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**.

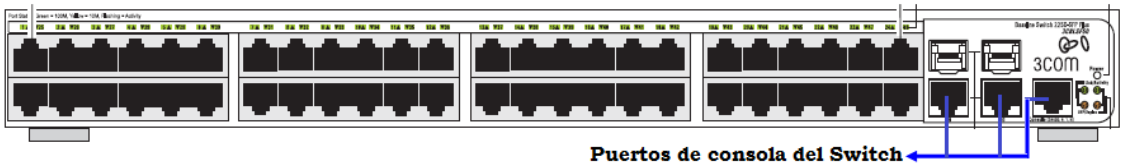


Figura IV.1. Panel Frontal de Switch 3Com Baseline 2226-SFP Plus

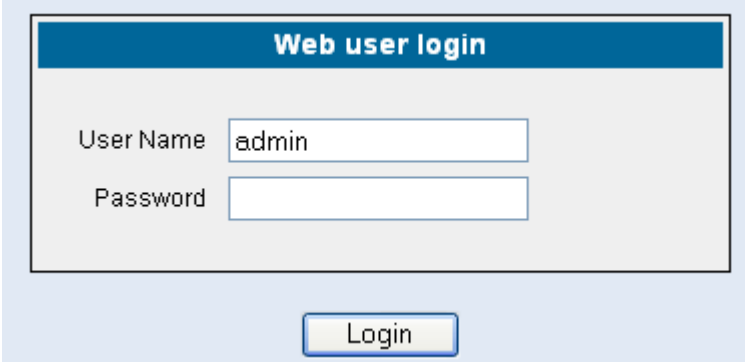


Figura IV.2. Solicitud de usuario y contraseña

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**.

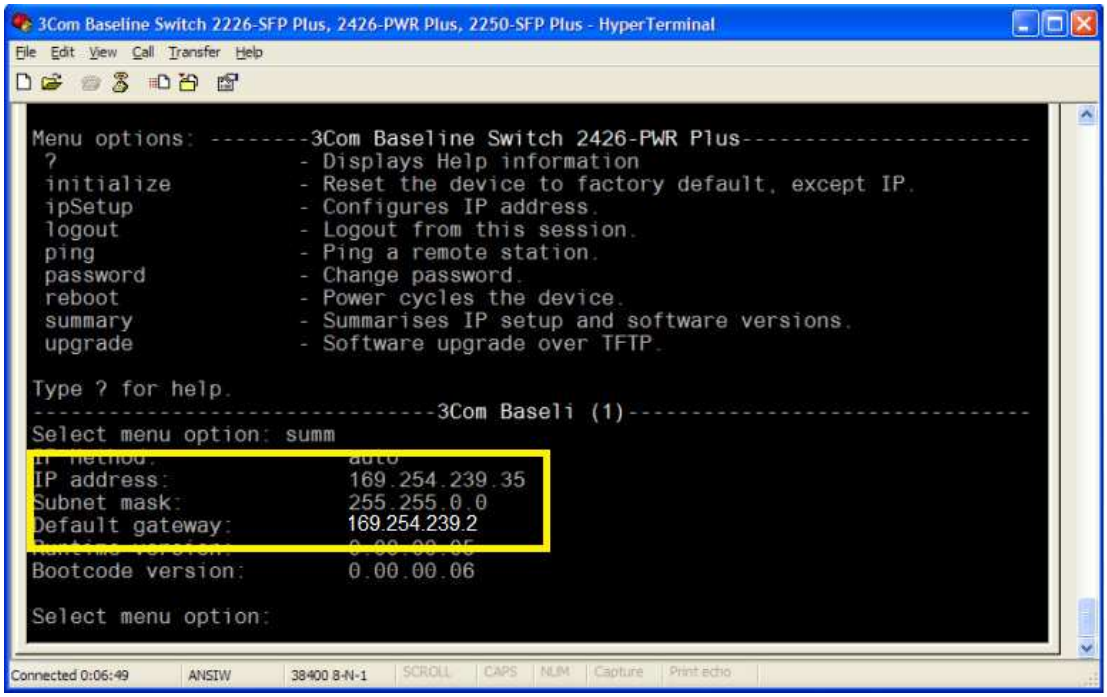


Figura IV.3 Direcciones tomadas automáticamente por el switch

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**.

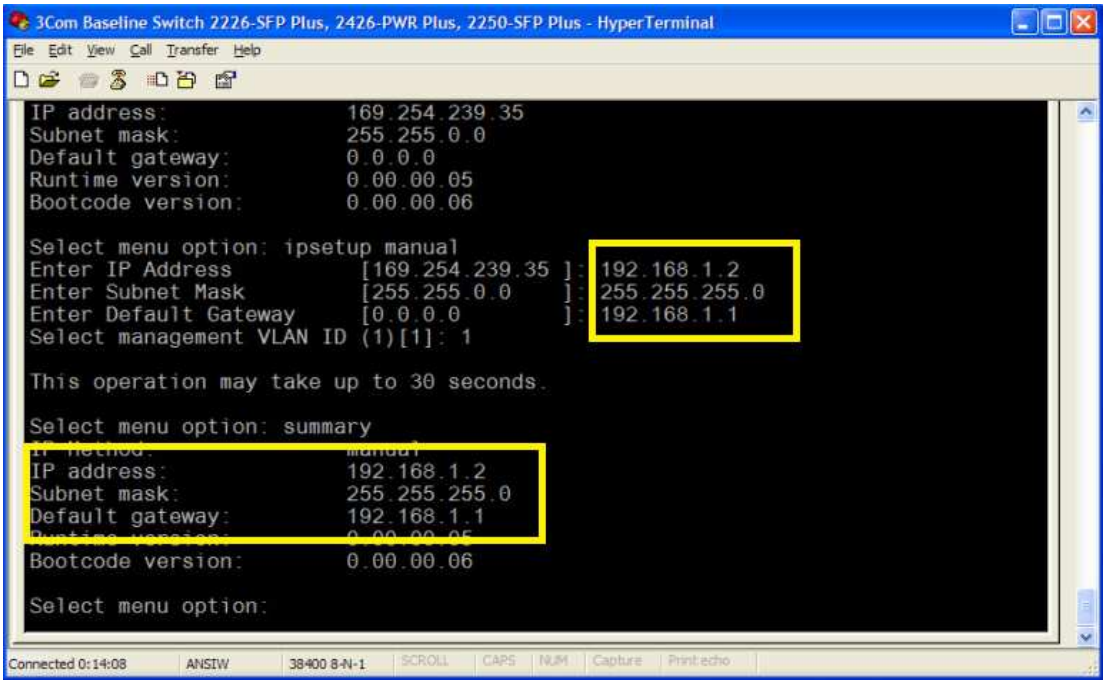


Figura IV.4 Configuración manual

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**.

