas redes permite satisfacer la necesidad de ancho de banda y de dar soporte a un mayor número de usuarios en la red, sin necesidad de que estos se encuentren en la misma ubicación.

Las Redes Virtuales permiten que diferentes grupos de trabajo se comuniquen entre sí, sin la necesidad de que estos se encuentren conectados físicamente al mismo cable e inclusive al mismo segmento de red de un edificio. Por lo tanto, esta tecnología realiza sus funciones de manera lógica, en lugar de hacerlo físicamente, de tal manera que se puede llevar a cabo un control más inteligente y dinámico del tráfico.

En un Instituto Hospitalario, como sucede en otros lugares, existen diversas áreas de trabajo que hacen uso de la red, en este caso, por ejemplo, se pueden encontrar: personal administrativo, planeación, finanzas, sistemas y redes, torniquetes, plumas de estacionamientos; áreas de hospital como son: urgencias, consulta externa, terapia intensiva, rayos X, archivo clínico, servicio a residentes, fotocopiadoras, impresoras, torre de investigación, virología, etc.; solo por mencionar algunas, todos los usuarios, miembros de estas áreas requieren del acceso a los recursos y es evidente que no todos se encuentran dentro de la misma limitación geográfica. Es por ello que se

recurre al empleo de VLANs, ya que éstas proveen una mayor facilidad de movimientos y cambios en diferentes ubicaciones físicas, un considerable aprovechamiento del ancho de banda y una mejor segmentación de la red, así como la reducción de los dominios de broadcast, entre otras ventajas.

Es evidente que no todas las instituciones y empresas cuentan con las mismas dimensiones, y como consecuencia de ello, en algunas existen más departamentos que en otras. Al presentarse esta situación el llevar a cabo el uso de redes virtuales proporciona una gran ventaja, la cual consiste en asignar una VLAN a cada departamento de la empresa o instituto; de manera que pueda controlarse que dichos departamentos sean independientes o no entre sí, y a su vez se permita liberar direcciones IP de la red origen.

Dentro del área de redes, se llevan a cabo las configuraciones necesarias, en switches, puertos y otros elementos que determinan el funcionamiento de las VLANs.

Por todo lo ya mencionado es que el objetivo principal de este proyecto de tesis es llevar a cabo la administración y configuración de las VLANs de un Instituto Hospitalario, y para poder lograr dicho objetivo, es necesario alcanzar a su vez ciertos objetivos particulares, los cuales se citan en seguida:

- Adquirir las bases y fundamentos teóricos acerca de las Redes Virtuales en específico de las VLANs.
- Conocer sus antecedentes, qué son, cómo funcionan, cuántos tipos existen, y de acuerdo a esto saber cuál es la que más se adecua para su aplicación en el Instituto Hospitalario.
- Practicar y justificar de qué forma se generan estas redes, qué recursos se consumen en su implementación, ya sean de hardware, software, etc.
- Dar a conocer qué ventajas y desventajas proporciona el hecho de que un instituto hospitalario haga uso de las llamadas VLANs.

Para ello la presente tesis se estructura en cinco capítulos, de manera que en el capítulo 1, se establecen los fundamentos teóricos que permiten conocer más a fondo la manera en que funcionan las VLANs, las causas que originan su aparición, así como los diferentes modelos de redes virtuales que existen y sus propiedades principales. Por otra parte, se hace referencia a las características correspondientes al Instituto Hospitalario, y las razones por las que éste hace uso de la tecnología que permite la manipulación de VLANs.

En el capítulo 2 se hace mención de los diversos protocolos aplicados a las redes virtuales, así mismo se presentan los tipos de tecnología que pueden facilitar y que hacen posible el manejo las mismas, en conjunto con algunas herramientas que son utilizadas en la institución y que favorecen la administración y configuración de cada una de ellas.

La manera en que asignan las VLANs se trata en el capítulo 3, puesto que de ello depende la estructura que permita la creación de los grupos virtuales que pueden ser asignados a múltiples departamentos, correspondientes a las áreas de trabajo ubicadas en diferentes zonas del Hospital. En esta sección se habla también de la manera en que dichos grupos son asignados y las ventajas que éstos conllevan en cuanto a una mejor administración del tráfico que circula por la red; además, teniendo noción de cómo es que funciona la red con base a la división de grupos lógicos, se hace referencia a todas las VLANs implementadas en el Instituto, el funcionamiento con el que cumplen por separado, la manera en que éstas mantienen comunicación entre sí y los tipos de conexiones que permiten su comunicación.

Una vez que se ha logrado comprender el funcionamiento y las ventajas que otorgan las VLANs, se llega al punto medular del proyecto, pues es en el capítulo 4 en el cual se expone desde cómo crear redes virtuales, la forma en que se administran y se configuran, hasta llegar a aplicar estas actividades en algunos de los diferentes dispositivos informáticos con los que cuenta el Instituto Hospitalario y que se encuentran en pleno funcionamiento.

Casi para terminar el trabajo de tesis, se tiene el capítulo 5 donde se abarcan los problemas y soluciones que se consideran deben ser tomados en

cuenta específicamente en el Instituto, puesto que es en él en donde se llevaron a cabo todas las pruebas necesarias para cumplir con el objetivo principal de esta propuesta, no obstante, las recomendaciones van también dirigidas a cualquier red en general, puesto que los inconvenientes presentados suceden con frecuencia en todas las empresas e instituciones.

Finalmente se presentan las conclusiones a las cuales se llegaron al dar por terminado el desarrollo de este proyecto, dichas conclusiones hacen alusión no solamente al cumplimiento del objetivo del mismo, sino también a los beneficios adquiridos durante esta investigación y a las perspectivas a futuro que se tienen en lo que corresponde al tema de VLANs implementadas en esta organización.

I. Fundamentos Teóricos

1.1 Conceptos y antecedentes de las VLANs

Para poder entender qué es una VLAN, es importante tener presente el concepto de una red LAN (*Local Area Network – Red de Área Local*).

Una LAN es un conjunto de elementos físicos y lógicos, los cuales son capaces de proveer interconexión a una gran cantidad de dispositivos de comunicación de información en un área privada restringida; de manera más clara, una LAN es un conjunto de equipos que se encargan de configurar una red de comunicación para que ésta permita la transmisión de datos de un dispositivo a otro, ya sea dentro de una habitación, un edificio o un conjunto de edificios.

Las estaciones de trabajo y computadoras personales en oficinas, normalmente están conectadas en una red LAN, como la mostrada en la **Figura I.1,** lo cual permite que los usuarios puedan enviar y recibir información y compartan el acceso a la misma. Cada uno de los equipos que se encuentra conectado a una LAN recibe el nombre de nodo.

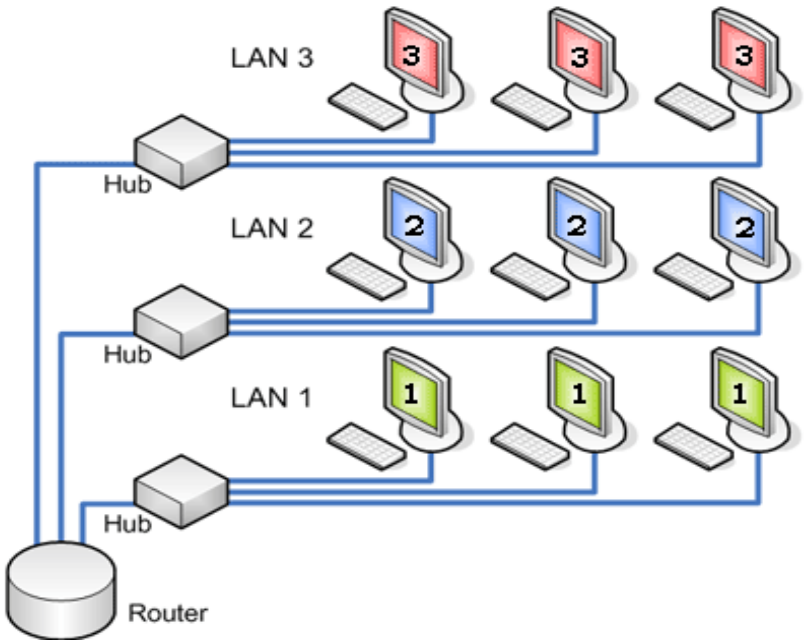


Figura I.1 LAN Tradicional

La velocidad de transferencia de datos en una LAN puede alcanzar hasta 10 Mbps, por ejemplo en una red Ethernet, y 1 GPS en una red FDDI o

GigabitEthernet. Aunque ésta también depende de la capacidad de los equipos y de los medios de transmisión utilizados.

Las redes LAN pueden operar de dos formas:

1. En una red *de igual a igual (P2P):* donde la comunicación se lleva a cabo de un equipo a otro sin la necesidad de contar con un dispositivo central, es decir, cada uno de ellos desempeña la misma función.
2. En un entorno *cliente/servidor:* en el cual existe un equipo central que se encarga de brindar servicios de red a los usuarios.

Tomando en cuenta lo anterior, puede ahora definirse y entenderse el concepto de VLANs.

Las VLANs *(Virtual Local Area Networks - Redes Virtuales de Área Local)* como su nombre lo indica, son LANs virtuales que representan agrupaciones de trabajo, las cuales se encuentran definidas por software y además mantienen comunicación entre sí, como si estuvieran conectadas a un mismo concentrador; aunque realmente estén localizadas en diferentes segmentos de red pertenecientes a algún edificio.

Las VLANs son redes conmutadas, esto quiere decir que son redes que consisten en un conjunto de dispositivos de red conectados entre sí (hubs, bridges, switches, estaciones de trabajo, etc.), a través de medios de transmisión (cables), que generalmente emplean una topología de red tipo malla, donde la información se transfiere partiendo desde el nodo origen, hasta el nodo destino mediante conmutación entre nodos intermedios.

Este tipo de transmisiones se da en tres etapas:

1. Establecimiento de la conexión.
2. Transferencia de la información.
3. Liberación de la conexión.

La **Figura I.2** muestra cómo los nodos pertenecientes a una VLAN pueden encontrarse en el mismo medio físico o bien pueden estar ubicados en distintos sectores de la red.

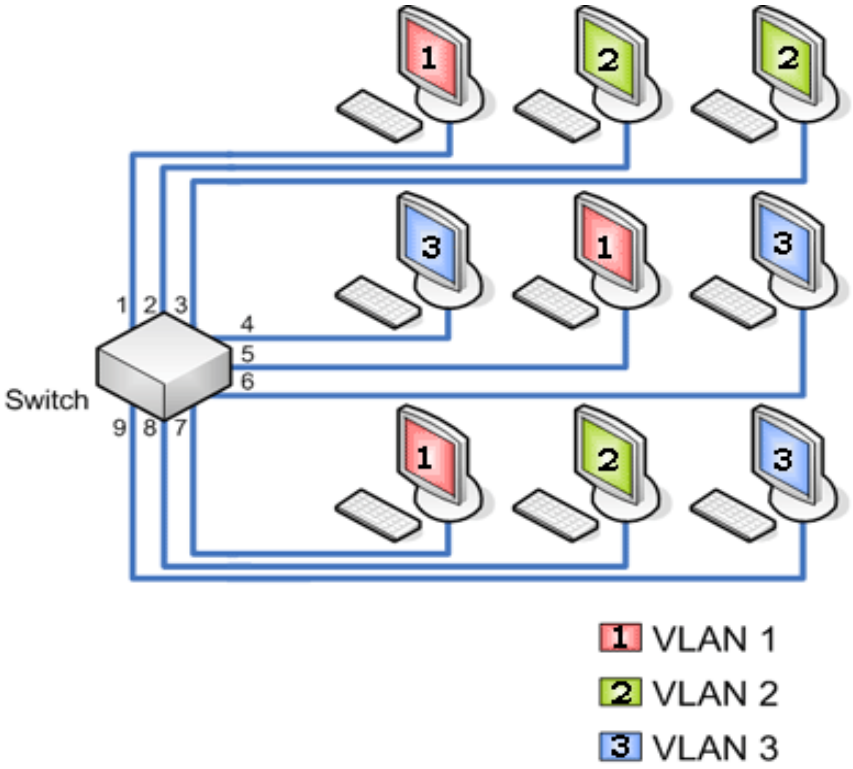


Figura I.2 VLAN

Una VLAN se segmenta lógicamente basándose en funciones, es decir, en trabajadores de un mismo departamento, sin importar su ubicación física. Cabe destacar que las VLANs siguen compartiendo las características de los grupos de trabajo físicos, en el sentido en que todos los usuarios mantienen conectividad entre ellos y comparten sus dominios de broadcast. Dichas características son las siguientes:

- El núcleo de una VLAN es un switch.
- Cada puerto del switch puede ser asignado a una VLAN. Los puertos que no pertenezcan a la misma no podrán compartir el tráfico broadcast, y por consecuencia, el desempeño de la red será mejor.
- La comunicación entre VLANs es provista a través de enrutamiento de capa 3.

- Cuando se lleva a cabo la agrupación de puertos y usuarios a través de diversos switches, una VLAN es capaz de cubrir un edificio completo, comunicar varios edificios o incluso redes WAN.

Teniendo claro el concepto de VLAN, se procederá entonces a hablar sobre su historia y características, así como la manera en que éste tipo de redes surge como consecuencia de las exigencias que tanto usuarios, como dispositivos de red han requerido a lo largo de la evolución de Internet.

Cada día las aplicaciones requieren de un mayor ancho de banda que permita la transferencia de grandes cantidades de información a través de la red.

La característica principal de una LAN, como ya se mencionó, es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo.

Los modelos de red basados en la compartición de ancho de banda, presentes en las arquitecturas LAN a inicio de los 90's carecían de la potencia suficiente para proporcionar dicho recurso, el cual era requerido en las aplicaciones multimedia.

En la actualidad se necesitan nuevos modelos capaces de proporcionar la potencia adecuada no solo para satisfacer la creciente necesidad de ancho de banda, sino también para soportar un mayor número de usuarios en la red.

Inicialmente se llevaba a cabo la utilización de hubs o concentradores los cuales son dispositivos que funcionan como repetidores, es decir, escuchan las tramas por todos los puertos y de la misma forma las repiten al resto de los equipos para asegurar que la información llegue en algún momento a su destino. Un hub es un dispositivo que simplemente une conexiones y no altera las tramas que llegan a él. En la **Figura I.3** se puede observar la conexión básica de un hub con otros equipos.

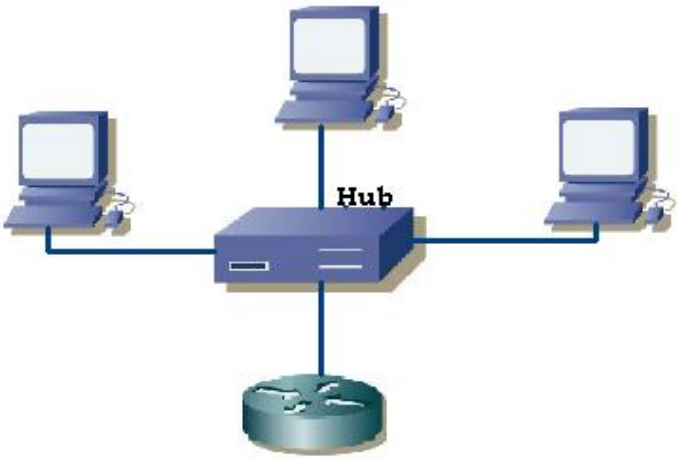


Figura I.3 Conexión de un hub

Un hub funciona a la velocidad del dispositivo más lento de la red, lo cual provoca que entre más estaciones de trabajo estén conectadas a él, menor sea el desempeño y aprovechamiento del mismo, ocasionando a su vez un aumento en el número de colisiones.

Para evitar lo anterior, se comienzan a utilizar los switches, que son dispositivos que mejoran el rendimiento de una red debido a que segmentan o dividen los dominios de colisiones, es decir, en una LAN cada uno de los puertos de un switch se encuentra asignado a cada uno de los equipos pertenecientes a la red, los cuales disponen de todo el ancho de banda que la misma proporciona, con el objetivo de evitar las colisiones que puedan existir en un medio compartido, en este caso el switch.

El switch es considerado un "hub inteligente" ya que cuando es inicializado, comienza a reconocer las direcciones MAC, que generalmente son enviadas a cada puerto, por consecuencia, cuando llega cierta información al switch, éste tiene un mayor conocimiento sobre que puerto de salida es el más apropiado y por lo tanto evita el hecho de tener que repetir la información a todos los equipos que se encuentren conectados a él, como se muestra en la **Figura I.4**.

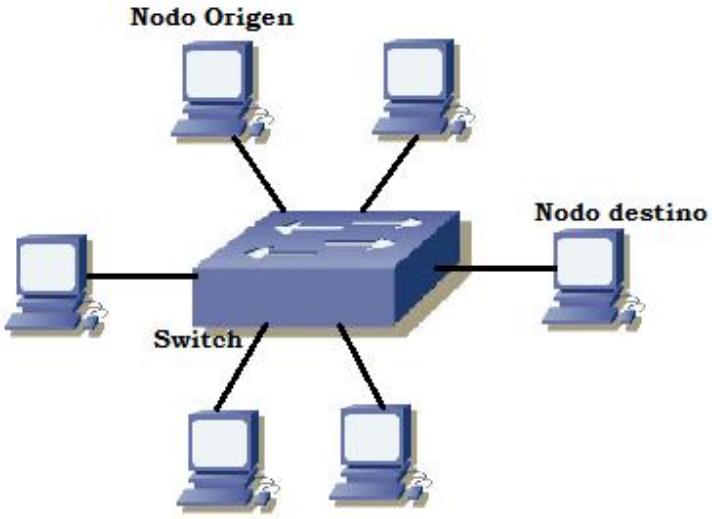


Figura I.4 Funcionamiento del switch

Sin embargo, algo que no pueden evitar ni el hub, ni el switch, es el envío de mensajes broadcast, los cuales son transmitidos a través de todos los puertos, independientemente del dispositivo. Por ejemplo, si una computadora quiere comunicarse con otra, y no sabe dónde se encuentra, entonces comienza a buscar dentro de la LAN, lo cual genera tráfico innecesario en la misma y además ocasiona que todos los equipos que pertenezcan a la red escuchen el mensaje, aunque solo el que se esté buscando sea el que pueda contestarlo, sin importar si éste se encuentra o no conectado al switch o concentrador; como sucede en la **Figura I.5**.

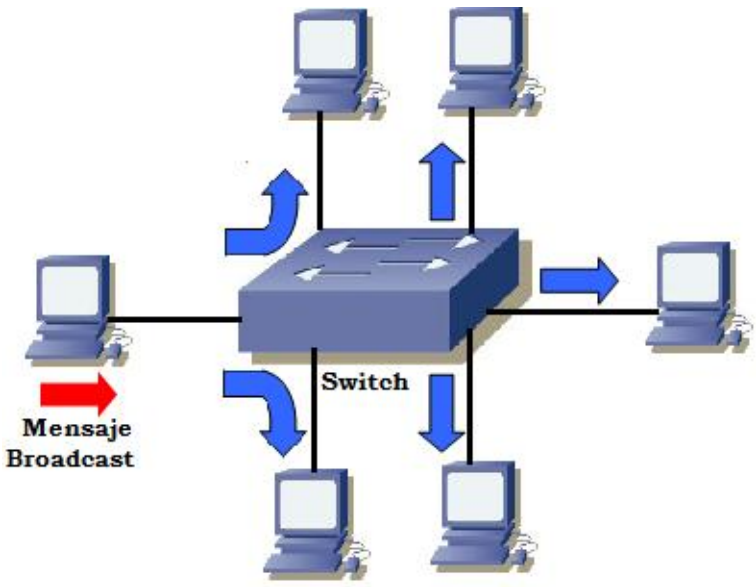


Figura I.5 Envío de mensajes broadcast

Para solventar dicha situación surgen las llamadas VLANs, las cuales se encuentran configuradas dentro de los switches y se encargan de dividir en diferentes dominios de broadcast al switch, con el objetivo de no afectar a todos los puertos del dispositivo, por el contrario, logran crear dominios más pequeños y aislar las consecuencias que pudieran tener los mensajes broadcast a solamente algunos puertos, afectando así una menor cantidad de equipos.

Las VLANs han surgido de un conjunto de propuestas que tenían como objetivo conmutar las Redes de Área Local, dichas propuestas fueron realizadas por los mayores distribuidores de equipamiento de redes LAN, este hecho comenzó entre los años 1994 y 1995.

La técnica idónea para poder lograr lo anterior es la conmutación, mediante la cual cada estación de trabajo y cada servidor poseen una conexión dedicada dentro de la red.

En una LAN conmutada, la función tradicional del switch pasa a ser realizada por un conmutador LAN, quedando aquél destinado a funciones relacionadas con la mejora de prestaciones en lo que respecta a la gestión de la red. Con este nuevo papel del switch se pueden contener de 100 a 500 usuarios.

Sin embargo, el continuo despliegue de conmutadores, dividiendo la red en más y más segmentos, no reduce la problemática del contenido de broadcast.

Las VLANs representan una solución alternativa a los switches con función de gestores de red. Gracias a la implementación de conmutadores en unión con VLANs cada segmento de la red puede contener como mínimo un usuario, mientras los dominios de broadcast pueden contener 1000 usuarios, o incluso más. Además, las VLANs permiten enrutar movimientos de las estaciones de trabajo hacia nuevas localizaciones, sin necesidad de tener que reconfigurar manualmente las direcciones IP.

I.2 Clase s y tipos de VLANs y características principales

Como respuesta a los problemas generados en las redes LAN, dígase colisiones, tráfico broadcast, movilidad, etc., se creó una red con agrupamientos lógicos independientes del nivel físico.

Las VLANs forman grupos lógicos para definir los dominios de broadcast, así aunque físicamente las máquinas estén conectadas al mismo equipo, lógicamente pertenecen a una VLAN distinta dependiendo de sus aplicaciones, puesto que con la implementación de VLANs existe una segmentación lógica o virtual.

Existen dos clases de VLANs:

- VLANs implícitas
- VLANs explícitas

En el funcionamiento de las VLANs implícitas no se modifican las tramas, ya que de la misma forma en que reciben la información la procesan, ejemplo de ello son las VLANs basadas en puertos.

Por otro lado, contrario al funcionamiento de las redes virtuales implícitas, las VLANs explícitas se basan en las modificaciones, adiciones y cambios en las tramas.

Asimismo, existen diferentes tipos de VLANs que pueden clasificarse en 10 y los cuales se describen a continuación.

1.2.1 VLAN por puerto

Consiste en una agrupación de puertos físicos que pueden tener lugar sobre un conmutador o también en algunos casos, sobre varios conmutadores, sin embargo, sólo se puede tener una VLAN por puerto. En este tipo de red virtual todos los nodos que se encuentran conectados a puertos dentro de la misma red virtual tienen asignado un solo identificador, que es igual para

cada uno de ellos. La **Figura I.6** muestra la pertenencia a una VLAN por puerto, lo que facilita el trabajo del administrador y hace que la red sea más eficiente debido a que:

- Los usuarios se asignan por puerto.
- Las VLANs se pueden administrar fácilmente.
- Existe una mayor seguridad entre las diferentes redes.
- Los paquetes transmitidos no se filtran a otros dominios.

Cualquier operación, ya sea añadir, mover o cambiar a un usuario se produce normalmente con la reconfiguración del puerto correspondiente y algunas aplicaciones gráficas de gestión de VLANs que permiten automatizar totalmente esta reasignación. Además de que es necesario tener un control manual de todos los nombres de VLANs, número de puertos y nodos asociados. Este tipo de red virtual como la indicada en la **Figura I.6** se configura por una cantidad "n" de puertos, en la cual se puede indicar qué puertos pertenecen a cada VLAN; además se implementan fácilmente y su funcionamiento es muy sencillo de entender.

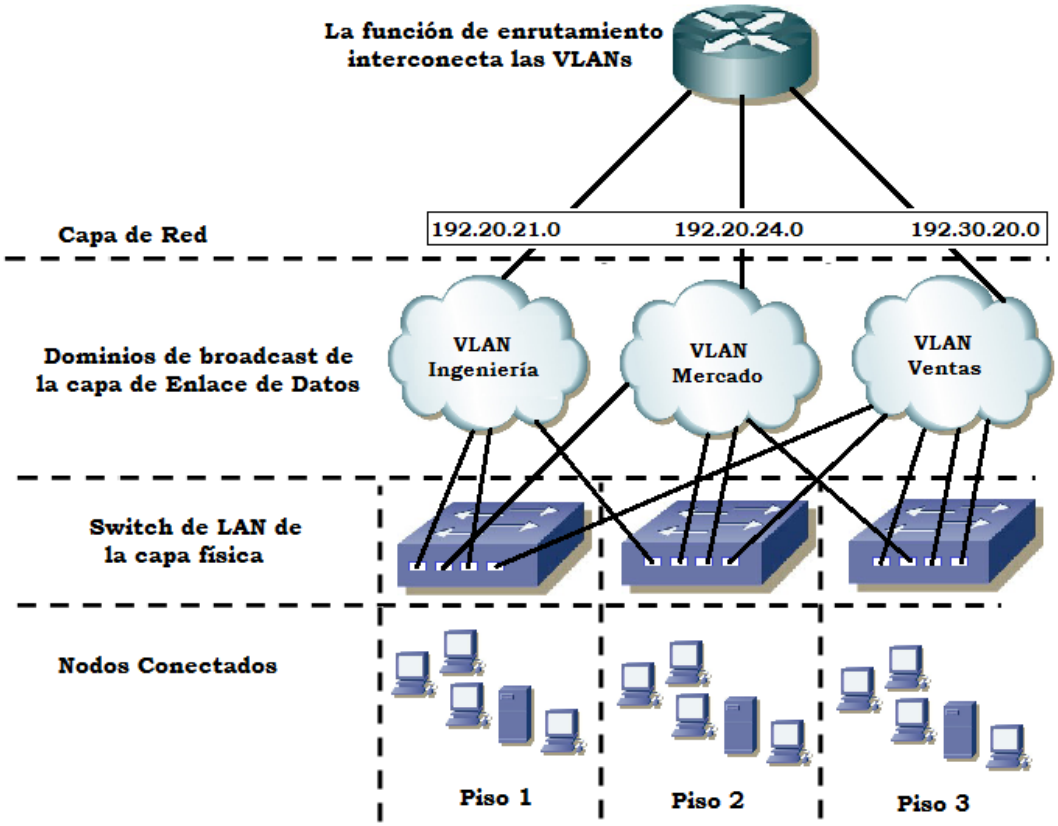


Figura I.6 VLAN por puerto

La definición de VLAN por puerto implica que el tráfico broadcast de una red virtual no afecta a las estaciones del resto de las VLANs, puesto que es siempre interno a aquella en la cual se origina, así mismo es independiente del protocolo o protocolos utilizados en las diferentes estaciones de trabajo.

1.2.2 VLAN estática

Este tipo de VLANs tal como la que se puede observar en la **Figura I.7,** es posiblemente el tipo de redes virtuales más usado debido a la administración y seguridad que pueden proveer. Algunas características de una VLAN estática son las siguientes:

- Los puertos del switch están pre-asignados a las estaciones de trabajo, dichos puertos se asignan estáticamente, y mantienen sus configuraciones de VLAN asignadas hasta que se decida cambiarlas nuevamente.
- Cuando un equipo se conecta a un puerto, asume automáticamente la VLAN a la que éste fue asociado.
- Las VLANs estáticas tienen un buen desempeño en las redes en las que el movimiento se encuentra controlado y administrado.

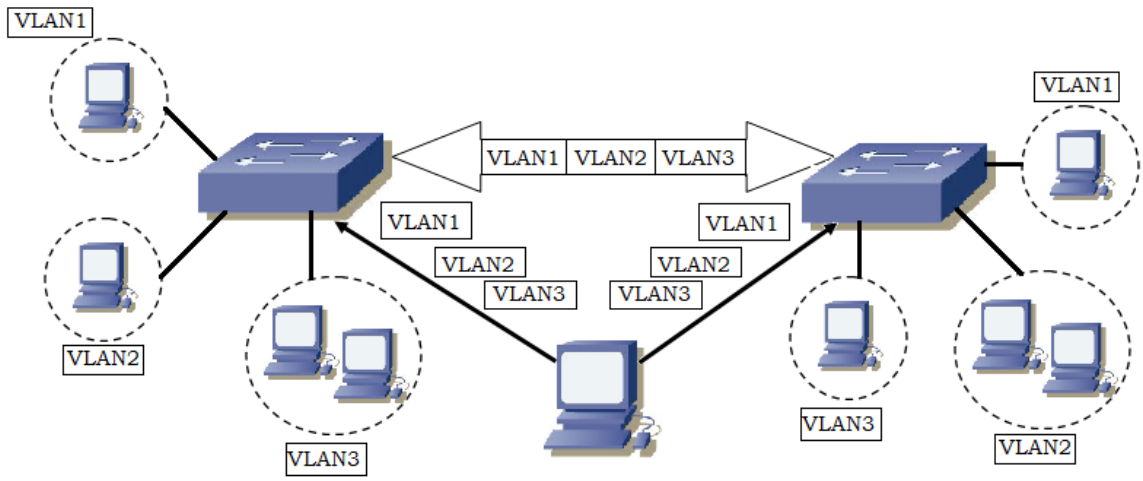


Figura I.7 VLAN Estática

1.2.3 VLAN por dirección MAC

La relación de pertenencia en este tipo de VLAN se basa en la dirección MAC, ya que opera agrupando estaciones finales en base a dichas direcciones. Esto puede observarse en la **Figura I.8.**

Este método requiere que las direcciones MAC de cada estación sean añadidas manualmente a una red específica, lo que permite que una determinada estación sin importar su ubicación en la red sea miembro de esa VLAN.

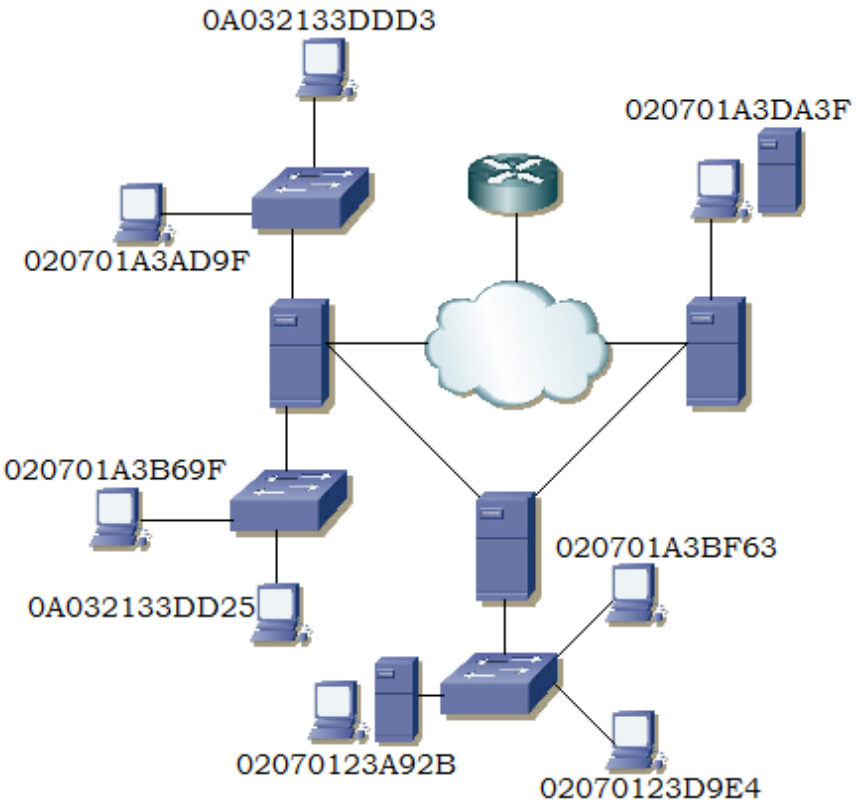


Figura I.8 VLAN por dirección MAC

A partir de que las direcciones MAC se encuentran implementadas directamente sobre la tarjeta de interfaz (NIC), las VLANs basadas en direcciones MAC permiten a los administradores mover las estaciones de trabajo a localizaciones físicas distintas dentro de la red y aún así mantener su pertenencia a la VLAN, por lo tanto, este tipo de redes virtuales pueden ser vistas como redes orientadas al usuario.

Uno de los inconvenientes de las VLANs basadas en MAC es que en un inicio todos los usuarios deben estar configurados para poder pertenecer al menos a una VLAN. La desventaja de tener que configurar inicialmente la red es más evidente en redes grandes, donde miles de usuarios deben ser asignados explícitamente a una VLAN en particular.

1.2.4 VLAN por protocolo

Este tipo de VLAN puede configurarse cuando en una red se opera con más de un protocolo, tal como ilustra la **Figura I.9**, lo cual permite que pueda ser programada basándose en un protocolo en específico.

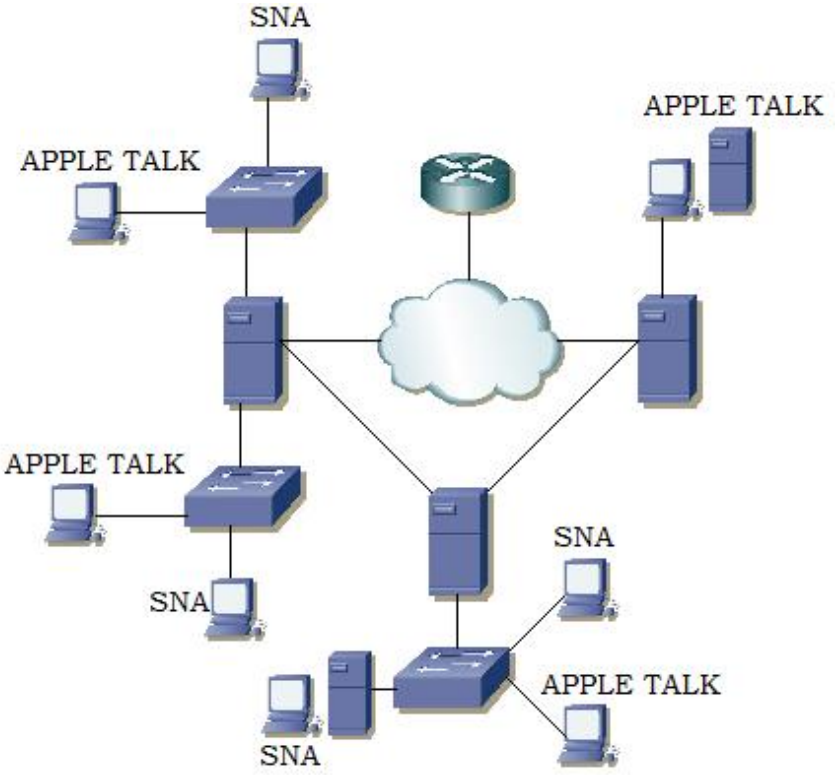


Figura I.9 VLAN por protocolo

La ventaja de estas VLANs es que a menudo las aplicaciones que se utilizan en una red, usan algún protocolo en particular, de esta forma, la segmentación de tráfico por tipo de protocolo permite formar redes VLAN de aplicación específica, así los usuarios pueden moverse por toda la red reteniendo su membresía, siempre y cuando mantengan su protocolo.

