

**DISEÑO DE UN LABORATORIO PARA LA IMPLEMENTACIÓN Y  
CONFORMACIÓN DE REDES DE ÁREA LOCAL VIRTUALES (VLAN)  
PARA EL PROGRAMA DE LA ESPECIALIZACIÓN EN  
TELECOMUNICACIONES DE LA UNIVERSIDAD INDUSTRIAL DE  
SANTANDER**

**LEANDRO IGNACIO PATIÑO CASTILLO  
GABRIEL EDUARDO VARGAS HERNANDEZ**

UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE CIENCIAS FÍSICOMECÁNICAS  
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES  
ESPECIALIZACION EN TELECOMUNICACIONES  
2006

DISEÑO DE UN LABORATORIO PARA LA IMPLEMENTACIÓN Y  
CONFORMACIÓN DE REDES DE ÁREA LOCAL VIRTUALES (VLAN)  
PARA EL PROGRAMA DE LA ESPECIALIZACIÓN EN  
TELECOMUNICACIONES DE LA UNIVERSIDAD INDUSTRIAL DE  
SANTANDER

LEANDRO IGNACIO PATIÑO CASTILLO  
GABRIEL EDUARDO VARGAS HERNANDEZ

TRABAJO DE GRADO

DIRECTOR

**SAMUEL GONZALOPINZÓN BARRIOS**

**Magíster en Ingeniería**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER**

**FACULTAD DE CIENCIAS FÍSICOMECÁNICAS**

**ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES**

**ESPECIALIZACION EN TELECOMUNICACIONES**

**2006**

A Dios por brindarme una familia. A  
mis padres darme la vida y su  
incondicional apoyo durante el

desarrollo de mi vida. A mi hermano por su compañía incondicional y creencia en mí. A mi familia por su gratitud y confianza y apoyo brindado.

Leandro Ignacio

A mis padres, por su incondicional apoyo y cariño a lo largo de toda mi formación profesional. A mi hermana por su constante ayuda y muestra de interés en mi crecimiento como ingeniero. A mis mejores amigos por estar siempre ahí.

Gabriel Eduardo

### **Agradecimientos**

Los autores de este trabajo dan su agradecimiento a cada uno de los docentes de la Especialización de Telecomunicaciones de la UIS, por darnos nuevas herramientas de trabajo para sortear los difíciles caminos del mundo tanto profesional como laboral.

Al ingeniero Samuel Gonzalo Pinzón Barrios por su constante apoyo durante el desarrollo del trabajo de grado, ya que con sus consejos y sugerencias se inicio y se culmino este documento para satisfacción de muchos y ayuda a otros.

A la Universidad Industrial de Santander UIS por permitirnos desarrollar dentro de sus instalaciones este magnifico proyecto el cual nos ha dado alegrías y sobretodo satisfacciones ya que ello vimos que nuestro sacrificio por ser cada día mejor ha cosechado sus frutos.

A todos nuestros compañeros de la cohorte V, ya que gracias a ellos superamos los obstáculos vistos durante el desarrollo y culminación de esta nueva etapa de nuestra vida tanto profesional como humana.

En fin, a todas aquellas personas que de uno u otra forma participaron durante el desarrollo de esta gran meta iniciada y culminada con gran alegría y entusiasmo, ya que cada día de la vida venimos aprendiendo cosas nuevas para obtener un mejor futuro.

## RESUMEN

TÍTULO: Diseño de un laboratorio para la implementación y conformación de Redes de Área Local Virtuales (VLAN) para el programa de la Especialización en Telecomunicaciones de la

Universidad Industrial de Santander UI\*S.

AUTOR:

Leandro Ignacio Patiño Castillo

Gabriel Eduardo Vargas Hernández\*\*

PALABRAS

VLAN, Switch, Practicas, OSI, IEEE, Configuración,

CLAVES:

Programación,

Este trabajo presenta el esquema general y específico en procedimientos de una serie de prácticas de laboratorio para la configuración de VLAN a través de los switches 3Com 3226, D-Link DES3326SR y Avaya Cajun P333R respectivamente.

Una de las fallas más comunes es la escasez de manuales de procedimiento para usuarios en el desarrollo de prácticas de laboratorio y estándares en el manejo y utilización de elementos y equipos en aplicaciones para la configuración de redes. Debido a la falta de dichos procedimientos, manuales y estándares, ha venido ocasionando descontentos y interrogantes por parte de los estudiantes, como lo son la falta de aplicación de conocimientos adquiridos en las aulas de clases de tal forma que se pueda corroborar estos con nuevas aplicaciones y generación de proyectos logrando adquirir destreza y habilidad de manejo de los equipos adquiridos por la institución.

Este trabajo permite superar de una manera eficaz dichas fallas descritas permitiéndole a la Especialización el rediseñando sus prácticas de acuerdo a un nuevo formato establecido para estandarizar todos los procedimientos de cada uno de sus laboratorios.

El diseño e implementación de VLAN por medio de una práctica en laboratorio utilizando cada uno de los equipos y elementos adquiridos por parte de la Universidad entre los que tenemos como lo son los switches 3Com, D-Link y Avaya entre otros; estas practicas de VLAN se encuentran dentro de los aspectos requeridos a los nuevos lineamientos establecidos; permitiendo de esta manera un mayor interés entre sus estudiantes de forma tal que no verán obstaculizadas sus expectativas tanto en la formación profesional como en la rama laboral ya que podrán realizar un comparativo entre la teoría y la práctica dándoles una mayor habilidad y destreza en el manejo de estos equipos.

---

\* Trabajo de Grado

\*\* Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones, Especialización en Telecomunicaciones, Director: Ing. Samuel Gonzalo Pinzón Barrios, Magíster en Ingeniería.

## ABSTRAC

TITLE: Design of laboratory's exercise with the purpose of shaping and implementation of Virtual Local Area Networks (VLAN) for the Telecommunications program at Universidad Industrial de Santander (UIS) \*

AUTHORS: Leandro Ignacio Patiño Castillo  
Gabriel Eduardo Vargas Hernández\*\*

KEY WORDS: VLAN, Switch, Exercises, OSI, IEEE, Configuration, Programming,

This work presents the general and specific scheme in the procedures of several Laboratory's that aim to the configuration of Virtual Local Area Networks employing for this three switches: 3Com 3226, D-Link DES3326SR and Avaya Cajun P333R.

One of the most common fails is the lack of user's manuals for supporting the solving of laboratory's exercises and the absence of standards for the adequate management of the elements and devices involved in Network configuration. Because of this fails in procedures, manuals and standards, there are doubts and dissatisfaction among the students, also the absence in the application of the room class acquired knowledge not allowing to corroborate the experience with new applications and projects engineering for the skill improving in the management of the devices acquired by the institution.

This works allows excelling in an effective way those fails allowing the Specialization program redesign of its laboratory's exercises according to a new established standard for the creation of all the procedures in all the exercises for Laboratory learning.

---

\* Word of Degree

\*\* Electrical, Electric and Telecommunications Engineering School, Specialization in Telecommunications; Directed By : Msc. Samuel Gonzalo Pinzón Barrios.