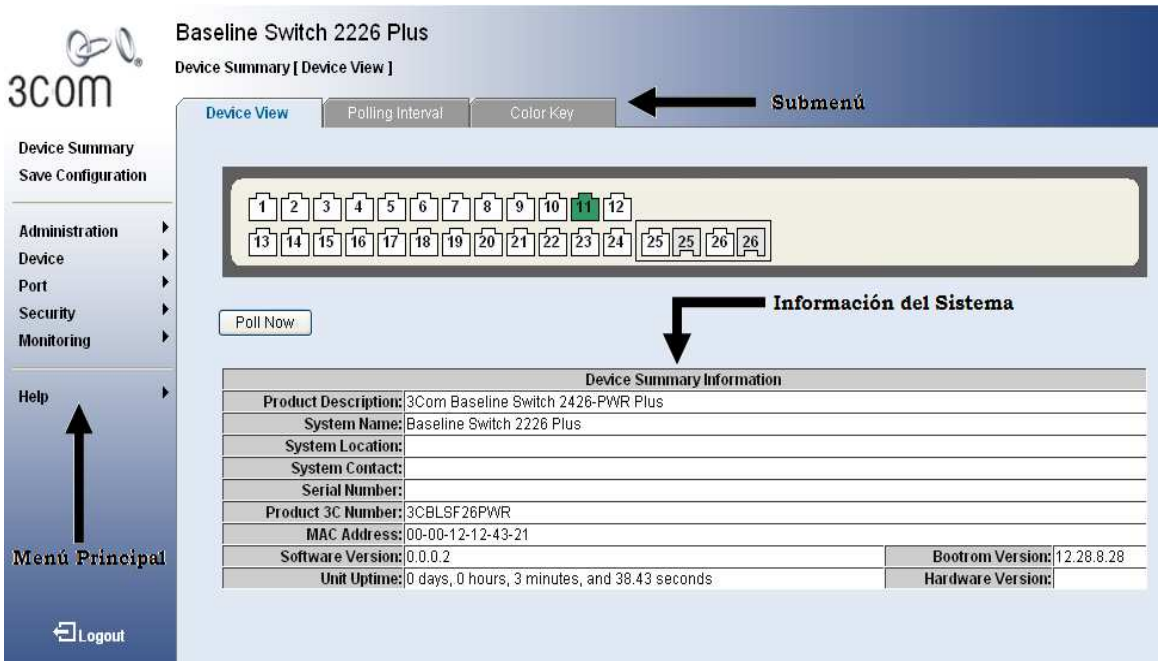


Figura IV.5 Interfaz del switch

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.*

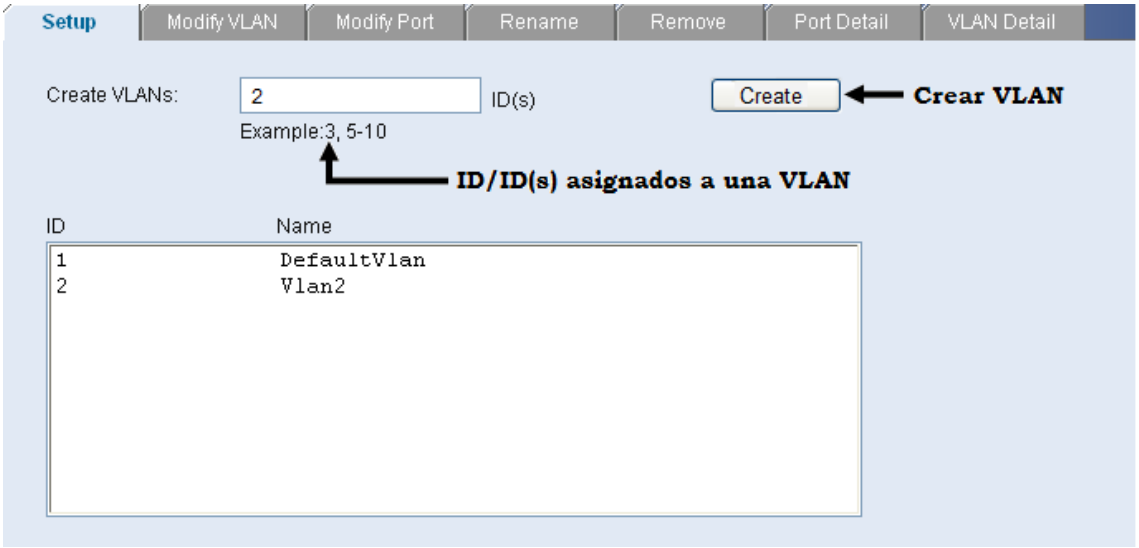


Figura IV.6 Creación de una VLAN

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.

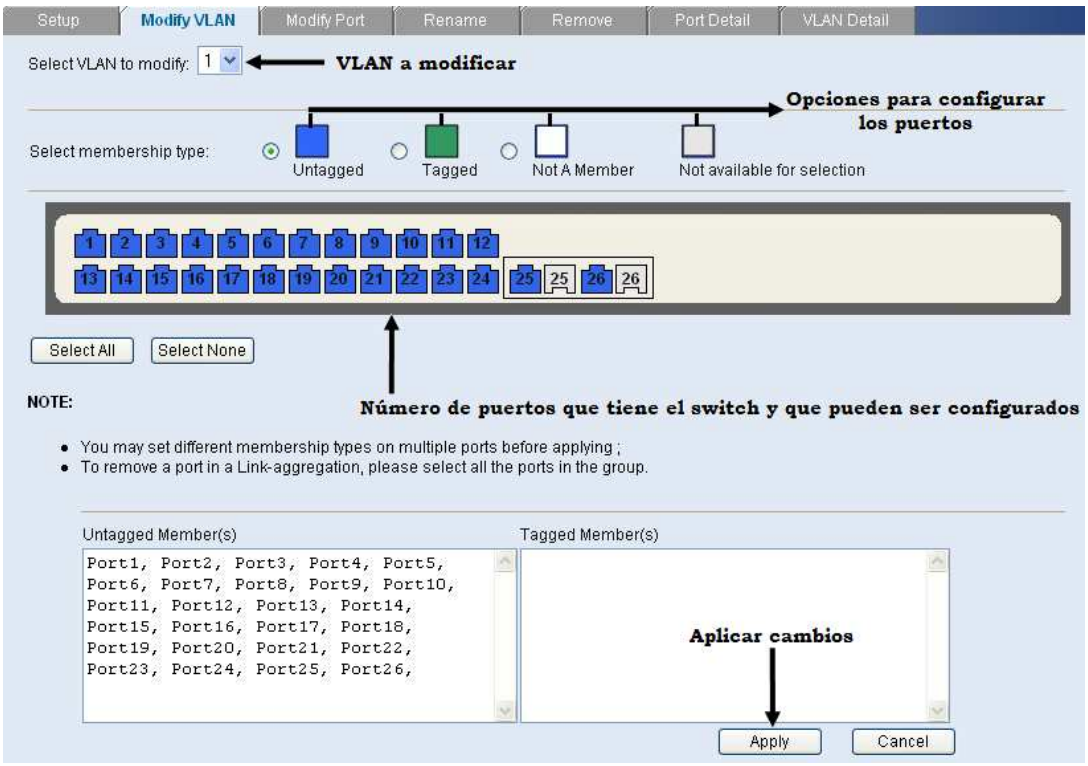


Figura IV.7 Modificar VLAN

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**.

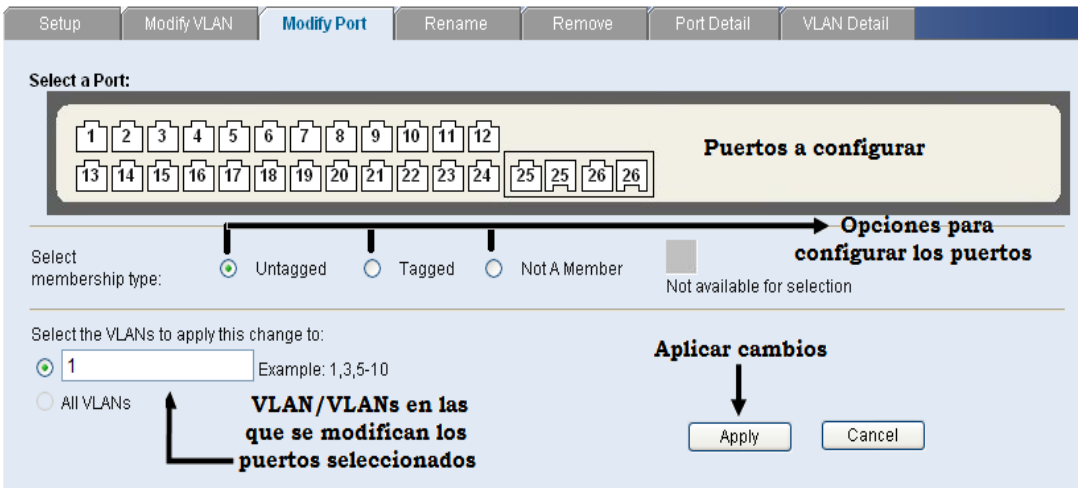


Figura IV.8 Modificar puerto

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**.

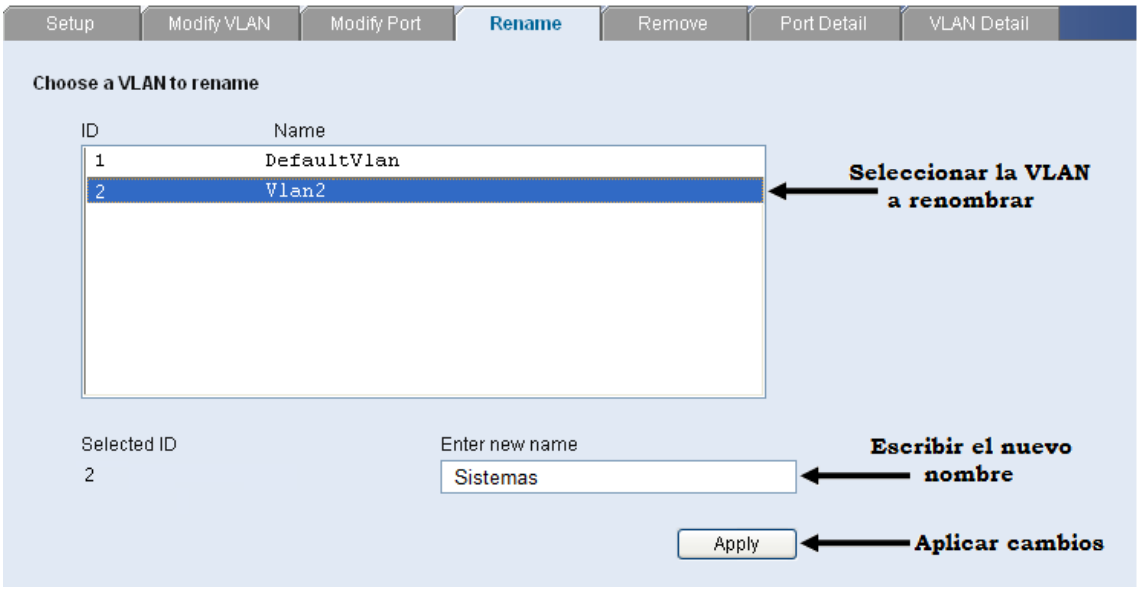


Figura IV.9 Renombrar VLAN

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.