Sin embargo, al igual que las VLANs basadas en MAC, las direcciones deben ser asignadas manualmente, lo cual resulta incómodo, y además si la tarjeta NIC o la PC se averían y en consecuencia tienen que ser reemplazadas, será necesario reconfigurar de nuevo la VLAN en el switch.

1.2.5 VLAN por direcciones IP

Este tipo de VLAN es el más fácil de configurar, y hace uso del protocolo IP. IP es un protocolo que asigna una dirección individual a cada nodo, así, pueden agruparse distintos nodos IP para integrar una VLAN.

Debido a que las direcciones IP generalmente se asignan por rangos, este tipo de red virtual debe de ser programada de tal modo que coincida con un rango de dichas direcciones, denominado subred. Por lo tanto si una VLAN utiliza el protocolo DHCP, no podrá ser administrada en base a IPs, ya que el protocolo DHCP asigna una dirección diferente cada vez que un usuario se conecta a la red. El tipo de switch que conforma a estas redes actúa como un agrupador, es decir, simplemente agrupa un tráfico de subred dentro de una VLAN. En la **Figura I.10** se ilustra el ejemplo de una VLAN basada en direcciones IP.

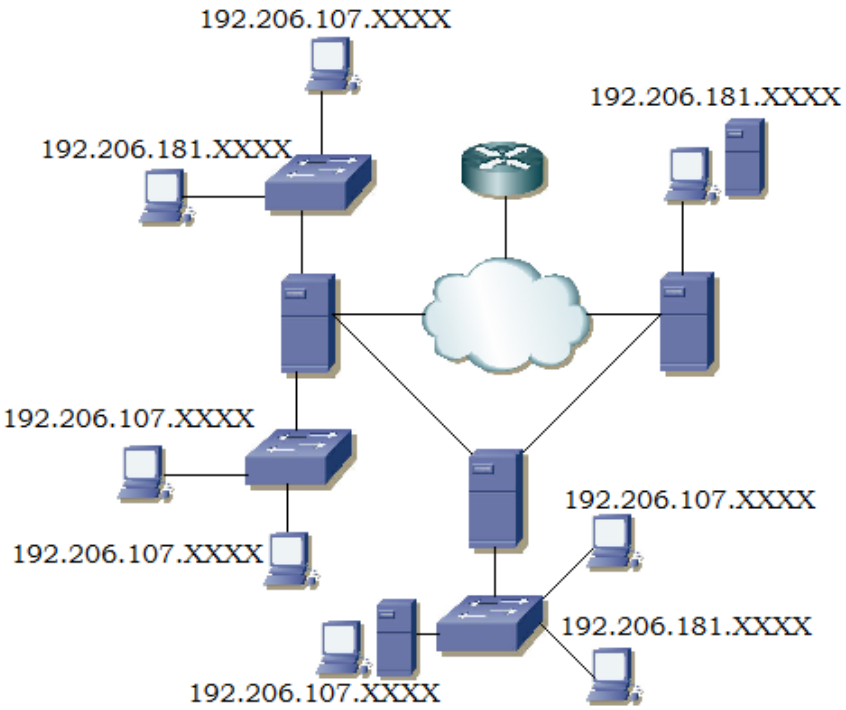


Figura I.10 VLAN por direcciones IP

1.2.6 VLAN por nombre de usuario

Estas VLANs se basan en la autenticación del usuario y no en las direcciones MAC o IP de los dispositivos. Por ello, facilitan y aseguran la movilidad de los usuarios dentro de alguna institución o empresa.

Generalmente una VLAN de este tipo, opera de la siguiente manera:

1. Acceso y presentación de privilegios de conexión de usuario.
2. El servidor de seguridad autentica y autoriza los privilegios del usuario perteneciente a la VLAN.
3. Se autoriza el permiso para que el cliente se conecte a una VLAN específica.

El funcionamiento anterior se ilustra en la Figura **I.11.**

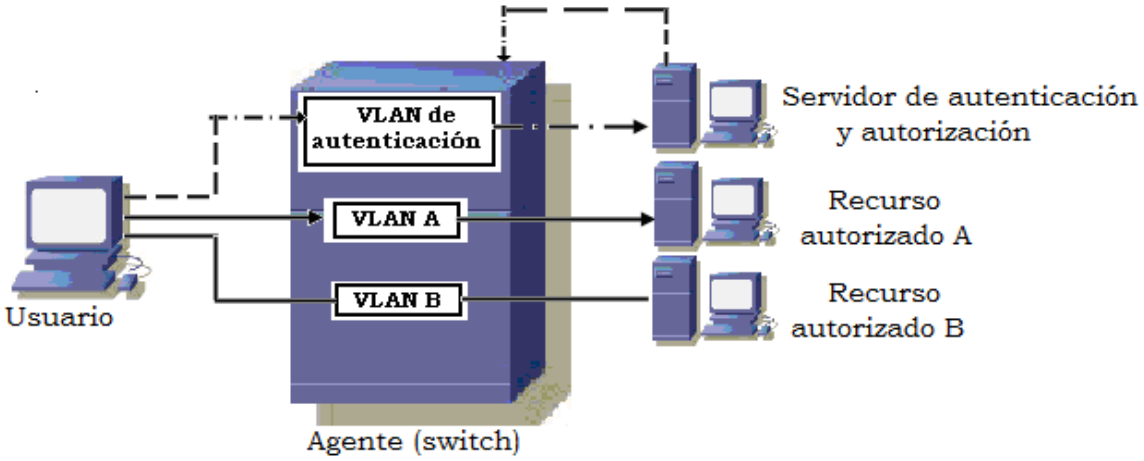


Figura I.11 VLAN por nombre de usuario

1.2.7 VLAN dinámica (DVLAN)

Las VLANs dinámicas son puertos del switch que automáticamente determinan a qué red virtual pertenece cada puesto de trabajo. El funcionamiento de éstas se basa en direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a una VLAN, el switch revisa la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas, y

automáticamente se configura el puerto dependiendo de la configuración de la VLAN al que vaya dirigido, esto se puede representar en la **Figura I.12.**

El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se agregan o se cambian de lugar las estaciones de trabajo, y además también cuenta con notificaciones centralizadas cuando un usuario desconocido pretende ingresar a la red.

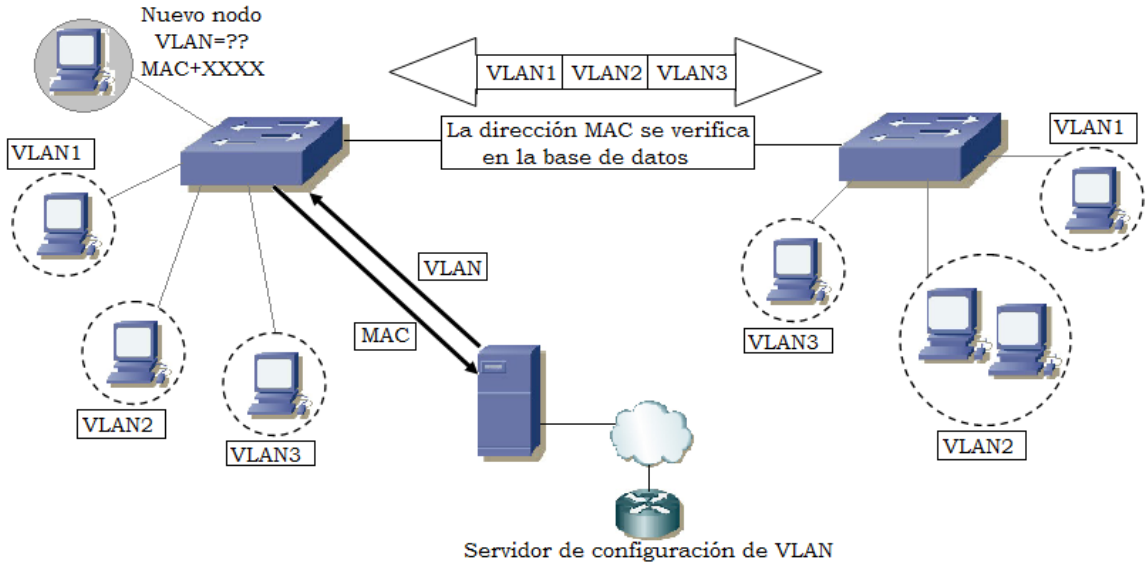


Figura I.12 VLAN Dinámica

1.2.8 VLAN de capa 3 (Layer 3-Based VLAN)

Las redes virtuales de capa 3 toman en cuenta el tipo de protocolo (si varios protocolos son soportados por la máquina) o direcciones de la capa de red para determinar la pertenencia a una VLAN, y generalmente son utilizadas cuando es aplicado el protocolo TCP/IP. Aunque estas VLANs se basan en información de la capa 3, esto no constituye una función de encaminamiento y no debería de ser confundido con el enrutamiento de la capa de red.

Este tipo de VLANs permite la segmentación por protocolo, asimismo los usuarios pueden mover físicamente sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de las mismas y permite

eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores, reduciendo así los gastos de transporte.

Sin embargo, el inspeccionar direcciones de la capa 3 en paquetes, consume más tiempo que buscar una dirección MAC en tramas. Por ésta razón los conmutadores que usan información de la capa 3 para la definición de VLANs generalmente son más lentos que los usados en capa 2.

La diferencia entre estas redes virtuales y las VLANs por direcciones IP radica en que cuando una VLAN se basa en IPs, la configuración en dicha red debe realizarse agrupando un rango de direcciones, es decir, una subred; lo que permite configurar más de una VLAN en uno o más switches. En cambio las redes virtuales de capa 3 aunque toman en cuenta el protocolo TCP/IP y como consecuencia las direcciones IP asignadas a cada uno de los usuarios, también consideran el tipo de información que se transmita a través de ellas. En este caso para poder pertenecer a una VLAN de este tipo, tiene que ser específicamente información de capa 3 sin que sea obligatorio el etiquetado de las tramas transmitidas.

1.2.9 VLAN basada en reglas (Policy Based VLAN)

Este esquema es uno de los más potentes y flexibles, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. En este caso, no se tiene un diagrama representativo, ya que las VLANs basadas en reglas, como su nombre lo indica se basan precisamente en normas establecidas por los administradores de la red, y las cuales se supone deben de ser convenientes para ofrecer un acceso adecuado y eficiente. Las reglas establecidas deben de ser cumplidas por los usuarios pertenecientes a estas redes, para así permitir que sigan formando parte de los grupos de trabajo que se encuentran definidos en ellas.

Un ejemplo de lo anterior, pueden ser las reglas de acceso, con el objetivo de tener cierto nivel de seguridad. El conjunto de reglas en las cuales se basará la VLAN, constituye la política a implementar en dicha red.

1.2.10 VLAN por DHCP

Las VLANs basadas en servidores DHCP son aquellas que permiten asignar una IP automática a cada uno de los usuarios. De esta forma cuando el usuario enciende la computadora, la dirección física de la misma es detectada por el DHCP, el cual comprueba que el equipo que desea acceder a la red se encuentre dado de alta, de ser así tome la dirección IP que le corresponde y en base a esta acción asigne al usuario a la VLAN indicada. Esta política de VLAN es de las últimas generaciones y su implementación evita el hecho de que los host conectados a una VLAN tengan la necesidad de contar con una configuración de IPs fijas.

Ya ha sido mencionado, tanto el concepto de VLAN, así como la clasificación y tipos de redes virtuales que pueden ser implementadas. Ahora se hablará un poco respecto a la institución a tratar en esta propuesta.

1.3 Precedentes y características del Instituto Hospitalario

Entre algunos de los problemas a los que se enfrentaba la sociedad a finales de la década de los 60s, se encontraban las conductas antisociales como: abandono, orfandad, agresiones a la salud y enfermedades infecciosas.

Debido a ello el Gobierno decidió crear un organismo cuyo objetivo primordial fuera el establecimiento de hospitales dedicados a los niños, casas cuna, casas hogar, internados, asilos y en general instituciones dedicadas a la atención del menor en situación de abandono.

Entre sus atribuciones estaba también la formación de recursos humanos profesionales y técnicos, así como la investigación y coordinación con organismos públicos y privados para apoyo mutuo.

Luchando por este objetivo se logró que el 19 de agosto de 1968 naciera una institución interesada en el cuidado y salud de la niñez, la cual era conformada por diversos hospitales del país. Dicha institución abrió sus

puertas el 6 de noviembre de 1970, con el propósito de ofrecer a la niñez mexicana atención pediátrica integral de contenido social.

La idea era construir una red de atención pediátrica nacional con hospitales infantiles en donde se aprovecharían tanto recursos humanos como físicos.

Al cabo de casi tres décadas y media de servicio, esta fundación se ha convertido en un organismo muy importante para la sociedad, ya que ofrece atención especializada a la población infantil de todo el país y extiende su influencia de atención a otros países latinoamericanos.

El personal se ha dedicado con entusiasmo y profesionalismo a la atención, cuidado y rehabilitación de los niños enfermos que acuden a la consulta externa o que ingresan a hospitalización; los investigadores han aportado nuevos conocimientos a la ciencia médica y muchas generaciones de alumnos se han formado con las enseñanzas de los profesores.

Actualmente el Instituto Hospitalario que se trata en esta propuesta, es un organismo público descentralizado del Sector Salud, cuyo objetivo principal es la investigación científica en el campo de la salud, la formación y la capacitación de recursos humanos calificados, así como la prestación de servicios de asistencia a la salud de alta especialidad para los padecimientos de la población infantil hasta la adolescencia, y cuyo ámbito de acción comprende todo el territorio nacional.

Como toda organización, el Instituto Hospitalario cuenta con: una misión, una visión y una política de calidad, las cuales se presentan a continuación.

Misión

Desarrollar modelos de atención a la infancia y adolescencia, apoyándose en la investigación científica básica, clínica y epidemiológica, aplicada a las necesidades de la población.

Visión

Ser una institución líder en la investigación, caracterizada por tener alto rigor científico, y de esta manera lograr la formación de recursos humanos de alta calidad y la creación de modelos de atención a la salud de la infancia y la adolescencia.

Política de Calidad

Compromiso para implementar, aplicar y mejorar sistemas médicos, técnicos y administrativos que lleven a la obtención del cumplimiento de los objetivos en las áreas de investigación, enseñanza y asistencia.

El Instituto Hospitalario cuenta con diferentes departamentos, cada uno de los cuales desempeña una función en específico. La estructura y organización de dichos departamentos es la siguiente:

Para la conducción de las actividades de investigación dentro del Instituto Hospitalario, se ha constituido una Dirección de Investigación, la cual depende directamente de una Dirección General.

Dependen de la Dirección de Investigación la Subdirección de Medicina Experimental y la Subdirección de Investigación Médica.

De la Subdirección de Medicina Experimental dependen:

- La Unidad de Genética de la Nutrición INP-IBBM (UNAM)
- El laboratorio de Neurofisiología INP-Facultad de Psicología (UNAM)
- Los laboratorios de Seguimiento de Neurodesarrollo, Farmacología, Patología Experimental, Neuroquímica, Toxicología Genética, Bioquímica Genética, Oncología Experimental, Cirugía Experimental, Histomorfología, Neuromorfometría, Microscopía Electrónica, Bacteriología, Parasitología Médica y Reproducción Animal (bioterio).

De la Subdirección de Investigación Médica dependen:

- Departamento de Metodología de la Investigación.
- Departamento de Investigación en Epidemiología en los Centros Rurales de Investigación en Morelos (Tlaltizapán y Huatecalco).
- Departamento de Genética Humana.
- Unidad de Apoyo a la Investigación Clínica.

Adicional a los campos médicos, existen otras áreas que contribuyen a que todas las anteriores desempeñen correctamente su funcionamiento, algunas de ellas relacionadas también con la investigación y otras relacionadas con los recursos tanto físicos, como humanos y administrativos.

Entre dichas áreas se encuentran:

- Farmacia
- Almacén General
- Mantenimiento
- Enseñanza
- Planeación
- Personal
- Administración y finanzas
- Comedor
- Estacionamientos
- Checadores
- Biblioteca
- Archivo clínico
- Tecnologías de la Información

Todos los departamentos que conforman al Instituto Hospitalario son de gran importancia, y ya sea directa o indirectamente, se relacionan entre sí para poder cumplir tanto con las funciones correspondientes a cada una de ellas, como con las del Instituto en general.

1.4 Función que desempeñan las VLANs en el Instituto

Hoy en día, es de suma importancia contar con la comunicación y tecnología necesaria para que una institución de este tipo pueda cumplir adecuadamente con sus actividades.

Como ya se mencionó, el Instituto Hospitalario cuenta con diversos departamentos, los cuales requieren ciertas herramientas que les permitan ejercer adecuadamente todas las funciones que el Instituto exige que se cumplan.

Muchas de estas funciones pueden ser realizadas únicamente si se cuenta con acceso a la red, por ejemplo:

- Sistemas dedicados a administrar la situación tanto de los pacientes que ingresan, como de los que egresan del Instituto. Dichos sistemas demandan la entrada a servidores de bases de datos, lo cual es posible solo si se cuenta con una conexión a Internet.
- En el área de investigación es siempre necesaria la búsqueda de información para poder llevar a cabo los experimentos e indagaciones requeridas, así como contar con la asesoría y conocimientos necesarios que faciliten el desarrollo de los mismos.
- Se realiza el envío de información, documentos, archivos, etc., de un departamento a otro e incluso a lugares e instituciones externas al Instituto Hospitalario, lo cual se da a través de correos electrónicos o de equipos compartidos, o remotos que únicamente pueden comunicarse si cuentan con un enlace a la red.

Solo por mencionar algunas de las numerosas actividades realizadas dentro del Instituto.

Sin lugar a dudas, el Internet es un gran recurso tecnológico que tiene un profundo impacto en el trabajo y conocimiento de la sociedad en general, y evidentemente este organismo no es la excepción.

El Instituto Hospitalario, cuenta con aproximadamente 2000 trabajadores, de los cuales, alrededor de 1400 son usuarios de la red, quienes a su vez se encuentran distribuidos en diversas áreas del Hospital.

La implementación de VLANs dentro del instituto, permite asignar una VLAN por cada uno de los departamentos que lo constituyen, permitiendo si es necesario, que exista la comunicación entre algunas de ellas.

Además permiten que el responsable de la administración de la red traslade y agregue fácilmente las estaciones de trabajo al sistema, y también que pueda cambiar de una manera más sencilla la configuración de dicha red, controlando el tráfico de la misma.

Por otra parte, los usuarios que tengan que trasladarse de un lugar a otro dentro del Instituto, y que cuenten con un equipo móvil, pueden sin problema alguno tener acceso a la red, lo cual quiere decir que se eliminan fronteras físicas entre dichos usuarios.

Los edificios principales que son el hospital y la torre de investigación, así como algunas otras áreas, cuentan con diferentes pisos. Por cada piso se encuentra asignado un IDF *(Intermediate Distribution Facility – Instalación de Distribución Intermedia)*, dentro del cual se localizan conexiones de cables UTP, fibras ópticas, enlaces, servidores, switches, etc. Todos los enlaces pertenecientes a los IDFs llegan al site principal que es denominado MDF *(Main Distribution Facility – Instalación de Distribución Principal)*.

El uso de VLANs permite que exista una comunicación administrable entre todos los dispositivos mencionados, para así lograr un mayor y mejor aprovechamiento de la red.

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.**

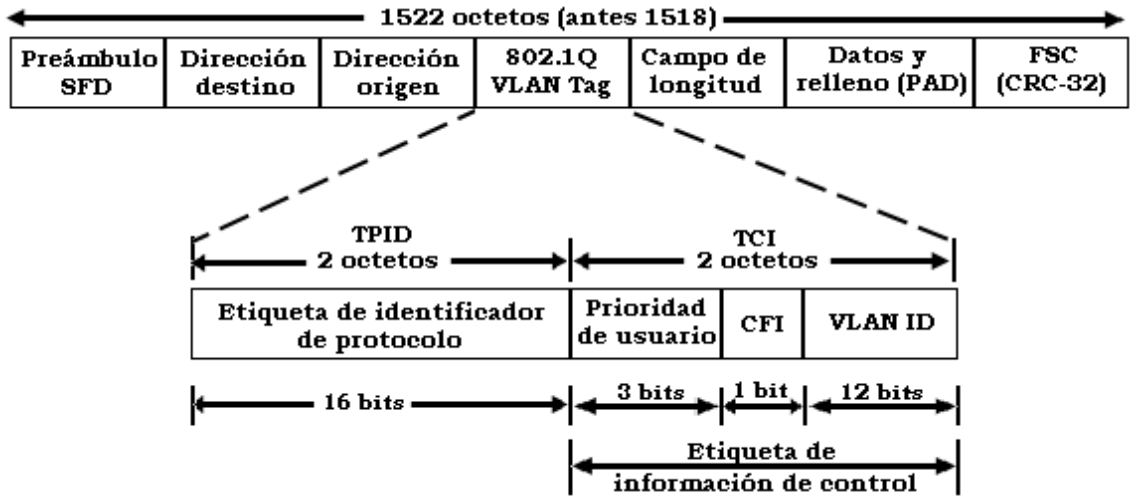


Figura II.1 Trama de la norma 802.1 Q

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*).

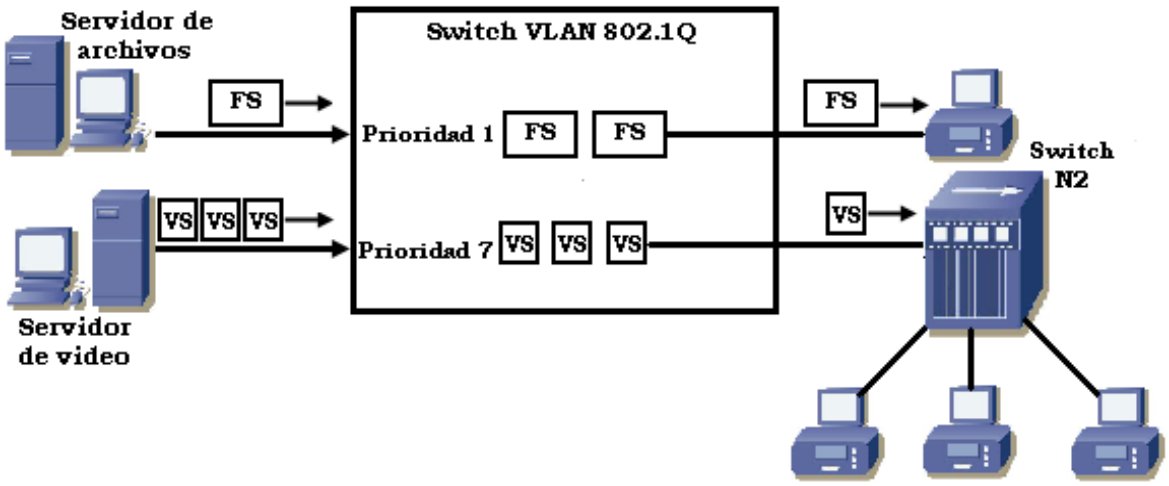


Figura II.2 Aplicación de la norma 802.1 Q

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.**

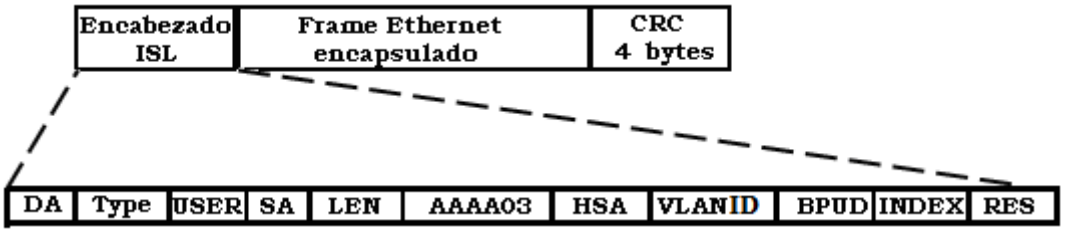


Figura II.3 Encapsulamiento ISL

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.

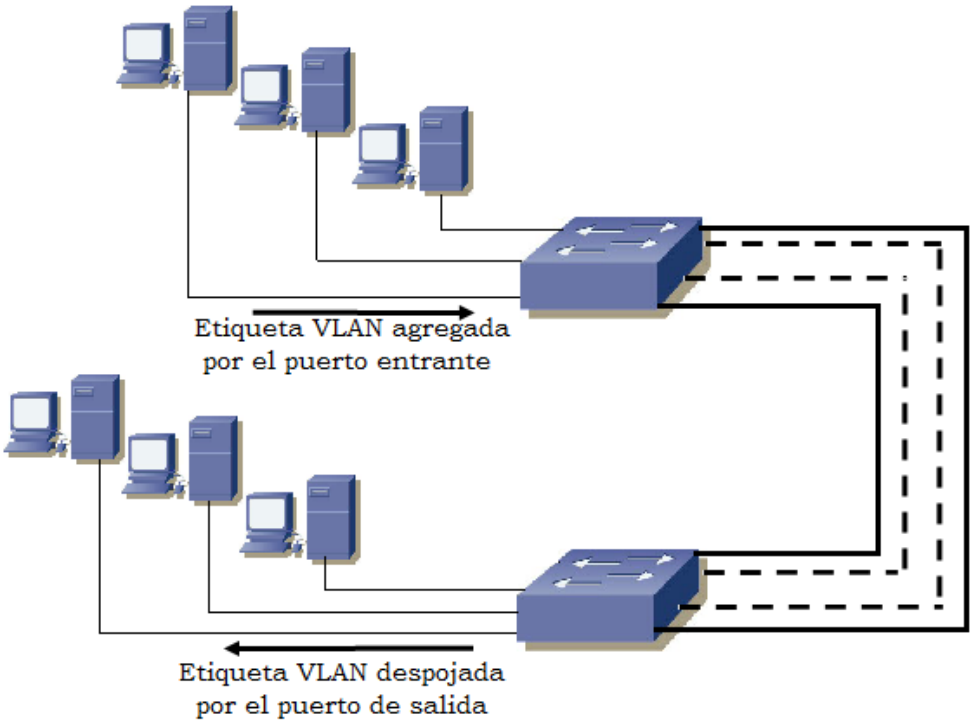


Figura II.4 ISL Tagging

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.

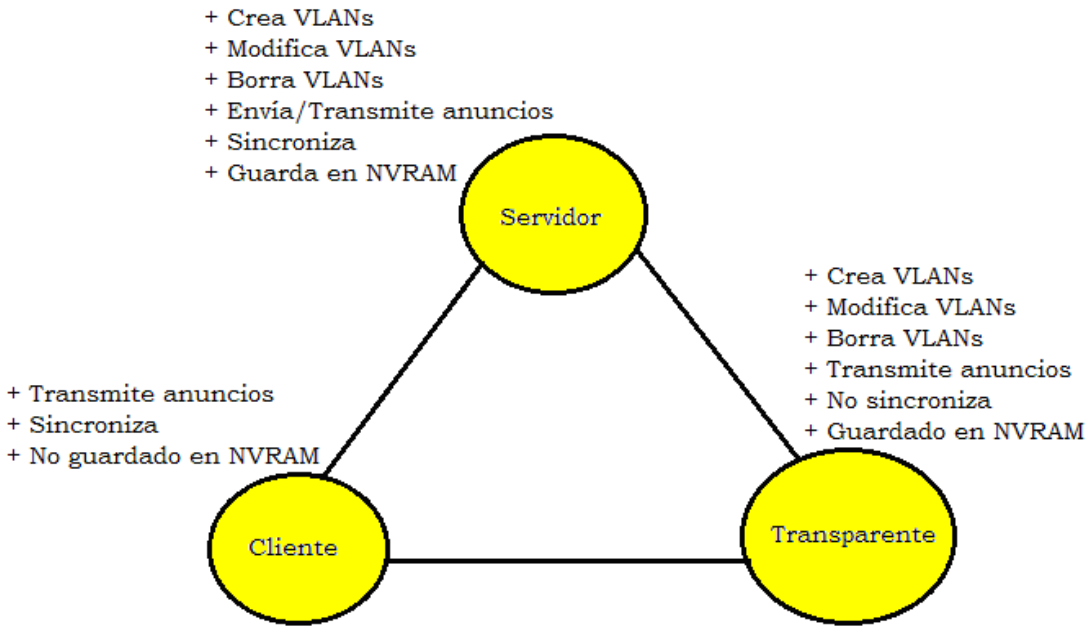


Figura II.5 Modos VTP

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**.

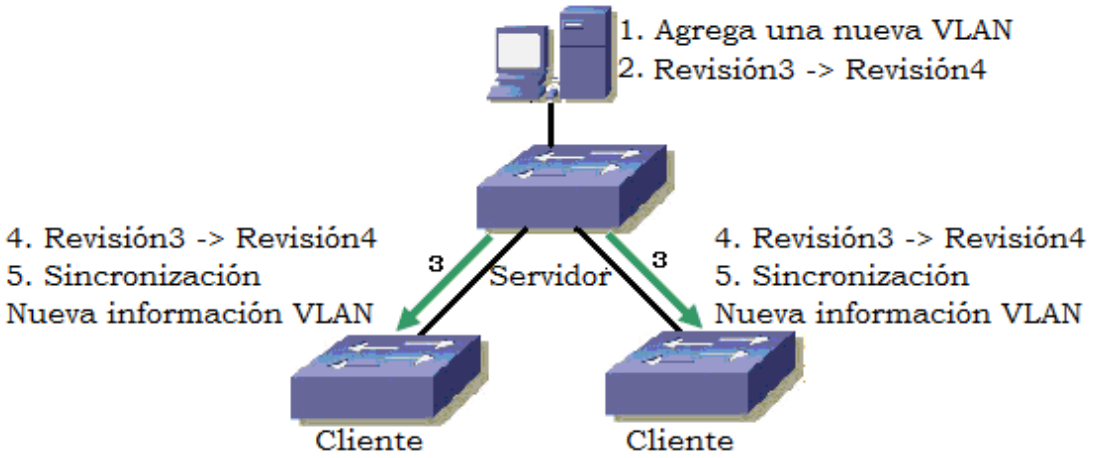


Figura II.6 Funcionamiento de VTP

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).

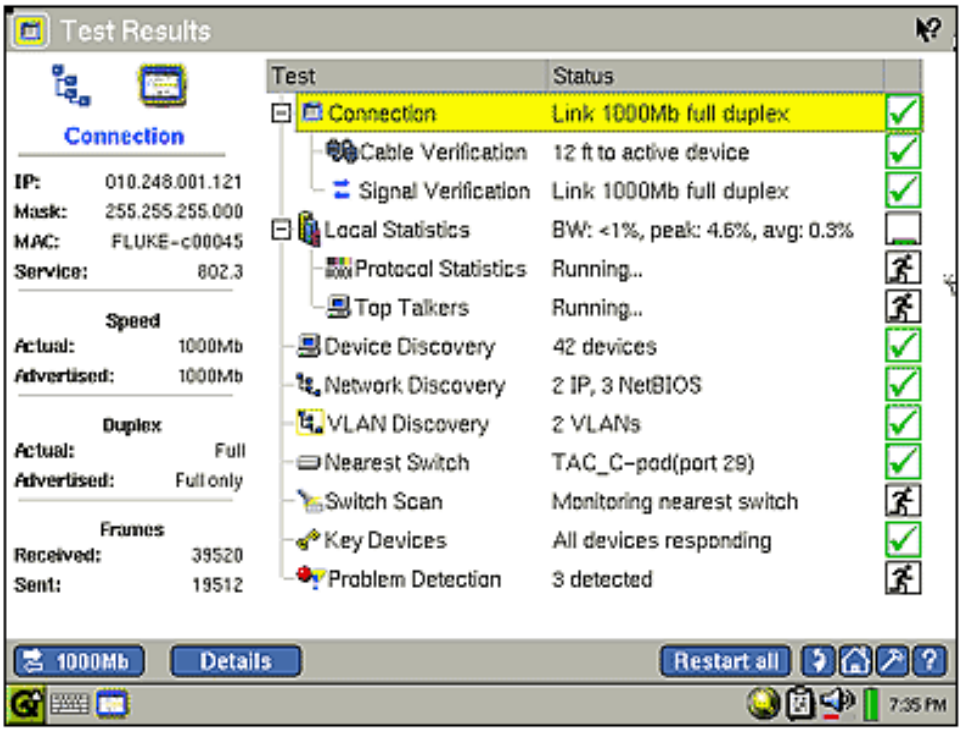


Figura II.8 Prueba automatizada en EtherScope

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.

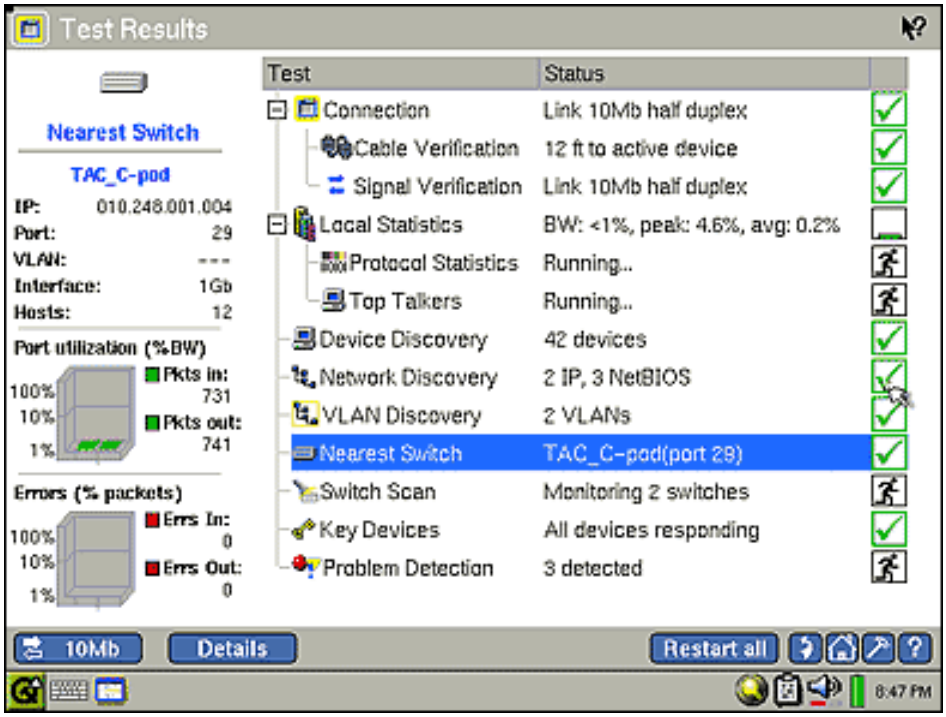


Figura II.9 Detección del switch más cercano

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.