Design and implementation of VLAN by means of a laboratory's exercise employing each one of the elements and devices acquired by the University, among those devices there are the switches 3Com, D-Link y Avaya and others. This VLAN laboratory's exercises were elaborated according to the new requirements established, allowing in this manner a better interest for the students who overlook for bigger expectative in his professional development and working life because of availability of comparison between theory and empiricism, this will give them a better understanding and skill in the management of the devices.

## GLOSARIO

**BACK PRESSURE<sup>1</sup>** (Contrapresión): Habilita el modo de contrapresión en el puerto. El modo de contrapresión se utiliza con el modo dúplex medio para inhabilitar la recepción de mensajes en los puertos.

**CLI<sup>2</sup>**: (command line interface), es un método de interacción del usuario con un computador. Los comandos son ingresados como líneas de texto ( secuencia de caracteres) por medio de un teclado y la salida es dada en forma de texto

---

<sup>1</sup> Definición tomada de [http://support.avaya.com/elmodocs2/cajun/cajun\\_documentation/P330/routing-redis.pdf](http://support.avaya.com/elmodocs2/cajun/cajun_documentation/P330/routing-redis.pdf).

<sup>2</sup> Definición tomada de [http://en.wikipedia.org/wiki/Command\\_line\\_interface](http://en.wikipedia.org/wiki/Command_line_interface)

**CRC**<sup>1</sup>: Código de Redundancia Cíclica. Se trata de un método matemático a través del cual, permite detectar errores en la información. Es comúnmente utilizado en la transmisión de datos a través de comunicaciones y en los archivos Zip. Valor usado para comprobar que los datos no se alteren durante la transmisión. El transmisor calcula una CRC y envía el resultado en un paquete junto con los datos. El receptor calcula la CRC de los datos recibidos y compara el valor con la CRC del paquete. El cálculo de una CRC es más complejo que una cifra de comprobación, pero puede detectar más errores de transmisión.

**HUB**<sup>2</sup>: ó concentrador, Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta de forma que todos los puntos tienen acceso a los datos. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central.

**INTERFAZ**<sup>3</sup>: modulo de hardware o de software que permite la comunicación con el exterior de un sistema o de un subconjunto.

**MAC** <sup>4</sup>(**Media Access Control address**): Dirección de Control de Acceso al Medio en español cuyo acrónimo es **MAC**, es un identificador físico –un número, único en el mundo, de 48 bits– almacenado en fábrica dentro de una tarjeta de red o una interfaz usada para asignar globalmente direcciones únicas en algunos modelos OSI (capa 2) y en la capa física del conjunto de protocolos de Internet.

---

<sup>1</sup> Definición tomada de [http://ramcir\\_cjm.tripod.com/codigo.htm](http://ramcir_cjm.tripod.com/codigo.htm)

<sup>2</sup> Definición tomada de <http://es.wikipedia.org/wiki/Concentrador>

<sup>3</sup> Definición tomada del Diccionario El Pequeño Larousse Ilustrado, Edición 2005, Pág. 569.

<sup>4</sup> Definición tomada de [http://es.wikipedia.org/wiki/MAC\\_address](http://es.wikipedia.org/wiki/MAC_address)

**MODELO OSI<sup>1</sup> (Open Systems Interconnection):** es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos. Un sistema abierto se refiere a que es independiente de una arquitectura específica. Se compone el modelo, por tanto, de un conjunto de estándares ISO relativos a las comunicaciones de datos.

**QoS<sup>2</sup> (Quality of Service):** Protocolo de calidad de servicio, garantiza que se transmitirá cierta cantidad de datos en un tiempo dado (throughput).

**RIP<sup>3</sup>:** son las siglas de Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o IGP (Internet Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

**ROUTER<sup>4</sup>:** (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadores que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

**SWITCH<sup>5</sup>:** (en castellano "conmutador") es un dispositivo de interconexión de redes de ordenadores / computadoras que opera en la capa 2(nivel de enlace de datos) y capa 3 ( nivel de red) del modelo OSI (Open Systems Interconnection).

---

<sup>1</sup> Definición tomada de [http:// es.wikipedia.org/wiki/Modelo\\_OSI](http://es.wikipedia.org/wiki/Modelo_OSI)

<sup>2</sup> Definición tomada de [http://es.wikipedia.org/wiki/Calidad del Servicio](http://es.wikipedia.org/wiki/Calidad_del_Servicio)

<sup>3</sup> Definición tomada de [http://es.wikipedia.org/wiki/ RIP\\_%28protocolo%29](http://es.wikipedia.org/wiki/RIP_%28protocolo%29)

<sup>4</sup> Definición tomada de <http://es.wikipedia.org/wiki/Router>

<sup>5</sup> Definición tomada de <http://es.wikipedia.org/wiki/Switch>

**THROUGHPUT<sup>1</sup>:** Tasa de transferencia, rendimiento o **throughput** es el término para todo el proceso – se refiere a cuántos datos se mueven durante una cierta cantidad de tiempo.

**TRUNKING<sup>2</sup>:** El Trunking es una función para conectar dos switches o routers, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los switches. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores. El protocolo es 802.1q.

**VLAN<sup>3</sup> (Red virtual de área local):** es una red de equipos los cuales funcionan como si estuvieran conectados a un mismo cable de interconexión (hubs o switches), aun cuando pueden estar físicamente en diferentes segmentos de una LAN (zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios).

---

<sup>1</sup> Definición tomada de <http://www.jegsworks.com/lessons-sp/lesson7/lesson7-3.htm>

<sup>2</sup> Definición tomada de [http://es.wikipedia.org/wiki/Trunking\\_\(red\)](http://es.wikipedia.org/wiki/Trunking_(red))

<sup>3</sup> Definición tomada de <http://es.wikipedia.org/wiki/VLAN> y Revista RED; La comunidad de expertos en redes, Junio 2001 Edición 129.

## CONTENIDO

	Pág.
INTRODUCCIÓN	18
1. VLAN (Virtual Lan Área Network): REDES VIRTUALES DE ÁREA LOCAL	19
1.1. GENERALIDADES DE LAS VLAN	19
1.1.1. Por Puertos	20
1.1.2. Por MAC	21
1.1.3. Por Protocolo	22
1.2. FUTURO DE LAS ARQUITECTURAS VLAN	23
1.2.1. Implementación Infraestructural de VLAN	23
1.2.2. Implementación Basada en el Servicio	24
1.3. BENEFICIOS DE LAS VLAN	25
2. ESTÁNDAR IEEE 802.1Q	26
2.1. ESTÁNDAR IEEE 802.1Q EDICIÓN 2003	26
2.2. VISIÓN GENERAL	28
2.3. ALCANCE	28
2.4. ESTRUCTURA DEL ENCABEZADO DE LA ETIQUETA	30