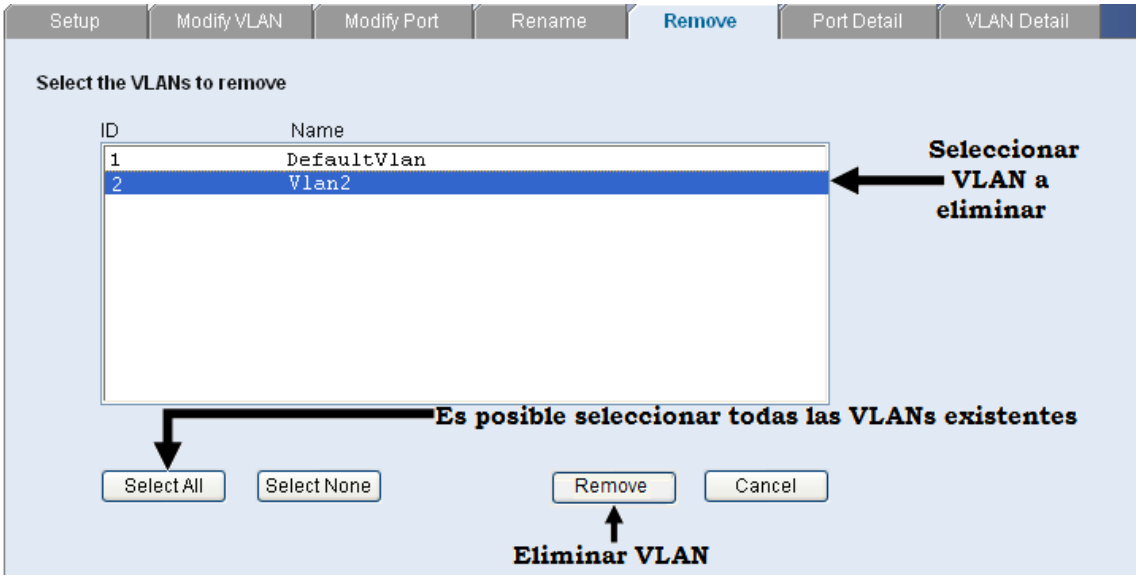


Figura IV.10 Eliminar una VLAN

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**

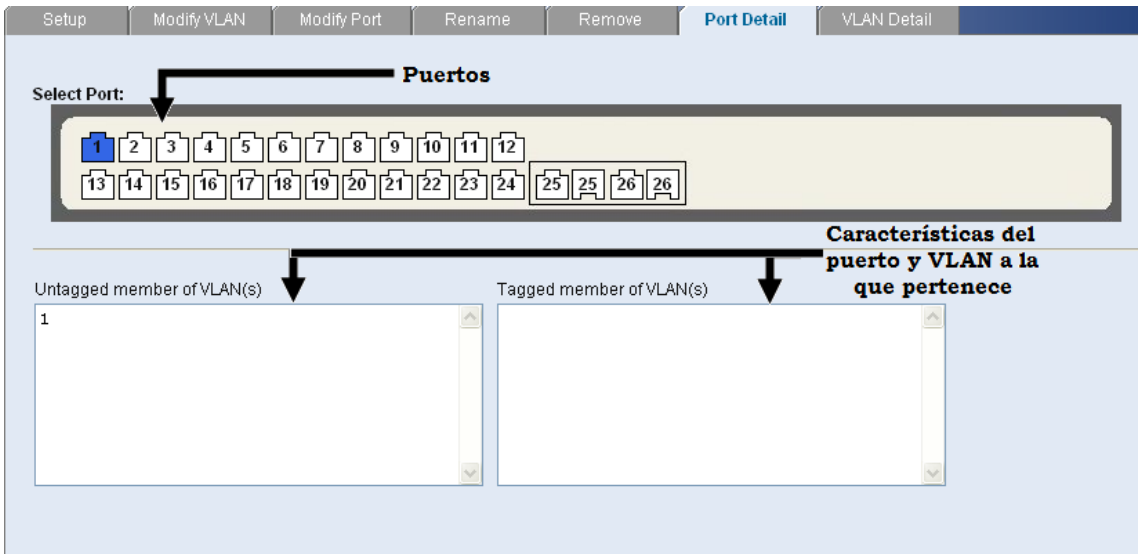


Figura IV.11 Detalles de puertos

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**.

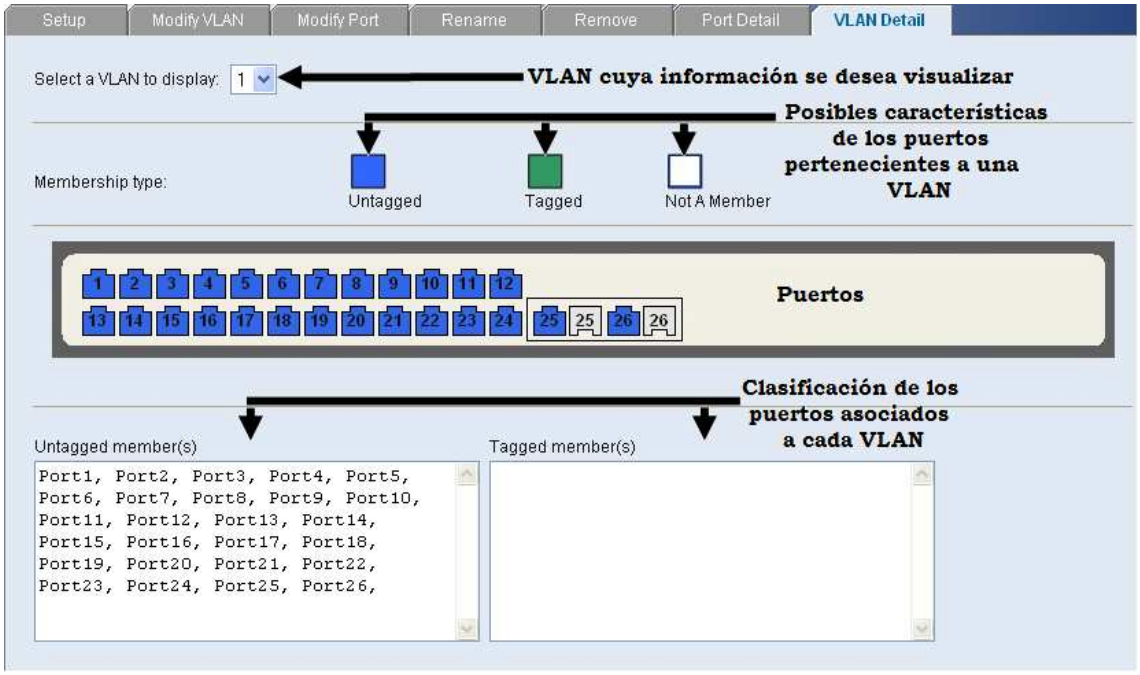


Figura IV.12 Detalles de VLAN

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.

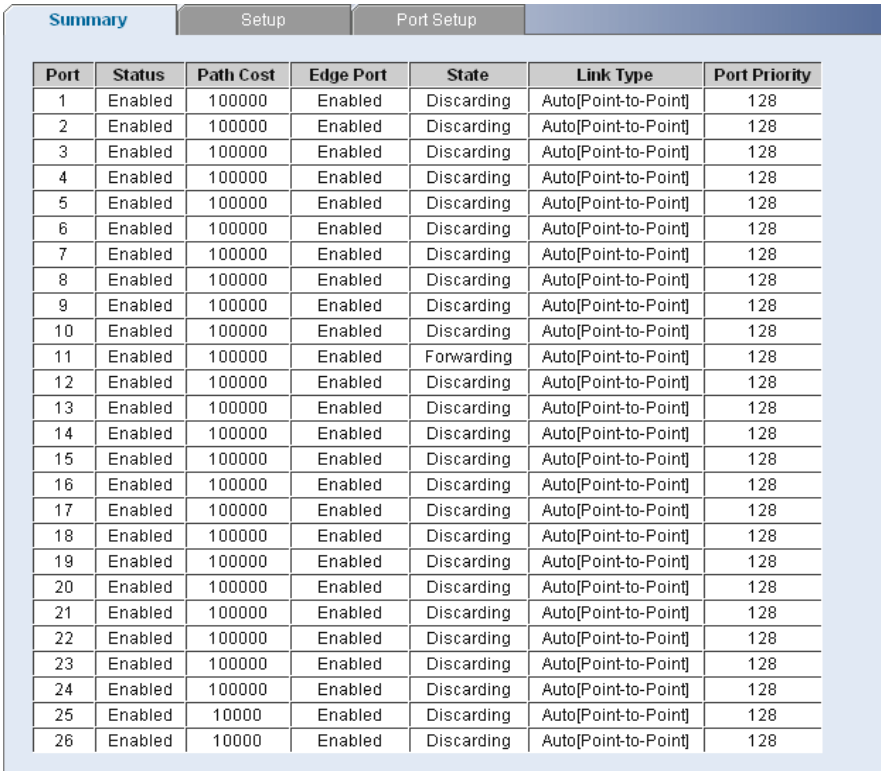
Dentro de lo que es la administración de VLANs vía Web, existe también la manipulación de STP, únicamente en el caso de que los switches sean compatibles con el estándar, por ello es importante tener una noción de lo que este protocolo es capaz de hacer, puesto que las configuraciones realizadas en los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