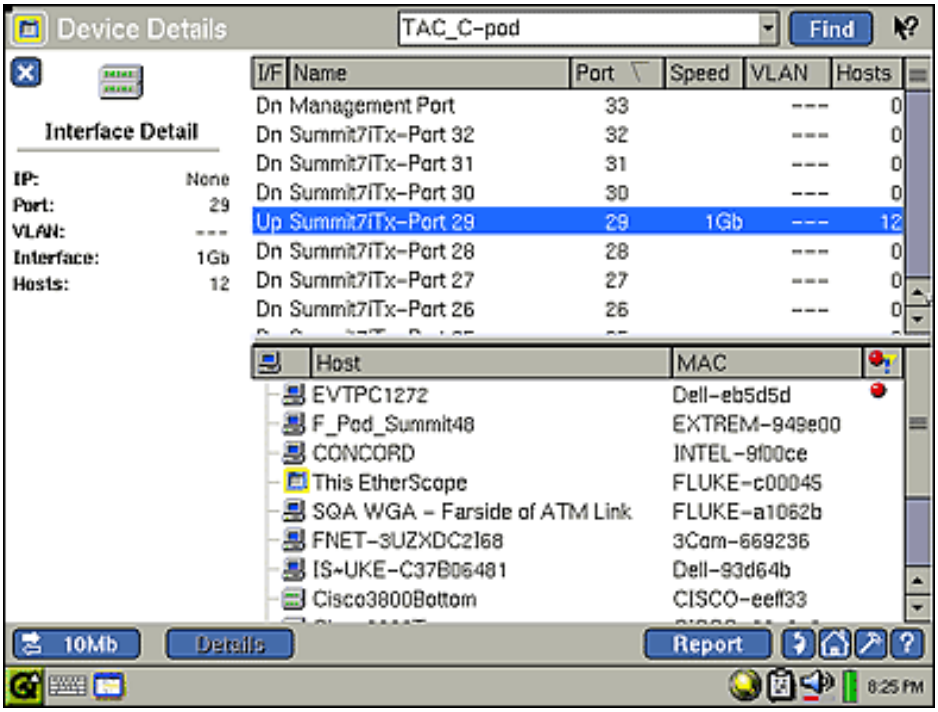


Figura II.10 Diagnóstico del puerto de un switch

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.

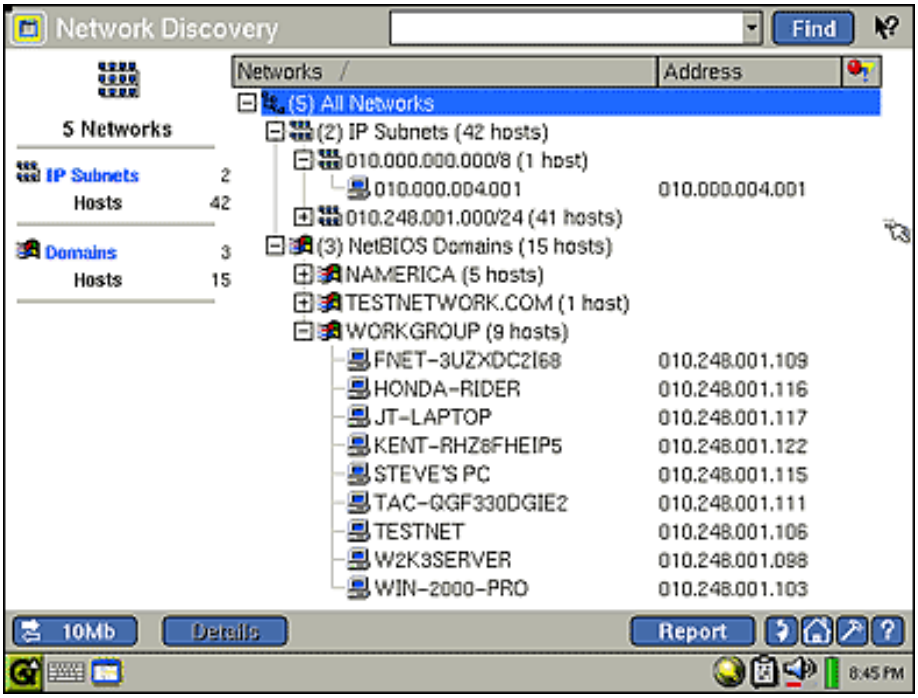


Figura II.11 Detección de redes LAN

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.

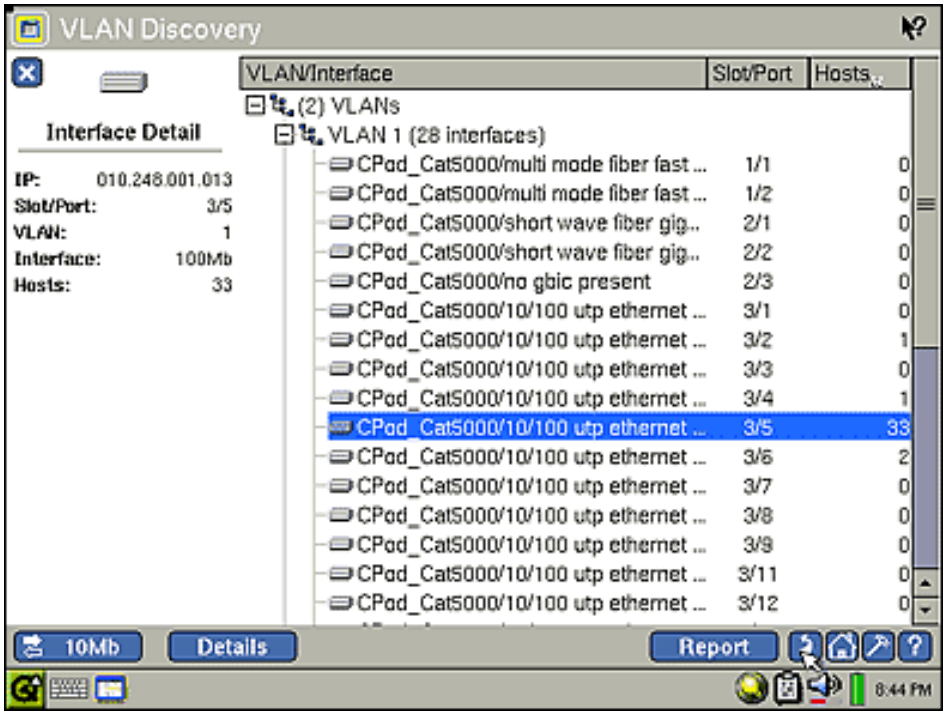


Figura II.12 Identificación de una VLAN

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**.

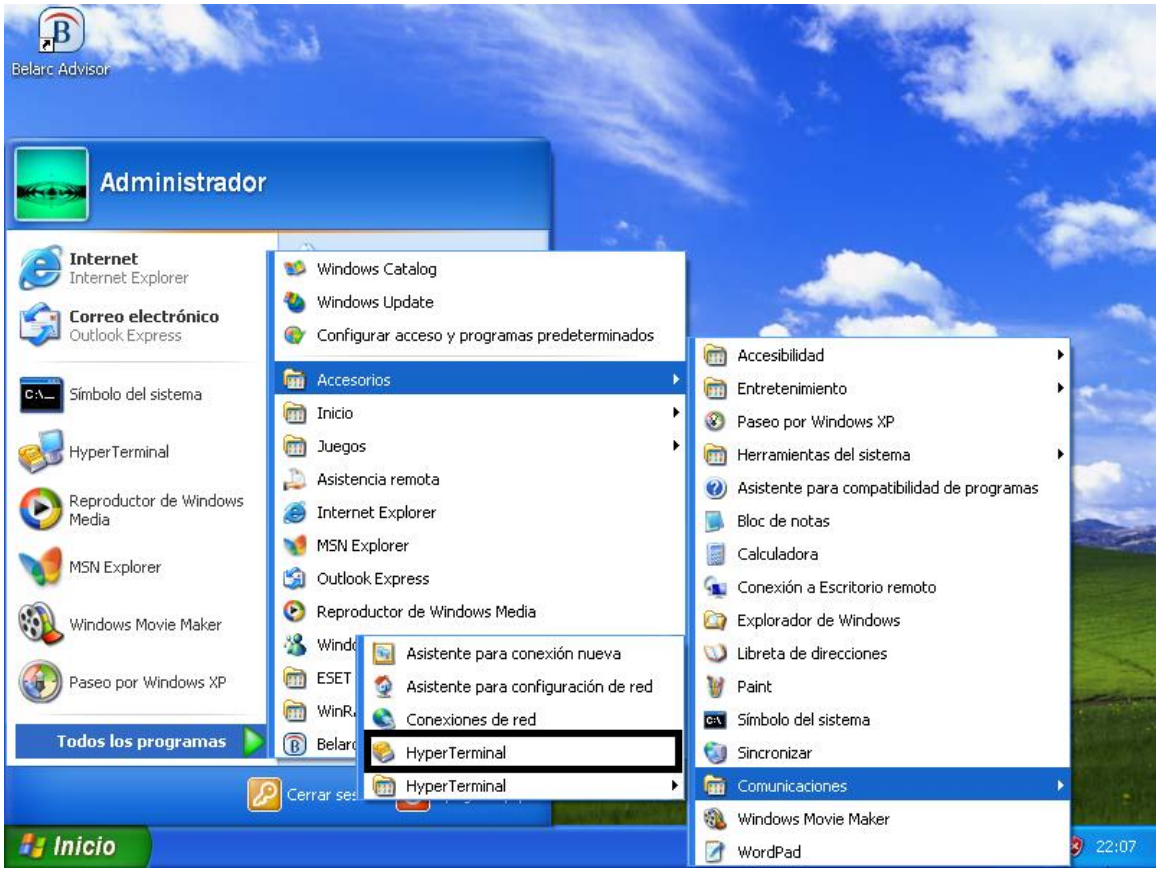


Figura II.13 Herramienta de Windows HyperTerminal

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**.

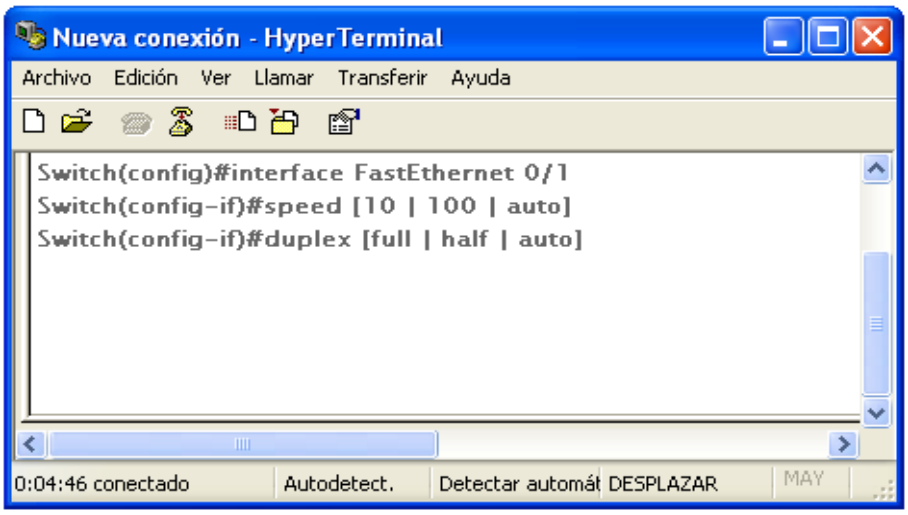


Figura II.14 Conexión HyperTerminal

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.

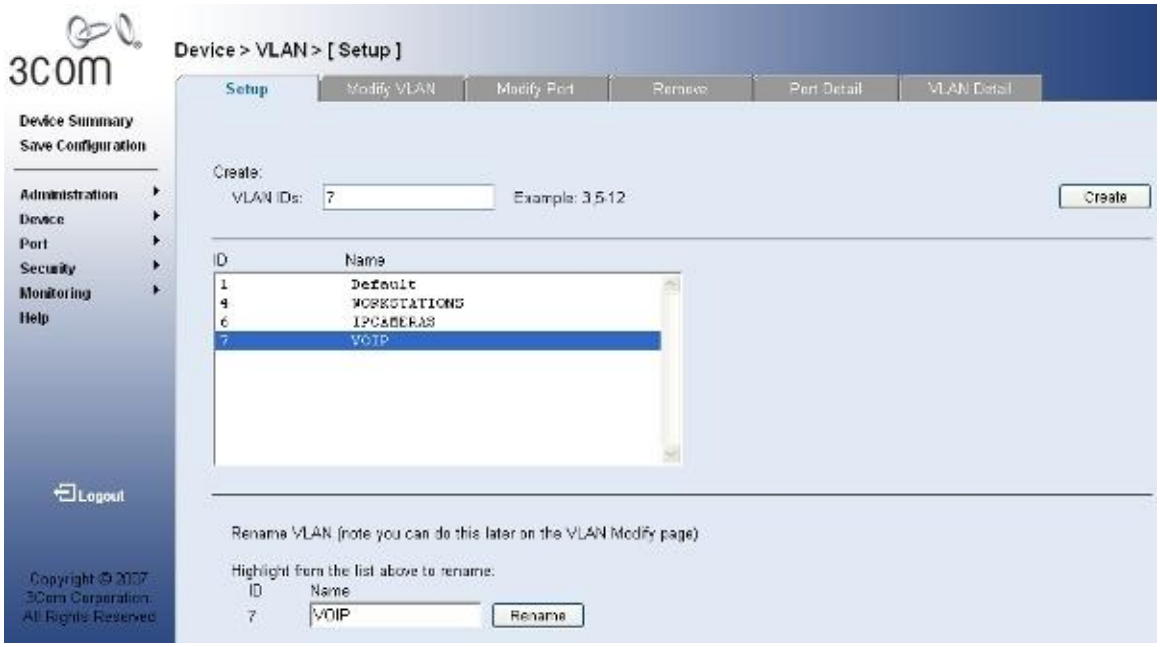


Figura II.15 VLANs configuradas en un switch 3Com

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.

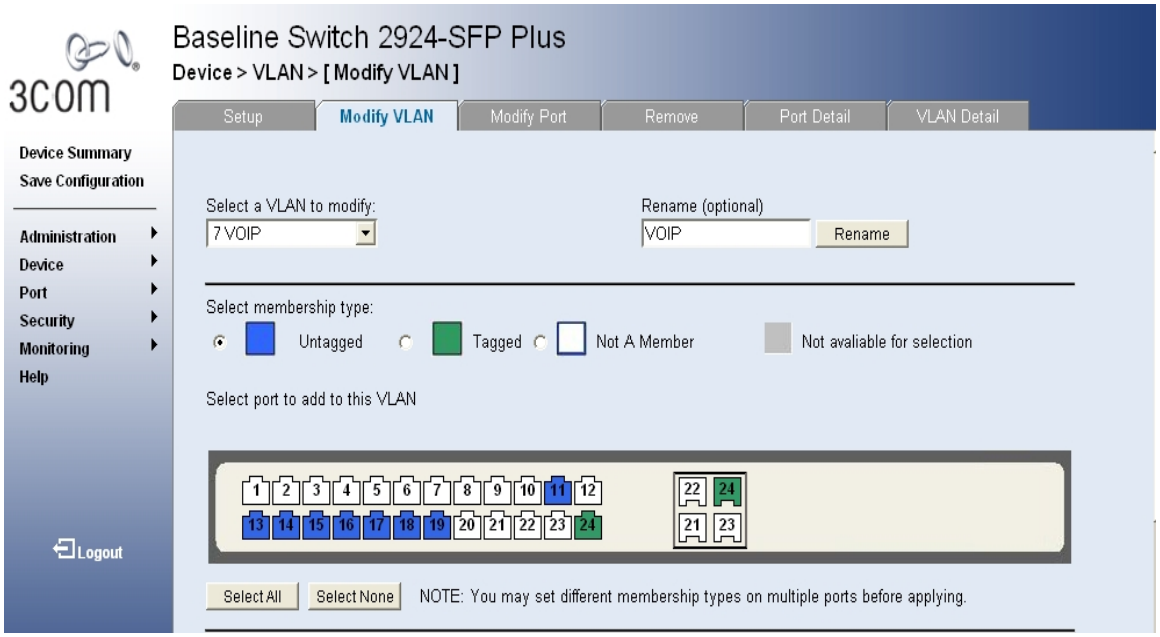


Figura II.16 Puertos asignados a una VLAN en un switch

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.

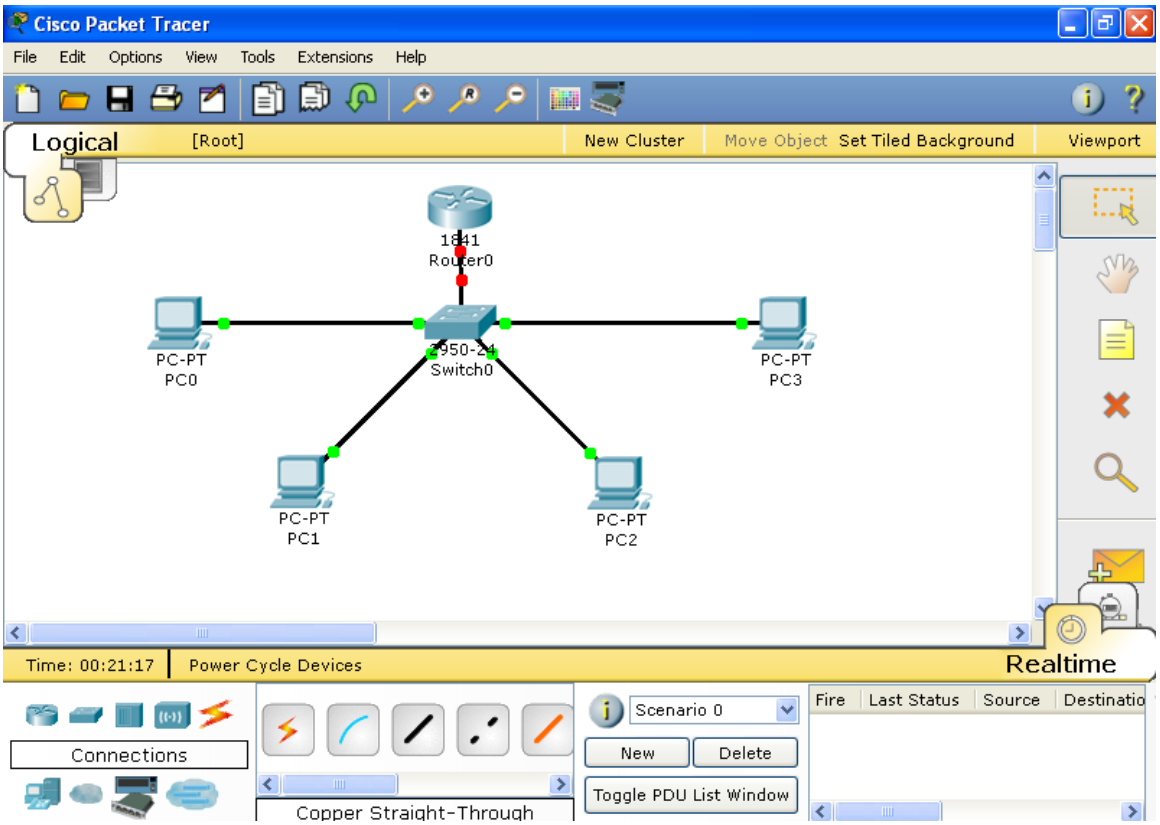


Figura II.17 Interfaz de Packet Tracer

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.

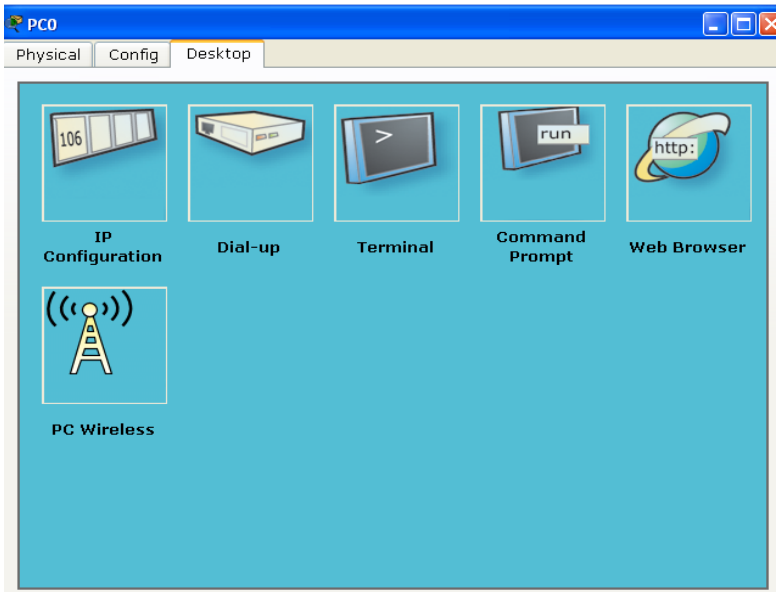


Figura II.18 Configuración de una PC en Packet Tracer

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**.

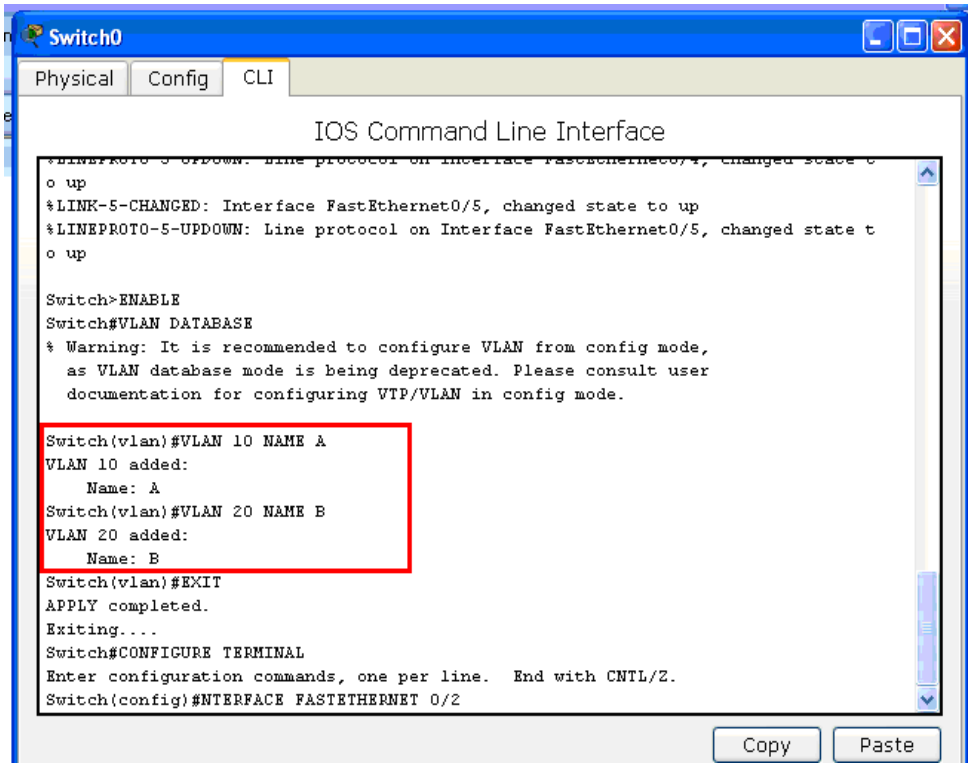


Figura II.19 Configuración de VLANs en Packet Tracer

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.

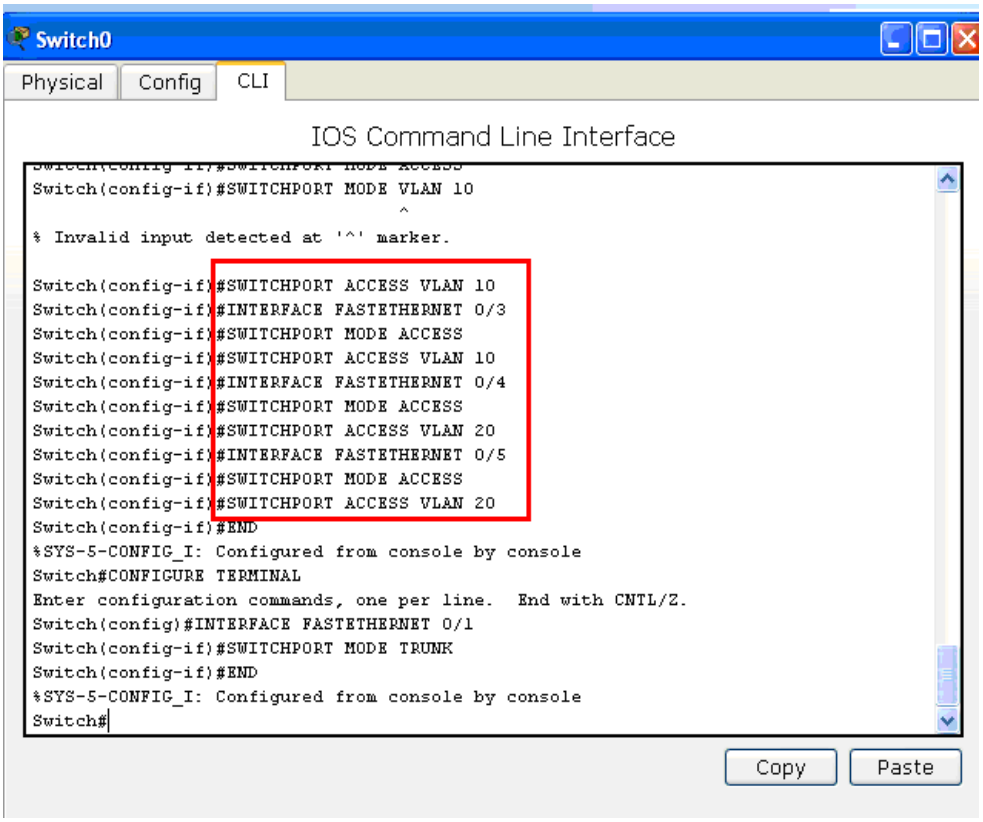


Figura II.20 Asignación de puertos a una VLAN en Packet Tracer

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.**

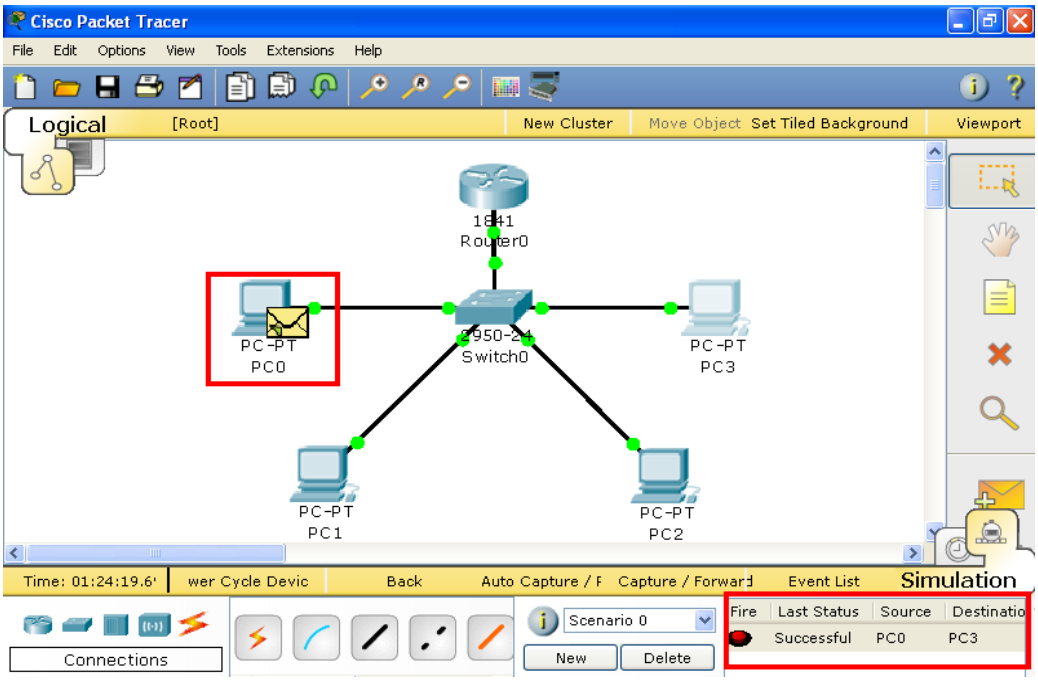


Figura II.21 Simulación del envío de paquetes a través de una VLAN

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.

III.

Comunicación entre VLANs del Instituto Hospitalario

3.1 Grupos virtuales y optimización del ancho de banda

3.1.1 Grupos virtuales

Como ya se mencionó en los capítulos anteriores, las VLANs facilitan la administración de grupos lógicos o virtuales de estaciones de trabajo y servidores, para que éstos se puedan comunicar como si estuvieran en el mismo segmento fisico de una LAN, lo cual permite limitar el tráfico broadcast y multicast, además de favorecer la administración de mudanzas, adiciones y cambios en los miembros de dichos grupos.

Un grupo virtual o grupo de trabajo en una VLAN, representa a un conjunto de usuarios que comparten un dominio de broadcast en común, independientemente de su ubicación física en la interconectividad de la red.

Mediante el uso de la tecnología VLAN, se pueden agrupar los puertos de un switch, así como los usuarios conectados en grupos de trabajo lógicamente definidos. Un ejemplo de clasificación de usuarios podría ser el siguiente:

- Compañeros de trabajo del mismo departamento.
- Grupos de producción interfuncional, es decir, aquellos formados por integrantes de distintos departamentos o unidades de la organización. A este tipo de equipos se les confiere la responsabilidad de planear y realizar proyectos que exigen coordinación, cooperación y aportaciones considerables de todas las partes relacionadas.
- Grupos autoadministrados, los cuales tienen la autoridad y responsabilidad de tomar decisiones administrativas, a fin de lograr los objetivos del conjunto. La cantidad de autoridad delegada varía de una organización a otra.
- Diferentes grupos de usuarios que comparten la misma aplicación de red o software.

Todos los usuarios del Instituto se asocian en grupos de trabajo, ya sea con uno o diversos switches conectados, al hacer esto las VLANs pueden abarcar infraestructuras contenidas en un solo edificio, edificios conectados entre sí o incluso redes WAN (*Wide Area Network – Redes de Área Amplia*).

En las empresas e instituciones actuales, existe una continua reorganización (aproximadamente del 20 al 40% de los trabajadores por año), esto supone que de la misma forma, la red requiere una continua renovación. Las VLANs ofrecen un mecanismo efectivo para controlar esos cambios y reducir en gran parte el costo asociado con las reconfiguraciones de hubs y routers. Los usuarios en una VLAN pueden compartir el mismo espacio de dirección de red (es decir, la subred IP), sin importar su ubicación.

Por otro lado, es bien sabido que el tráfico de broadcast se produce en todas las redes. La frecuencia de éste depende de los tipos de aplicaciones y servidores empleados, de la segmentación lógica y por supuesto del uso que se le da a los recursos de la red. Aunque las aplicaciones se han perfeccionado durante los últimos años para poder reducir la cantidad de broadcast que se envía, se siguen desarrollando nuevas aplicaciones multimedia que producen un exceso de tráfico.

La implementación de VLANs en el Instituto ha permitido extender la capacidad de los firewalls, desde los routers hasta la estructura de los switches, lo que a su vez proporciona la capacidad de protección contra la problemática de broadcast, que en ocasiones resulta ser potencialmente peligrosa.

Se pueden crear firewalls asignando puertos de switch o usuarios a grupos virtuales de VLAN específicos, ya sea dentro de switches individuales y/o a través de múltiples de estos dispositivos conectados. Así, el tráfico broadcast dentro de una VLAN no se transmite fuera de ella; por el contrario, los puertos adyacentes no reciben el tráfico generado desde otras VLANs. Este tipo de configuración reduce sustancialmente el broadcast producido, liberando de esta forma el ancho de banda para el tráfico real de los usuarios, y reduciendo

a su vez la vulnerabilidad general de la red ante circulación innecesaria de información.

También pueden asignarse VLANs basadas en el tipo de aplicación, lo cual permite agrupar a los usuarios que comparten una utilidad en común, y si fuera el caso de que ésta se encuentre produciendo tráfico no deseado, se puede optar por reunir a los usuarios en un mismo grupo perteneciente una VLAN en específico, y así distribuir la aplicación a través del campus o edificio.

Las cuatro situaciones principales para el uso de los grupos de trabajo, o bien grupos virtuales son las siguientes:

1. *VLAN inhabilitada:* La red no utiliza VLANs, pero es posible configurar el Acces Point para emplear varios SSID, es decir, varios códigos que son incluidos en todos los paquetes de una red inalámbrica para identificarlos como parte de la misma.
2. *VLAN habilitada con una sola etiqueta VLAN ID:* todos los grupos de trabajo pertenecientes a una red virtual usan una etiqueta única de VLAN ID.
3. *VLAN habilitada con etiquetas VLAN ID diferentes:* cada grupo de trabajo emplea una etiqueta VLAN ID distinta, para separarlos y distinguirlos entre sí.
4. *VLAN habilitada con o sin etiquetas:* una mezcla de grupos de trabajo que pueden estar etiquetados y sin etiquetar.

3.1.2 Optimización del ancho de banda

Se puede definir al ancho de banda como la cantidad de información que se envía a través de una conexión de red en un periodo de tiempo dado.

Se sabe que el término que corresponde a la unidad más básica de información es el bit e igualmente se conoce que la unidad básica de tiempo es el segundo; de manera que si se trata de describir la cantidad de información que fluye en un periodo determinado de tiempo, podrían

utilizarse las unidades "bits por segundo" para representar dicho flujo. Bits por segundo es una unidad de ancho de banda.

Por supuesto, si la comunicación en una empresa, institución o incluso en el hogar, se produjera a esta velocidad, la transmisión de información y el desempeño de la red sería muy lento, y por lo tanto, ineficiente para poder realizar las actividades deseadas. La **Tabla 3.1** proporciona un resumen de las diversas unidades de ancho de banda.

Tabla 3.1. Unidades de ancho de banda

Unidad que indica el ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps
Kilobits por segundo	Kbps	1 Kbps = 1 000 bps
Megabits por segundo	Mbps	1 Mbps = 1 000 000 bps
Gigabits por segundo	Gbps	1 Gbps = 1 000 000 000 bps

En el Instituto Hospitalario que se trata en esta propuesta, el ancho de banda que se maneja es el de una red Gigabit Ethernet, también conocida como GigaE, la cual proporciona una capacidad de transmisión de 1 Gigabit por segundo, correspondiente a unos 1000 megabits por segundo de rendimiento.

El contar con este ancho de banda resulta ser de gran beneficio para el Instituto en general, ya que actualmente la necesidad de contar con mayor capacidad para transmitir más y más información ha ido en aumento; ya sea porque cada día existen mayores facilidades para que las personas cuenten con servicio de Internet, o porque las empresas e instituciones hacen uso de nuevas tecnologías que les permiten tener un crecimiento superior.

Los esquemas tradicionales de los servicios han evolucionado y ahora se requiere mayor ancho de banda o capacidad en ambos sentidos de transmisión, es decir, la velocidad con la que lo datos pueden ser transferidos de un servidor a un cliente (*downstream*), así como la velocidad a la que se transfieren de cliente a servidor (*upstream*); tal es el caso de Internet. Las nuevas aplicaciones requieren de altas velocidades no solo para la descarga de

información, sino también para los datos que los clientes envían a través de la red.

Lo que es evidente, es que el ancho de banda muchas veces parece insuficiente, ya que el empleo de este recurso es cada día más necesario dado que los servidores y las nuevas aplicaciones empresariales demandan mayor capacidad. Así pues, es imprescindible que cada institución plantee cómo administrar de una mejor manera el ancho de banda disponible, para evitar en la medida de lo posible los inconvenientes de no tener caudal suficiente por el cual transmitir toda la información, sobre todo si la organización se encuentra en plena expansión y se necesitan utilizar nuevas aplicaciones que van a consumir más recursos, por la integración de nuevo personal, adquisición de nuevo equipo, etc.