2.4.1.	Trama estándar de Ethernet	30
2.4.2.	Trama VLAN Etiquetada	30
2.5.	ESTRUCTURA DE LA ETIQUETA VLAN	30
3.	PLANTILLA PRÁCTICAS DE LABORATORIO	33
3.1.	FORMATO GENERAL	33
3.2.	EQUIPOS DISPONIBLES	35
3.3.	DISTRIBUCION DE PRACTICAS DE LABORATORIO vs. EQUIPOS DISPONIBLES	36
4.	PRÁCTICAS DE LABORATORIO	38
4.1.	LABORATORIO DE CONFIGURACIÓN DE VLAN CON SWITCH D-LINK DES-3326SR	38
4.1.1.	Título	38
4.1.2.	Objetivo General	38
4.1.3.	Objetivos Específicos	38
4.1.4.	Conocimientos Previos y Marco Teórico	39
4.1.5.	Equipo Requerido	41
4.1.6.	Sugerencias y Recomendaciones	41
4.1.7.	Procedimiento	42
4.1.8.	Bibliografía	56
4.2.	LABORATORIO DE CONFIGURACIÓN DE VLAN CON SWITCH 3COM 3226	57
4.2.1.	Título	57
4.2.2.	Objetivo General	57
4.2.3.	Objetivos Específicos	57
4.2.4.	Conocimientos Previos y Marco Teórico	57
4.2.5.	Equipo Requerido	59
4.2.6.	Sugerencias y Recomendaciones	60
4.2.7.	Procedimiento	60
4.2.8.	Bibliografía	72
4.3.	LABORATORIO DE CONFIGURACIÓN DE VLAN CON SWITCH AVAYA Cajun P333R.	73
4.3.1.	Título	73
4.3.2.	Objetivo General	73
4.3.3.	Objetivos Específicos	73
4.3.4.	Conocimientos Previos y Marco Teórico	73

4.3.5.	Equipo Requerido		76
4.3.6.	Sugerencias y Recomendaciones	76	
4.3.7.	Procedimiento		76
4.3.8.	Bibliografía		88
CONCLUSIONES Y OBSERVACIONES			89
BIBLIOGRAFÍA			90

## LISTA DE FIGURAS

Pág.

Figura 1.	Configuración de VLAN por puerto	20
Figura 2.	Configuración de VLAN por MAC	21
Figura 3.	Implementación infraestructural de VLAN	24
Figura 4.	Implementación Basada en el servicio de VLAN	25
Figura 5.	Trama estándar de Ethernet	30
Figura 6.	Trama VLAN etiquetada.	30
Figura 7.	Estructura de etiqueta VLAN	31
Figura 8.	Etiqueta VLAN IEEE 802.1Q	31
Figura 9.	Estructura de envío de paquetes	32
Figura 10.	Inserción de Etiqueta IEEE 802.1Q	32
Figura 11.	Conexión del Switch D-Link DES3326SR y estaciones de trabajo	42
Figura 12.	Acceso al Switch ambiente Telnet	44
Figura 13.	Acceso al Switch ambiente Web	45
Figura 14.	Acceso al las opciones de VLAN en el switch	46
Figura 15.	Vista de la VLAN por defecto del switch D-Link DES3326SR	47
Figura 16.	Edición de VLAN para switch D-Link DES3326SR	47
Figura 17.	VLAN por defecto editada para switch D-Link DES3326SR	48
Figura 18.	Creación de VLAN para switch D-Link DES3326SR	48
Figura 19.	Nueva lista de VLAN creadas en el switch D-Link DES3226SR	49
Figura 20.	Reconfiguración de las direcciones IP para el switch D-Link DES3326SR.	50
Figura 21.	Acceso al las opciones de capa 3 en el switch D-Link DES3326SR	51
Figura 22.	Habilitación del protocolo RIP en el switch D-Link DES3326SR	52
Figura 23.	Listado de interfaces en el switch D-Link DES3326SR	52
Figura 24.	Creación de una interfaz nueva para el switch D-Link DES3326SR	53
Figura 25.	Nuevo listado de interfaces en el switch D-Link DES3326SR	53
Figura 26.	Listado de las interfaces y su estado en el switch D-Link DES3326SR	54
Figura 27.	Menú de edición de las interfaces en el switch D-Link DES3326SR	54
Figura 28.	Listado de VLAN con sus puertos asignados a rutas estáticas en el switch D-Link DES3326SR	55
Figura 29.	Edición de los puertos para rutas estáticas en el switch D-Link DES3326SR	55

Figura 30.	Segundo listado de VLAN con sus puertos asignados a rutas estáticas en el switch D-Link DES3326SR	56
Figura 31.	Conexión del Switch 3COM 3226 y estaciones de trabajo.	60
Figura 32.	Menú inicial de la interfaz de línea de comandos en el Switch 3COM 3226	61
Figura 33.	Entradas para configuración de IP para el Switch 3COM 3226	62
Figura 34.	Vista Web del estado del switch 3COM 3226 y sus puertos.	63
Figura 35.	Opciones para trabajar con VLAN en el switch 3COM 3226	64
Figura 36.	Ventana de creación de VLAN en el switch 3COM 3226	65
Figura 37.	Menú de Edición de VLAN en el switch 3COM 3226	66
Figura 38.	Reconfiguración de las direcciones IP para el switch 3COM 3226.	67
Figura 39.	Ruta para acceder a las opciones de RIP en el switch 3COM 3226	68
Figura 40.	Cuadro de dialogo para habilitar RIP en el switch 3COM 3226	69
Figura 41.	Ruta para acceder al comando de edición de interfaces IP en el switch 3COM 3226.	70
Figura 42.	Ventana de interfaces en el switch 3COM 3226.	71
Figura 43.	Ventana de creación de interface en el switch 3COM 3226.	72
Figura 44.	Conexión del Switch Avaya Cajun P333R y estaciones de trabajo.	76
Figura 45.	Ejecución del comando set interface en el CAJUN P333R	77
Figura 46.	Respuesta al comando show interface en el switch Cajun P333R	78
Figura 47.	Ingreso al switch Cajun P333R por TELNET	78
Figura 48.	Creación de las VLAN con el comando set vlan en el CAJUN P333R	78
Figura 49.	Aplicación del comando show vlan en el CAJUN P333R	79
Figura 50.	Uso del comando set port vlan en el CAJUN P333R	79
Figura 51.	Empleo del comando show port en el Cajun P333R	80
Figura 52.	Guardado de cambios en el Cajun P333R	81
Figura 53.	Reconfiguración de las direcciones IP para el Switch Avaya Cajun P333R.	81
Figura 54.	Entrada al modo enrutador en el Switch Cajun P333R.	82
Figura 55.	Creación de interfaces en el Switch Cajun P333R	82
Figura 56.	Creación de las VLAN en el modo enrutador en el Switch Cajun P333R.	83
Figura 57.	Configuración de las interfaces en el Switch Cajun P333R.	83
Figura 58.	Listado de las interfaces en el Switch Cajun P333R.	84

Figura 59.	Segundo guardado de cambios en el Cajun P333R	84
Figura 60.	Conexiones para prueba de VLAN inter switches.	85
Figura 61.	Creación de la VLAN3 para la prueba inter switches	86
Figura 62.	Verificación de la VLAN3 para prueba inter switches.	86
Figura 63.	Verificación de los puertos del Avaya con comando show trunk	87
Figura 64.	Empleo del comando set trunk para habilitar el estándar IEEE 802.1Q en el puerto 24 del switch CAJUN P333R.	87
Figura 65.	Creación de la vlan3 en el CAJUN P333R	88
Figura 66.	Asignación del puerto 24 al CAJUN P333R	88