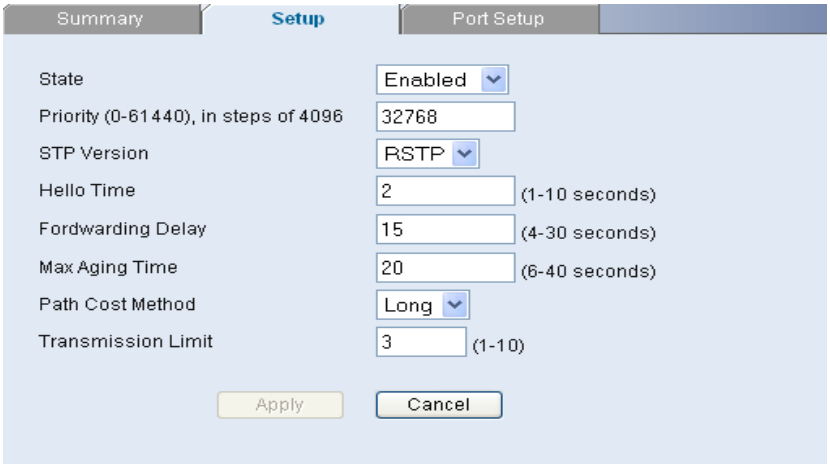


Figura IV.14 Setup

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.**

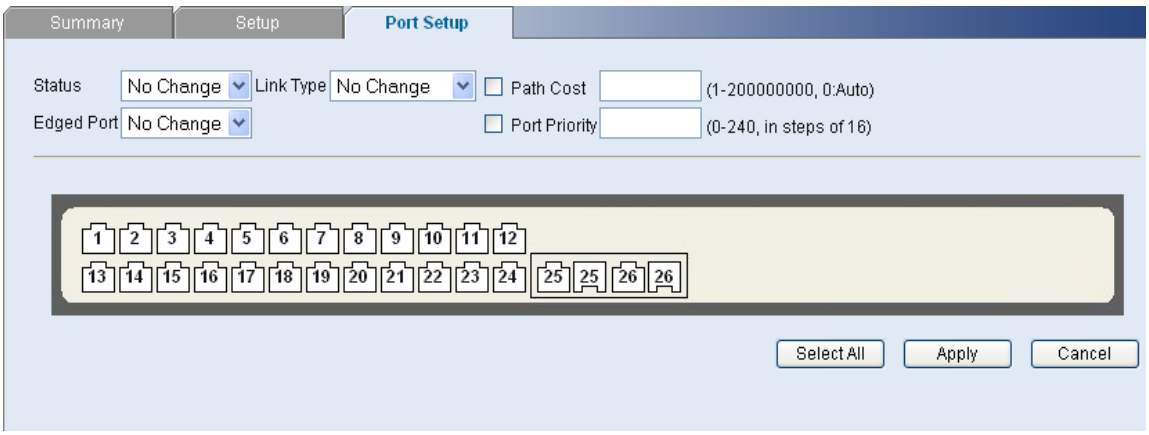


Figura IV.15 Port Setup

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.**

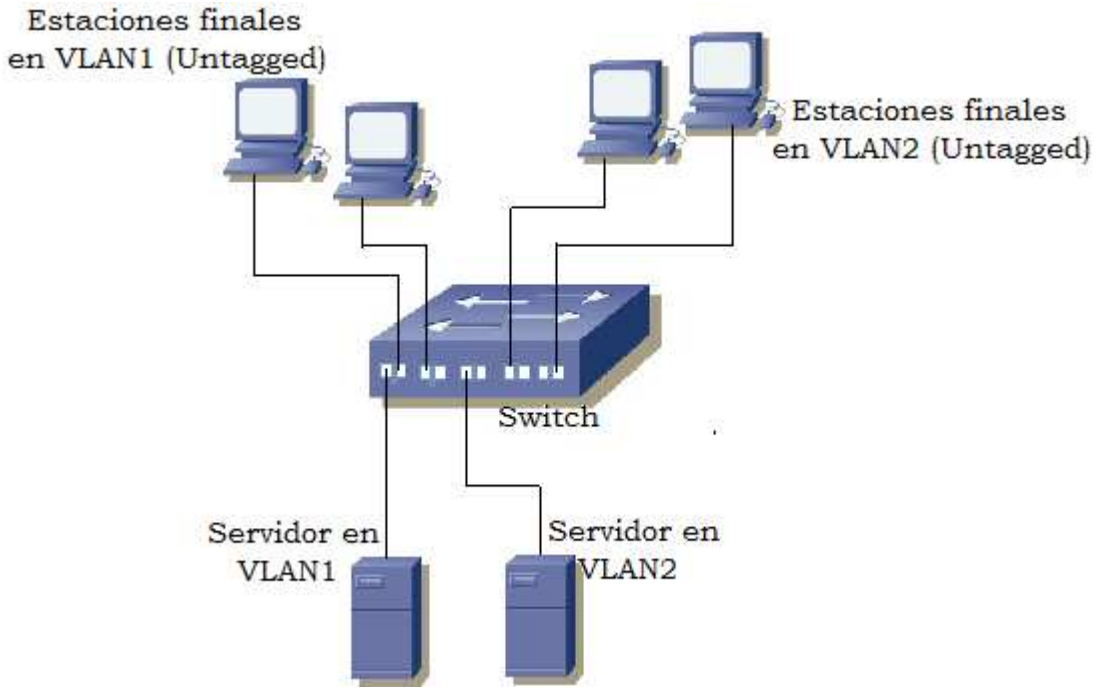


Figura IV.16 Configuración de puertos Untagged

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.

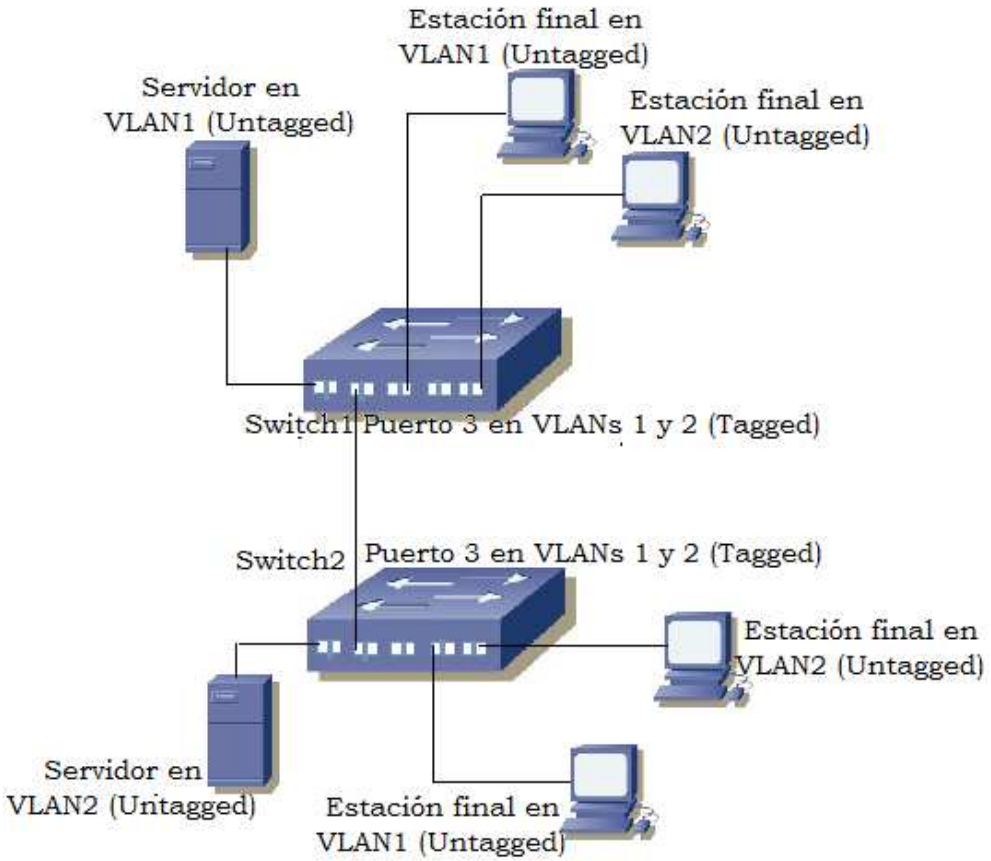


Figura IV.17 Configuración de puertos Tagged

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.