Las redes virtuales resuelven este problema. Un dominio de broadcast en una buena implementación de red virtual puede desplegarse a un edificio, campus o ciudad, de tal manera que la necesidad de enrutamiento sea minimizada y el tráfico en la red sea mucho más rápido.

La función de las VLANs en el Instituto Hospitalario es restringir los broadcast a los dominios lógicos donde han sido generados.

Pero, independientemente de qué herramientas usar, hay puntos que no deben perderse de vista al momento de afrontar un aspecto crítico como es el ancho de banda del que se dispone. Aunque parezca obvio, al establecer normas en cuanto a este tema, siempre se tienen que tomar en cuenta las necesidades específicas de cada departamento, así como las de los individuos que los componen. Por lo tanto, es importante abordar la asignación de prioridades, que permitan anteponer unos recursos frente a otros, sin afectar las actividades realizadas por las diferentes áreas de trabajo.

Para lograr lo anterior se debe estudiar a fondo cuáles son las necesidades reales de tráfico de la institución y realizar una jerarquía de cada tipo de tráfico en importancia.

3.2 Distribución de VLANs en las áreas del Instituto Hospitalario.

En el Instituto Hospitalario existen diversos departamentos enfocados ya sea a la atención médica, educación, investigación, administración, comunicación, planeación, etc. Sin embargo, cada uno de dichos departamentos se encuentra ubicado en diferentes áreas del Instituto.

El Instituto Hospitalario se divide fisicamente en las siguientes áreas:

- Hospitalización
- Urgencias
- Rehabilitación/Ortopedia
- Toma de productos
- Planeación
- Residencia médica
- Administración
- Torre de investigación
- Archivo general
- Banco de Sangre
- Publicaciones
- Casa de máquinas
- Transportes

En la **Figura III.1** se presenta un plano visto desde arriba (azoteas) en el cual se pueden observar las áreas antes mencionadas, que son todas con las que cuenta el Instituto Hospitalario.

Sin embargo, en la **Figura III.2** se muestran más a detalle las divisiones con las que cuenta cada área, el caso mostrado en esta imagen representa la planta baja general, que como se puede observar, al ser un número considerable de subdivisiones, es evidente que la cantidad de usuarios que las ocupan también es abundante. Cada una de estas áreas cuenta con usuarios pertenecientes a diferentes departamentos los cuales son asignados a VLANs específicas.

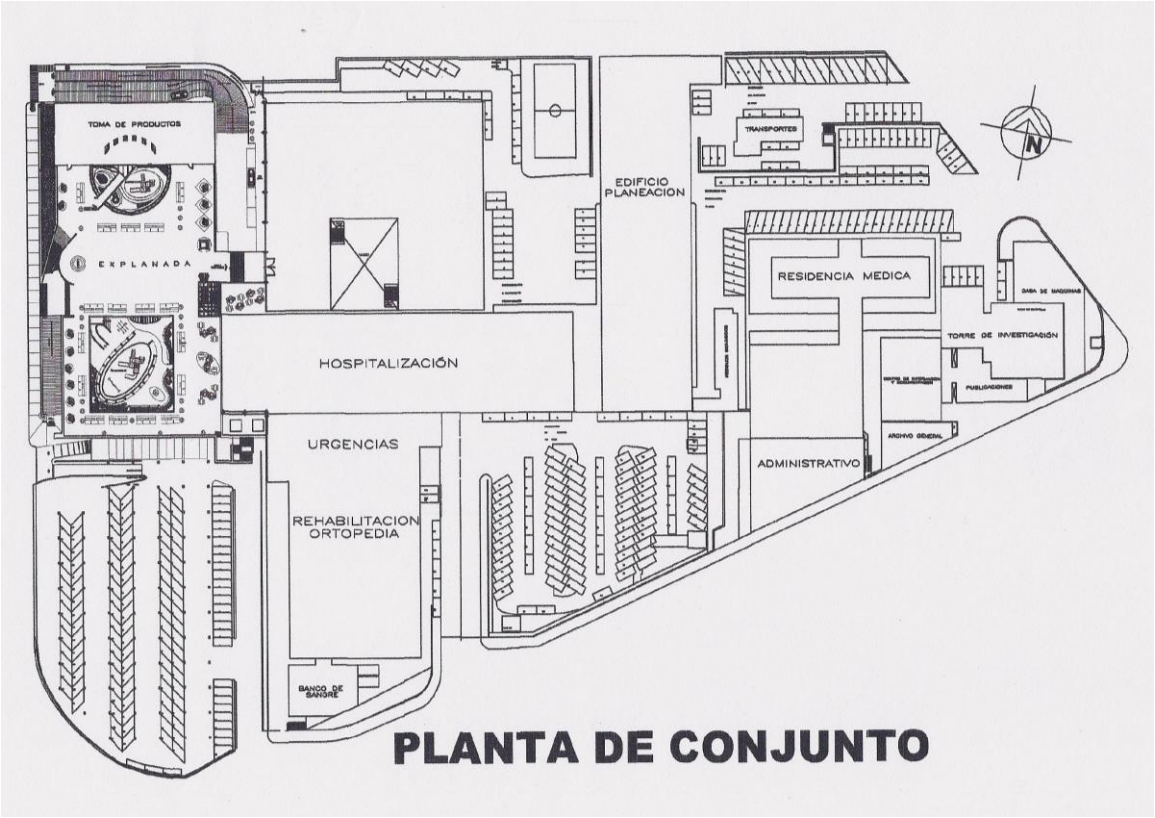


Figura III.1 Planta de conjunto del Instituto Hospitalario

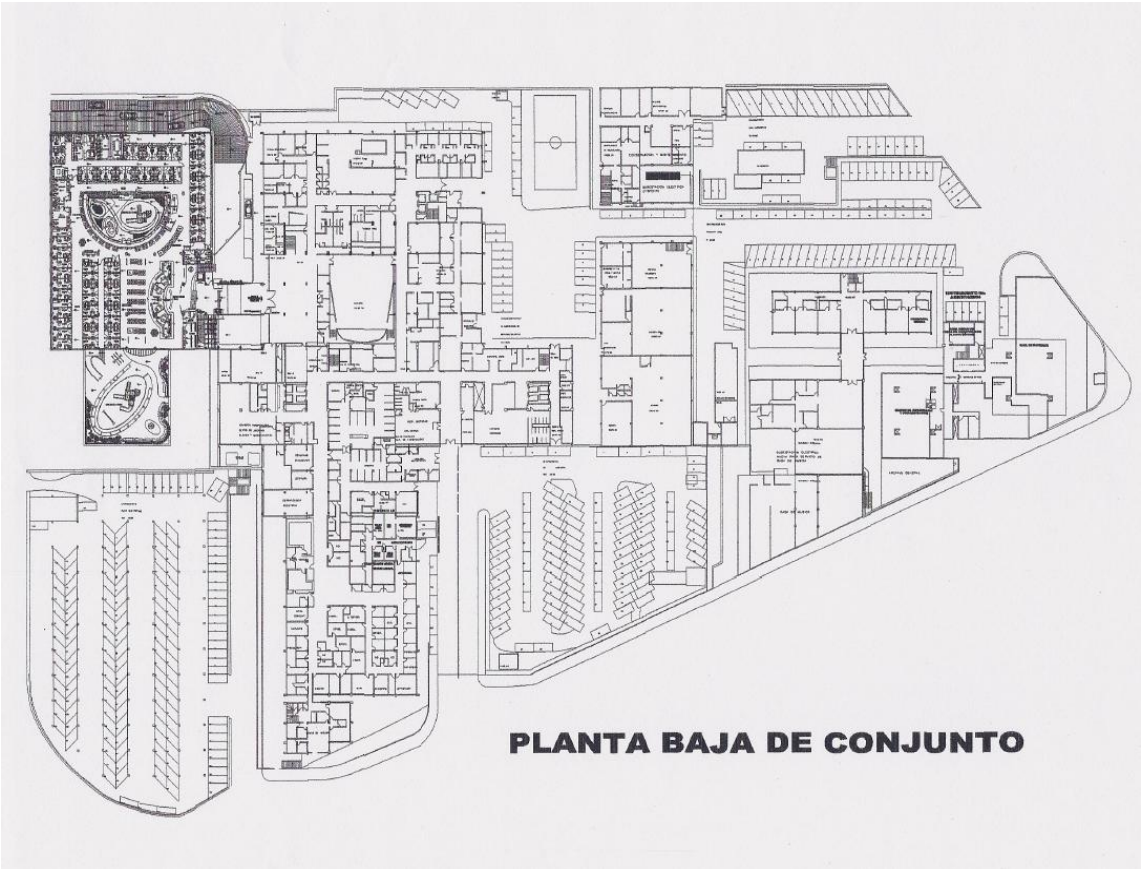


Figura III.2 Planta baja de conjunto del Instituto Hospitalario

En el Instituto Hospitalario se encuentran implementadas 9 VLANs, cada una identificada por un ID. La **Tabla 3.2** muestra los IDs y nombres de dichas redes virtuales.

Tabla 3.2. VLANs en el Instituto Hospitalario

VLAN	VLAN Nombre
1	Default_VLAN
2	Sistemas
3	Meds
4	InUn
5	Rx-Lab
6	InSalud
7	Maxc
8	IN
9	Pacs

La VLAN 1, "Default_VLAN" es una red virtual que se encuentra predefinida en todos los switches que cuentan con esta tecnología; y en ella se encuentran agregados todos los puertos del dispositivo. A medida que se crean nuevas VLAN y los puertos son asignados a las mismas, éstos serán desconectados de la Default_VLAN.

La VLAN creada para sistemas, es la asignada precisamente, como su nombre lo indica a los sistemas que se emplean en el Instituto Hospitalario, generalmente éstos se enfocan a la administración de recursos financieros, farmacéuticos, mantenimiento, registro de personal e investigación; muchos de los cuales son creados por los programadores de sistemas dentro del Instituto; sin embargo, también se manejan algunos pertenecientes a proveedores externos a la organización. Los usuarios que emplean esta VLAN se encuentran ubicados en diferentes áreas del hospital, como son: torre de investigación, toma de productos, administración, archivo general, etc.

Meds es una VLAN creada exclusivamente para el uso de un solo sistema, el cual consiste en llevar la historia clínica de cada uno de los pacientes que acuden al Instituto, es por ello, que al ser un gran número de personas las

que se registran y asisten diariamente al hospital, existe una VLAN enfocada únicamente para dicho tráfico.

Las VLANs 4,6 y 7, que son InUn, InSalud y Maxc respectivamente, son redes virtuales que proveen servicio de red a los diversos usuarios que laboran en el Instituto, ya sea para consultas de investigación, correos, contacto con otras organizaciones, información de los sistemas, etc. En este caso, los usuarios también se encuentran en distintos edificios, pero al ser considerable la cantidad de personas que requieren el servicio de internet, dicho recurso es repartido entre las 3 VLANs mencionadas.

La VLAN 5, Rx-lab, se encarga de administrar y proveer información entre los usuarios que se encuentran asignados a ella , los cuales son principalmente médicos y/o enfermeras, que hacen uso de rayos "X", ecocardiografías, ecocardiogramas, ultrasonidos etc.

IN es una VLAN con la cual se están llevando a cabo diversas pruebas, las cuales consisten en reunir todos los segmentos de red del Instituto en una sola red, y así asignar a todos los usuarios IP's dinámicas, para ser administradas en servidores DHCP.

La VLAN 9 "PACS" es un sistema otorgado por proveedores externos, que consiste en lo último en tecnología para sustituir el uso de radiografías impresas en placas o películas fotográficas. En lugar de analizar las radiografías como se conocen comúnmente, se guardan directamente en un equipo que se encarga únicamente de almacenar las mismas, pero de manera digital, permitiendo realizar un análisis con mayor exactitud y profundidad.

Cuando se comenzó a utilizar esta tecnología en el Instituto (principios de 2009), fue muy difícil para los médicos acostumbrarse a ella, y en diversas ocasiones muchos de ellos se negaban a emplearla, sin embargo, observando las facilidades que puede otorgar, y el avance científico comparado con las antiguas radiografías, su utilidad es totalmente favorable, eficaz y agradable para los usuarios. En la **Figura III.3** puede observarse un ejemplo de dicha

tecnología, en donde un médico analiza estudios en una plataforma de este tipo.

Figura III.3 PACS Plataforma para médicos

Una vez que se ha explicado la asignación de cada VLAN, es necesario aclarar de qué manera se lleva a cabo la conectividad entre ellas. Lo cual se trata en el siguiente punto.

3.3 Tipos de conectividad entre VLANs

En general, cuando una institución hace uso de la tecnología de redes virtuales, es necesario que los dispositivos de los usuarios alcancen los host que no son locales. De la misma forma es evidente, como ya se ha mencionado, que no todos los usuarios se encuentran ubicados en la misma área de trabajo, y por ello dependiendo de las funciones que realicen son asignados a una VLAN específica, por lo tanto, también se requiere que los host pertenecientes a diferentes VLANs puedan comunicarse entre sí.

La conectividad entre VLANs se clasifica en dos tipos:

1. Conectividad lógica.
2. Conectividad física.

La conectividad lógica involucra una conexión única, o un enlace troncal desde el switch hasta el router, dicho enlace admite la implementación de diversas VLANs. Esta topología es también denominada "router en palo" porque existe una sola conexión al router. Sin embargo, hay también diversas conexiones lógicas entre el router y el switch.

De esta manera el tráfico que viaja a través de las diferentes VLANs atraviesa un backbone de capa 2, lo que le permite llegar al router; una vez que esto sucede, el tráfico podrá desplazarse entre las múltiples redes virtuales, por supuesto, este funcionamiento tiene que ver con el protocolo 802.1Q del cual se hablo a detalle en el capítulo anterior, sin embargo se presenta aquí de una manera gráfica para un mejor entendimiento. Posteriormente, el tráfico viaja de vuelta hacia la estación final utilizando el método de envío de capa 2 normal. En la **Figura III.4** se ejemplifica este tipo de conectividad.

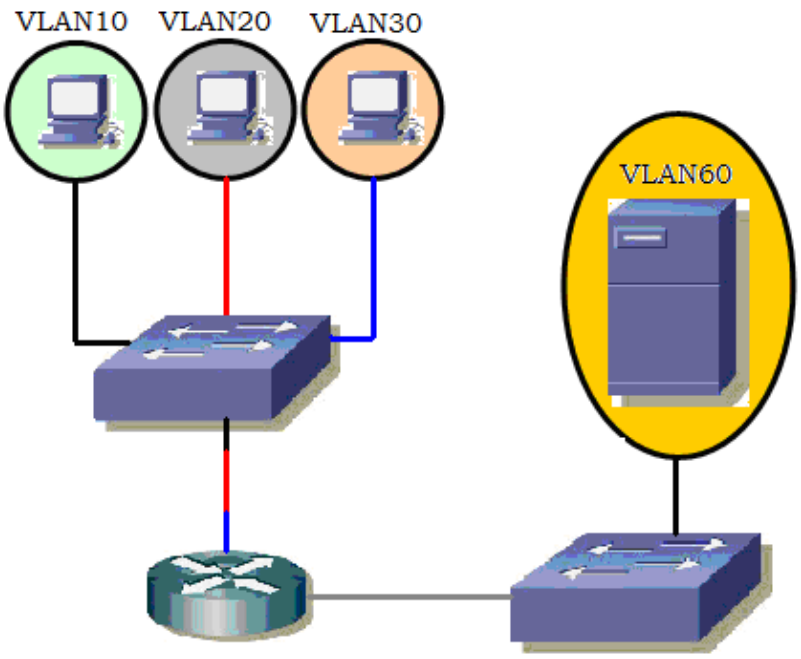


Figura III.4 Un enlace troncal puede admitir varias VLANs

Por otro lado la conectividad física, como su nombre lo indica, implica una conexión física para cada VLAN que se tenga implementada, lo que significa que el número de interfaces físicas debe ser igual al número de VLANs con las que se cuente. Por ejemplo una red con cuatro VLANs requeriría cuatro conexiones físicas entre el switch y el router externo, esto puede visualizarse en la Figura **III.5.**

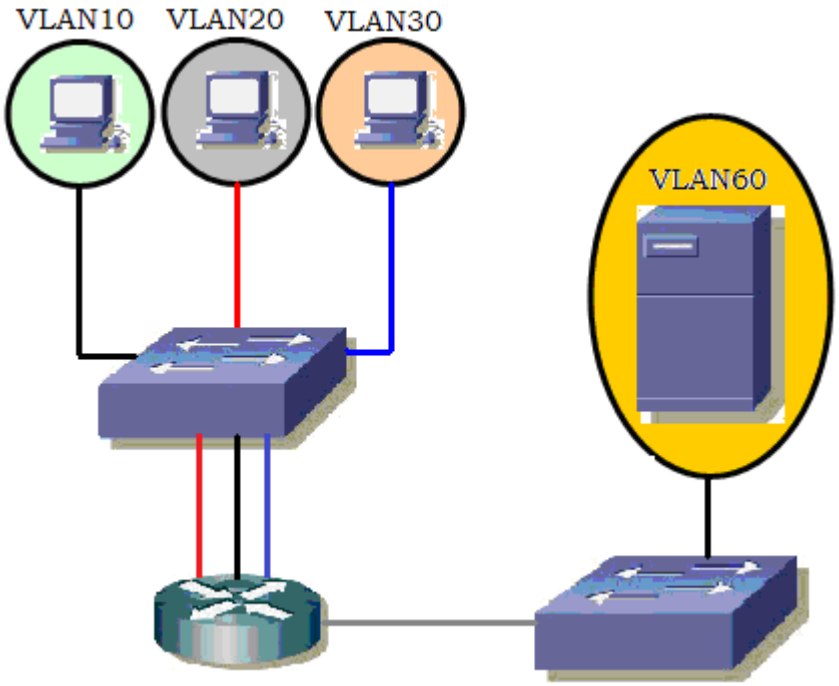


Figura III.5 Se admite una VLAN por interfaz.

Por lo tanto, es conveniente que redes que cuentan con muchas VLANs utilicen enlaces troncales, para asignar más de una red virtual a una sola interfaz de router, el cual podrá admitir varias interfaces lógicas en enlaces físicos individuales.

Lo anterior ayuda a reducir la cantidad de puertos a utilizar, tanto de los routers, como de los switches empleados; y por consiguiente es posible un ahorro en lo que respecta a costos, así como la disminución en la complejidad de la configuración.

3.4 Enrutamiento de VLANs

En un entorno VLAN, los paquetes se conmutan únicamente entre puertos designados para residir en el mismo dominio de broadcast. Las VLANs llevan a cabo peticiones en la red y separación de tráfico en la capa 2. Por consiguiente, la comunicación entre VLANs no puede tener lugar sin un dispositivo de capa 3, como un router, responsable de establecer comunicación entre distintos dominios de difusión.

De manera predeterminada, los usuarios asignados a redes virtuales no podrían comunicarse. Existe únicamente una manera para que éstos puedan hacerlo: El enrutamiento entre VLANs.

Se define al enrutamiento entre VLANs como el proceso que permite reenviar el tráfico de la red desde una VLAN a otra, haciendo uso de un router.

Para llevar a cabo funciones de enrutamiento entre las redes virtuales, deben de considerarse las siguientes circunstancias:

- El router debe de contar con la tecnología necesaria para llegar a todas las VLANs interconectadas, y de esta forma determinar cuáles son los dispositivos finales, incluyendo las redes que están conectadas a alguna VLAN. Cada dispositivo final debe estar dirigido con una dirección IP.
- Todos los routers empleados deben conocer la ruta hasta cada red LAN destino. El dispositivo, una vez configurado, cuenta con la información referente a las redes que se encuentran conectadas directamente, lo que le permite aprender las rutas hacia las redes que por el contrario, no están conectadas de esa forma.
- Debe existir una conexión física en el router para cada VLAN, o en el mejor de los casos, y dependiendo del número de VLANs configuradas, se debe tener una conexión lógica, habilitando un enlace troncal en una conexión física individual.

Las VLANs están asociadas a subredes IP únicas en la red. Esta configuración de subred facilita el proceso de enrutamiento en un entorno de múltiples VLANs.

Cuando se utiliza un router para facilitar el enrutamiento entre las diferentes redes virtuales, las interfaces del mismo pueden conectarse a VLANs separadas. Los dispositivos en dichas VLANs envían el tráfico a través del router hasta llegar a las otras redes.

Por ejemplo en la **Figura III.6** se muestra como el tráfico de la PC1 en la VLAN 10 está enrutado por medio del router R1 para llegar a PC3 en la VLAN 30.

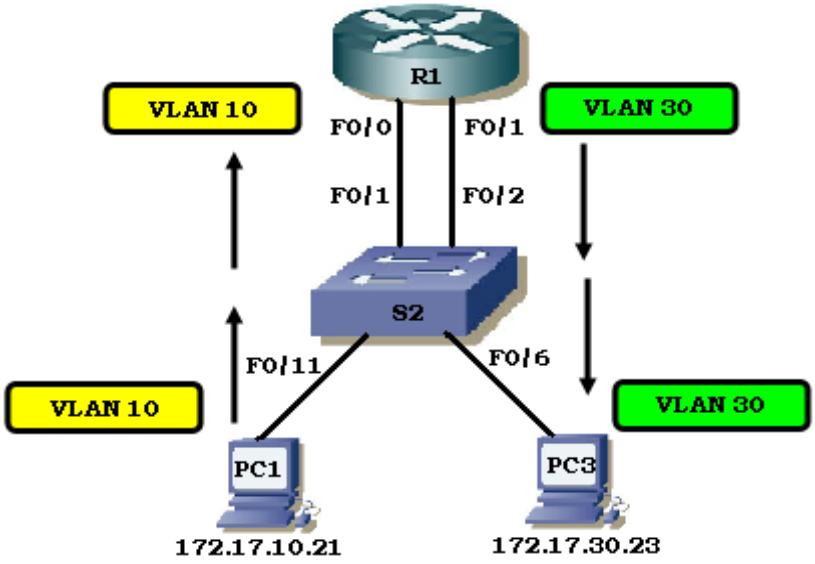


Figura III.6 Enrutamiento entre 2 VLANs

El enrutamiento entre VLANs requiere de múltiples interfaces físicas en los routers y switches.

Sin embargo no todas las configuraciones del enrutamiento entre VLANs requieren de diversas interfaces físicas; ya que hoy en día existe software que ya viene incluido en algunos routers, el cual permite configurar interfaces del dispositivo como enlaces troncales. Esto abre nuevas posibilidades para el enrutamiento a través de VLANs.

Existen también las llamadas subinterfaces, que son múltiples interfaces virtuales asociadas a una interfaz física, las cuales se encuentran configuradas de manera independiente en el router, con una asignación de VLAN y dirección IP, para funcionar en una red específica.

Las subinterfaces están configuradas en diferentes subredes que corresponden a la VLAN estipulada a cada una de ellas, esto facilita el enrutamiento lógico, antes de que la VLAN etiquete las tramas de datos y las reenvíe por la interfaz física.

Algunos switches pueden realizar funciones de capa 3, lo que reemplaza la necesidad de utilizar routers dedicados a realizar el enrutamiento básico en una red, tal es el caso de los switches multicapa.

En cuanto al aspecto económico, resulta menos costoso utilizar subinterfaces, en lugar de interfaces físicas separadas. Por lo tanto si se tuviera un router con un número considerable de interfaces físicas, esto provocaría que cada una de ellas requiriera la conexión a un puerto del switch por separado, lo cual evidentemente se reflejaría en el uso de una mayor cantidad de puertos físicos del dispositivo en cuestión, que bien podrían ser considerados puertos adicionales para ser usados en caso de que se llegue a generar algún cambio importante en la red, o para ocuparlos en la realización de pruebas.

Los puertos de un switch resultan ser un recurso costoso, especialmente en switches de alto rendimiento, como es el caso de algunos utilizados en el Instituto Hospitalario.

El uso de subinterfaces para llevar a cabo el enrutamiento entre VLANs tiene como resultado una configuración física menos compleja que en el caso del uso de interfaces físicas separadas. Esto se debe a que la cantidad de cables que interconectan los switches y routers es menor.

Al disminuir el número de cables empleados, es posible evitar problemas de ubicación y conexiones pertenecientes a enlaces y puertos en un switch determinado.

En la **Tabla 3.3** se muestra una comparación entre una interfaz y una subinterfaz en un router.

Tabla 3.3. Comparación entre interfaz y subinterfaz de un router

Interfaz física	Sub-interfaz
Una interfaz física por VLAN	Una sola interfaz física para múltiples VLANs
No existe contención de ancho de banda	Contención de ancho de banda
Conectado para acceder a través de determinado puerto de un switch	Conectado para establecer un enlace troncal
Más costoso	Menos costoso
Configuración de la conexión física más compleja	Configuración de la conexión física menos compleja

Dado que generalmente las VLANs en el Instituto son interconectadas mediante enlaces troncales en un enlace físico único, resulta más fácil resolver el problema de las conexiones físicas.

IV.

Administración y Configuración de VLANs del Instituto Hospitalario

Con base en lo mencionado a lo largo de los capítulos anteriores, como tipos de redes virtuales, ancho de banda utilizado, conectividad entre VLANs etc., en la **Tabla 4.1** se muestra un listado de las diferentes opciones a considerar en la implementación de VLANs, así como las más adecuadas para el uso de dicho tipo de redes en el Instituto Hospitalario.

Tabla 4.1. Opciones de implementación de VLAN

Opciones para la implementación de una VLAN		Opción implementada en el Instituto Hospitalario
Tipos de VLANs	Por puerto, estática, por dirección MAC, por direcciones IP, por nombre de usuario, dinámicas, de capa 3, basadas en reglas, por DHCP	El tipo de VLANs que se configura en los equipos es por puerto, ya que resulta mucho más fácil llevar una administración y control respecto a la pertenencia de cada uno de los puertos a una red virtual en específico. Además en estas VLANs es posible el uso de servidores DHCP, los cuales permiten la asignación de IPs automáticas.
Uso de grupos virtuales en VLANs	VLAN inhabilitada VLAN habilitada con una sola etiqueta VLAN ID VLAN habilitada con etiquetas VLAN ID diferentes VLAN habilitada con o sin etiquetas	En este caso las VLANs se encuentran habilitadas con etiquetas VLAN ID diferentes, puesto que en la configuración que se lleva a cabo en los equipos siempre se asigna un ID distinto a las redes virtuales, para así poder identificar más fácilmente a cada una de ellas.
Ancho de banda utilizado	Bits por segundo Kilobits por segundo Megabits por segundo Gigabits por segundo	El ancho de banda empleado en el Instituto es el correspondiente al de una red con la mejor tecnología, es decir, se trata de una red Gigabit (1000 Mb/s). Esto permite una capacidad de transmisión lo suficientemente buena para el desempeño de las actividades en el Hospital
Tipo de conectividad entre VLANs	Conectividad lógica Conectividad física	Para dar un mejor aprovechamiento a los recursos de red con los que se cuentan, es importante considerar el número de VLANs que se desean implementar en el Instituto, por lo tanto es más conveniente realizar una conexión lógica

4.1 Creación de una VLAN

Como se mencionó en el Capítulo 2, existen diversas herramientas que facilitan el manejo de VLANs. El primer paso para poder iniciar una interacción entre la red virtual, el dispositivo y el administrador es evidentemente que la VLAN exista.

La creación de una VLAN dentro de un dispositivo que soporte esta tecnología, dependerá de las características del mismo, por ejemplo, la marca; en general, en el Instituto se utilizan switches Cisco, 3Com, conmutadores como el Allied Telesyn AT 8024M, etc. Sin embargo, los pasos a seguir en cada uno de ellos son en general muy similares.

A continuación se presenta el procedimiento a seguir para la creación de una VLAN en un switch 3Com. La manipulación de redes virtuales para este ejemplo se lleva a cabo vía Web, se muestra también la manera en que inicialmente el switch solicita un nombre de usuario y una contraseña.

En primer lugar, para poder acceder a través de la red a la interfaz del switch, es necesario contar con uno o más de los siguientes elementos:

- Cable de consola del switch.
- Aplicación para la detección del switch 3Com, la cual se encuentra incluida en el CD-ROM que se suministra al adquirir el switch, al igual que el cable de consola.
- Una computadora que esté conectada al switch, y que cuente con un navegador Web, lógicamente con acceso a Internet.

Adicional a los elementos anteriores, es indispensable conocer la dirección IP del switch asignada por el administrador a través del servidor DHCP.

Para ver dicha IP, se tiene que conectar el cable desde el puerto de consola del switch, que en este caso se localiza en la parte frontal del dispositivo, como se ilustra en la **Figura IV.1**, al puerto COM de la computadora, y

posteriormente se debe establecer una sesión en HyperTerminal o vía Web, cuya ejecución solicita un nombre de usuario y una contraseña, **Figura IV.2**.

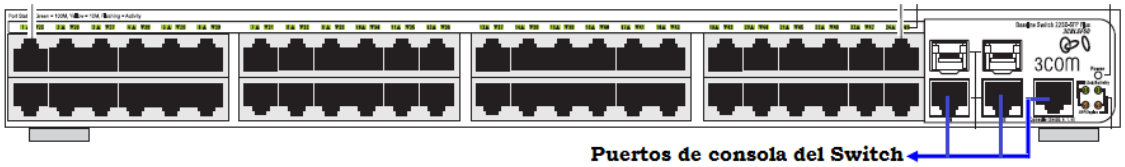


Figura IV.1. Panel Frontal de Switch 3Com Baseline 2226-SFP Plus

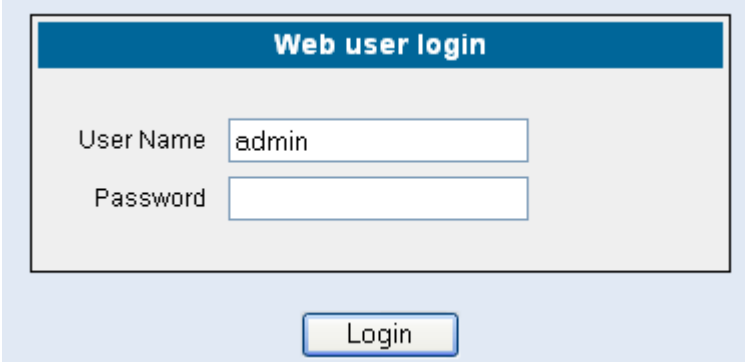


Figura IV.2. Solicitud de usuario y contraseña

Una vez realizado lo anterior, aparece un menú en donde se selecciona la opción *Summary*, la cual despliega información referente al equipo, entre la que se incluye:

- Dirección IP
- Máscara de subred y
- Puerta de enlace predeterminada.

El switch tarda un máximo de 2 minutos para obtener la IP; como ésta ha sido dada de alta en el DHCP, todas las direcciones anteriores se presentan rápidamente, **Figura IV.3**.

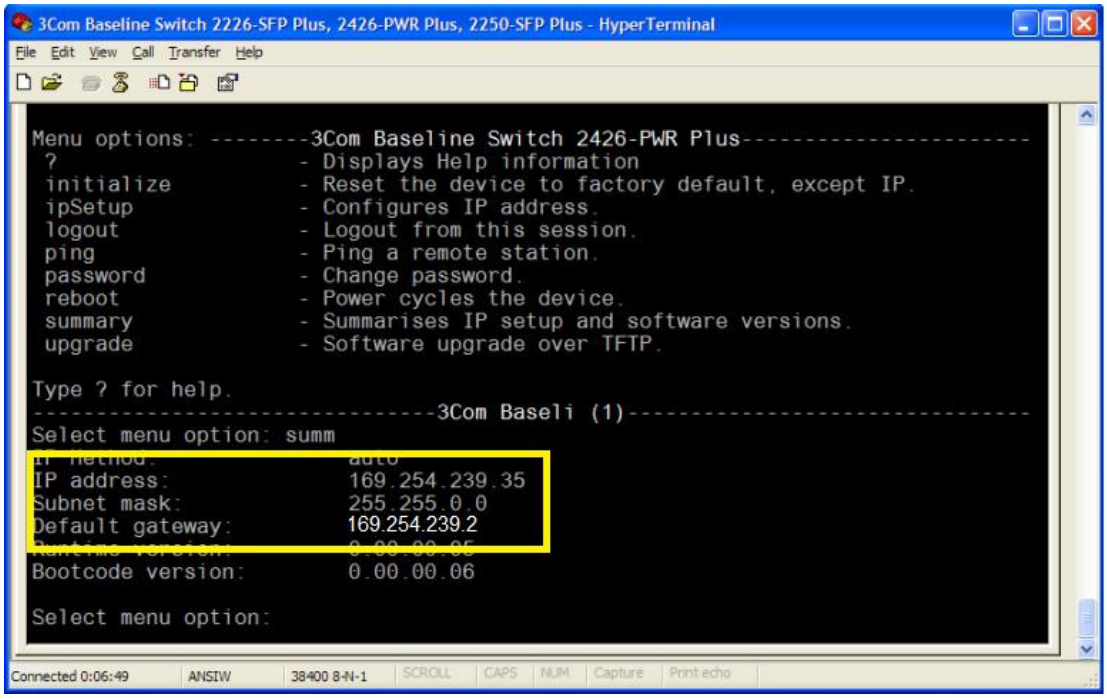


Figura IV.3 Direcciones tomadas automáticamente por el switch

La IP que aparece en la interfaz, es la que se toma en cuenta para el acceso al switch vía Web. De existir algún problema con la asignación de IP, la dirección puede ser establecida manualmente, **Figura IV.4**.

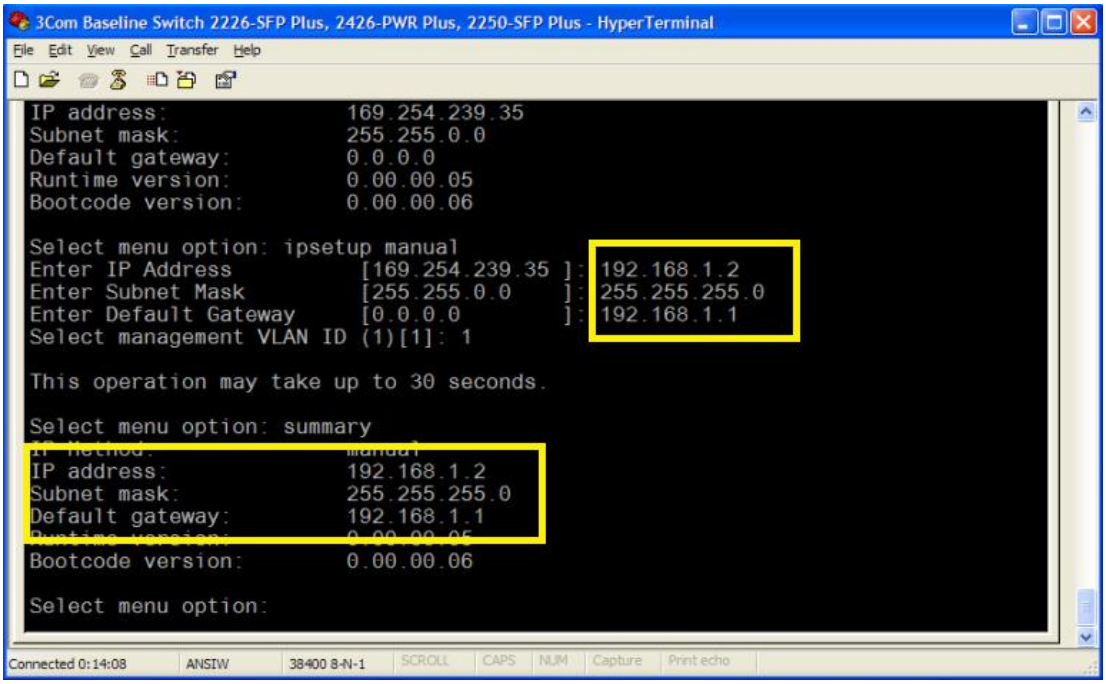


Figura IV.4 Configuración manual

Una vez conocidas las direcciones correspondientes al switch, se procede a teclear la IP en el buscador Web, nuevamente se solicita el usuario y la contraseña, al ingresar los datos es posible entrar a la interfaz del switch como se observa en la **Figura IV.5**.