## LISTA DE TABLAS

	<b>Pág.</b>
Tabla 1. Formato general de la plantilla de prácticas de laboratorio.	33

## LISTA DE ANEXOS

		<b>Pág.</b>
<b>ANEXO A.</b>	<b>SWITCH 3COM - 3226</b>	<b>91</b>
<b>ANEXO B.</b>	<b>SWITCH AVAYA Cajun P333R</b>	<b>103</b>

<b>ANEXO C.</b>	<b>SWITCH D-LINK DES-3326 SR</b>	<b>121</b>
<b>ANEXO D.</b>	<b>FLUJOGRAMA PRÁCTICAS DE LABORATORIO</b>	<b>131</b>
<b>ANEXO E.</b>	<b>EQUIPOS UTILIZADOS EN EL DESARROLLO DE LAS PRÁCTICAS DE LABORATORIO.</b>	<b>133</b>

## **INTRODUCCIÓN**

Una de las principales preocupaciones de toda entidad educativa es la de mejorar constantemente sus procesos de formación académica y profesional dirigidos a sus estudiantes y egresados; es por esto que el programa de la Especialización en Telecomunicaciones de la escuela de Ingeniería Eléctrica Electrónica y Telecomunicaciones de la Universidad Industrial de Santander, en la búsqueda de afianzar conocimientos y dar un estándar a sus prácticas de laboratorio para ofrecer un nivel de calidad superior en la formación profesional de su estudiantado, ha planteado la necesidad de crear una serie de prácticas de laboratorio en el área de configuración de redes. Este trabajo en particular está enfocado específicamente a la creación y configuración de Redes de Área Local Virtuales (VLAN) empleando los equipos con los que cuenta la Especialización.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red, los cuales funcionan de igual manera como lo hacen los de una LAN, pero con la diferencia de que las estaciones que constituyen la VLAN no necesariamente deberán estar ubicadas en el mismo segmento físico. Sin embargo, las VLAN siguen compartiendo las características de los grupos de trabajos físicos, en el sentido de que todos los usuarios comparten sus dominios de broadcast. La diferencia principal con la agrupación física, es que los usuarios de las VLAN pueden estar distribuidos a través de una red LAN, incluso situándose en distintos concentradores de la misma sin importar su ubicación geográfica. Así los usuarios pueden, a través de la red, mantener su propia pertenencia al grupo de trabajo lógico.

El enfoque de este trabajo de grado es el diseñar y elaborar prácticas de laboratorio haciendo uso de tres (3) switches que son: switch CAJUN P333R de fabricante Avaya, el switch DES 3326SR de fabricante D-Link y el switch 3226 de fabricante 3Com; que permitan al estudiante adquirir nuevos conocimientos y destrezas en la elaboración y conformación de VLAN familiarizando al estudiante con los switch mencionados.

Las prácticas de laboratorio fueron desarrolladas en los laboratorios de la Especialización ubicados en el Edificio de Eléctrica Antigua de la Universidad Industrial de Santander.

## **1. VLAN (Virtual LAN Área Network): REDES VIRTUALES DE ÁREA LOCAL**

En este capítulo entraremos al mundo de las VLAN, su definición, sus características, sus aplicaciones; sus clases, su estándar dado por la IEEE<sup>1</sup>. Adicionalmente sabremos de una forma más detallada y entendible cómo y por qué las VLAN han aumentado su uso en diferentes campos gracias a sus ventajas respecto a los demás tipos de redes existentes en el mundo.

### **1.1. GENERALIDADES DE LAS VLAN**

Los grupos de trabajo en una red se han identificado por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador.

Como consecuencia lógica de la forma tradicional de crear grupos de trabajo, estos grupos comparten el ancho de banda disponible y los dominios de broadcast, así como los problemas que se ocasionan por la dificultad de gestión cuando se producen cambios en los miembros del grupo. Y también la limitación geográfica que supone que los miembros de un determinado grupo de trabajo deben estar situados de forma continua, por su conexión al mismo segmento de la red o concentrador.

---

<sup>1</sup> **IEEE**, corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

Los esquemas de una Red Virtual de Área Local (VLAN) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de forma lógica, en lugar de física.

La tecnología de las VLAN se basa en el empleo de Switches, en lugar de Hubs o Concentradores, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI<sup>1</sup> y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente.

Entre las ventajas más importantes de las VLAN tenemos:

- Sus esquemas proporcionan medios adecuados que ayudan a la solución de problemas permitiendo realizar una agrupación lógica.
- Su tecnología se basa en el empleo de switches, a cambio de Hubs o concentradores, obteniendo de tal forma mayor control inteligente del trafico de la red.
- Su área de trabajo se encuentra en la capa 2 y en la capa 3 del modelo OSI, lo que permite generar mayor eficiencia en toda la red.

Como principales razones para establecer una red VLAN son la reducción de costos, la facilidad de cambios en la red, mayor seguridad de la red y un mayor control de tráfico de la red.

Por otra parte las VLAN se pueden configurar de las siguientes formas:

- VLAN por puerto.
- VLAN por MAC.
- VLAN por protocolo.

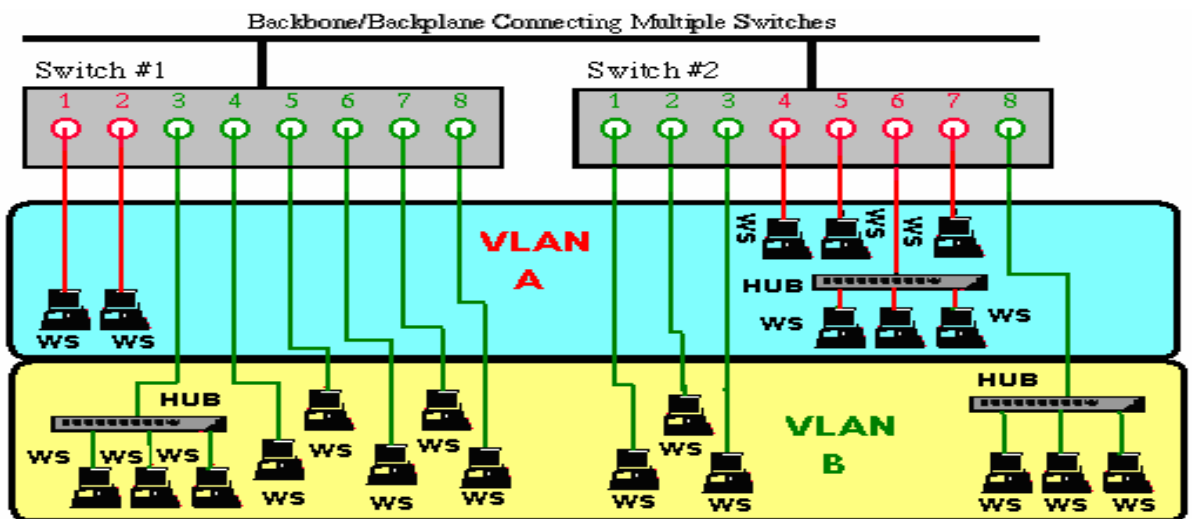
---

<sup>1</sup>OSI, modelo de referencia de Interconexión de Sistemas Abiertos

### 1.1.1. VLAN POR PUERTO

Para este tipo de configuración, cada uno de los puertos del switch son asignados a una VLAN, de tal forma que si trasladamos una estación de trabajo a otro puerto del switch, debemos realizar la configuración o reasignación a la VLAN a la que pertenecía dicha estación de trabajo o equipo como se muestra en la figura 1.