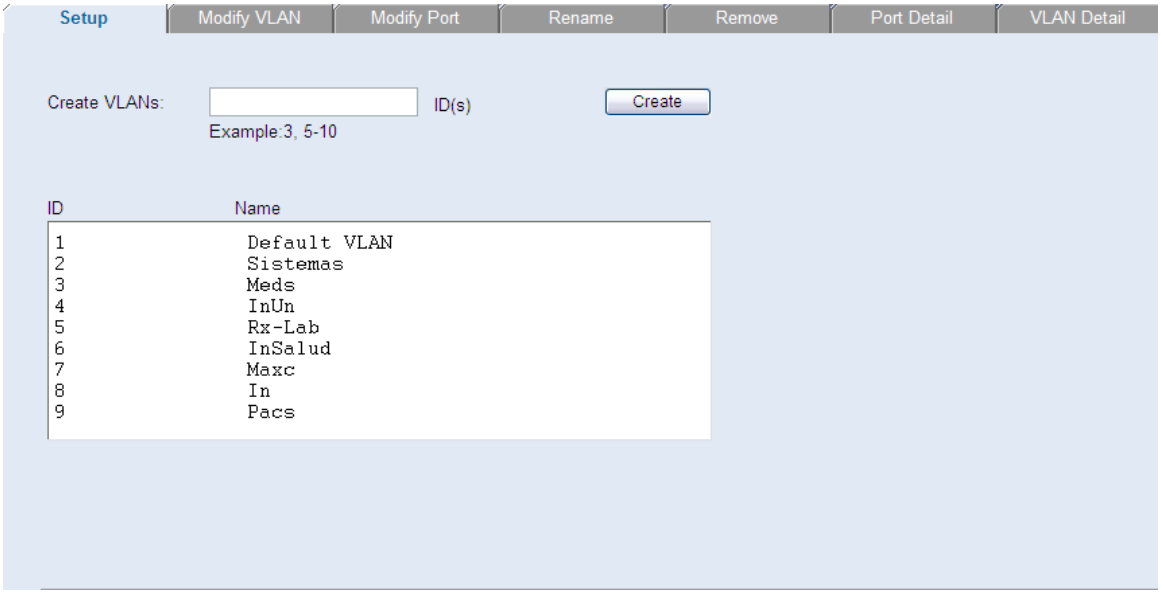


Figura IV.18 VLANs del Instituto Hospitalario

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

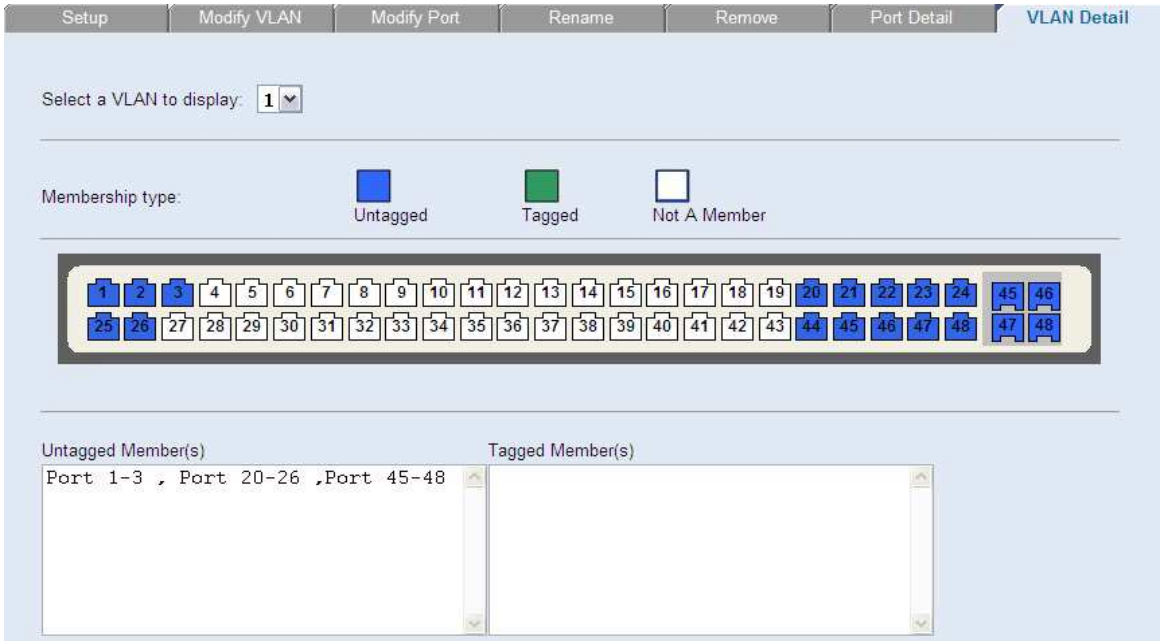


Figura IV.19 VLAN 1

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**.

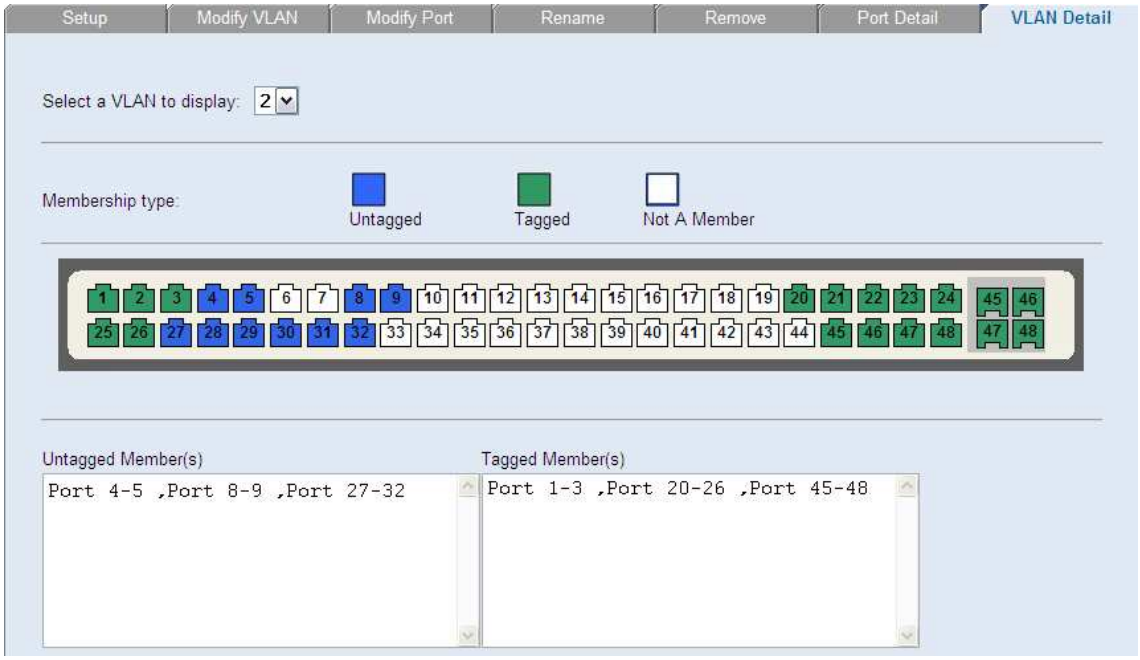


Figura IV.20 VLAN 2

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.

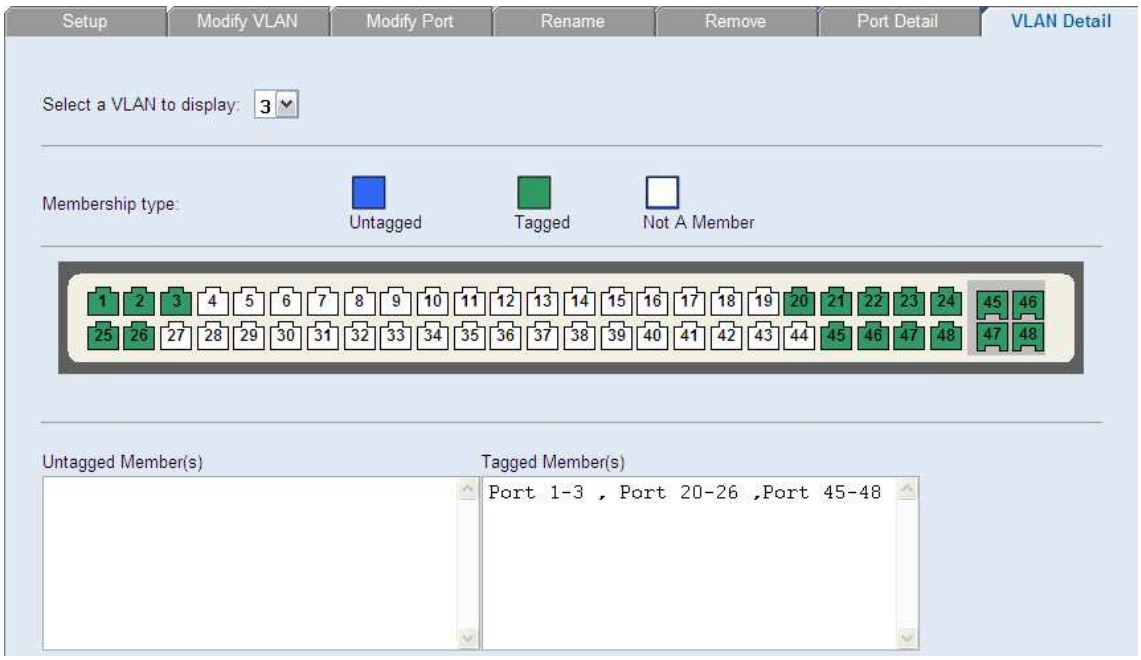


Figura IV.21 VLAN 3

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**.