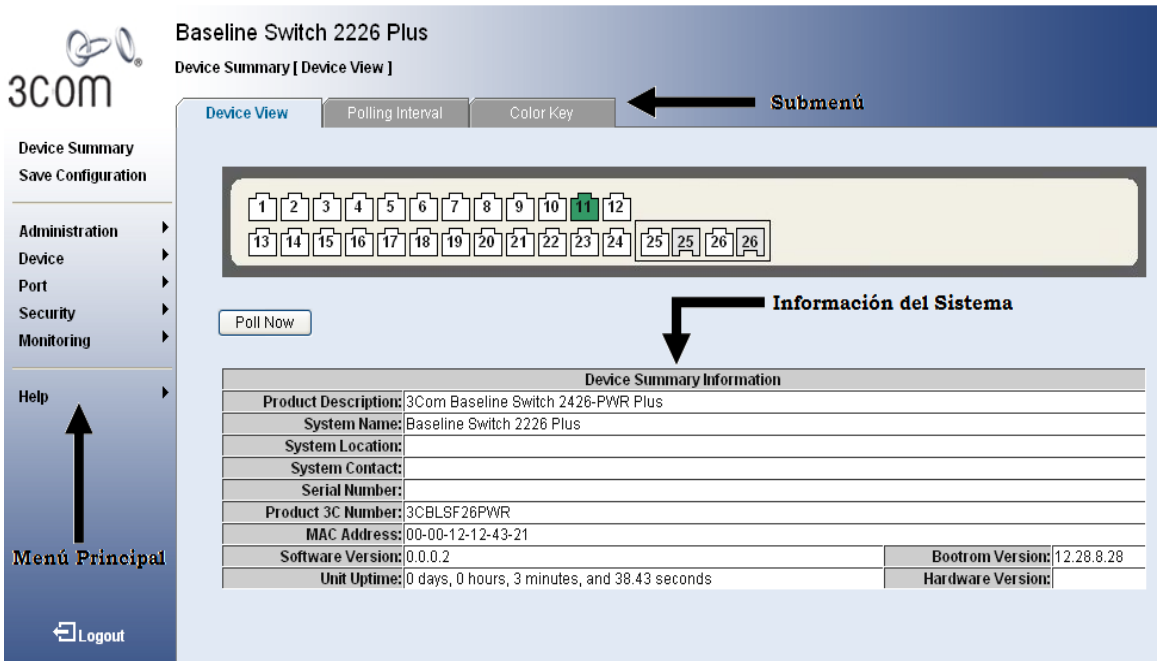


Figura IV.5 Interfaz del switch

Dentro del menú principal, se encuentra la opción *Device*, la cual cuenta con las siguientes opciones:

- VLAN
- Spanning Tree
- IGMP Snooping and Query
- Broadcast Storm
- QoS
- PoE

La opción de interés en esta propuesta es la de *VLAN*, que a su vez contiene el menú:

- Setup
- Modify VLAN
- Modify Port

- Rename
- Remove
- Port Detail
- VLAN Detail

Hasta este punto lo que se desea es dar a conocer la manera en que se crea una red virtual. Este proceso no consiste únicamente en dar un nombre a la red y en asignarle un identificador, existen diversos aspectos que deben tomarse en cuenta al momento de originar una VLAN, algunos de ellos se describen a continuación.

Para crear una VLAN, se accede a *Setup,* tal como se señala en la **Figura IV.6**, donde simplemente se introduce el ID que identificará a la red, y se da click en la pestaña *crear.*

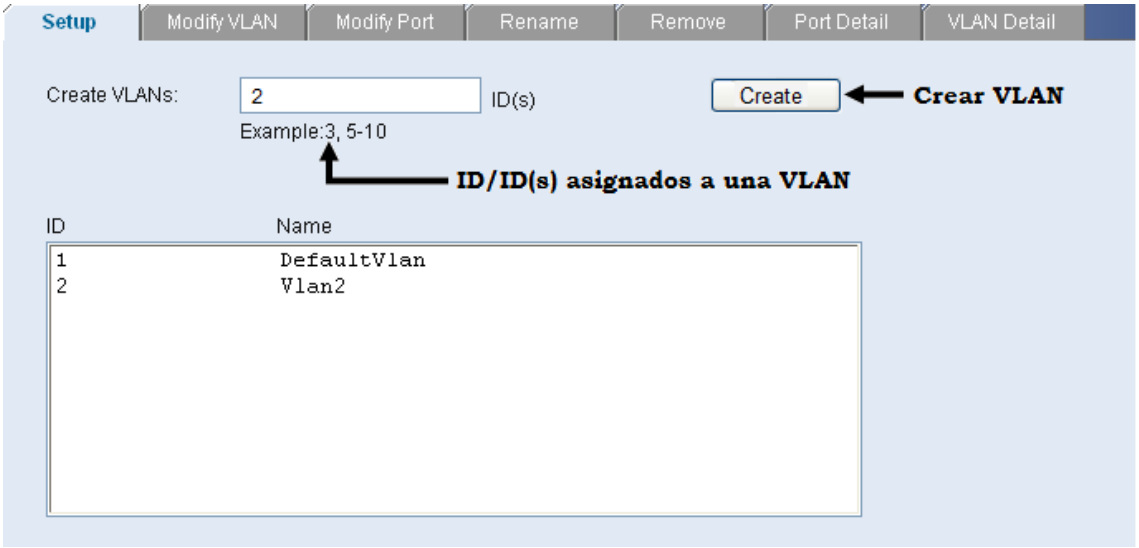


Figura IV.6 Creación de una VLAN

Las VLANs son generadas una a una o por rangos, es decir, es posible crear de la VLAN 2 a la 5 al mismo tiempo, y éstas aparecen en orden según el VLAN ID asignado.

Modify VLAN determina qué puertos pertenecen a una VLAN en específico, y la manera en que éstos son configurados inicialmente, ya sea como miembros *tagged* ó *untagged*. **Figura IV.7**

Cuando un switch no ha sido configurado, todos los puertos pertenecen a la VLAN configurada por default en el dispositivo. Como se observa en la imagen.

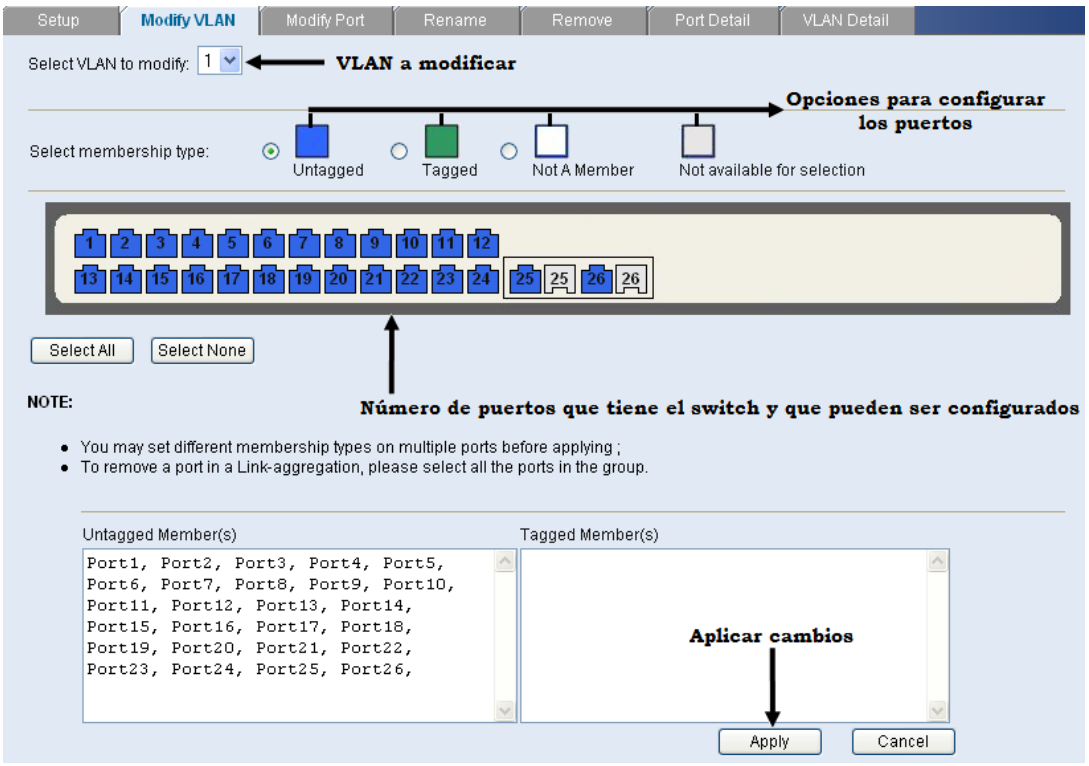


Figura IV.7 Modificar VLAN

Los puertos se configuran de acuerdo a las necesidades que la red local presente, para ello existe dentro del menú VLAN un apartado destinado a su modificación, denominado *Modify Port*, con las características que se muestran en la **Figura IV.8**.

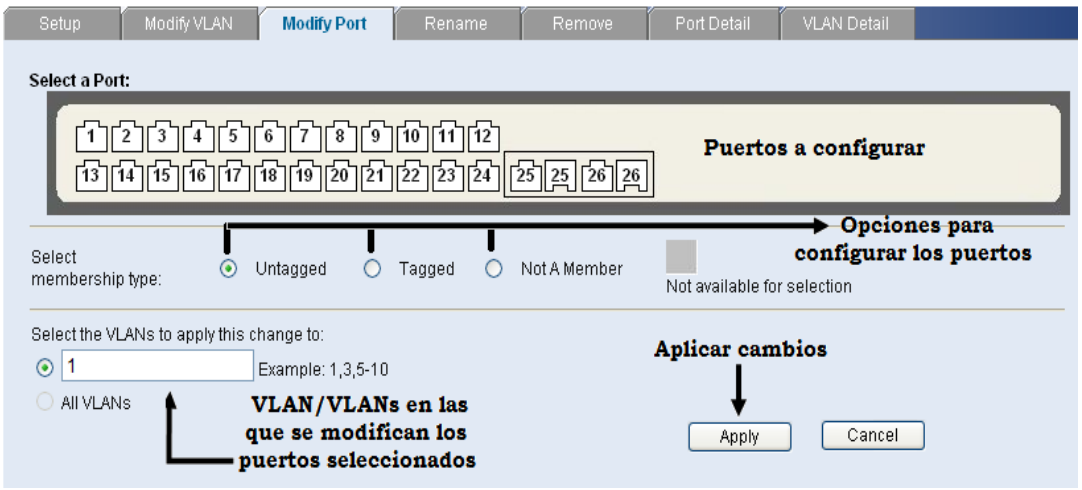


Figura IV.8 Modificar puerto

Aunque a cada VLAN se le asigna un ID diferente, es recomendable renombrar cada una de ellas, a través de la opción *Rename* **Figura IV.9**.

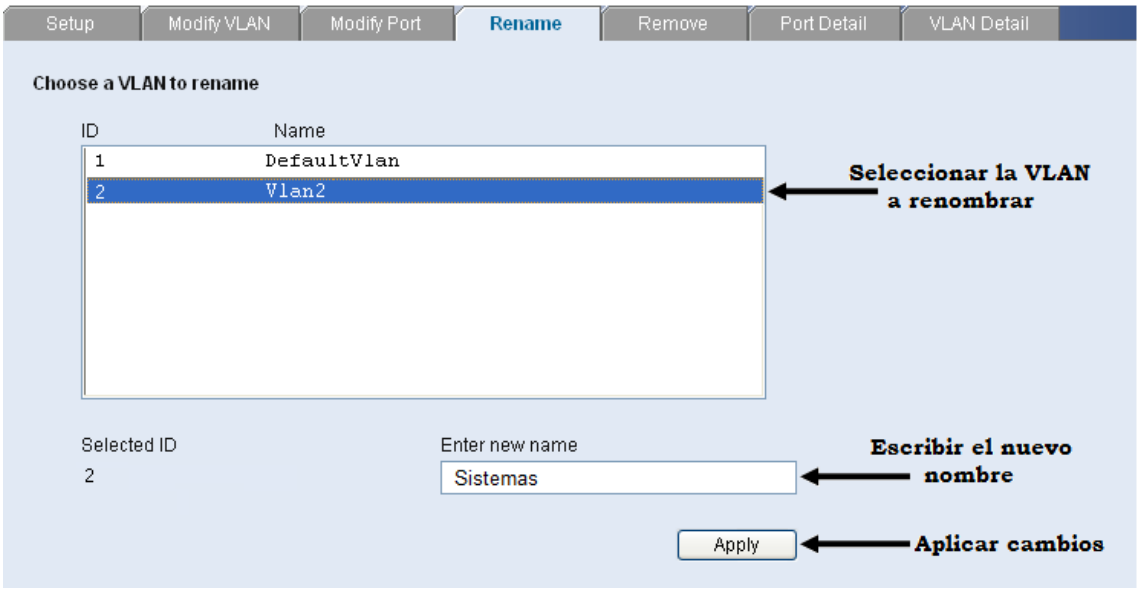


Figura IV.9 Renombrar VLAN

Por otra parte, la sección *Remove,* como su nombre lo indica, se utiliza para llevar a cabo la eliminación de alguna VLAN. Puede seleccionarse una o varias VLANs si así se desea. En la Figura **IV.10** se muestra un ejemplo donde se elige solo una red para ser removida.

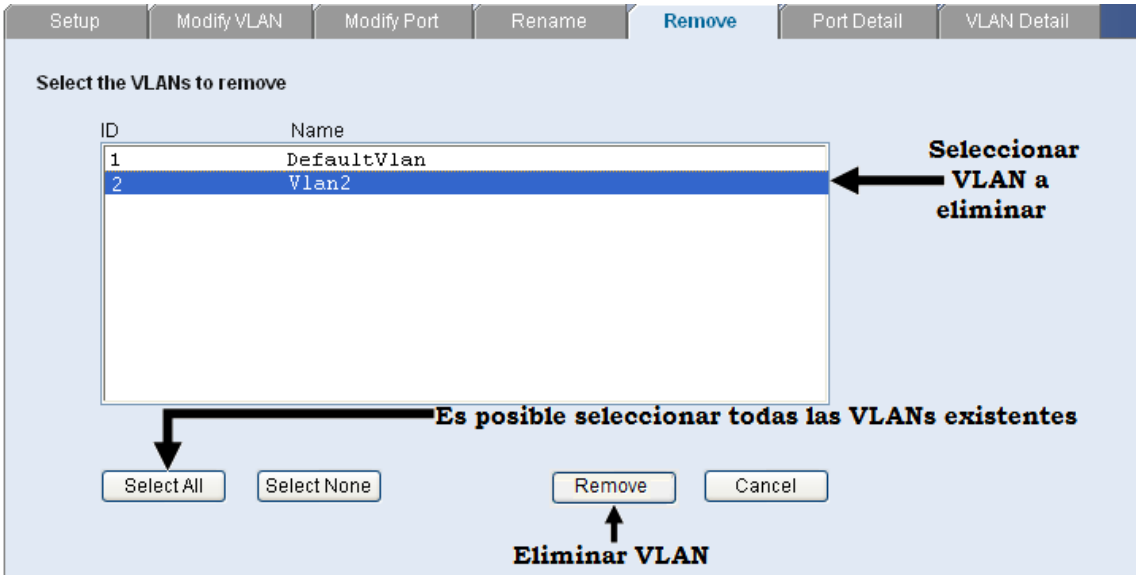


Figura IV.10 Eliminar una VLAN

Previo a suprimir cualquiera de las redes virtuales, es importante verificar que todos los puertos que pertenezcan a alguna de ellas sean removidos antes de proceder a borrar la VLAN.

Una de las ventajas que conlleva el manejo de redes virtuales vía Web, es que es posible observar las características de los puertos asignados a cada una, clasificándolos de acuerdo a su configuración, **Figura IV.11**

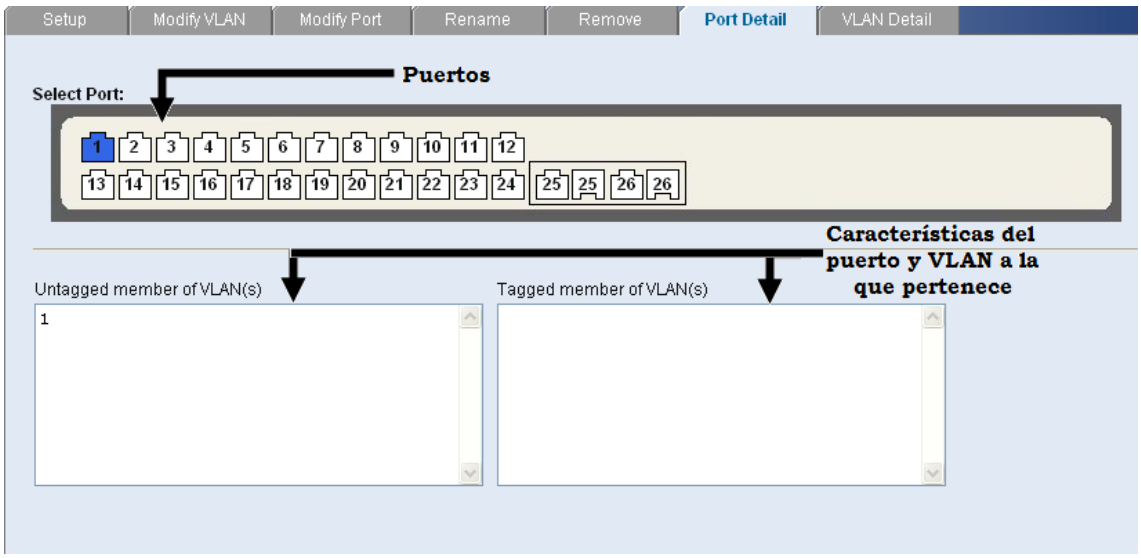


Figura IV.11 Detalles de puertos

También es posible conocer las propiedades de las redes virtuales accediendo a la pestañan de *VLAN Detail*. Un ejemplo de esta sección se muestra a continuación en la **Figura IV.12**.

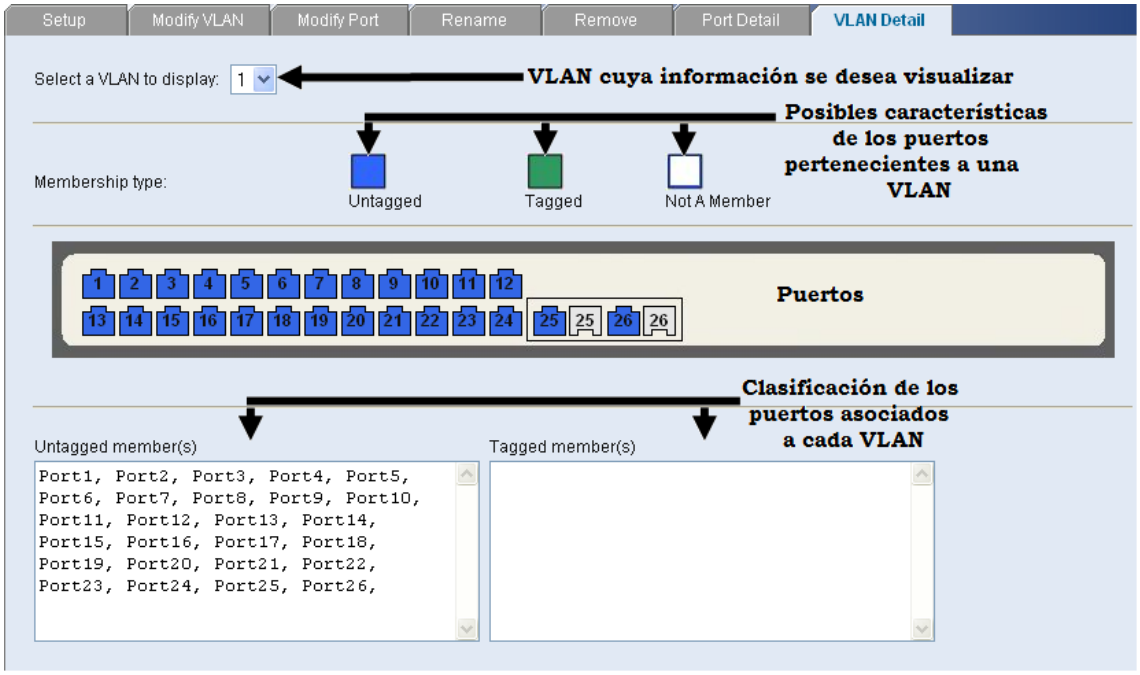


Figura IV.12 Detalles de VLAN

Una vez que se ha entendido todo lo que conlleva la creación de una VLAN, es mucho más fácil comprender la manera en que éstas se administran.

4.2 Administración de VLANs

Existen diversos aspectos que deben de tomarse en cuenta respecto a la administración de redes virtuales, por ejemplo:

- Planificación de capacidades
  - Tamaño de las VLANs.
  - Número de VLANs.
  - Número de usuarios de cada VLAN.
  - Perfiles de tráfico.
  - Tamaño del dominio de ejecución del algoritmo STP (*Spanning Tree Protocol – Protocolo de Árbol de Expansión*)
- Seguridad
  - Aislar subredes de acuerdo a privacidad.
  - Ubicación de servidores en sitios seguros, etc.

A continuación se explica con más detalle en qué consiste el punto referente al tamaño de dominio de ejecución del algoritmo STP.

STP es un protocolo de capa 2 del modelo ISO/OSI que se basa en el estándar IEEE 802.1D. Sirve para detectar y desactivar loops que se originan debido a la repetición infinita de datos en redes que presentan dicha información y además permite solucionar el problema de múltiples caminos entre segmentos de datos.

La repetición de loops se presenta cuando existen numerosas rutas a seguir entre los servidores de una red, y pueden ocasionar diversos inconvenientes en la misma, por ejemplo:

- *Broadcast storms.* Los dispositivos que pertenecen a una red, generan tráfico broadcast, lo que provoca la degradación en el funcionamiento de la misma e incluso la pérdida total de operatividad, esto depende de la magnitud del broadcast storm.
- *Inestabilidad en la tabla de MAC Address*. Se sabe que un switch maneja una tabla de direcciones físicas y que cada una de ellas se encuentra relacionada a un puerto; la presencia de loops genera la posibilidad de llegar a una misma MAC por diferentes puertos, en este caso el switch no va a saber por cuál de ellos debe enviar un frame cuando lo recibe.
- *Transmisión múltiple de frames*. Debido a lo mencionado en el punto anterior, los paquetes son enviados más de una vez, y esto hace que el host final reciba una copia del mismo frame.
- *Numerosos loops.* Dependiendo de la topología de la red, se genera no solo uno, sino diversos loops, lo que complica las problemáticas mencionadas ante dicha redundancia cíclica.

Como ya se mencionó, STP implementa el algoritmo IEEE 802.1D, intercambiando mensajes de configuración BPDU (*Bridge Protocol Data Unit – Protocolo de Puente de Unidades de Datos*) entre switches para detectar loops, de esta manera, existe cierta comunicación entre los dispositivos, lo que

permite determinar las rutas que éstos deben seguir y conocer la información de identificación para que cada uno de ellos pueda bloquear los caminos.

Así mismo es posible la implementación de trayectos paralelos para el tráfico de la red y asegura que:

- Las rutas redundantes sean bloquedas (o deshabilitadas) cuando las principales son operacionales, es decir, se encuentren en pleno funcionamiento.
- Las rutas redundantes sean habilitadas si el camino principal presenta alguna falla.

Todos los conmutadores en la red reúnen información respecto a otros a través de mensajes de datos BPDU, que no son más que mensajes que se transmiten entre los switches que utilizan el protocolo STP. Estos intercambios de datos realizan los siguientes pasos:

1. Eligen un conmutador raíz.
2. Encuentran las posibles rutas hacia el conmutador raíz.
3. Determinan el camino con el menor costo hacia el dispositivo raíz, calculando la suma de todos los costos de cada puerto que tiene que pasar para llegar hasta dicho dispositivo.
4. Deshabilitan todos los demás caminos, es decir, los puertos de los conmutadores se ponen en estado de respaldo y esto permite que no haya ciclos en la red.

Los BPDU son intercambiados aproximadamente cada 2 segundos, lo que permite a los equipos estar constantemente actualizados respecto a cualquier modificación que se realice en la red, activando y desactivando los puertos según se requiera.

Cuando algún componente es asignado por primera vez a un puerto, dígase una computadora, impresora, servidor, etc., éste no comienza a reenviar los

datos inmediatamente, sino que sigue los pasos ya mencionados mientras procesa los BPDU y determina la topología de la red, sin embargo, después de un retraso de 30 segundos pasa a los modos de aprendizaje y escucha. En caso de que otro switch sea conectado, el puerto puede pasar a modo de bloqueo si es que se detecta que el dispositivo es capaz de provocar un loop en la red.

Como ya se ha comentado, los puertos pueden tomar diferentes estados según lo que esté sucediendo en la red y la comunicación que mantengan los switches. Dichos estados se describen a continuación:

- *Modo de escucha (Listening).* Los switches envían mensajes BPDU entre ellos, los que permiten establecer la topología de la red y los caminos óptimos hacia sus diferentes segmentos. No se transmite ningún otro dato.
- *Modo de aprendizaje (Learning).* El puerto puede permanecer en este modo siempre y cuando no reenvíe los paquetes de información que se desean transmitir, simplemente aprende las direcciones fuente de los frames recibidos y las agrega a la base de datos del conmutador.
- *Modo de bloqueo (Blocking).* Si uno de los puertos es propenso a generar un loop en la red, ningún dato es enviado o recibido a través de él, sin embargo, si las rutas principales fallan por alguna razón, el puerto bloqueado pasa entonces al modo de reenvío.
- *Modo de reenvío (Forwarding).* Se considera que un puerto en este modo, lleva a cabo una operación normal, es decir, envía y recibe datos, mientras esto sucede STP realiza constantemente un monitoreo de los BPDU que llegan para determinar si es conveniente regresar el puerto al modo de bloqueo a fin de evitar la presencia de loops.
- *Modo deshabilitado (Disabled).* En general no es un modo estrictamente característico de STP, en este caso el administrador es quien decide si deshabilitar un puerto o no.

Cada uno de los puertos, cambia de un modo a otro, de la siguiente forma:

- Inicialización → Bloqueo
- Bloqueo → Escucha o Deshabilitado
- Escucha → Aprendizaje o Deshabilitado
- Aprendizaje → Reenvío o Deshabilitado

Existen diversos factores del conmutador raíz que afectan el funcionamiento del protocolo STP, entre ellos se encuentran los siguientes:

- *Hello Time (Tiempo de contacto).* Determina qué tan frecuente es el envío de mensajes de unos conmutadores a otros.
- *Maximum Age Timer (Temporizador de Edad Máxima)*. Mide qué tan atrasada es la información que reciben los puertos asegurando que sea descartada cuando ésta llegue a un límite máximo respecto al tiempo en el que fue enviada.
- *Forward Relay Timer (Temporizador de Retraso de Reenvío).* Se encarga de monitorear el tiempo que emplea cada puerto cuando éstos se encuentran en los modos de aprendizaje y escucha, dicho valor también es establecido en la configuración del dispositivo.

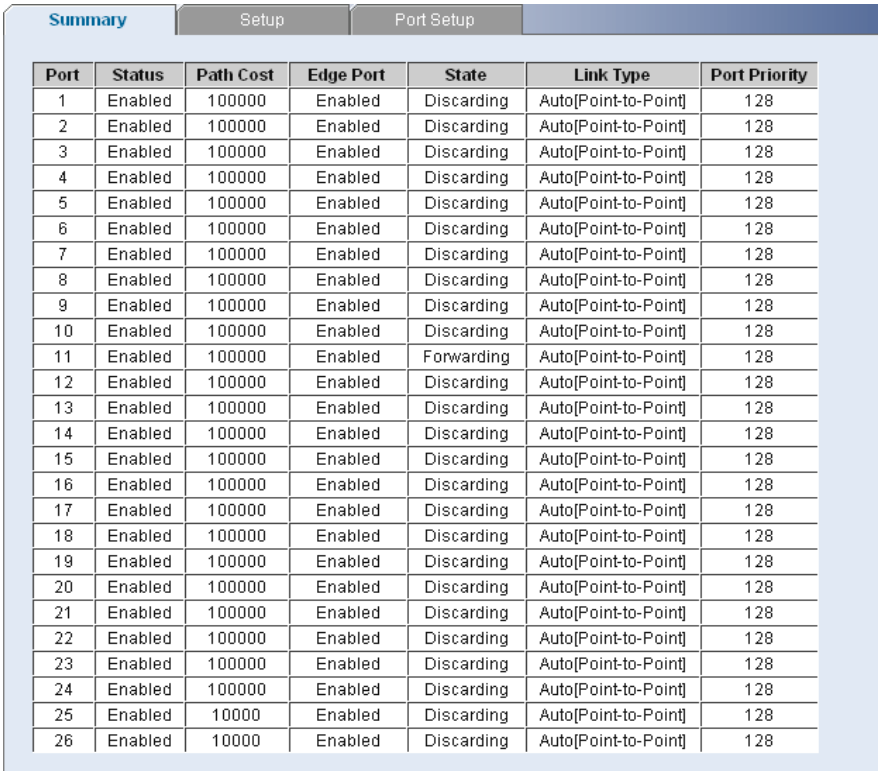
Dentro de lo que es la administración de VLANs vía Web, existe también la manipulación de STP, únicamente en el caso de que los switches sean compatibles con el estándar, por ello es importante tener una noción de lo que este protocolo es capaz de hacer, puesto que las configuraciones realizadas en los switches son las que repercuten en el desempeño del equipo y por lo tanto de la red.

Existen tres opciones en el menú de Spanning Tree dentro del switch que se ha estado utilizando para mostrar las opciones que permiten configurar una VLAN:

1. Summary
2. Setup

3. Port setup

La opción *Summary* permite desplegar la información referente a cada uno de los puertos, como se muestra en la Figura **IV.13.**



Port	Status	Path Cost	Edge Port	State	Link Type	Port Priority
1	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
2	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
3	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
4	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
5	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
6	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
7	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
8	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
9	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
10	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
11	Enabled	100000	Enabled	Forwarding	Auto[Point-to-Point]	128
12	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
13	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
14	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
15	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
16	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
17	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
18	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
19	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
20	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
21	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
22	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
23	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
24	Enabled	100000	Enabled	Discarding	Auto[Point-to-Point]	128
25	Enabled	10000	Enabled	Discarding	Auto[Point-to-Point]	128
26	Enabled	10000	Enabled	Discarding	Auto[Point-to-Point]	128

Figura IV.13. Summary

La pestaña *Setup*, permite al administrador configurar algunos parámetros referentes al STP, tales como State, Priority, versión de STP, Hello time, Forwarding Delay, Max Aging Time, etc. **Figura IV.14,** y cuyo significado se mencionó al describir el funcionamiento de STP.

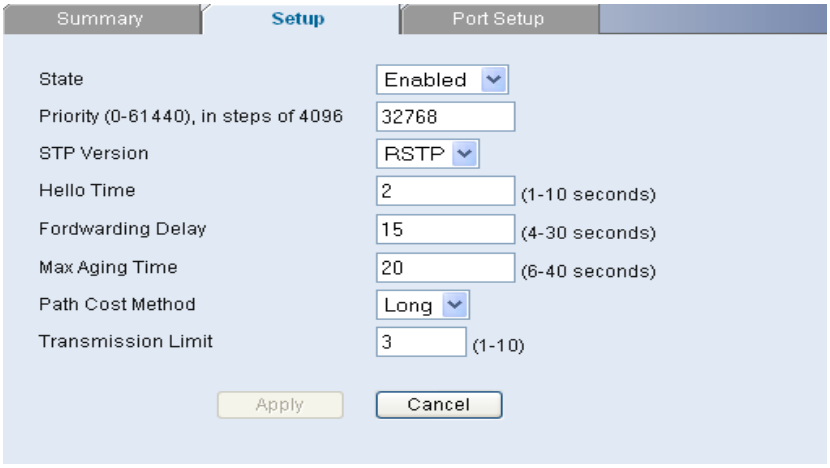


Figura IV.14 Setup

Por otro lado *Port Setup* es la opción en la que se realizan cambios respecto a las características del puerto, desplegadas en la sección *Summary*. Entre ellas se encuentran:

- *Status (Estado).* Activa o desactiva STP en cada puerto.
- *Edged port.* Son puertos que en ningún momento están destinados para la interconexión entre switches. En general son aquellos puertos configurados como *Portfast*, es decir, se configuran como tal cuando se sabe que nunca serán conectados hacia otro switch, de tal manera que pasan inmediatamente al estado de direccionamiento, sin esperar los pasos intermedios de STP (escucha y aprendizaje).
- *Type Link (Tipo de enlaces).* Existen diversas alternativas para elegir el enlace que se va a utilizar para la transmisión, tales como:
    - Punto a Punto.
    - Compartido.
- *Path Cost (Costo de la Ruta).* Este parámetro es utilizado para determinar la mejor ruta a seguir entre los dispositivos.
- *Port Priority (Prioridad de Puerto).* Este valor se emplea para seleccionar el dispositivo y puerto raíces, tomando en cuenta cuál de todos tiene el valor de prioridad más alto, sin embargo, si uno o más dispositivos tienen la misma prioridad, entonces se elige aquel con la dirección MAC de menor tamaño.

Los puntos mencionados se encuentran en la **Figura IV.15.**

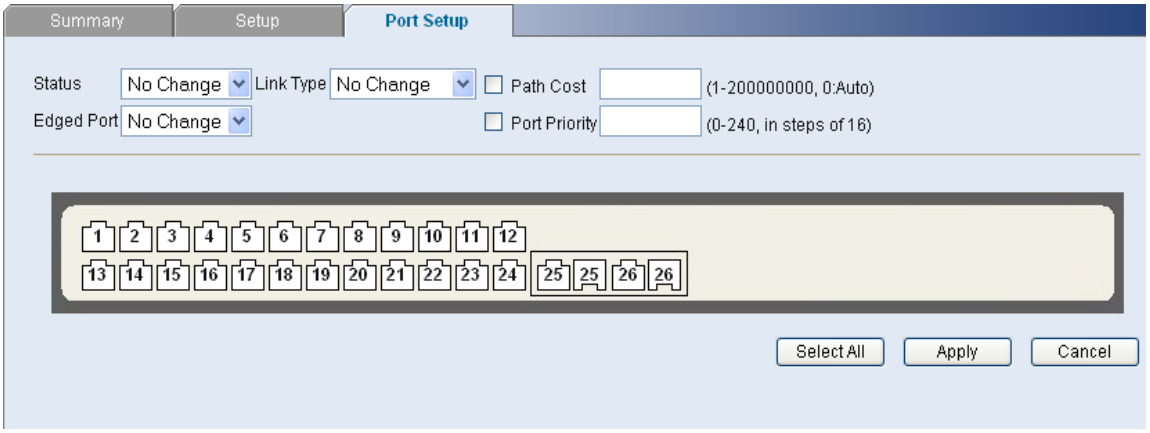


Figura IV.15 Port Setup

4.3 Tipos de configuración en una VLAN

A lo largo de esta propuesta se ha hecho referencia a diversos factores que deben tomarse en cuenta entorno a las VLANs. En el Capítulo 2, se explicó entre otras cosas, los tipos de conectividad que existen entre estas redes virtuales.