Figura 1. Configuración de VLAN por puerto.<sup>1</sup>



Este tipo de configuración tiene la ventaja que es un modelo de línea directa de visualización de la VLAN, al momento de presentar un problema es fácil detectar y solucionar ya que la asignación de puerto físico al equipo es conocido.

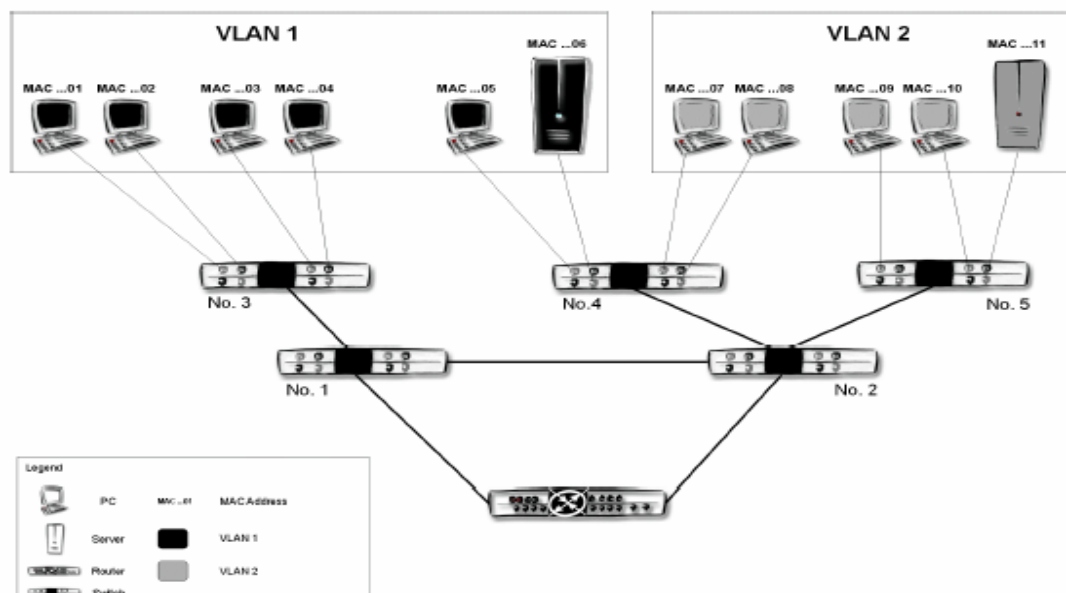
Esta es la manera más común de definir los grupos de trabajo en una VLAN, su facilidad depende de la "inteligencia" de cada Switch. Además, para implementar VLANs sobre múltiples Switches, se necesitan protocolos de señalización entre ellos, lo cual se convierte en un aumento de la utilización del ancho de banda.

### 1.1.2. VLAN POR MAC

<sup>1</sup> Tomada de Revista **Microbyte** N° 130 , Junio 1996, artículo : " VLANs, Redes Virtuales", Págs. 26, 27, 28

Para este tipo de configuración, la dirección MAC de una estación de trabajo es asignada a una red VLAN. Cada uno de los switches tiene una asignación de direcciones MAC con sus respectivas membresías o nombres de las VLAN. En esta configuración la dirección MAC fuente o destino nos determina a cual VLAN se pasara o es pasado un paquete como se muestra en la figura 2.

Figura 2. Configuración de VLAN por MAC<sup>1</sup>



Al mover una estación de trabajo de una VLAN a otra, se debe reconfigurar la dirección MAC a la nueva VLAN a la que se va a asignar; pero si es dentro de la misma VLAN, no es necesario realizar esta reasignación o reconfiguración de la dirección MAC.

Como ventaja principal de este método de configuración de VLAN en switch, es que no es necesario realizar la reconfiguración al momento de mover o trasladar una estación de trabajo de un puerto a otro. Otra importante ventaja es el excelente y buen servicio de soporte a los Hubs de medio compartidos.

<sup>1</sup> Figura tomada de <http://es.wikipedia.org/wiki/VLAN>.

Como desventaja se observa que cada una de las direcciones en este método debe ser asignada de forma manual al momento de la configuración principal si no utilizamos herramientas auxiliares, lo cual dificulta su administración. Como otra desventaja, una dirección MAC no puede ser de fácil asignación a múltiples o varias VLAN, lo que conlleva a la limitación de recursos compartidos de servidor entre más de una VLAN, lo que generaría problemas de alto nivel al trabajar con puentes y enrutadores.

La principal desventaja es la gran demanda en la administración de la red, que este tipo de configuración de VLAN requiere.

### 1.1.3. VLAN POR PROTOCOLO

En esta configuración, la entrega de paquetes depende de los protocolos (IP, IPX, NetBIOS, etc.) y de las direcciones de capa 3, donde esta es la variante más flexible que provee el agrupamiento de usuarios lógico.

La asignación basada en protocolos también permite al administrador a usar protocolos no enrutables, como NetBIOS o DECnet y asignarlos a VLAN más grandes que serían posibles con IP o IPX, lo que conduce a obtener una eficacia considerable de forma ascendente.

Otro aspecto importante de esta configuración con respecto a las otras configuraciones de VLAN es el método usado para indicar la membresía cuando un paquete es transferido entre los switches, se tienen dos clases:

- **Método Implícito**

La membresía de un paquete a la VLAN es indicada por la dirección MAC; cuando varios switches conectados, cada uno de ellos que soporten una VLAN deben tener una tabla de direcciones MAC y asignaciones la cual es compartida entre estos.

- **Método Explícito**

La membresía de un paquete a una VLAN es indicada por una marca que es añadida al paquete como tal. Este método es definido por el IEEE en su estándar 802.1Q.

Adicionalmente, cuando una estación de trabajo es trasladada dentro de la misma VLAN, esta no necesita ser reconfigurada; pero si se traslada a otra VLAN, entonces se debe reasignarle la dirección IP de la estación a la nueva VLAN.

Las VLAN deben ser rápidas, deben estar basadas en switches para que sean ínter operables totalmente, ya que los routers no dan la velocidad requerida. Su información deberá viajar a través del backbone y ser movibles, es decir, que el usuario u abonado no deba reconfigurar la máquina o estación de trabajo cada vez que se cambie de lugar en la VLAN.

## **1.2. FUTURO DE LAS ARQUITECTURAS VLAN<sup>1</sup>**

Existen dos futuros inmediatos para las VLAN: Implementaciones infraestructurales de VLAN y Implementaciones de VLAN basadas en el servicio.