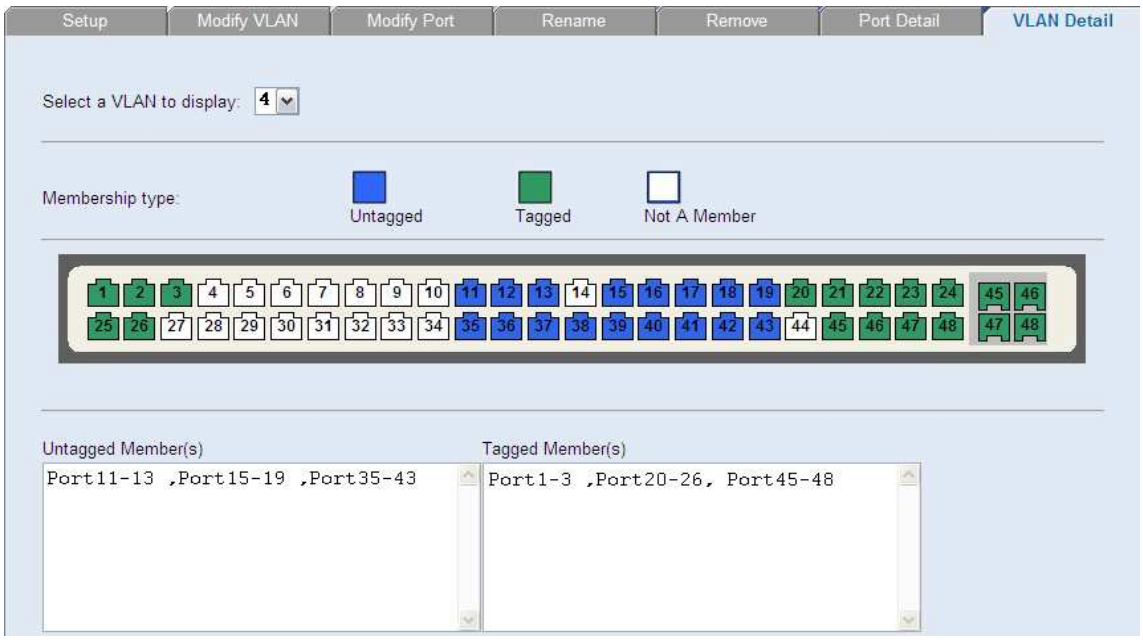


Figura IV.22 VLAN 4

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.**

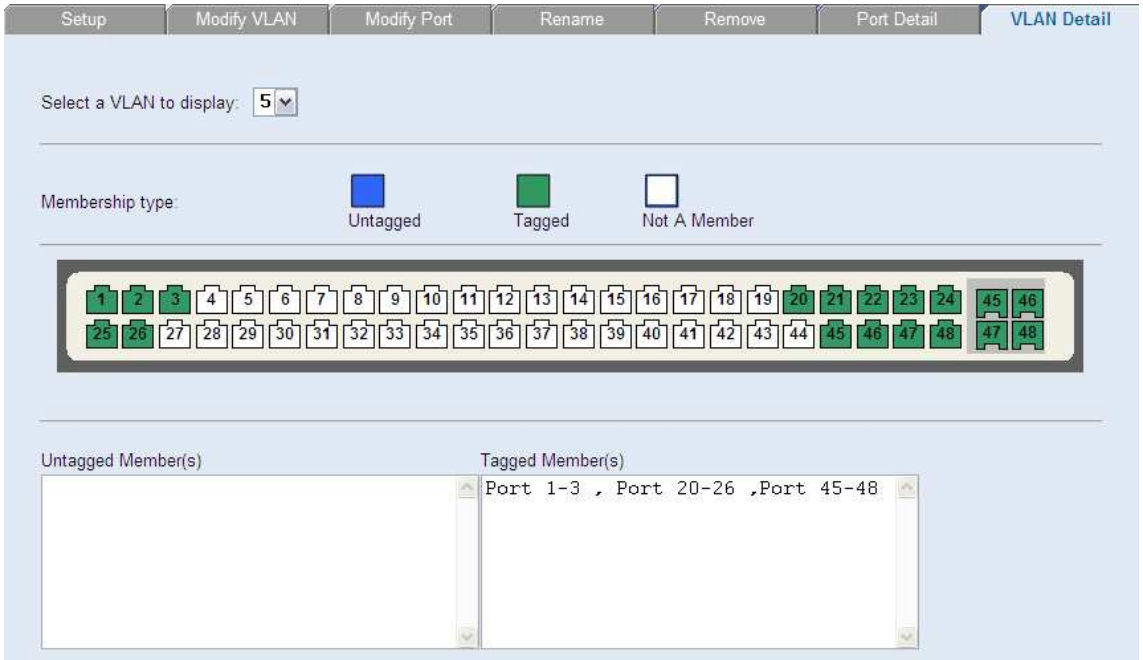


Figura IV.23 VLAN 5

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.**

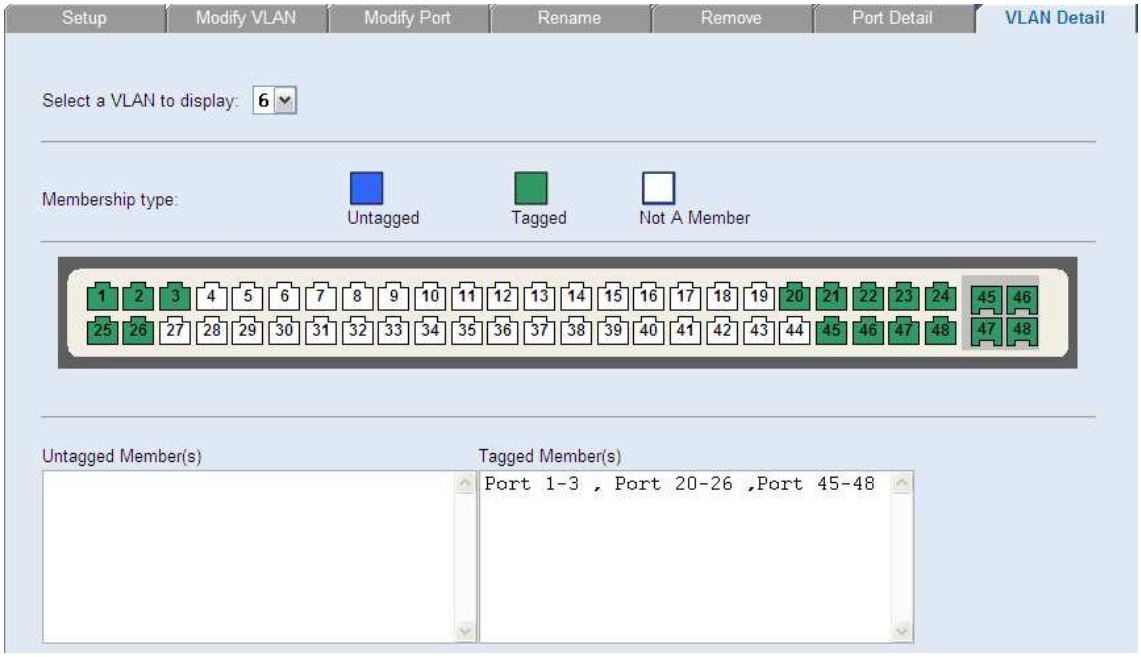


Figura IV.24 VLAN 6

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

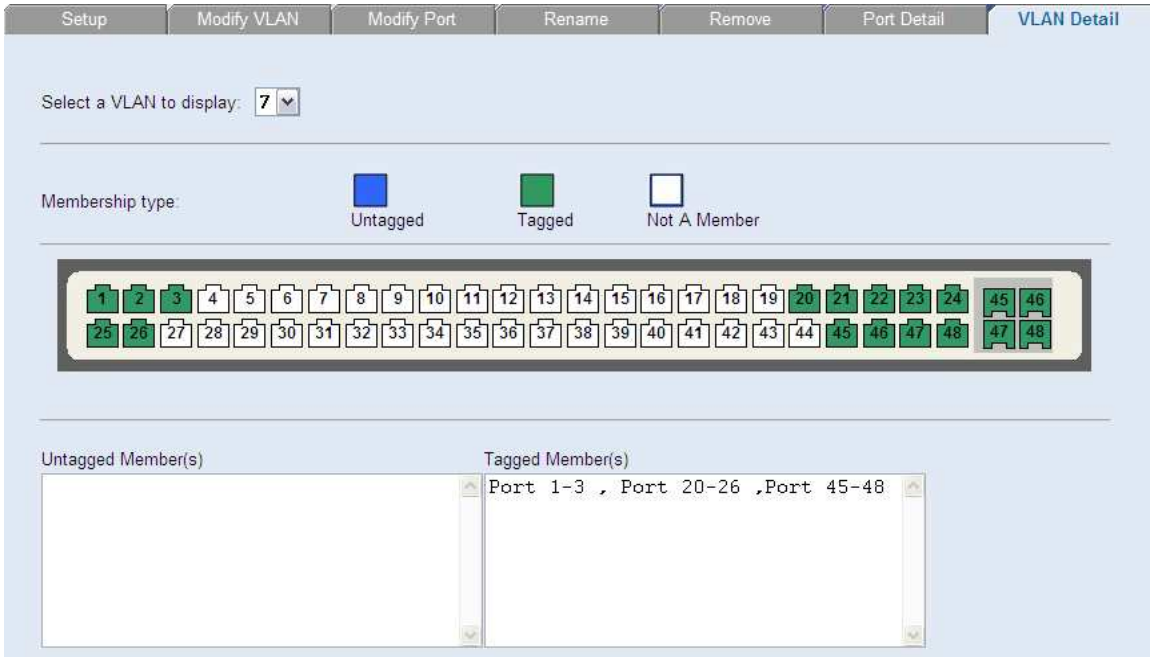


Figura IV.25 VLAN 7

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.