Esto representa un punto importante dentro de la configuración de las VLANs, puesto que al contar con una conectividad lógica a través de enlaces troncales, es posible manipular múltiples VLANs en un mismo dispositivo.

Una vez establecido el tipo de conectividad a utilizar, se pueden configurar las redes de acuerdo a las necesidades y criterios que el administrador considere convenientes, tomando en cuenta los factores mencionados respecto a la administración de las mismas.

Se ha hecho referencia a dos tipos de opciones con las cuales pueden ser asignados los puertos a una VLAN:

- Untagged
- Tagged

Es precisamente en esta sección donde se ve más a detalle en qué consiste cada una de dichas configuraciones, puesto que de ello depende el correcto funcionamiento de cada una de las redes virtuales con las que se trabaja en el Instituto.

Cuando los puertos en un switch son configurados como *untagged*, significa que éstos son miembros de una VLAN en específico y únicamente aceptan tráfico de la red virtual a la que corresponden, así exista más de una VLAN configurada en el mismo switch.

De manera más simple, puede decirse que los puertos *untagged* son puertos de acceso, que permiten llegar a las estaciones finales de determinada VLAN.

Un ejemplo de esta configuración se muestra en la Figura **IV.16.**

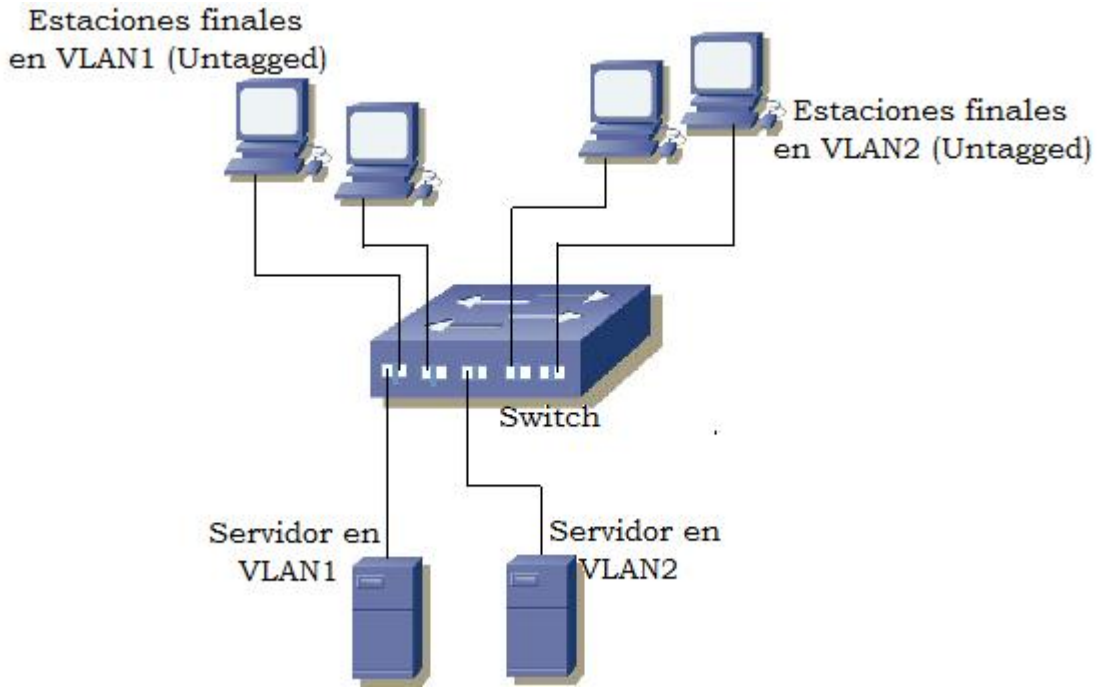


Figura IV.16 Configuración de puertos Untagged

Cuando se crean VLANs con puertos situados en switches distintos, que suele ser lo más común y que evidentemente es lo que sucede en el Hospital, es indispensable interconectar los switches para comunicar las VLANs entre sí. En este caso, es necesario un puerto en cada switch por VLAN, es decir, si

se quieren interconectar 2 switches para comunicar una red virtual, se consumen 2 puertos en total.

Para evitar esto el estándar 802.1Q, proporciona el llamado "*Tagging*", que permite que las tramas de múltiples VLANs circulen a través de un único enlace.

Como se sabe, las tramas correspondientes a diversas redes virtuales, son identificadas por un VLAN ID, sin embargo, esto no es suficiente para un correcto desempeño; si lo que se desea es que dos o más VLANs pasen por un mismo enlace, el o los puertos correspondientes tienen que ser configurados como *tagged*, y deben pertenecer a todas las redes asignadas a dicho enlace.

El enlace formado por dos puertos *tagged* es llamado Enlace Trunk, cuya explicación se vio a detalle en el Capítulo 3. Un ejemplo de esta configuración se ilustra en la **Figura IV.17** en la cual se incluyen también puertos configurados como untagged.

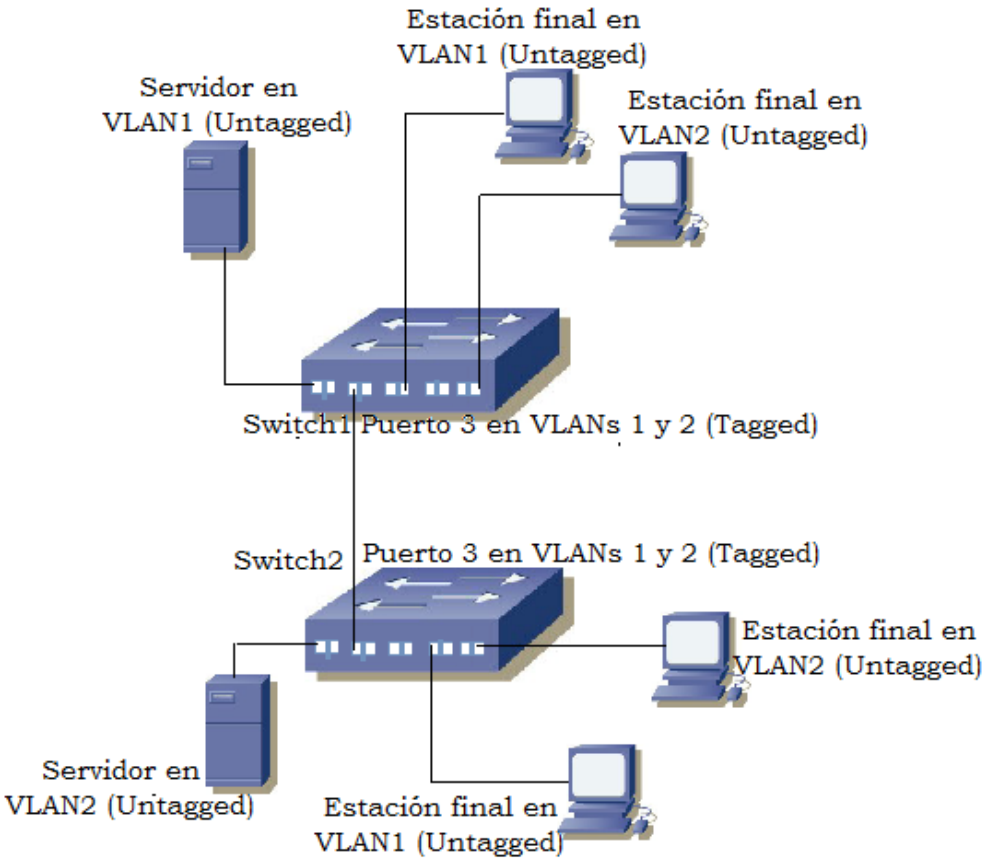


Figura IV.17 Configuración de puertos Tagged

Es importante llevar un registro tanto de los puertos que se encuentran configurados como Tagged, como de los puertos configurados como Untagged, ya que eso permitirá un mejor manejo de las redes virtuales y de los cambios que sufran sus miembros.

El switch empleado en el punto 4.1, contiene una opción más para los puertos, la cual es Not a Member, éstos no afectan en absoluto el funcionamiento de las redes, puesto que son puertos que no están activos.

4.4 Configuración de las VLANs del Instituto Hospitalario

El Instituto Hospitalario, como ya se ha mencionado, cuenta con diversas áreas que necesitan tener acceso a la red para poder realizar adecuadamente las actividades asignadas a cada una de ellas.

En el Capítulo 3, se dieron a conocer las VLANs implementadas en el Instituto, 9 en total, algunas de estas redes virtuales circulan por los mismos enlaces, que como se explicó en el punto anterior, deben de ser configurados en puertos *tagged*.

La razón por la cual se llevan a cabo este tipo de configuraciones es porque los miembros de las VLANs están distribuidos en diferentes ubicaciones.

Por cuestiones prácticas, en esta sección se muestra la configuración de las redes virtuales del Instituto Hospitalario vía Web en un swtich 3Com, y una configuración sencilla vía HyperTerminal en un conmutador Allied Telesis AT 8024M 24.

Debido a que la institución cuenta con una cantidad importante de estos equipos se considera adecuado mostrar únicamente estos ejemplos, puesto que en general las configuraciones son muy parecidas independientemente de la marca de los dispositivos.

Es recomendable contar con una bitácora de los cambios efectuados para una mejor administración de la red en general.

En la Figura **IV.18** se presenta el swtich 3Com localizado en la zona denominada Hospitalización que se puede apreciar en los planos mostrados en esta propuesta.

Pueden observarse las redes existentes en el Instituto, cada una con su correspondiente ID, las VLANs fueron creadas conforme a los pasos indicados en el punto 4.1.

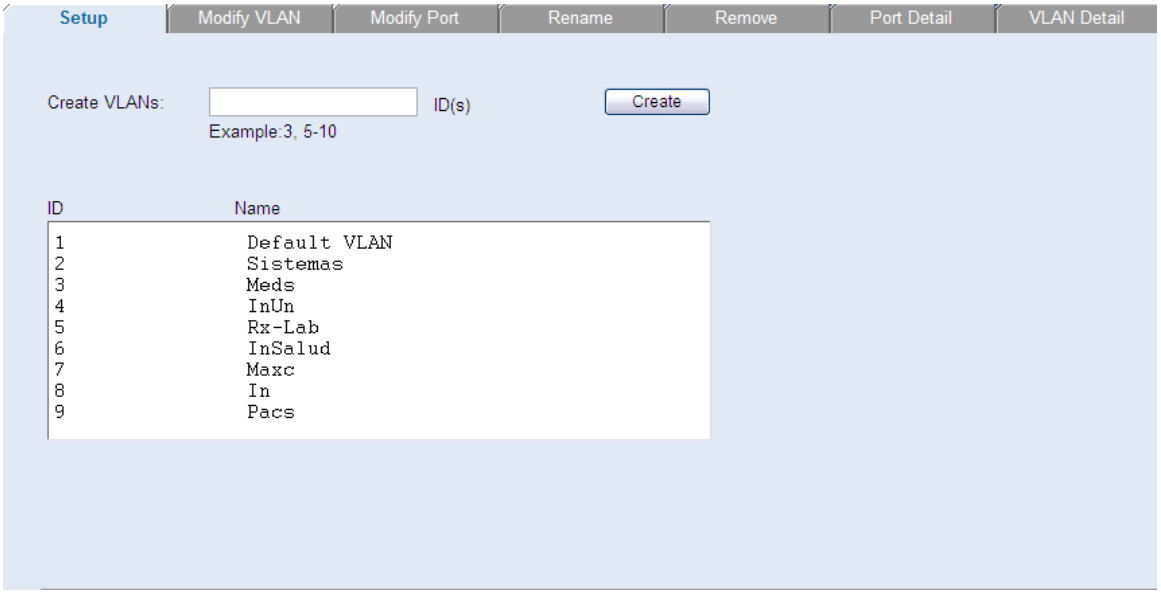


Figura IV.18 VLANs del Instituto Hospitalario

En la Figura **IV.19** se despliega la información en *VLAN Detail* de la red virtual 1, que es la Default VLAN.

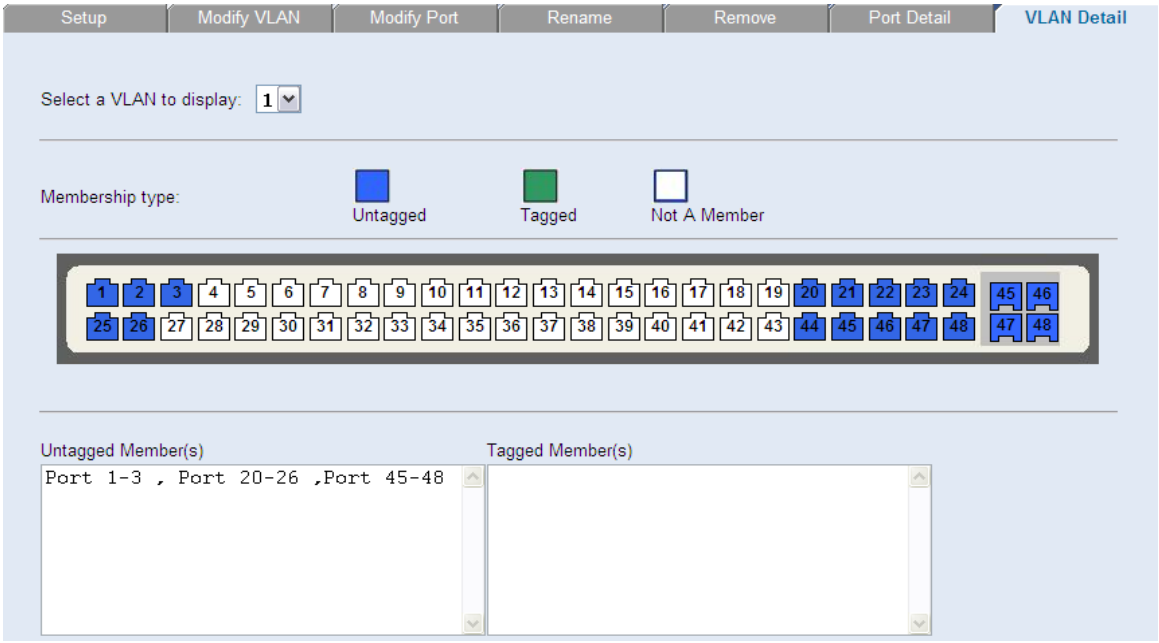


Figura IV.19 VLAN 1

En la VLAN 1, los puertos del 1 al 3, 20 al 26, y 44 al 48, están configurados como puertos *untagged*, por lo tanto, únicamente reciben tráfico de dicha VLAN; no cuenta con un enlace *tagging* ya que no se desea que estas tramas circulen en conjunto con las de otras VLANs.

La configuración de la VLAN 2 se aprecia en la **Figura IV.20**.

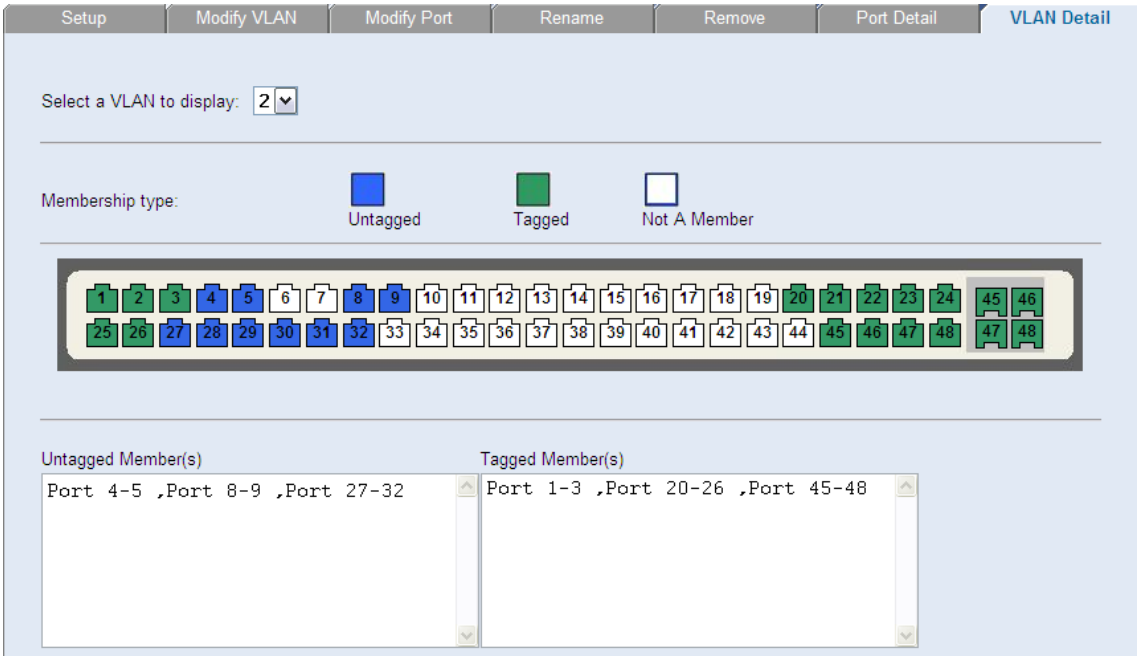


Figura IV.20 VLAN 2

En este caso los puertos 4, 5, 8, 9 y del 27 al 32 corresponden a los miembros *untagged*.

Los enlaces *tagging* contienen los puertos del 1 al 3, 20 al 26 y 45 al 48. Conforme se vayan mostrando las configuraciones de las redes virtuales restantes, será posible entender de qué manera se relacionan entre sí.

La Figura **IV.21** muestra las características de la VLAN 3: Meds.

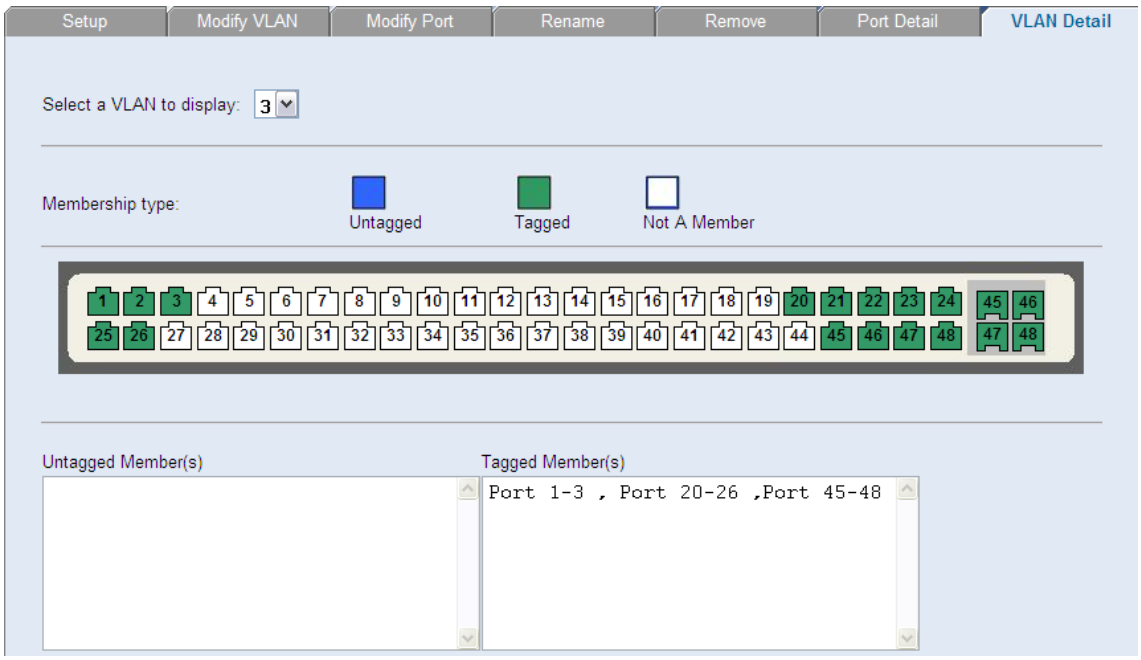


Figura IV.21 VLAN 3

En esta red virtual no existen miembros *untagged*. Los puertos 1 al 3, 20 al 26 y 45 al 48 son configurados como *tagged*.

A continuación se presenta la información de la VLAN 4 llamada InUn. **Figura IV.22**.

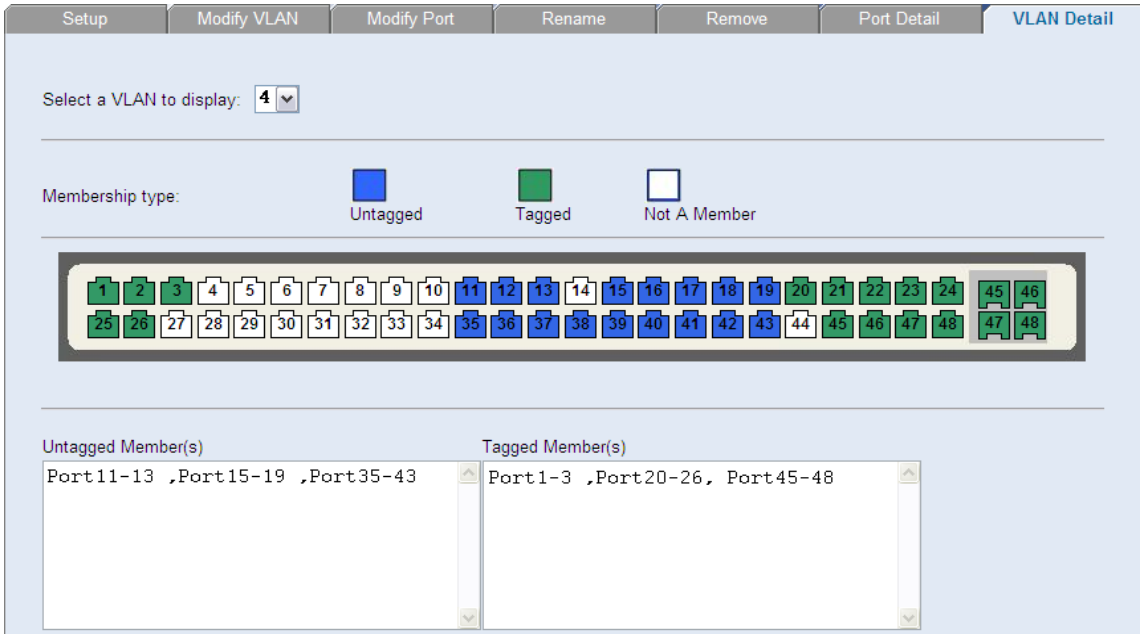


Figura IV.22 VLAN 4

Los miembros *untagged* de la VLAN 4 son los puertos 11 al 13, 15 al 19 y 35 al 43. Por otro lado los miembros *tagged* son del 1 al 3, 20 al 26 y 45 al 48.

La VLAN siguiente es Rx-Lab, con ID 5, como se ilustra en la **Figura IV.23.**

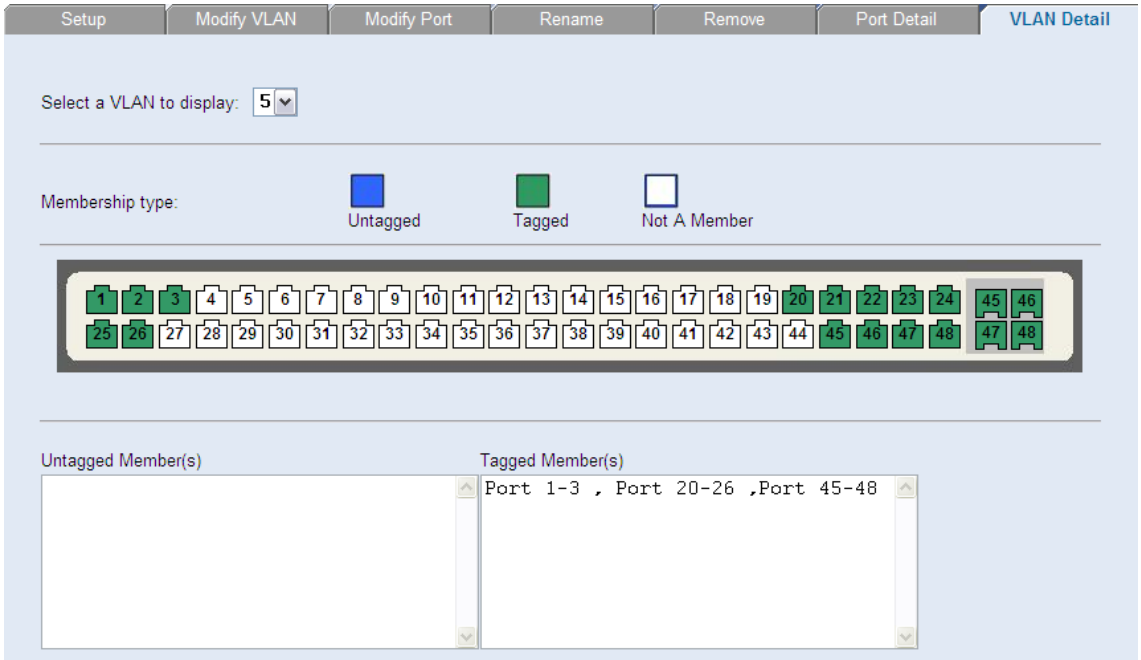


Figura IV.23 VLAN 5

En este caso, al igual que en la VLAN 3, no existen miembros *untagged*, y los puertos *taggeados* son del 1 al 3, 20 al 26 y 45 al 48.

La VLAN 6 denominada InSalud, tampoco cuenta con puertos *untagged* dentro de su configuración; y los puertos asignados para los enlaces *tagging* corresponden al mismo rango que el de las VLANs 3 y 5. **Figura IV.24.**

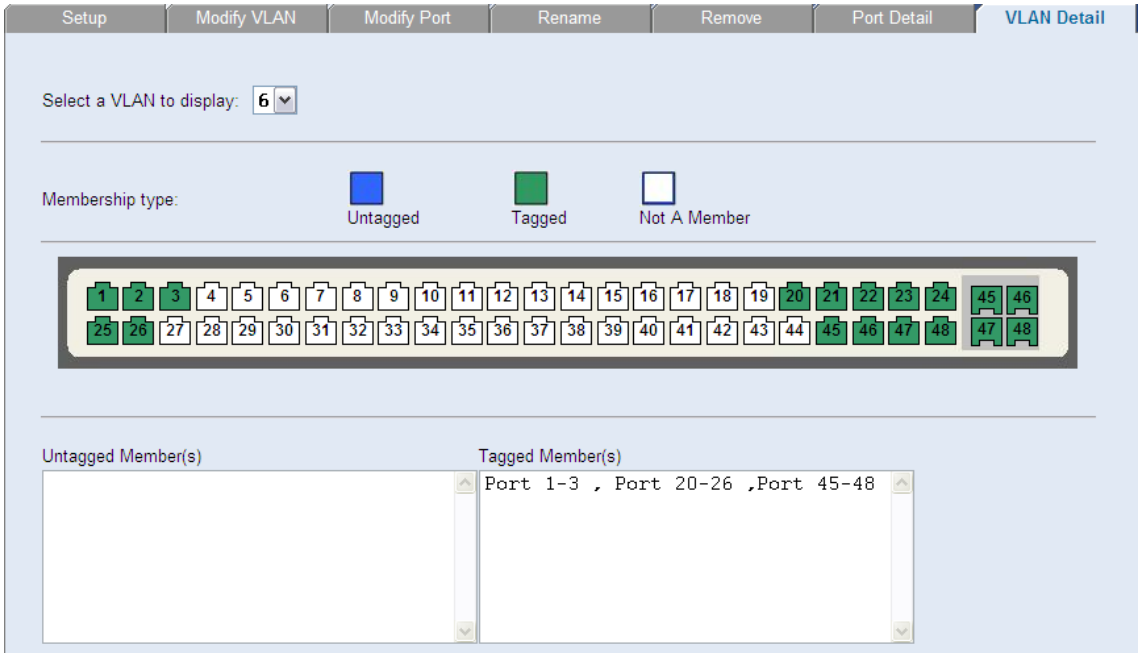


Figura IV.24 VLAN 6

Maxc, cuyo ID es el 7 solo cuenta con enlaces *tagging*, al igual que las VLANs 3, 5 y 6. **Figura IV.25**.

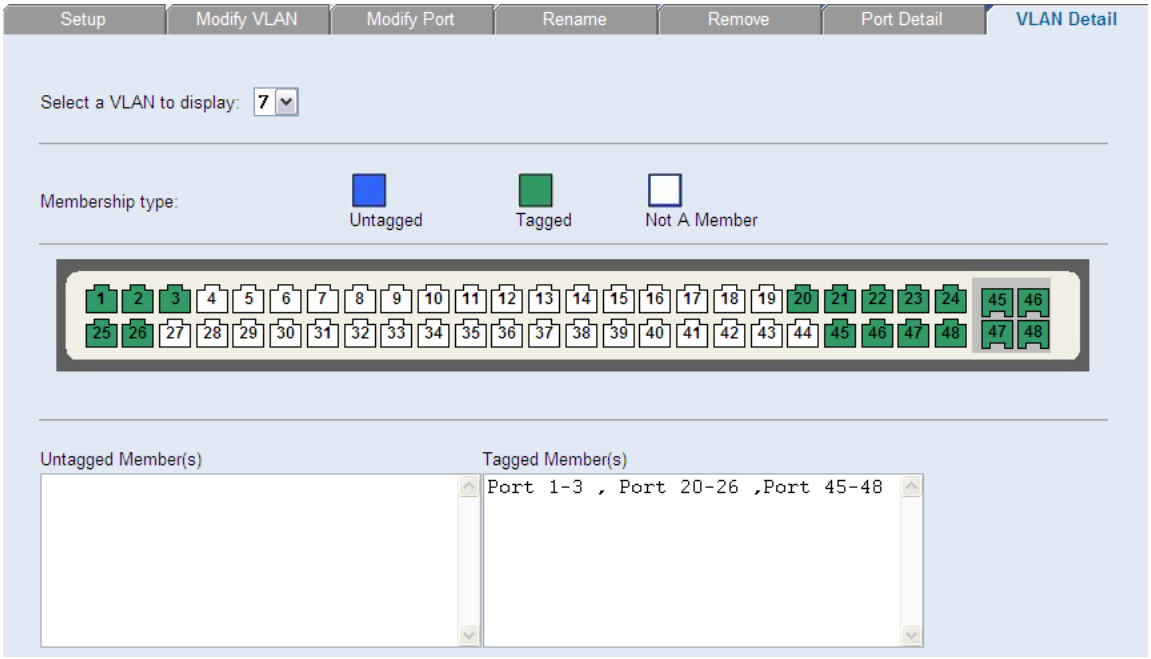


Figura IV.25 VLAN 7

En la siguiente VLAN los puertos 6, 7, 10, 14, 33 y 34 son los miembros *untagged*. Los puertos configurados como *tagged* son los mismos que la red virtual anterior. La **Figura IV.26** corresponde a la VLAN 8.

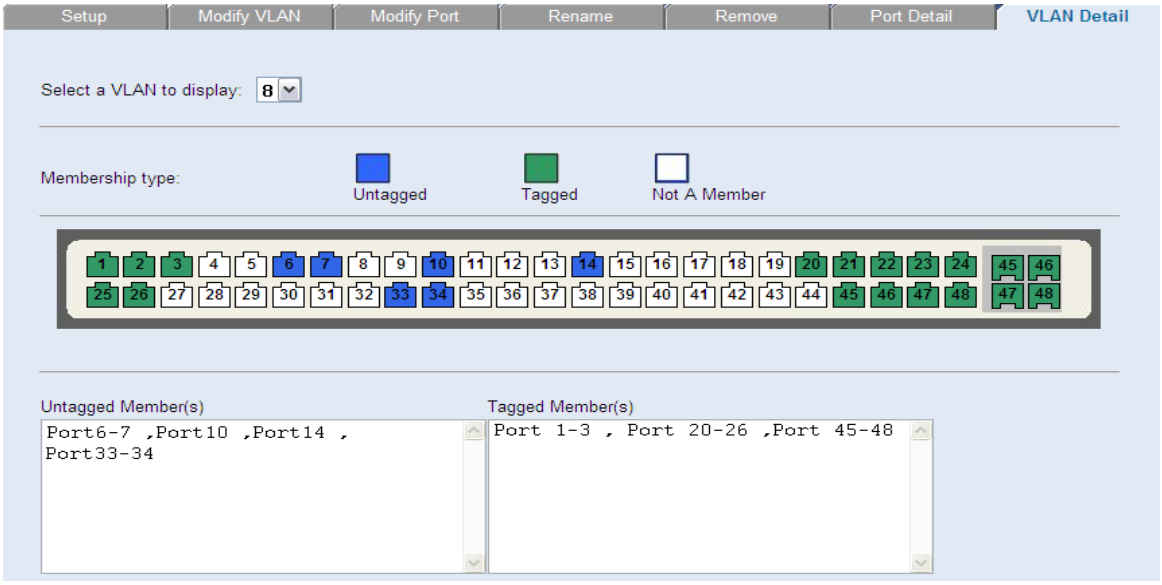


Figura IV.26 VLAN 8

Por último, la VLAN que se presenta a continuación cuenta únicamente con miembros *tagged* **Figura IV.27**.

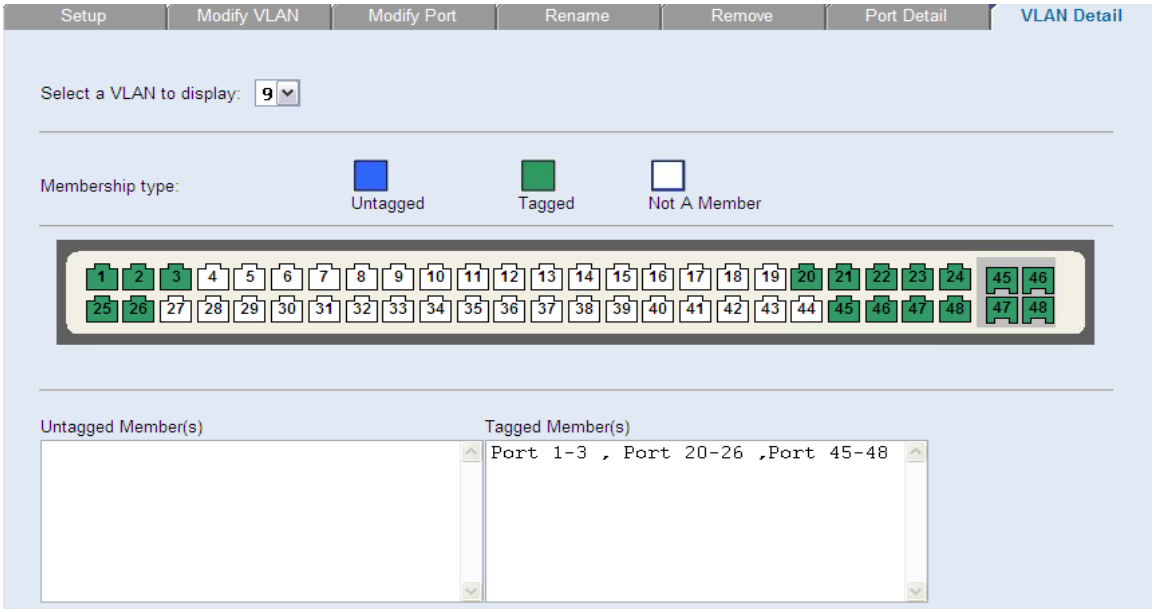


Figura IV.27 VLAN 9

Como se pudo observar, a excepción de la Default VLAN, el resto de las redes virtuales cuentan con puertos configurados como *tagged*, en este caso, el patrón de puertos es el mismo para todas, lo cual implica cierto orden, haciendo menos probable caer en confusiones al realizar nuevos cambios en los equipos.