### **1.2.1. Implementaciones Infraestructurales de VLAN**

Se basa en la estrategia tradicional de las VLAN, el formar grupos de trabajo de acuerdo a como están distribuidas las organizaciones. Cada grupo, departamento o sección tiene unívocamente definida su VLAN, basado a en la regla del 80/20, es decir, se asume que la mayoría de tráfico se da dentro de la VLAN.

Normalmente existirán solapamientos al acceder fuentes comunes a todas las VLAN, lo cual se resolverá al ubicar estos recursos en servidores; esto evita que se empleen routers para poder controlar el tráfico al acceder estos recursos.

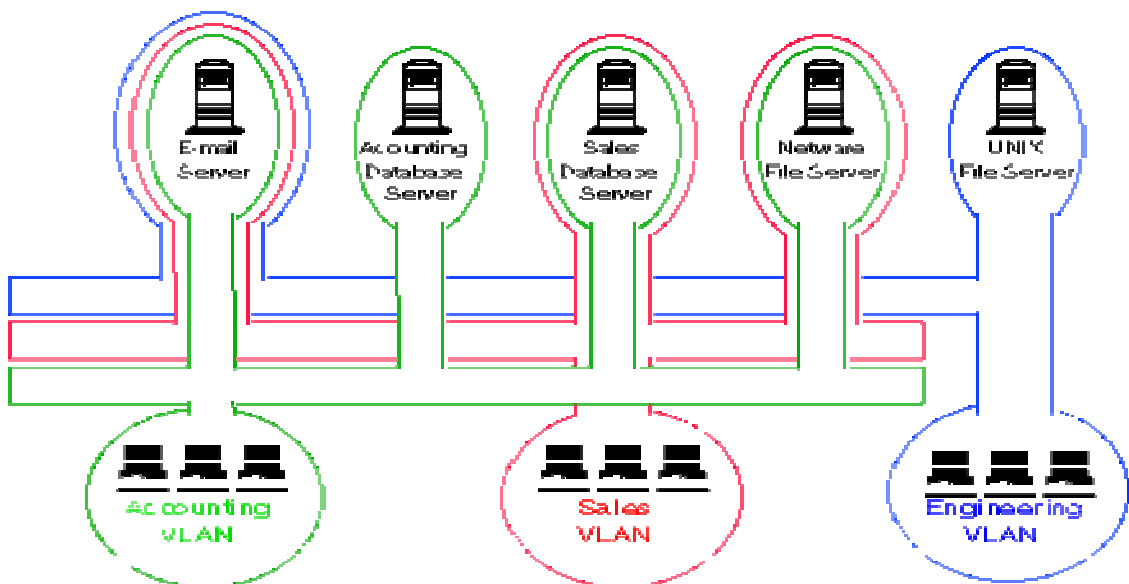
---

<sup>1</sup> Tomado de Revista RED; La comunidad de expertos en redes, Junio 2001 Edición 129. y <http://www.redescomm.com/thurlm.htm>

- Esto incluye todas las ventajas que pueda tener este tipo de implementación: Administración sencilla y centralizada.
- Permite mantener fronteras organizacionales discretas.
- Bajo costo de desarrollo.
- Buen grado de privacidad.
- Permite alcanzar una alta eficiencia de la red.

La figura 3 permite visualizar la implementación infraestructural de VLAN en un futuro.

Figura 3. Implementación infraestructural de VLAN<sup>1</sup>



### 1.2.2. Implementación Basada en el Servicio

En esta clase de aproximación, no se tienen grupos o algo similar, cada VLAN presta un servicio, es responsable de administrar un recurso específico y ningún servidor podrá pertenecer a múltiples VLAN; a diferencia de los usuarios que

<sup>1</sup> Figura tomada de <http://www.redescomm.com/thurlm.htm>

accederán a servicios de correo, bases de datos, aplicaciones, etc. a través de una VLAN independiente. Por naturaleza, esta clase de implementación, más dinámica que la anterior, posee serios inconvenientes para administrar la memoria a cada VLAN.

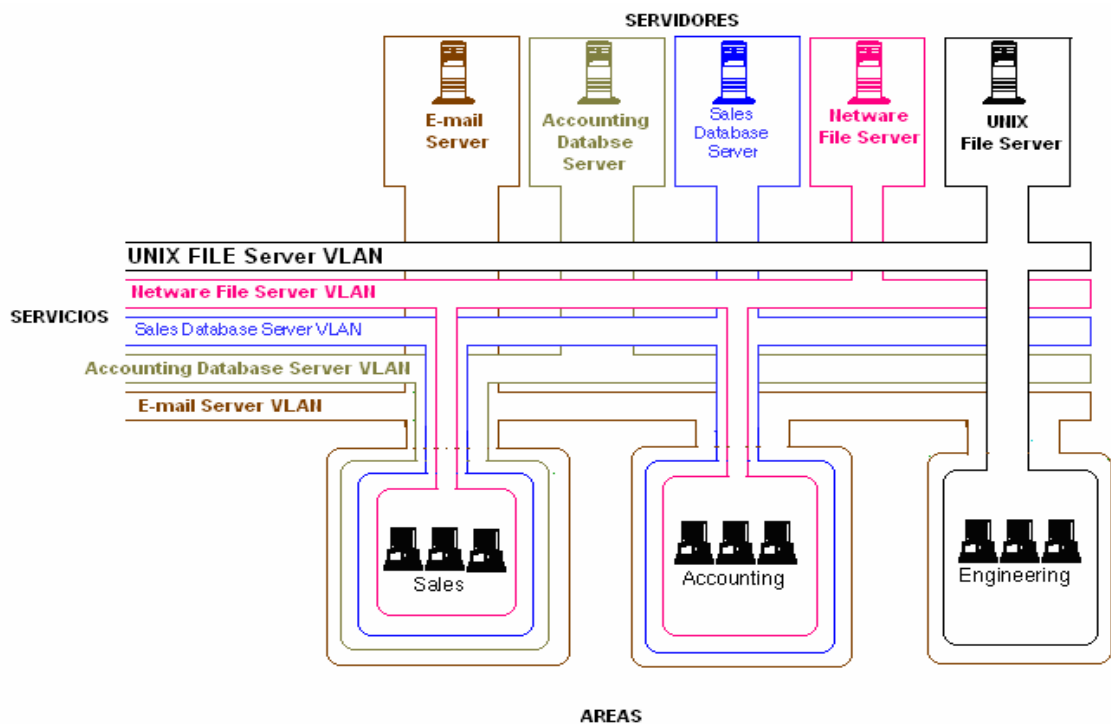
Esto conlleva a un alto grado de automatización en la configuración de las VLAN. Las VLAN perderán la característica estática o semi-estática de dominios previamente definidos, para cambiar a canales a los cuales suscribirse. Los usuarios, simplemente ejecutarán determinada aplicación por cierto tiempo, el cual será limitado dependiendo de la persona.

La implementación basada en el servicio se puede observar de forma clara en la figura 4.