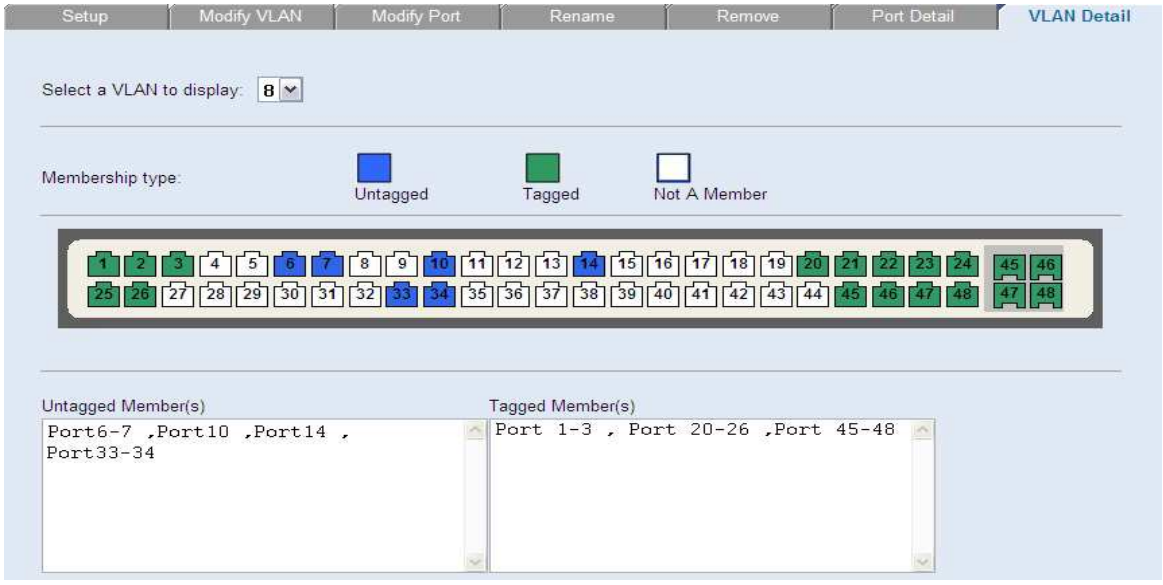


Figura IV.26 VLAN 8

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

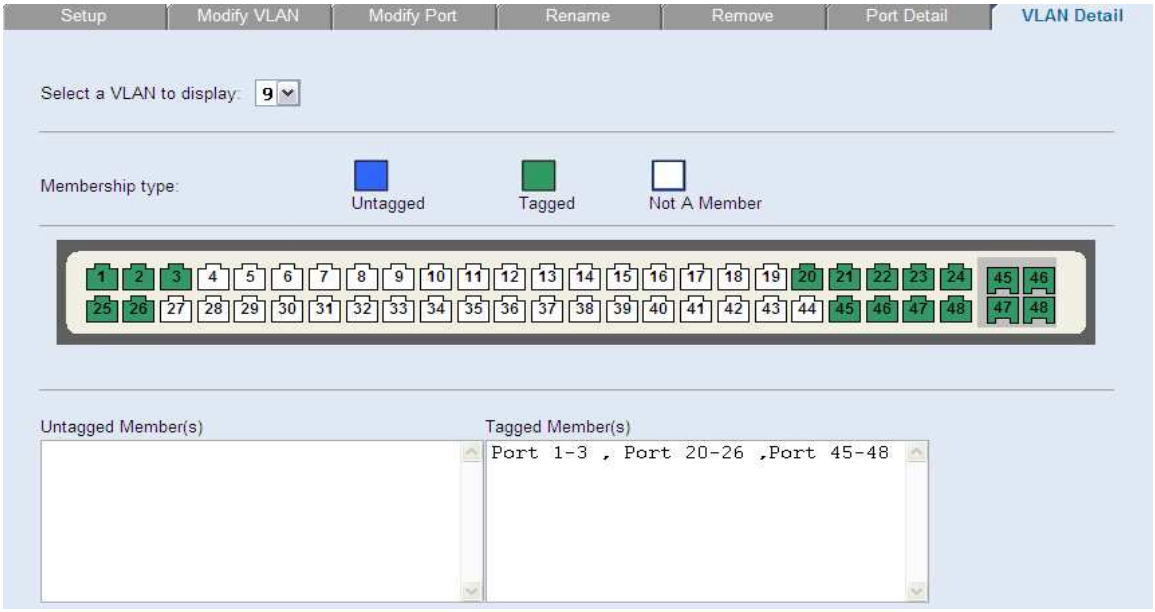


Figura IV.27 VLAN 9

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**.

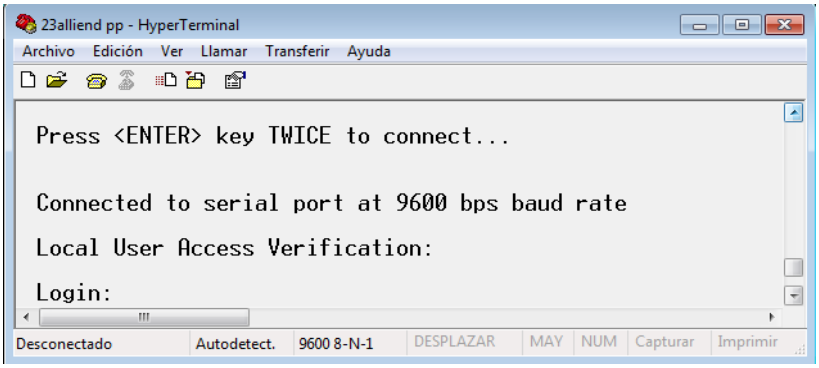


Figura IV.28 Establecer una sesión en HyperTermial

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

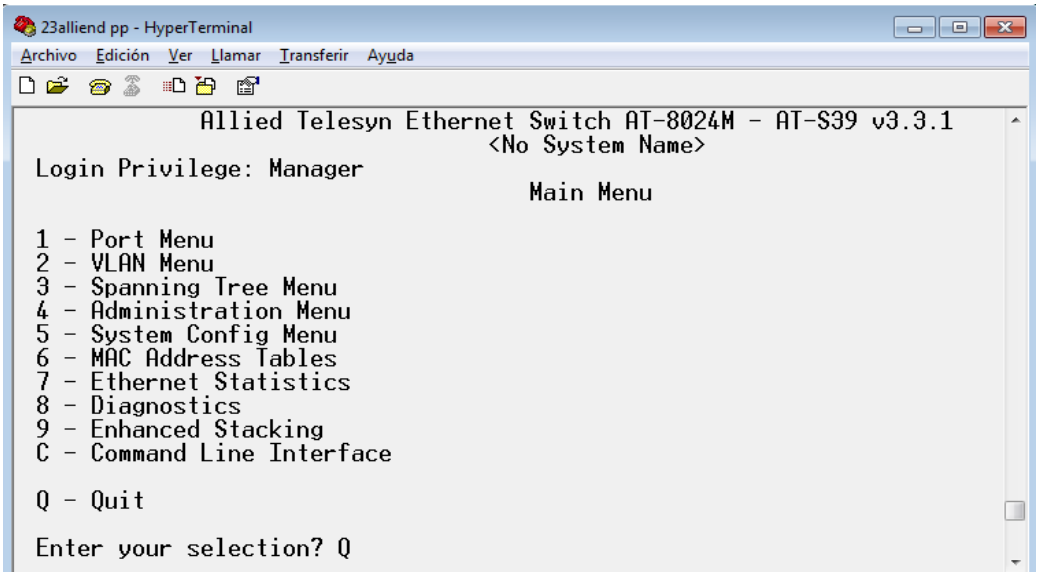


Figura IV.29 Menú Principal

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

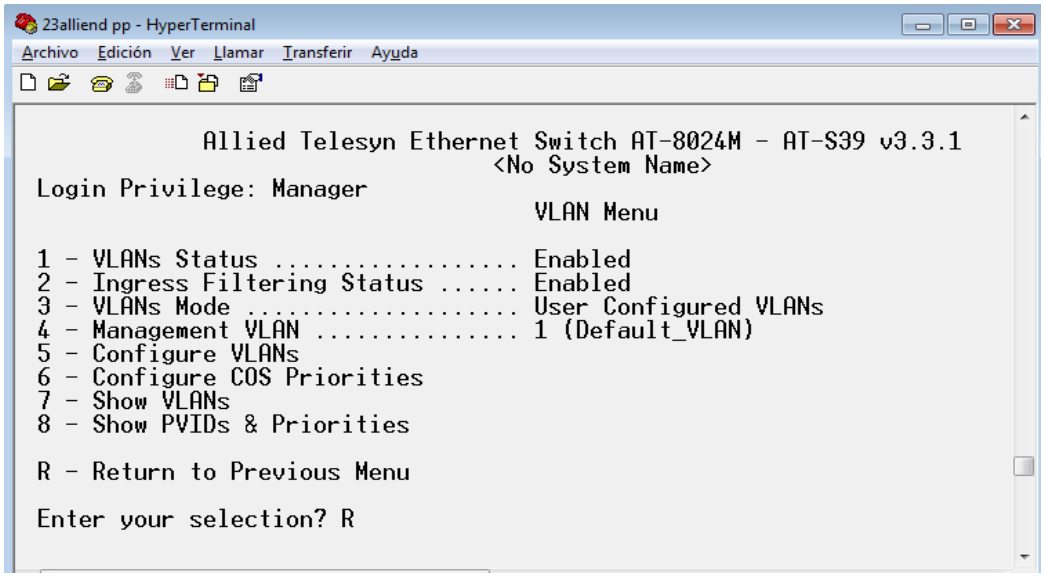


Figura IV.30 VLAN Menú

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.