Por lo tanto, a través de los puertos 1 al 3, 20 al 26 y 45 al 48 circulan tramas de las VLANs 2 a la 9, es por ello la importancia de que cada una cuente con un identificador que permita que la información llegue a las estaciones finales.

Para el caso de este switch como en muchos otros, solo algunas de las VLANs cuentan con miembros *untagged*, tales como la 2, 4 y 8, las cuales consumen la mayor parte de los puertos del dispositivo, independientemente de los configurados como *tagged*; esto quiere decir que la capacidad del switch fue aprovechada para contener a miembros de las VLANs mencionadas, quedando libres únicamente los puertos 33, 34 y 44, que posteriormente podrían asociarse a las redes ya asignadas a este dispositivo o simplemente ser utilizados para realizar pruebas.

La mayor parte de los switches utilizados en el Instituto cuentan con esta tecnología, lo que hace posible configurar los puertos de dichos equipos en torno a las 9 VLANs existentes.

En el siguiente caso, solo se muestran opciones que se pueden llevar a cabo por medio de una sesión establecida en la herramienta HyperTerminal para acceder a un conmutador y desde dicha sesión realizar las configuraciones. El procedimiento es muy parecido, pero a diferencia del método anterior no se presenta un entorno tan gráfico. Al conectarse al conmutador se solicita un usuario y una contraseña, **Figura IV.28**.

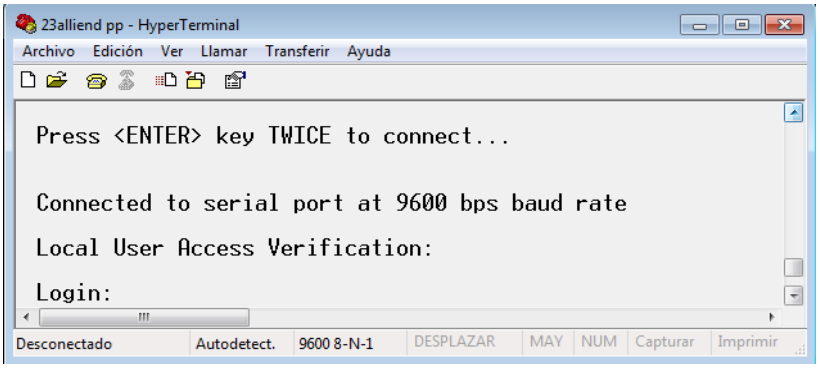


Figura IV.28 Establecer una sesión en HyperTermial

Si la información es correcta se despliega el menú con las diferentes opciones. **Figura IV.29.**

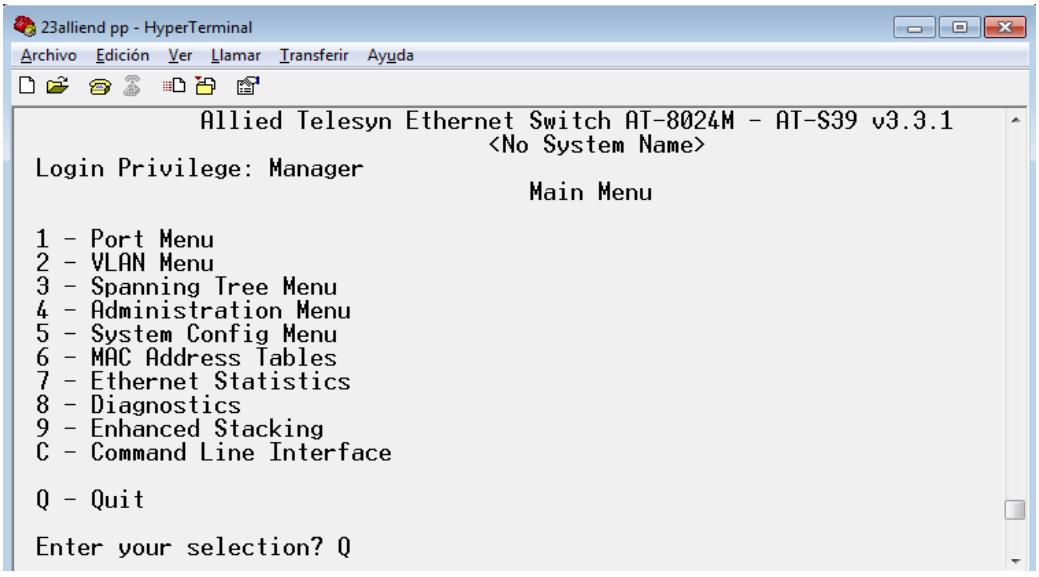


Figura IV.29 Menú Principal

El interés principal dentro de este menú es el punto 2 *VLAN Menu*, cuyas características aparecen en la **Figura IV.30.**

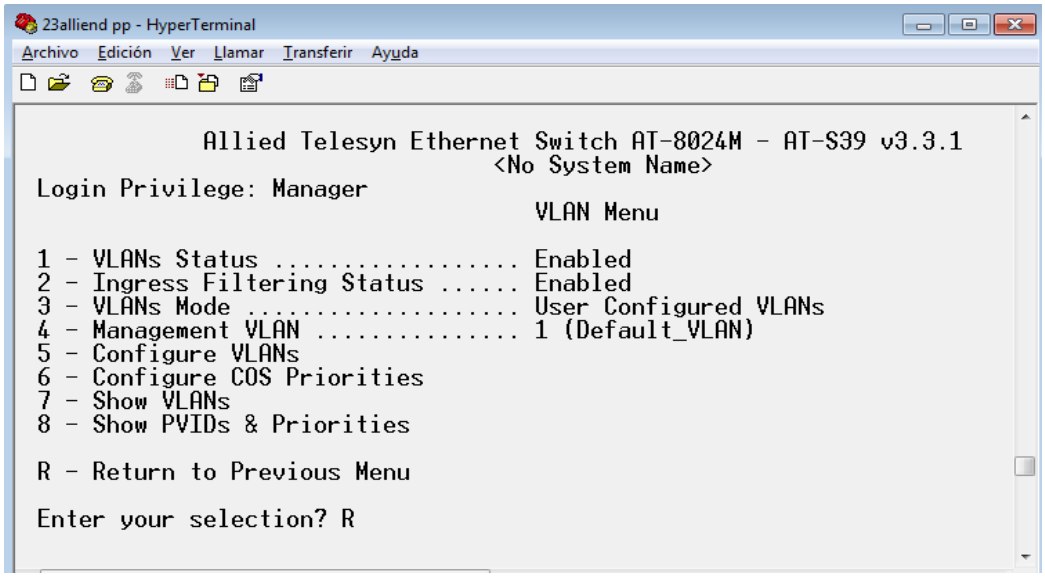


Figura IV.30 VLAN Menú

Se observa que se presentan alternativas como estado de la VLAN, configuración, mostrar VLANs, etc. La configuración de las VLANs cuenta también con su propio menú. Figura IV.31.

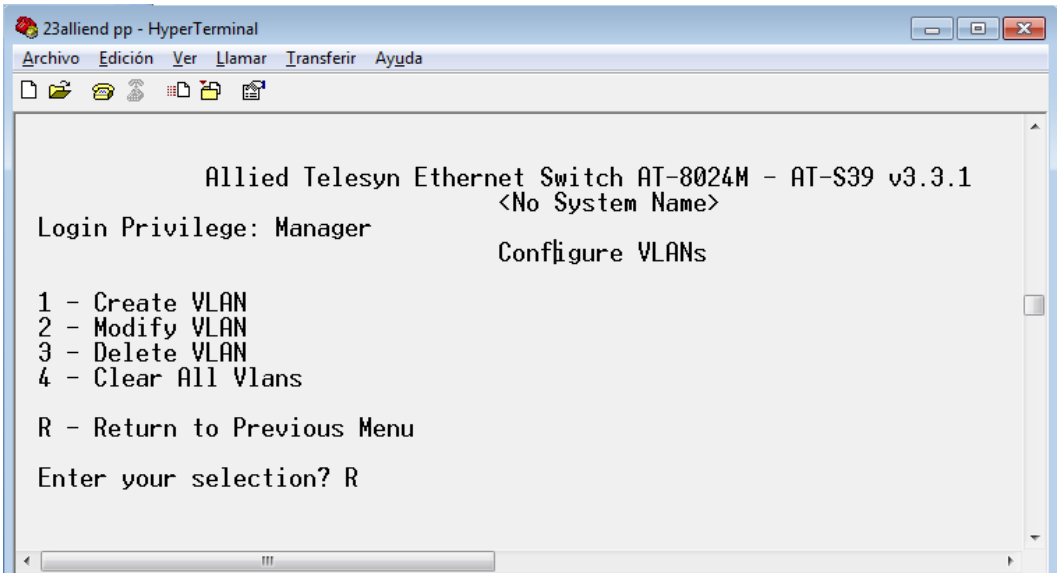


Figura IV.31 Configurar VLANs

Existe también la sección *Modify VLAN*. **Figura IV.32.**

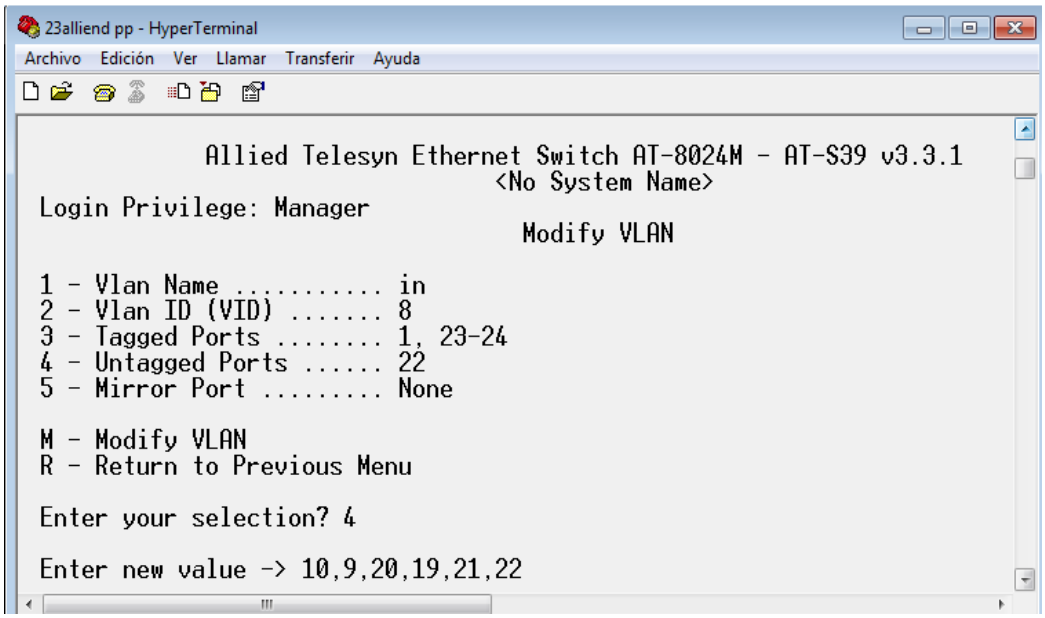


Figura IV.32 Modificar VLAN

Las selecciones se van indicando, de acuerdo a lo que se desea realizar, en el ejemplo de la figura anterior se optó por la opción 4, que permite configurar puertos como miembros *untagged*, una vez señalada la opción, se introducen el número de los puertos a modificar, lo mismo es para configurar miembros *tagged*, para asignar un nuevo ID o nombrar una VLAN. Al terminar cualquier cambio hecho, se debe introducir la "M" correspondiente a *Modify VLAN*, y posteriormente guardar las modificaciones.

Seleccionando *Show VLANs* del menú principal es posible observar la manera en que están configuradas las VLANs de este conmutador. **Figura IV.33** y **IV.34.**

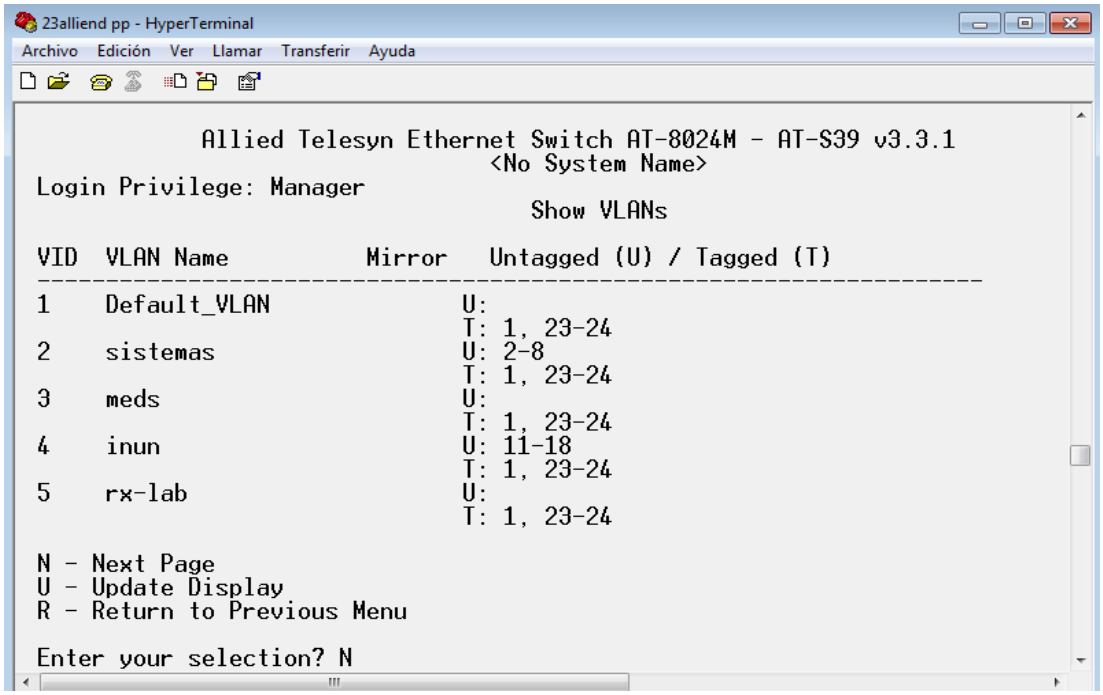


Figura IV.33 VLANs de la 1 a la 5

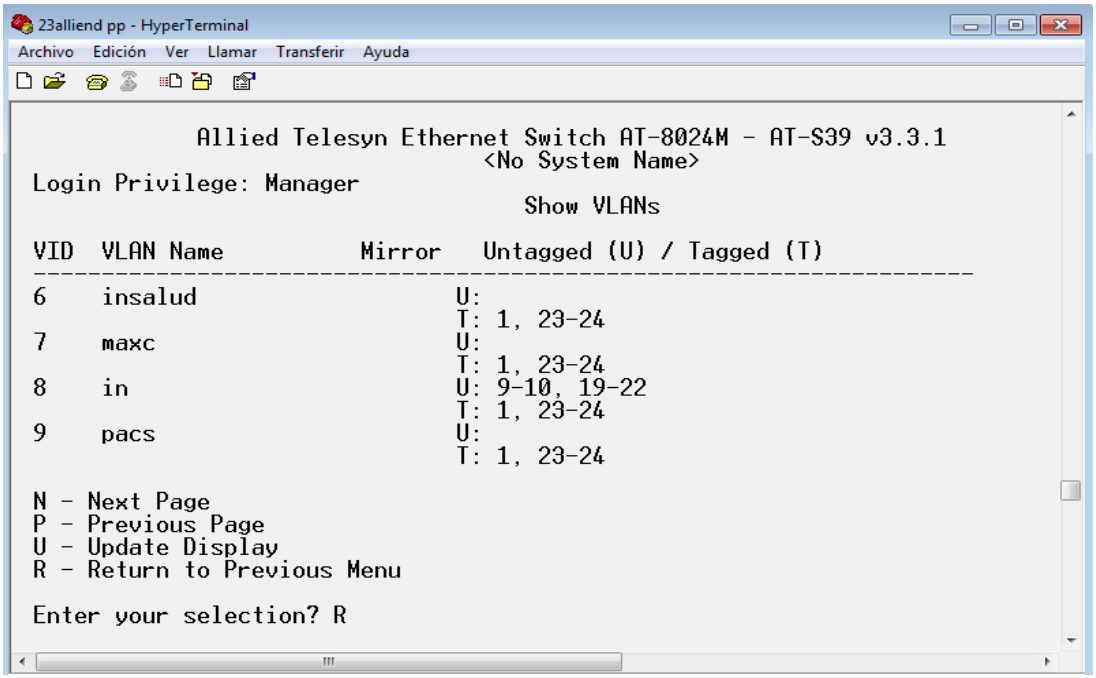


Figura IV.34 VLANs de la 6 a la 9

En este caso todas las VLANs tienen configurados los puertos 1, 23 y 24 como puertos *tagged*, y solo algunas de ellas cuentan con puertos *untagged*.

El comutador correspondiente a este ejemplo se localiza en la zona denominada Torre de Investigación; como pudo observarse, ambos dispositivos tiene en común los puertos 1, 23 y 24 configurados como *tagged*, sin embargo, el switch 3Com cuenta con más miembros de este tipo que coinciden con los de otros dispositivos ubicados en diferentes áreas del Instituto.

También es posible notar que las redes virtuales siguen el mismo orden de nombres y VLAN ID que en el equipo configurado para Hospitalización, además los puertos configurados para efectuar la comunicación entre VLANs, independientemente de tener ciertas diferencias en ambos dispositivos, son los mismos para las VLANs en cada uno de ellos

Para salir de la sesión HyperTerminal, es necesario volver al menú principal e introducir Q y esperar hasta que se indique que se ha desconectado del equipo. **Figura IV.35.**

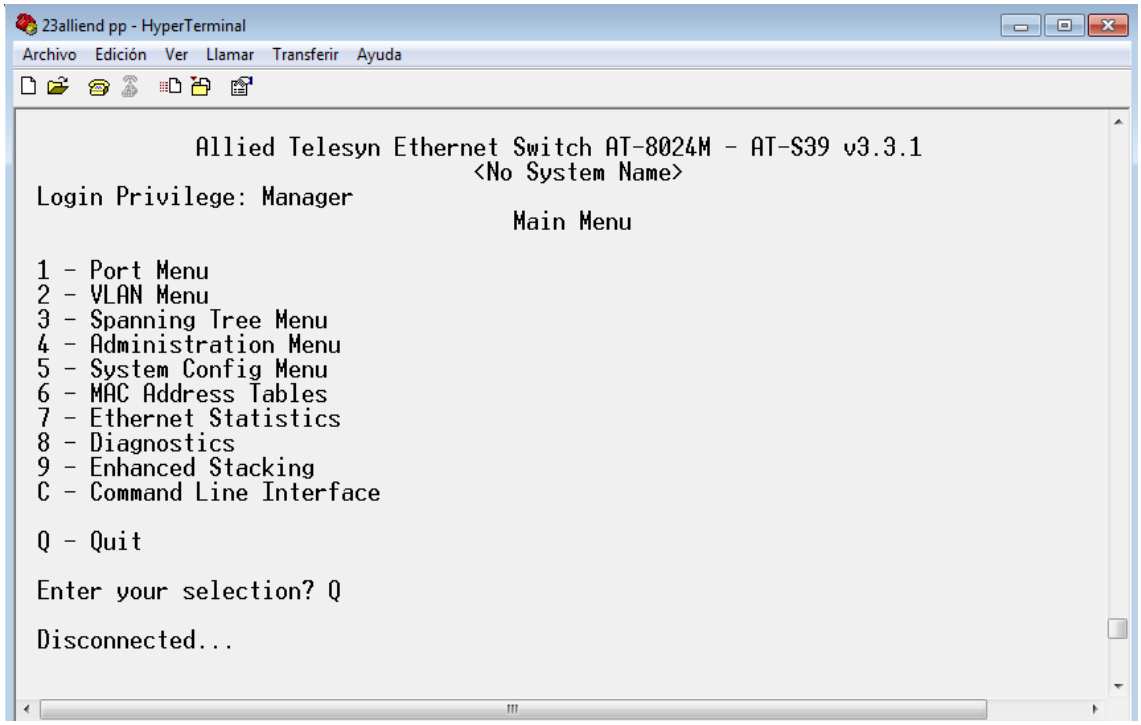


Figura IV.35 Salir de la sesión de HyperTerminal

En general, la configuración de redes virtuales es sencilla dentro de cierto contexto, y depende mucho de la institución.

Es importante que el/los encargados de la administración de los dispositivos, sean personas capacitadas y cuenten con los conocimientos suficientes para poder realizar dicha función, puesto que cualquier error al realizar la configuración de los equipos, repercute totalmente en el funcionamiento de la red.

V.

Problemas y Soluciones

5.1 Inconvenientes presentados

Es claro que la tecnología referente a las VLANs se encuentra ya implementada en muchas instituciones y empresas, y que su uso mejora considerablemente el desempeño de una red.

Como tal, no puede decirse que el empleo de redes virtuales genere algún tipo de problema o dificultad. Es bien sabido que la mayor parte de los inconvenientes que puedan presentarse son errores generados por usuarios e incluso por los administradores y la organización que llevan los mismos.

Por lo tanto, el uso de VLANs solo representa algunas consecuencias que el administrador debe tener presentes, pero que en realidad no son consideradas ciertamente como problemas si éstas son atendidas a tiempo y adecuadamente.

A continuación se presentan algunos puntos importantes, los cuales requieren determinada atención por parte de las personas responsables, puesto que en diversas ocasiones por no ocuparse de ellos, el desempeño de los equipos no es el correcto y muchas actividades no pueden realizarse a consecuencia de estos descuidos.

a) Ciertos usuarios conocen la manera en que una dirección IP es asignada manualmente, esto provoca que lleguen a tomarse IPs que no han sido concedidas por los administradores, y que incluso pueden estar ya ocupadas, en el peor de los casos, que pertenezcan no a usuarios, si no a una VLAN en específico. Sin embargo, dichos usuarios no saben y no tienen idea de que al realizar una acción de esta naturaleza es posible que se encuentren afectando las actividades de otras personas e impidiendo a su vez un correcto desempeño de la red.

b) Los administradores generalmente llevan un listado con el registro que señala qué usuarios están dados de alta en el hospital, en qué zona del mismo se encuentran ubicados, a qué VLAN corresponden, así como la IP que tienen asignada, no obstante, se presentan ocasiones en que por ejemplo una persona llega al departamento de redes a solicitar que

se le proporcione el servicio de Internet, ante esta petición el o los administradores tomando en cuenta que realmente es indispensable otorgar el servicio, deben asignar a dicha persona una IP que se encuentre libre, el punto radica en que hay veces en que solo con encontrar una dirección libre, ésta se asigna y el listado no es actualizado en el instante en que un nuevo usuario es dado de alta. Por lo tanto, al querer saber si ciertas IPs están o no disponibles, no se tiene la total seguridad de que así sea, y eso puede causar conflictos en la red, además de que los usuarios que en teoría deberían pertenecer a determinada VLAN, forman parte de redes virtuales a las que no corresponden de acuerdo al orden que previamente ya se ha establecido.

c) No existe una organización adecuada en lo que respecta a la ubicación y acomodo de diversos equipos que son parte de la red, ya sean routers, cableado, antenas, etc.; existen muchos dispositivos que se encuentran ubicados incorrectamente, por ejemplo, hay switches en los que las VLANs son configuradas y que aunque están protegidos por una caja metálica son empotrados en armarios en los que también se ubican tuberías de todo tipo, como aire caliente, agua, gas, etc., esto resulta muy peligroso para esta clase de aparatos, e incluso para quienes se encargan de realizar modificaciones en los mismos, ya que además de estar expuestos al polvo y a la falta de iluminación, no hay una garantía de que no ocurra un accidente. También se da el caso de que muchos equipos se hallan en un espacio muy reducido, lo que implica que además de desorden, cuando se quieran hacer cambios, pruebas o modificaciones, sea difícil realizar estas actividades, y se produzcan errores, o se mueva por equivocación alguna conexión.

d) No se lleva un registro y orden adecuado de los cambios realizados en los puertos pertenecientes a los switches que trabajan con las VLANs. Esto representa un serio problema, porque por ejemplo, al realizar diversas pruebas para el desarrollo de ciertos proyectos es necesario acceder a los sites y conectar y/o desconectar algunos cables, así como llevar a cabo diferentes configuraciones en los equipos, todo esto debe ser registrado para saber y recordar, si así se requiere, cuáles fueron las

modificaciones hechas; una vez terminadas dichas pruebas, es evidente que todo debe dejarse tal y como se encuentra en un principio, aún así, hay ocasiones en que ni se realiza una bitácora, ni tampoco se regresa todo al lugar al que corresponde, lo que puede generar loops en la red, y dejar a una parte de los usuarios sin servicio, aunado a eso, la problemática crece cuando por no llevar las anotaciones de los cambios, no sé sabe en dónde y porqué se originan los inconvenientes. Un caso particular de este desorden se presentó cuando al realizar configuraciones para diversas pruebas, en uno de los puertos de un switch estaban circulando tramas de 2 VLANs, cuando originalmente dicho puerto no se encontraba configurado para llevar a cabo esa función, esto generó pérdida tanto de servicio a los usuarios, como de información y tiempo.

e) Muchas veces es increíble que existiendo alternativas que permitan evitar los contratiempos en una red, éstas no sean tomadas en cuenta, tal es el caso de los apagones que en diversas ocasiones se generan en la institución; evidentemente muchos equipos y dispositivos se ven afectados por la falta de suministro de energía, indistintamente del tiempo de duración del problema. Un ejemplo claro se presenta en el caso de los servidores DHCP que se encargan de la asignación de IPs a cada uno de los equipos que soportan las VLANs, así como de todos sus miembros; dichos equipos no cuentan con una fuente de energía que los respalde en caso de que se genere una falla eléctrica, cuando esto sucede los servidores se apagan, y los usuarios dados de alta pierden momentáneamente el servicio, hasta que los DHCP se reinician nuevamente, y aunque éstos lo hacen de manera automática, lo ideal sería que no se apagaran, o en el peor de los casos que se apagaran correctamente.

f) La falta de planeación a futuro es uno de los grandes problemas que enfrentan en su mayoría todo tipo de instituciones, y el Instituto Hospitalario no es la excepción, es claro que siempre van a surgir cambios y que éstos afectan la manera en que las actividades se llevan a cabo, en este caso, puede ser el aumento en el número de usuarios, disponibilidad de espacio para la ubicación de nuevas adquisiciones,

sustitución de equipos obsoletos por nuevos, etc. Si no se tiene una perspectiva correcta de las necesidades de la red y de cuánto puede llegar ésta a crecer, los costos generados evidentemente serán mayores.

Es indiscutible que siempre se van a presentar dificultades al administrar una red, sin embargo, durante el desarrollo de este proyecto, las mencionadas anteriormente fueron las que se presentaron con mayor frecuencia, y es por ello que son las tratadas en este capítulo.

En el siguiente punto se presenta una serie de soluciones, las cuales son consideradas las más adecuadas para tratar cada una de las cuestiones precedentes.

5.2 Soluciones planteadas

El orden en que se presentan las soluciones va de acuerdo a los incisos mostrados en el punto 5.1.

a) Para evitar que los usuarios puedan acceder a la pestaña de *propiedades* perteneciente a Estado de Conexión de Área Local, como se muestra en la **Figura V.1**, es conveniente deshabilitar dicha pestaña para que de esta manera no sea posible entrar a las Propiedades de Conexión de área local **Figura V.2**, y a su vez se logre evitar el cambio u ocupación de IPs sin consentimiento del administrador, en la sección de Protocolo Internet TCP/IP ilustrado en las **Figura V.3.**

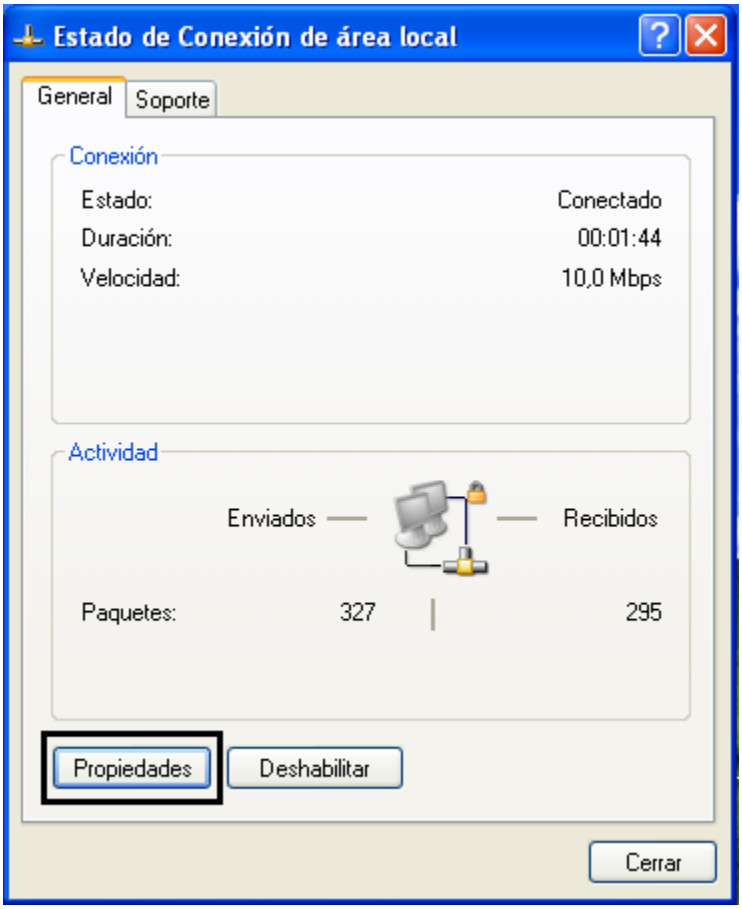


Figura V.1 Estado de Conexión de área local

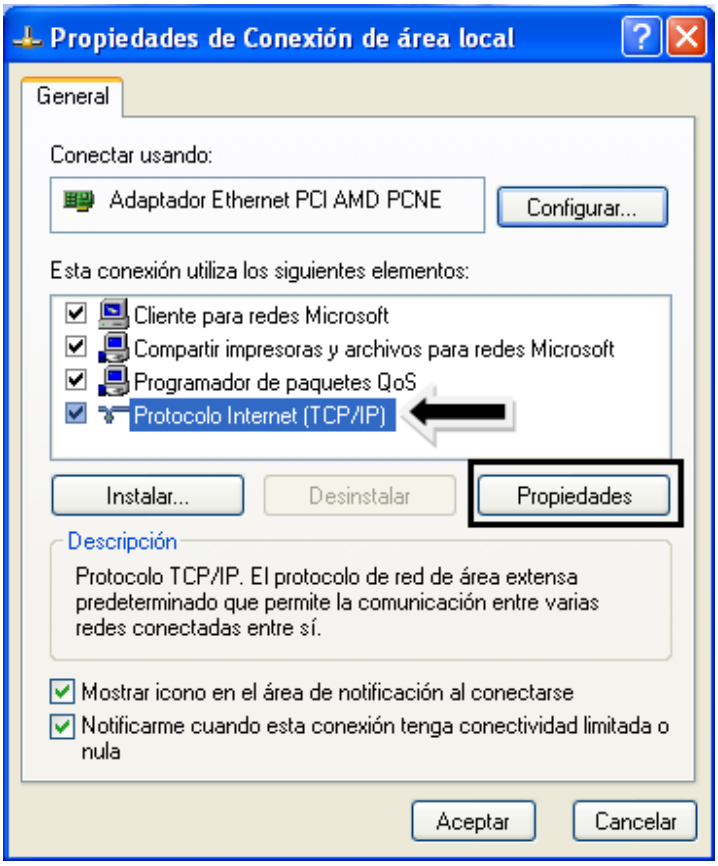


Figura V.2 Propiedades de Conexión de área Local

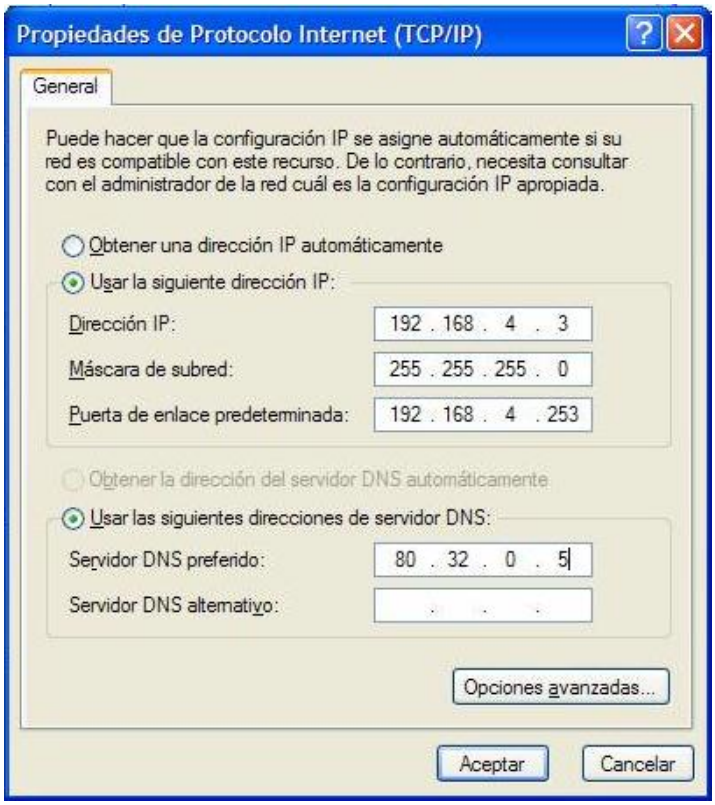


Figura V.3 Propiedades de Protocolo Internet (TCP/IP)

Lo que se tiene que hacer para inhabilitar estás propiedades es ejecutar el comando *gpedit.msc*, **Figura V.4**.