Figura 4. Implementación Basada en el servicio de VLAN<sup>1</sup>

---

<sup>1</sup> Figura tomada de <http://www.redescomm.com/thurlm.htm>



### 1.3. BENEFICIOS DE LAS VLAN

Las VLAN apuntan a ofrecer los siguientes beneficios:

- a) Las VLAN son soportadas en todos los protocolos LAN MAC de IEEE 802, y sobre las LAN de medio compartido así como las LAN punto a punto.
- b) Las VLAN facilitan la fácil administración de grupos lógicos de estaciones que se pueden comunicar como si estuvieran sobre la misma LAN. Ellos también facilitan la administración de movimientos, adiciones y cambios en los miembros de esos grupos.
- c) El tráfico entre las VLAN esta restringido. Los Puentes envían tráfico unicast, multicast y broadcast solamente en los segmentos de LAN que sirven a la VLAN a la que pertenece el tráfico.

- d) Tanto como sea posible, las VLAN mantienen la compatibilidad con puentes existentes y estaciones terminales.

Si todos los puertos puente están configurados para transmitir y recibir tramas sin etiquetas, los puentes trabajarán en el modo plug and play del estándar IEEE 802.1D. Las estaciones finales estarán en capacidad de comunicarse a través de la LAN con puentes.

## **2. ESTÁNDAR IEEE 802.1Q**

Este estándar<sup>1</sup> define la arquitectura para las redes de área local unidas virtualmente, también define los servicios provistos en las VLAN y los protocolos y algoritmos involucrados en la provisión de estos servicios.

### **2.1. Estándar IEEE 802.1Q edición 2003**

Observando el desarrollo de este estándar partiendo del estándar IEEE 802.1 D Edición de 1993, se cuenta con que las actividades de estandarización de los puentes MAC que resultaron en el desarrollo de el estándar IEEE 802.1D-1993 introdujeron el concepto de servicios de filtrado en las LAN con puentes virtuales y los mecanismos con los que el filtrado de información en tales LAN puede ser tomado y guardado en una Base de datos de filtrado.

El estándar IEEE 802.1D de 1998 es una versión enmendada del estándar IEEE 802.1D edición 1993, la primera extiende el concepto de servicios de filtrado con el fin de definir capacidades adicionales en las LAN con puentes con miras a:

- a) La provisión de capacidades de tráfico apresurado, para soportar la transmisión de información crítica en el tiempo en el ambiente de la LAN.

---

<sup>1</sup> Tomado de IEEE Std 802.1Q™, 2003 Edition , IEEE Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks

- b) El uso de información prioritaria de usuario indicado como la base para la identificación de clases apresuradas de tráfico.
- c) La provisión de servicios de filtrado que soporten la definición dinámica y el establecimiento de grupos en una LAN y el filtrado de tramas en los puentes de forma que las tramas direccionadas a un grupo particular son enviadas solamente a los segmentos de la LAN que permitirán alcanzar a los miembros de ese grupo.
- d) Incluye un Protocolo de Registro de Atributos Genérico (GARP) que es usado para soportar los mecanismos que proveen la capacidad de filtrado de grupo, y también se ha hecho disponible para usarse en otras aplicaciones de registro de atributos.

La primera publicación del estándar IEEE 802.1Q fue la edición de 1998, esta hace uso de los conceptos y mecanismos de la creación de puentes en la LAN que fueron introducidos en el estándar IEEE 802.1 de 1998, además define mecanismos adicionales que permiten la implementación de LAN con puentes Virtuales. Cuenta con las siguientes características:

- a) Servicios de VLAN en las LAN con puentes.
- b) La operación de procesos de envío que son requeridos con el fin de soportar las LAN con puentes Virtuales.
- c) La estructura de la base de datos de filtrado que es requerida con el fin de soportar las LAN con puentes virtuales.
- d) La naturaleza de los protocolos y procedimientos que son requeridos con el fin de proveer servicios de VLAN, incluyendo la definición de los formatos de trama empleados para representar la identificación de la información de la VLAN y los procedimientos usados para insertar y remover los identificadores VLAN y las cabeceras en las tramas que se encuentren estos.

- e) La habilidad para soportar señalización Terminal-a-Terminal de información prioritaria de usuario independientemente de la habilidad intrínseca de los protocolos MAC para señalar la información prioritaria del usuario.
- f) El protocolo de registro GARP VLAN (GVRP) que permite la distribución y registro de información de miembros de la VLAN (el protocolo descrito hace uso de el protocolo GARP definido en la ISO/IEC 15082-3).
- g) Los servicios de administración y operaciones que son requeridos para configurar y administrar las LAN con puentes virtuales.

La edición del estándar IEEE 802.1Q del año 2003 incorpora tres enmiendas, los estándares: IEEE 802.1u, IEEE 802.1v-2001 y IEEE 802.1s-2002, que son incluidos dentro del texto del IEEE 802.1Q 1998. Estas enmiendas describen mejoras en el estándar que permiten:

- a) Registro de VLAN y grupo dinámico para ser restringido, basado en los contenidos de las entradas de filtrado estático.
- b) Clasificación de las VLAN de acuerdo al tipo de protocolo de capa de enlace.
- c) Soporte para las VLAN que se llevan múltiples instancias de árbol de expansión.

## **2.2. Visión General**

Las LAN que cumplan con el estándar IEEE 802 de todos los tipos pueden ser conectadas juntas con puentes MAC, tal como se especifica en el estándar IEEE 802.1D de 1998. Este estándar define la operación de los puentes de VLAN que permiten la definición, operación y administración de las topologías VLAN dentro de la infraestructura de una VLAN con puentes.

### 2.3. Alcance

Para el propósito de interconexión compatible de equipos de tecnología de información empleando el servicio MAC de IEEE 802 soportado por LAN del estándar IEEE 802 interconectada empleando métodos de MAC diferentes o idénticos, este estándar especifica un método general para la operación de los puentes MAC que soporta la construcción de VLANs, para este fin:

- a) Posiciona la función de las VLANs dentro de una descripción arquitectural de la supcapa MAC.
- b) Define mejoras para soportar el servicio MAC, como se describió y definió en el estándar IEEE 802.1D de 1998, para el propósito de crear puentes de VLAN.
- c) Especifica un servicio de subcapa interno mejorado que provee a las funciones independientes de acceso al medio que provee relevo de tramas en el puente de la VLAN.
- d) Especifica la operación de las funciones que proveen relevo de tramas en el puente de la VLAN.
- e) Define la estructura, codificación e interpretación de la información de control de la VLAN transportada en las tramas con etiqueta en una VLAN.
- f) Especifica las reglas que gobiernan la inserción y remoción de la información de control de la VLAN en las tramas.
- g) Especifica las reglas que gobiernan la habilidad de transportar datos en formato canónico y no canónico empleando diferentes métodos LAN MAC.

- h) Establece los requerimientos para la configuración automática de la información de topología de la VLAN y también especifica sus significados.
- i) Define la funcionalidad de administración que se puede proveer en un puente de VLAN con el fin de facilitar el control administrativo sobre las operaciones de la VLAN.
- j) Define la operación de algoritmo y protocolo de Árbol de Expansión Múltiple (MSTP)<sup>1</sup>.
- k) Define las mejoras hechas al algoritmo y al protocolo del Árbol de Expansión Múltiple con el fin de crear el MSTP.
- l) Describe los protocolos y procedimientos necesarios para soportar la interoperabilidad entre los puentes MST<sup>2</sup> y SST<sup>3</sup> en la misma LAN con puentes.
- m) Especifica los requerimientos a ser satisfechos por los equipos que requieren conformidad con este estándar.