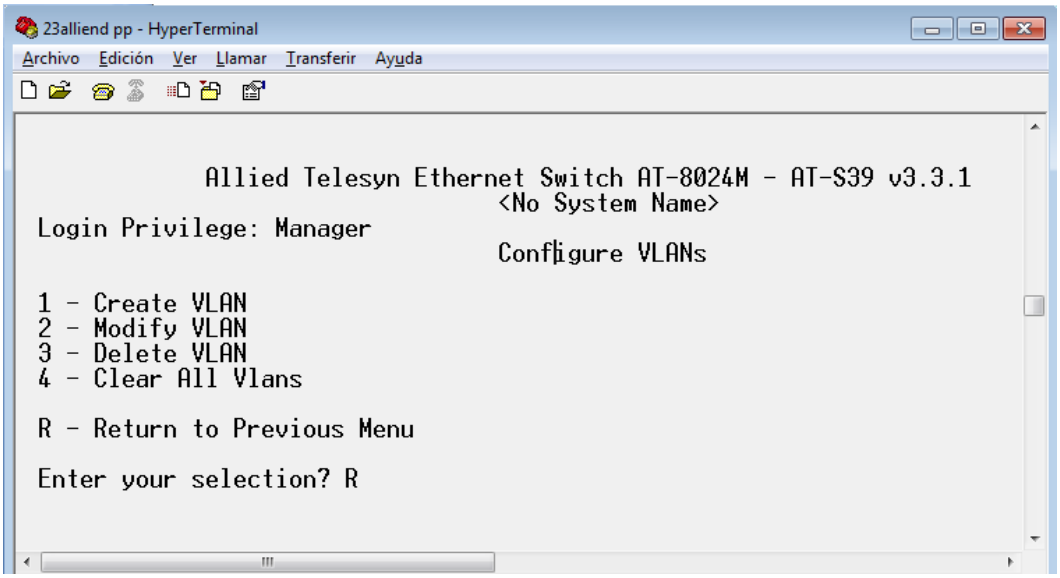


Figura IV.31 Configurar VLANs

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

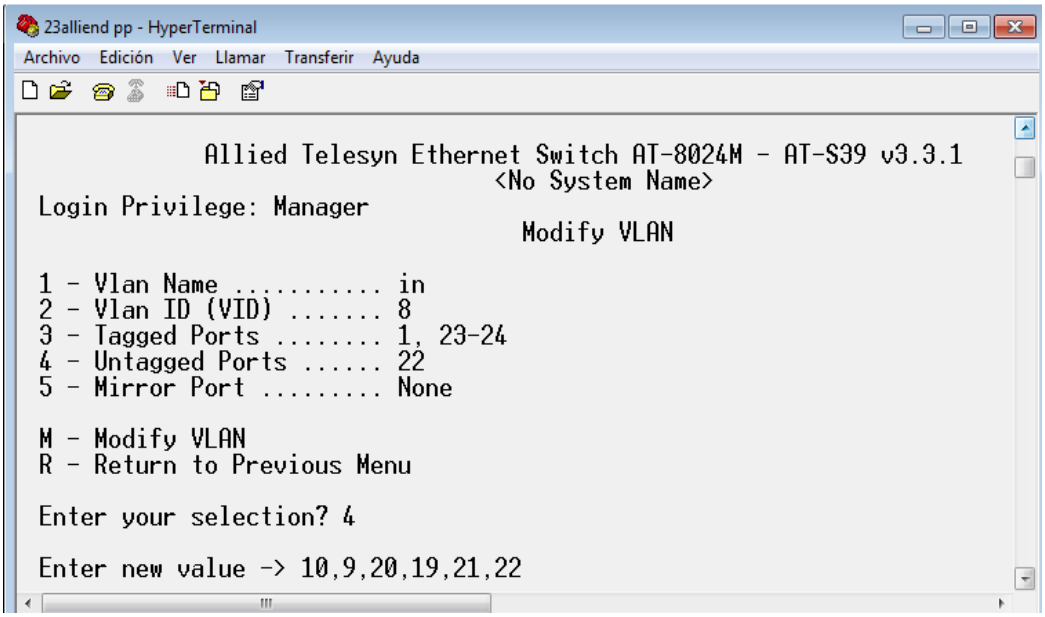


Figura IV.32 Modificar VLAN

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.**

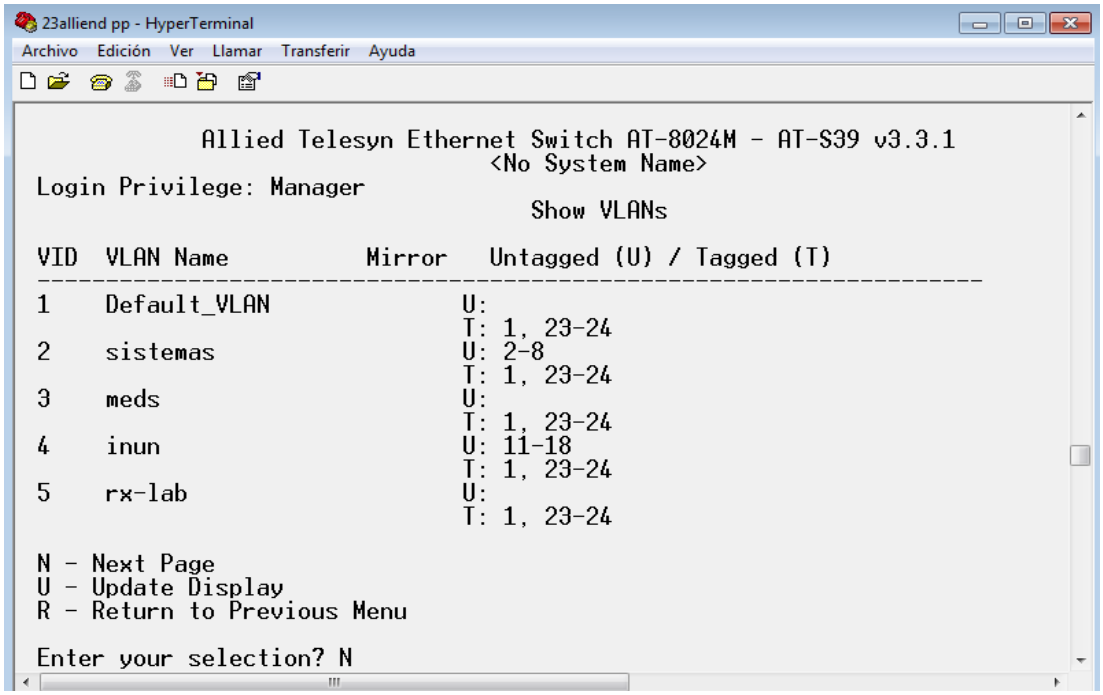


Figura IV.33 VLANs de la 1 a la 5

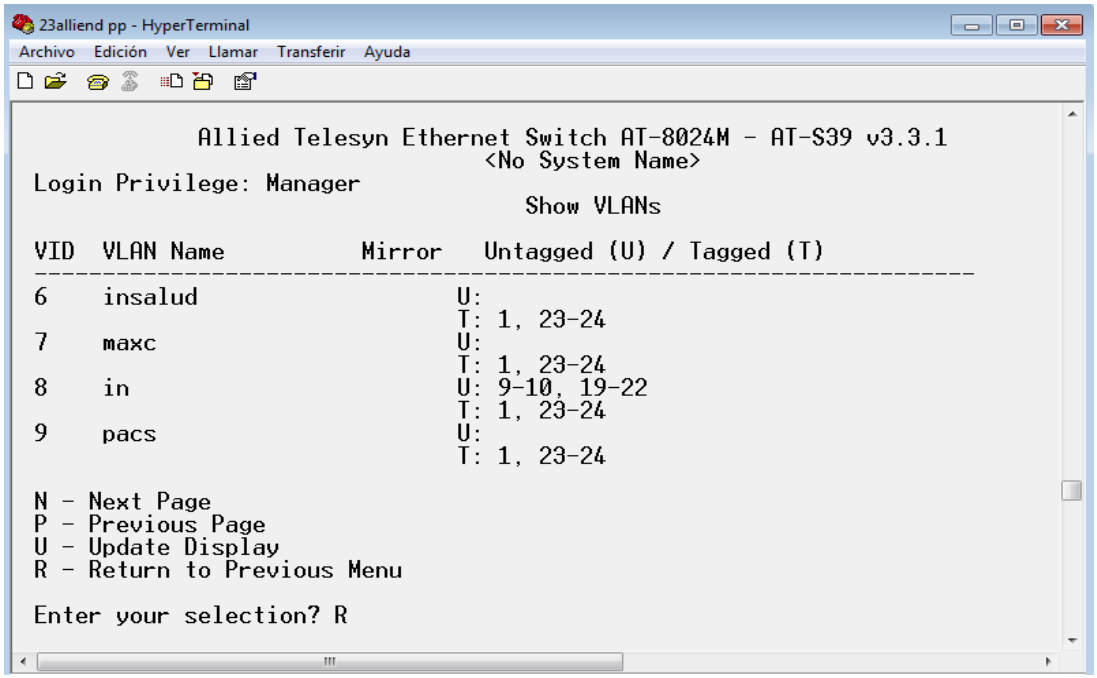


Figura IV.34 VLANs de la 6 a la 9

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.**

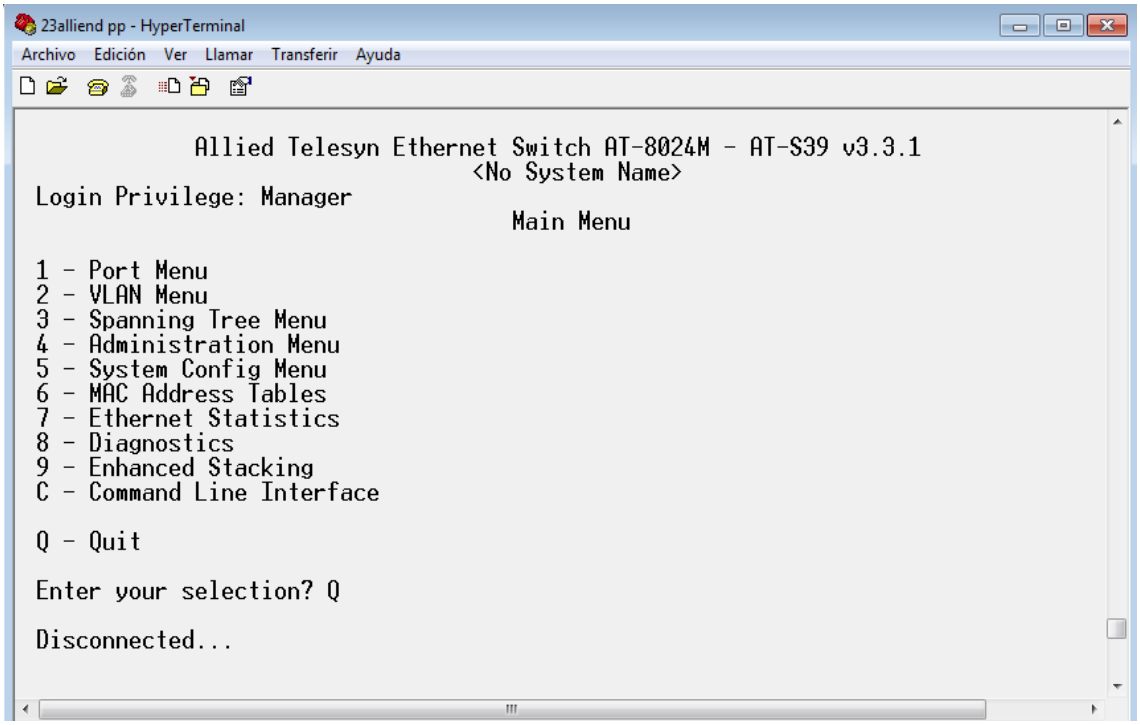


Figura IV.35 Salir de la sesión de HyperTerminal

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.