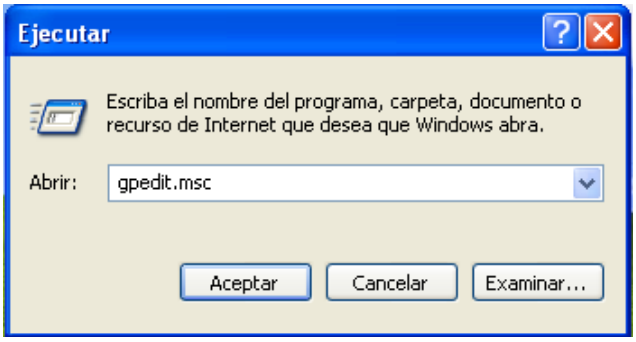


Figura V.4 Ejecución del comando gpedit.msc

Posteriormente aparece la ventana de Directiva de grupo, en donde se tiene que acceder a *Configuración de usuario* → *Plantillas administrativas* → *Red* → *Conexiones de red*, en donde se muestra un listado de opciones a modificar, **Figura V.5**.

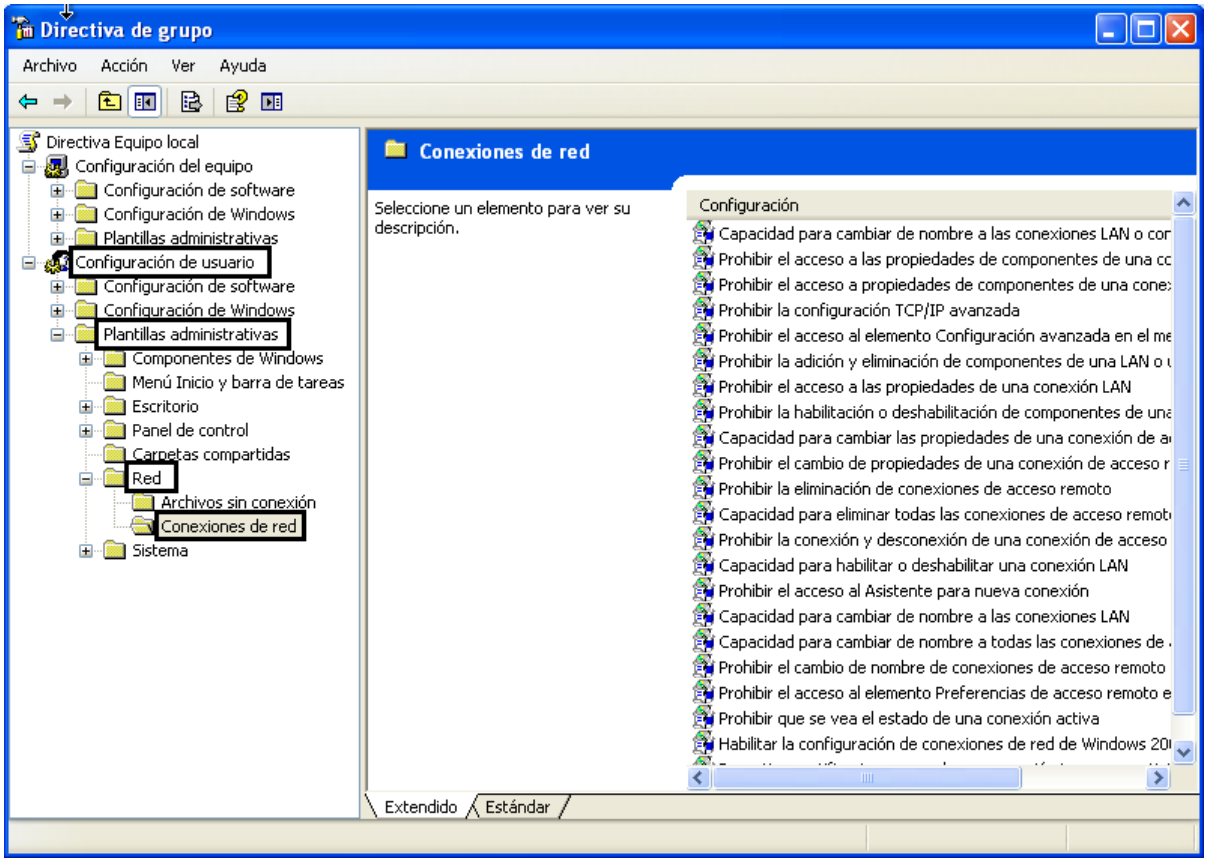


Figura V.5 Conexiones de red

En el listado mostrado en conexiones de red existen 2 opciones que son las que se tiene que habilitar:

- Prohibir el acceso a las propiedades de una conexión LAN y
- Habilitar la configuración de conexiones de red de Windows 2000 para administradores.

Es muy sencillo habilitarlas simplemente se da doble click sobre cada una de ellas, se elige la opción habilitar y se aplican los cambios realizados, **Figura V.6**; al abrir nuevamente la ventana de Estado de Conexión de área local, se observa que la pestaña de propiedades ya no puede ser utilizada, **Figura V.7**, y por lo tanto la IP asignada por el administrador es la única que podrá emplearse.

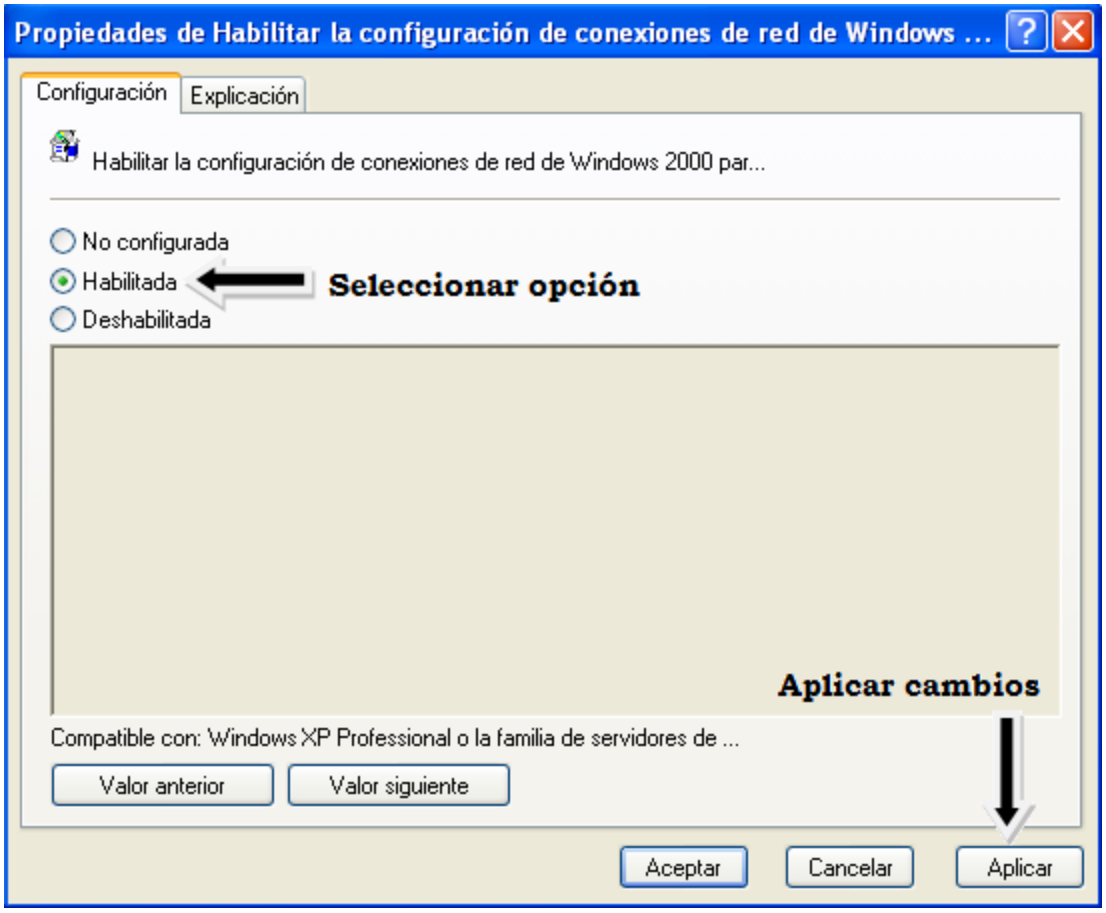


Figura V.6 Habilitar opciones

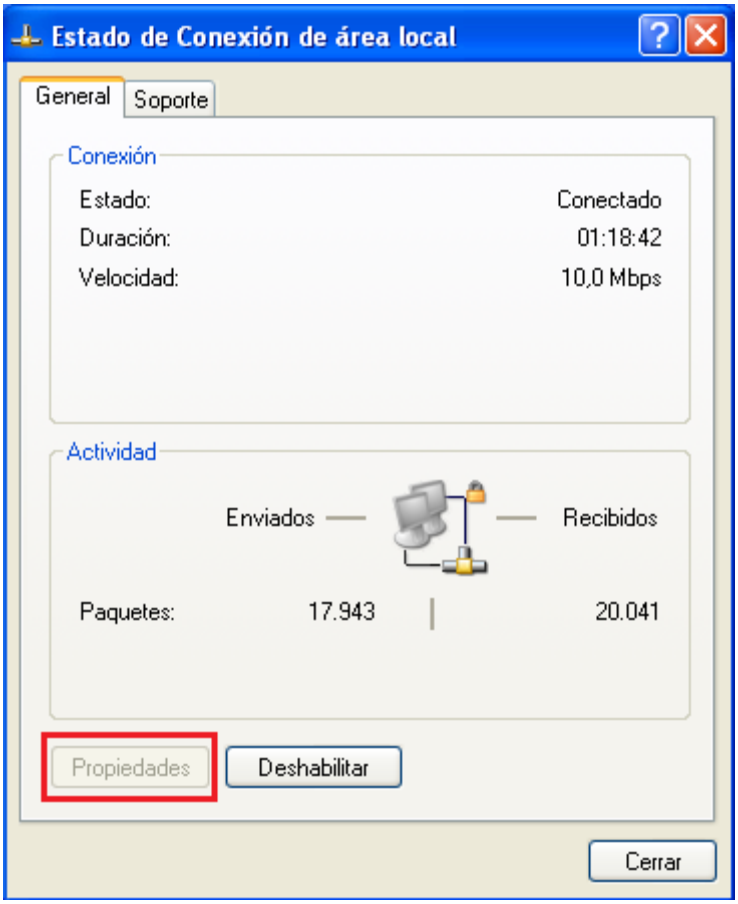


Figura V.7 Estado de Conexión de área local, propiedades deshabilitadas

Es importante mencionar que los pasos anteriores fueron aplicados a Sistemas Operativos Windows XP, ya que en su mayoría es el que los equipos del Instituto tienen instalado.

Por otra parte, la configuración anterior no garantiza el hecho de que los usuarios no descubran cómo habilitar nuevamente las propiedades, puesto que es cuestión de investigación, en el caso de los equipos en los que se les realizo esta actividad, no volvieron a presentar el problema, sin embargo, si así sucediera, otra medida que puede tomarse es sancionar a las personas que no respeten las normas establecidas por los encargados de la red.

b) Como ya se ha mencionado, las VLANs permiten establecer diferentes grupos de trabajo independientemente de la ubicación de quienes los integran, cada VLAN cuenta con un nombre y un ID que las identifica; además de la relación que dichos parámetros tienen con las tramas y la

información de las redes virtuales, éstos permiten seguir un orden que facilita la manera en que los usuarios van a ser distribuidos, este orden tiene que ser respetado por los administradores, puesto que los miembros no deben ser asignados conforme se encuentren lugares disponibles o acorde al tiempo en que se presentan las solicitudes. Una solución planteada ante este problema es que en primer lugar, cuando alguien demande que se le proporcione el servicio de red, tendrá que llenar una forma en la cual se incluyan los datos del interesado, el área de trabajo que ocupa en el Instituto, y las razones y fundamentos por las cuales considera que requiere dicho servicio. Posteriormente, el administrador debe analizar y determinar en un plazo máximo de 3 días si realmente es indispensable realizar la prestación, y si es así proceder a ubicar al nuevo usuario en la VLAN correspondiente en base a los datos incluidos en la forma y registrar la IP que se le pretende asignar. De esta manera, el encargado de la red no caerá en confusiones al querer saber si una dirección de internet está o no ocupada, la agrupación de los miembros de las VLANs será respetada, y por otra parte no se otorgará el servicio innecesariamente, puesto que hay personas que no le dan un uso realmente productivo y que contribuya al beneficio de las actividades realizadas en el Instituto Hospitalario.

c) Difícilmente los equipos ya establecidos, acomodados y en funcionamiento serán cambiados de lugar, aunque esto sin duda sea en diversas ocasiones lo más recomendable, aún así es posible prevenir que este tipo de errores suceda nuevamente, ya sea que al adquirir un nuevo dispositivo se consideren múltiples opciones del área en donde va a ser ubicado, así como la generación de espacios nuevos y de uso exclusivo para los equipos informáticos, y que por supuesto cumplan con las normas y estándares necesarios que permitan una mejor interoperabilidad de la red.

d) Una bitácora resulta ser la solución más aconsejable en este punto, ya que un registro de las actividades realizadas en los sites resulta de mucha ayuda para conocer qué cambios se han hecho, qué puertos son los que se configuran, de qué forma se hace, cómo se encontraban originalmente, en qué fecha se realizó alguna modificación, incluso se

pueden aplicar configuraciones pasadas que se sabría funcionaron adecuadamente, o mejor aún, es posible evitar caer en errores ya experimentados al realizar cambios, etc., todo esto siempre y cuando se hagan todas las anotaciones pertinentes y de una manera clara y detallada. Por otro lado, otra propuesta, y que aplica para todas las redes es tener un orden adecuado en el cableado de los sites, ya que resulta muy común tener todo revuelto y enredado, tal es el ejemplo de la **Figura V.8**.

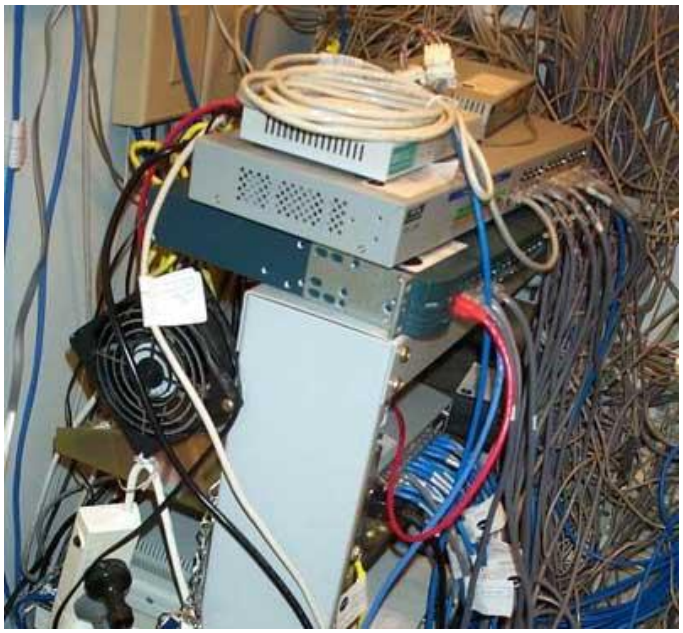


Figura V.8 Incumplimiento de normas en una red

Se recomienda etiquetar los cables, acomodarlos correctamente en los gabinetes destinados para los equipos, también registrar qué IP corresponde a cada dispositivo. De esta manera será poco probable generar loops en la red y que las VLANs se encuentren en enlaces incorrectos.

e) En el Capítulo 1 se mencionó que el Instituto cuenta con diferentes IDFs ubicados en diversas áreas del Hospital y que existe también un site principal denominado MDF, al cual llegan absolutamente todos los enlaces de la red. Este cuarto principal cuenta con un UPS *(Uninterruptible Power Supply - Sistema de alimentación ininterrumpida)*, que no es más que una fuente de abastecimiento eléctrico que posee una batería con el fin de otorgar energía por un periodo de tiempo a uno

más dispositivos en caso de que se produzca una interrupción eléctrica, lo cuestionable en esta situación es que este tipo de equipo solo existe en el site principal, cuando debería de existir de manera obligatoria en cada uno de los cuartos que albergan los dispositivos que conforman la red, y que por lógica soportan y contienen las configuraciones de las VLANs, como son switches, routers, firewalles, servidores DHCP, etc., para impedir que éstos se apaguen al presentarse alguna falla momentánea, o de ser el caso, se apaguen correctamente si el problema persiste durante un tiempo considerable; ya que a largo plazo, los equipos pueden sufrir ciertos daños o dependiendo de la magnitud del problema, quedar inservibles totalmente, lo que generaría a su vez mayores gastos. Así que es mejor realizar un gasto que si bien puede ser fuerte, permitiría ayudar a mantener no solo un buen desempeño de la red, y a alargar el tiempo de vida de los equipos, sino también el evitar realizar gastos aún mayores en un futuro, así como la generación de pérdidas, ya sea de información o de dispositivos.

f) El crecimiento de las redes es inevitable, es por ello que un administrador y/o diseñador debe tomar en cuenta los aspectos que a largo plazo podrían afectar el desempeño de las mismas. En lo que respecta al Instituto Hospitalario, nunca se pensó que el número de usuarios aumentaría de una manera tan considerable, puesto que en sus inicios, cuando se empezaba a otorgar el servicio de Internet, eran pocas las personas que contaban con dicho privilegio. La tecnología ha avanzado a lo largo de los años, tanto así que ahora se puede hacer uso de las redes virtuales, los equipos que soportan esta tecnología son equipos costosos, por lo tanto no deben ser adquiridos sin antes planificar los puntos que se pretenden cubrir cuando una red va a sufrir cambios que tengan como objetivo brindar un mejor desempeño. Por ejemplo, si en determinado momento se quiere tener una VLAN en un switch para 20 usuarios, sería más recomendable comprar un equipo de 48 puertos, a comprar uno de 24, ya que es probable que en un periodo de tiempo el número de miembros de la VLAN aumente, o tal vez se desee implementar otra red virtual en el mismo switch, otra sugerencia en lo que respecta a la obtención de nuevos aparatos es optar por aquellos que a largo plazo puedan seguirse utilizando, es

decir, que no sean considerados como obsoletos o incompatibles con tecnologías que quizá ya existen, pero que aún no se encuentran bien implementadas. Generalmente el Instituto opta por realizar de esta manera sus adquisiciones, sin embargo, aún existen equipos en funcionamiento que ya no son compatibles con la mayoría de los dispositivos, o que por su tiempo de vida llegan a presentar algunas fallas, si éste es el caso es mejor llevar a cabo el cambio de equipo obsoleto por nuevo.

Resulta muy interesante conocer los aspectos en que el desempeño de una red puede mejorarse, pero este hecho no solo radica en tener el conocimiento de qué es lo que está bien o lo que está mal.

Es muy importante que quienes son responsables de desarrollar las alternativas para cumplir con ese objetivo tengan la iniciativa y la constancia de llevar a cabo todas las actividades que permitan una adecuada interacción entre los usuarios, los equipos, la red en general y los administradores mismos.

Conclusiones

CONCLUSIONES

En cuanto a la administración y configuración de VLANs del Instituto Hospitalario, resultó de gran ayuda llevar a cabo una investigación detallada respecto a las características, funciones, necesidades, beneficios y aplicaciones de dichas redes, puesto que se conoció más a fondo la manera en que este tipo de tecnología funciona, lo que a su vez facilitó la comprensión de los pasos a seguir para poder realizar las configuraciones adecuadas que permitan otorgar un servicio de calidad a los diversos usuarios, y que contribuyan no solo al buen aprovechamiento de las nuevas tecnologías, sino también a una mejor administración de las redes y del tráfico que circula por ellas.

El uso de VLANs en esta institución resulta de gran ayuda, ya que al ser considerable la cantidad de usuarios, las redes virtuales permiten tener un mejor control del tráfico que circula por la red. De esta forma las labores que se desempeñan en el hospital se llevan a cabo de una manera más óptima. Por otro lado es evidente que el separar los dominios de broadcast y tener grupos de trabajo proporciona una mayor seguridad a los mismos, además de lo que ya se ha mencionado a lo largo de todo este proyecto, que es que hay una administración mucho más organizada y flexible en lo que respecta a cambios, movimientos o adición de usuarios, lo que es muy importante pues siempre se presentan situaciones en las que se dan bajas de usuarios, llegan nuevos, o simplemente cambian de ubicación. Todo esto aplica en el Instituto, y las VLANs hacen posible la realización de dichas acciones.

Las desventajas como tal en el uso de redes virtuales no existen, más bien deben tenerse presentes ciertas consideraciones que ayudan a un correcto funcionamiento de la red; éstas dependen del tipo de red virtual que se esté utilizando, en este caso al ser VLANs por puerto, lo que se tiene que tomar en cuenta es que es de gran ayuda llevar un registro de los puertos asignados a cada red y la manera en que se tienen configurados, a qué estaciones finales llegan los enlaces de cada uno de ellos, etc., todo esto permite que la gestión de la red sea mucho más sencilla, y de presentarse algún problema se puedan ubicar con mayor facilidad las posibles fuentes del inconveniente.

Este proyecto de tesis, permitió interactuar de manera directa con los equipos, realizar configuraciones en tiempo real y conocer las problemáticas que se presentan al momento de realizar modificaciones en los dispositivos, así como los diferentes factores que de cierta manera impiden llevar una buena administración.

Sin embargo, de la misma forma en que se incurrió en errores, posteriormente se lograron implementar configuraciones adecuadas y se tomaron en cuenta diversos puntos que permitieron tener una mejor organización de las redes virtuales.

Todo lo anterior, y lo descrito a lo largo de los capítulos confirma que la implementación de VLANs es hoy en día una solución para las problemáticas de ancho de banda y crecimiento presentes en muchas instituciones debido a que su uso simplifica de manera considerable tanto el tráfico de broadcast innecesario, como las limitaciones de movilidad y ubicación en los grupos de trabajo.

Por otro lado, cabe destacar que durante la realización de este proyecto, incluso los administradores adquirieron nuevos conocimientos en lo que respecta a las redes virtuales, que verdaderamente resulta ser un tema muy amplio e interesante. Por ejemplo, no conocían todos los tipos de redes virtuales que pueden ser implementados, solo unos cuantos, ni la manera en que trabajan internamente los protocolos que estandarizan las VLANs, esta investigación contribuyó a una mayor comprensión de las normas que deben seguirse al realizar configuraciones, puesto que en diversas ocasiones se modifican parámetros que tienen que ver con algún protocolo en particular. Además se pusieron en práctica algunas propuestas que mejoran el funcionamiento de los equipos, como llevar una buena administración de las IPs asignadas a los miembros de los grupos virtuales, etiquetar las conexiones pertenecientes a los switches y realizar una bitácora de los cambios efectuados durante la aplicación de pruebas o modificaciones.

Algunas de las perspectivas a futuro que se tienen para este proyecto, son: poner en práctica el resto de las alternativas propuestas para evitar en la

medida de lo posible los inconvenientes que pudieran generarse en la red, también que esta investigación se tome como referencia cuando se desee conocer de qué manera funcionaría el hecho de implementar redes VLANs administradas con base a otras características, como direcciones MAC, VLAN por nombres de usuario, por protocolo, etc., y exponer así cuáles tienen ventajas sobre otras, y por úlitmo realizar un seguimiento sobre la forma en que la tecnología de este tipo avanza, y las diversas aplicaciones que vayan surgiendo para su manejo.

Las Redes Virtuales de Área Local son un recurso que debe aprovecharse al máximo, pues brindan grandes beneficios: pueden reducir costos, proporcionar mayor seguridad, creación de grupos de aplicación específica, minimizar el broadcast y multicast, etc.

Glosario

GLOSARIO

A

Ancho de banda: Cantidad de información que una determinada conexión es capaz de soportar (enviar y recibir).

Apple Talk: Apple Talk es una colección de protocolos que fue desarrollada por Apple Computer a principios de los 80s, de manera conjunta con la computadora de Macintosh. El propósito de AppleTalk es permitir a múltiples usuarios compartir recursos.

ATM: Es una tecnología de switching basada en unidades de datos de un tamaño fijo de 53 bytes llamadas celdas. ATM opera en modo orientado a la conexión, esto significa que cuando dos nodos desean transferir deben primero establecer un canal o conexión por medio de un protocolo de llamada o señalización. Una vez establecida la conexión, las celdas de ATM incluyen información que permite identificar la conexión a la cual pertenecen.

B

Backbone: Principales conexiones troncales de Internet. Está compuesto de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo.

Backplane: Conexión entre una tarjeta o un procesador de interfaz, los buses de datos y los de distribución de energía.

BPDU: *Bridge Protocol Data Unit – Protocolo de Puente de Unidades de Datos*, mensajes de datos intercambiados entre conmutadores o switches en una LAN ampliada con topología de protocolo de árbol de conmutación. Los paquetes BPDU garantizan que los datos lleguen al destino previsto. Contienen información sobre las direcciones, costos, puertos o prioridades.

Bridge: Tecnología de capa de enlace, las cual envía tráfico de datos basados en la dirección MAC destino de los frames.

Broadcast: modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

C

Colisión: Situación que ocurre cuando dos o más dispositivos intentan enviar una señal a través de un mismo canal al mismo tiempo. El resultado de una colisión es generalmente un mensaje confuso. Todas las redes de computadoras requieren de algún mecanismo de ordenamiento para prevenir las colisiones o para recuperarse de éstas cuando ocurren.

Conmutación: Es la conexión que realizan los diferentes nodos que existen en distintos lugares y distancias para lograr un camino apropiado que permita conectar dos o más usuarios en una red de telecomunicaciones. La conmutación permite la descongestión entre los usuarios de la red disminuyendo el tráfico y aumentando el ancho de banda.

CRC: Algoritmo que permite comprobar la fiabilidad y la no alternación de los datos.

D

DHCP: *Dynamic Host Configuration Protocol - Protocolo de Configuración Dinámica de Hosts,* protocolo para configuraciones TCP/IP que permite la asignación y administración estática y dinámica de direcciones IP.

DNS: *Domain Name System - Sistema de Nombre de Dominio,* es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y viceversa.

Downstream: Velocidad con que los datos pueden ser transferidos de un servidor a un cliente, lo que podría traducirse como velocidad de bajada (downloading).

E

Encapsulamiento: Proceso por el cual los datos que se envían a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otro tipo de información.

Ethernet: Tecnología de redes de área local (LAN) que transmite información entre computadores a una velocidad de 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) ó 1000 Mbps (Gigabit Ethernet), (también conocido como estándar IEEE 802.3

F

FDDI: Conjunto de estándares ANSI e ISO para la transmisión de datos en líneas de fibra óptica en redes LAN que se pueden extender hasta un radio de 200km. El protocolo FDDI está basado en el protocolo Token Ring, las redes de área local FDDI pueden soportan miles de usuarios.

Fastethernet: Nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo). El nombre Ethernet viene del concepto físico de *ether*. El prefijo *fast* se le agregó para diferenciarla de la versión original Ethernet de 10 Mbps.

G

GARP: Protocolo de propósitos generales que registra cualquier información de conectividad de red o de estilo de pertenencia.

Gestión de red: Planificación, organización, mantenimiento y control de los elementos que forman una red, para garantizar un nivel de servicio de acuerdo a un costo.

GigabitEthernet: Ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento

I

IDF: Rack de cables que interconecta y administra las telecomunicaciones entre el tráfico de un MDF y dispositivos de red. Los cables de una red en un edificio viajan a través de de IDFs individuales conectados todos a un MDF.

IEEE: *Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Electricistas y Electrónicos,* asociación técnico-profesional mundial dedicada a la estandarización.

Internetworking: Campo dentro de las redes de datos, que se encarga de integrar o comunicar una red de área local con otra, constituyendo redes MAN o WAN.

IPv6: Versión 6 del Protocolo de Internet, encargado de dirigir y encaminar los paquetes de información, fue diseñado en los años 70 con el objetivo de interconectar redes. Esta nueva versión del Protocolo de Internet está destinada a sustituir al estándar IPv4, el cual cuenta con un límite de direcciones de red, lo que impide el crecimiento de la red.

M

MDF: Es común que las redes de gran tamaño tengan más de un centro de cableado. Normalmente, cuando esto sucede, uno de los centros de cableado se designa como el servicio de distribución principal (MDF).

MTU: *Maximum Transmission Unit - Unidad máxima de Transferencia*, es un parámetro que indica el tamaño máximo que debe tener un datagrama para que sea transmitido por una interfaz IP sin que necesite ser fragmentado en unidades más pequeñas.

Multicast: Envío de la información en una red a múltiples destinos simultáneamente.

Multiplexar: Combinación de dos o más canales de información en un solo medio de transmisión.

N

NetBios: Protocolo de redes comúnmente usado en redes LAN. Provee redirección de impresoras y archivos, es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollada para enlazar un sistema operativo de red con hardware específico.

NIC: *Network Interface Card – Tarjeta de Red*, es el dispositivo electrónico que permite a un terminal (computadora, impresora, etc.) acceder a la red y compartir recursos (datos o dispositivos).

O

OSI: Open *System Interconnection - Modelo de Referencia de Interconexión de Sistemas Abiertos*, es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en 1984, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

P

P2P: Red de computadoras en la que todos o algunos aspectos de ésta funcionan sin clientes ni servidores fijos, sino como una serie de nodos que se

comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

Patch panel: Panel que contiene múltiples conexiones de los cables. También es conocido como un jackfield o bahía parche.

PoE: Es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de cable UTP / STP en una red Ethernet. PoE se rige según el estándar IEEE 802.3af y abre grandes posibilidades al momento de dar alimentación a dispositivos tales como cámaras de seguridad o puntos de acceso inalámbricos.

Protocolo: Convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. En su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación.

PVST: Protocolo perteneciente Cisco, el cual es utilizado para configurar STP en VLANs distintas dentro de un switch.

Q

QoS: Tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*).

S

SNAP: Estándar que se utiliza para distinguir protocolos encapsulados, es decir, añade un byte de cabecera en las tramas, con el que se indica cual es el protocolo que va encapsulado en cada paquete.

SSH: Secure SHell es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. SSH cifra la sesión de

conexión, haciendo imposible que alguien pueda obtener contraseñas no cifradas.

SSID: Nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de ésta. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

T

Tagged: Configuración que se puede asignar a un Puerto, si lo que se desea es que a través de él circules tramas de varias VLANs.

Telnet: Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).

Token Ring: Topología en la que los dispositivos están conectados como si formaran un círculo. Un *token* o paquete especial de red, viaja a través del anillo y permite que los equipos intercambien información entre sí.

U

Untagged: Configuración de un puerto que indica la pertenencia a una sola VLAN.

Upstream: Velocidad con que los datos pueden ser transferidos de un cliente a un servidor, lo que podría traducirse como velocidad de carga, subida (uploading).

V

VPN: *Virtual Private Network – Red Privada Virtual*, tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, por ejemplo Internet.

W

WAN: *Wide Area Network – Red de Área Extensa*, redes punto a punto que interconectan países y continentes, son capaces de transportar una gran cantidad de datos, su alcance es una gran área geográfica, por ejemplo: una ciudad o un continente.

WiFi: *Wireless Fidelity – Fidelidad Inalámbrica*, Es un conjunto de redes que no requieren de cables y que funcionan en base a ciertos protocolos previamente establecidos.

BIBLIOGRAFÍA

1. Barcelo, J. M., J. Iñigo, G. C y E. Peig. 2009. *Estructura de redes de Computadores.* Editorial UOC, Barcelona. 338 pp

2. Dordoigne, José y Atelin, Philippe. 2006. *Redes informáticas: Conceptos Fundamentales. Colección de Recursos informáticos.* Ediciones ENI, Barcelona. 451 pp.

3. Odom, W. 2003. *CCNA INTRO exam certification guide: CCNA self-study 640-821.* Cisco Press, USA. 613 pp.

4. Tanenbaun, Andrew S. 2003. *Redes de computadoras.* Pearson Prentice Hall, México. 891 pp.

MANUALES

1. 3Com Care Technical Education. 1995. *Curso de Tecnología Básica de Redes 3CS – MX1.* 434 pp.

2. 3Com Care Technical Education. 1999. *Certificación Switches Capa 3, 3CS – MX06.* 440 pp.

ENLACES WEB

- Greene, D. 2001. *802.1Q VLANs for better bandwidth.* Obtenida el 28 de noviembre de 2009 de,

  http://www.networkworld.com/news/tech/2001/0305tech.html

- Javvin Technologies, Inc. (n. d.). *VLAN: Virtual Local Area Network and IEEE 802.1Q***.** Obtenida el 18 de diciembre de 2009 de, http://www.javvin.com/protocolVLAN.html

- *Ethernet*. Obtenida el 15 de enero de 2010 de, http://www.mitecnologico.com/Main/Ethernet

- *LANs Virtuales*. Obtenida el 20 de enero de 2010 de, http://gemini.udistrital.edu.co/comunidad/profesores/jruiz/jairocd/texto/protocolos/temas/conmutacioncapa2/vlan/LANs%20Virtuales%20%5BModo%20de%20compatibilidad%5D.pdf
- Cisco. 2002. *Packet® Icon Library*. Obtenida el 20 de enero de 2010 de, http://www.slideshare.net/fmarches/cisco-icon-library
- Ledesma, R. 2008. *All Networking*. Obtenida el 3 de febrero de 2010. http://allnetworking.blogspot.com/2008/03/8021q.html
- Cisco. 2006. *Inter-Switch Link and IEEE 802.1Q Frame Format.* Obtenida el 10 de febrero de 2010 de,

  http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml#topic1
- Amaya, J. (n.d.). *VLAN Redes Virtuales.* Obtenida el 10 de febrero de 2010 de, http://www.angelfire.com/al4/vlan/LABORATO.htm
- Fluke Networks. (n. d.). *EtherScope™ Series II Network Assistant.* Obtenida el 10 de marzo de 2010 de, http://www.flukenetworks.com/fnet/es-es/products/Etherscope+Series+II/Overview.htm
- Microsoft Tech Net. 2010. *Introducción a HyperTerminal*. Obtenida el 20 de marzo de 2010 de, http://technet.microsoft.com/es-es/library/cc736511%28WS.10%29.aspx
- *VLAN s en PfSense 1.2 y 3Com 2924-SFP Plus. Sistema Voice VLAN. Parte 1.* Obtenida el 25 de marzo de 2010 de, http://www.homelesshosting.net/2009/03/06/vlans-en-pfsense-12-y-3com-2924-sfp-plus-sistema-voice-vlan/
- *Configuración de la VLAN/SSID Usuaria Típica.* Obtenida el 15 de abril de 2010 de,

  http://support.dell.com/support/edocs/network/tmap1170/sp/Configuration_options/Network_Parameters/Typical_User_VLAN_Configurations.htm
- *Terminología de redes*. Obtenida el 17 de abril de 2010 de, http://www.adrformacion.com/cursos/wserver/leccion1/tutorial3.html

- Muñoz, J. 2007. *Fiber Deep: Una alternativa para optimizar una red de cable.* Obtenida el 18 de mayo del 2010 de, http://www.cinit.org.mx/articulo.php?idArticulo=54
- Espinoza, J. 2002. *Red Virtual*. Obtenida el 30 de mayo de 2010 de, http://www.usmp.edu.pe/publicaciones/boletin/fia/info41/redprivada.html
- Valarezco, D. (n. d.). *Enrutamiento entre VLAN*. Obtenida el 13 de junio de 2010 de, http://www.slideshare.net/darwinnano/enrutamiento-entre-vlan
- *VLAN - LAN VIRTUALES: Seguridad, segmentación, flexibilidad.* Obtenida el 7 de julio de 2010 de, http://www.aprendaredes.com/boletin28.htm