En los casos en que un puente de VLAN vaya a operar en el modo del estándar IEEE 802.1D, este dependerá de la configuración de varios parámetros de puerto y base de datos de filtrado. Un puente de VLAN en su configuración por defecto es transparente a las tramas sin etiqueta pero no es transparente a las tramas con etiqueta, así que la operación de tales puentes en la presencia de tráfico con etiqueta difiere de la del puente del estándar IEEE 802.1D.

---

<sup>1</sup> **MSTP**, Protocolo de Árbol de Expansión Múltiple (Multiple Spanning Tree Protocol)[802.1D]

<sup>2</sup> **MST**, Árbol de Expansión Múltiple (Multiple Spanning Tree)

<sup>3</sup> **SST**, Árbol de Expansión Simple(Single Spanning Tree)

Si las opciones de configuración de los puentes de VLAN son cambiados de los valores por defecto definidos en este estándar, entonces la transparencia con respecto a las tramas sin etiqueta también puede ser afectada.

## 2.4. Estructura del Encabezado de la Etiqueta

### 2.4.1. Trama estándar de Ethernet

Figura 5. Trama estándar de Ethernet

Dirección destino	6 Bytes
Dirección fuente	6 Bytes
Longitud/tipo	2 Bytes
Datos	46–1500 Bytes
Secuencia de chequeo de la Trama	4 Bytes

### 2.4.2. Trama VLAN Etiquetada

Figura 6. Trama VLAN etiquetada.

Dirección destino
Dirección Fuente
Etiqueta VLAN
Longitud/tipo

Datos	6 Bytes
	6 Bytes
Secuencia de chequeo de la trama	4 Bytes
	2 Bytes

46-1500 Bytes

4 Bytes

## 2.5. ESTRUCTURA DE LA ETIQUETA VLAN

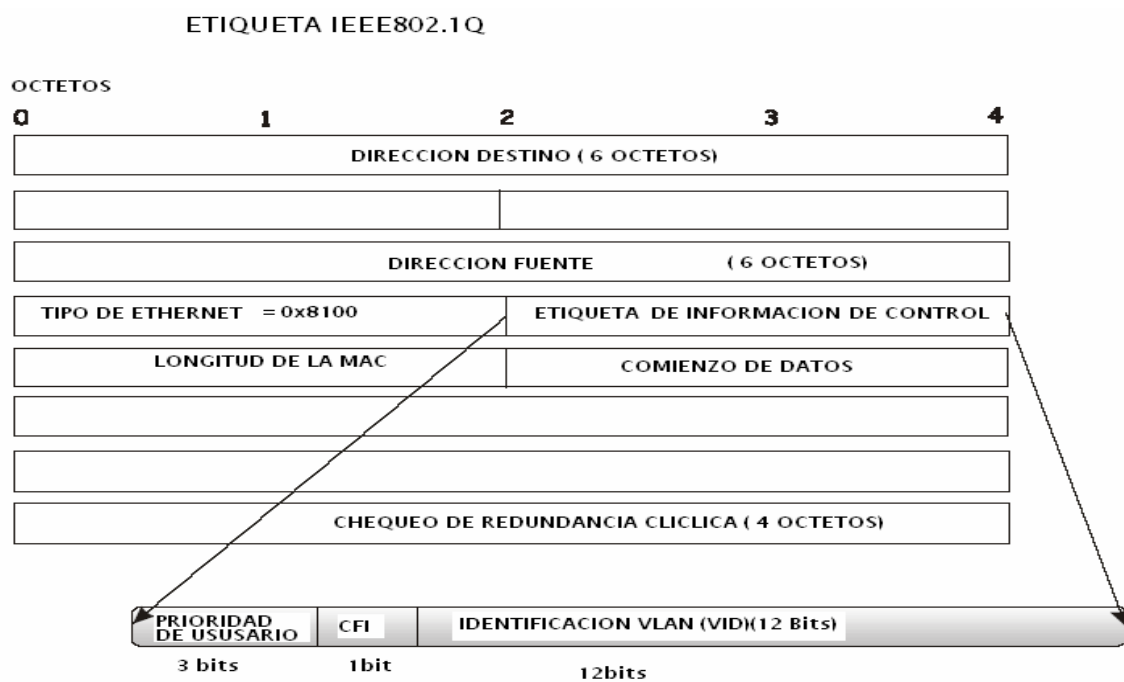
La etiqueta VLAN tiene la siguiente estructura mostrada en la figura 7.

Figura 7. Estructura de etiqueta VLAN

Identificador del Protocolo de la Etiqueta	Información de control de la Etiqueta		
	Identificación para el encabezado del VLAN: 0x8100 (16 BIT)	Prioridad del Usuario: 0-7 (3 BIT)	CFI (1 BIT)

La figura 8, permite visualizar de forma gráfica la etiqueta para VLAN según el estándar 802.1Q de la IEEE.

Figura 8. Etiqueta VLAN IEEE 802.1Q<sup>1</sup>



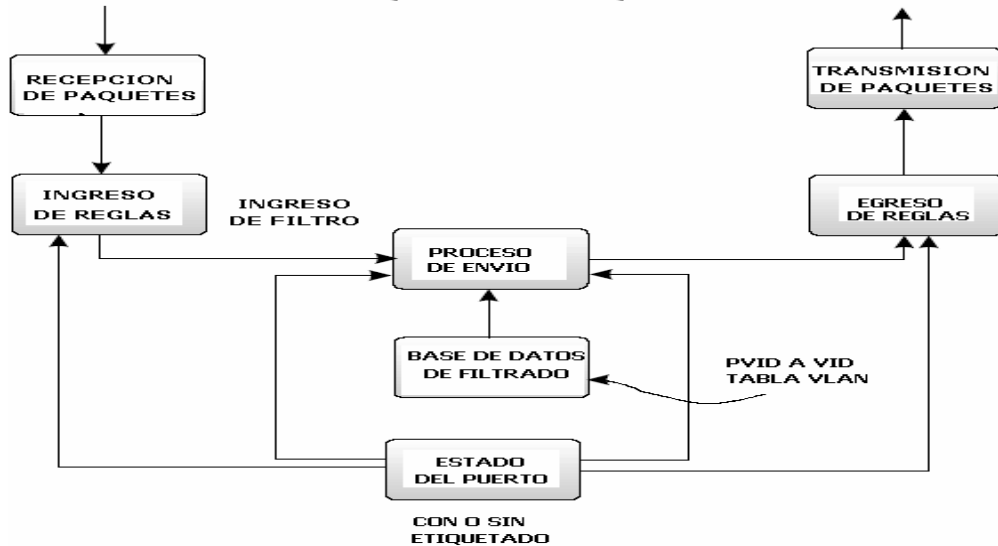
La estructura de la trama y envío de paquetes se observa en la figura 9.

Figura 9. Estructura de envío de paquetes.<sup>2</sup>

<sup>1</sup> Figura tomada de <http://monografia/investigacion/D-Link TechSupport - FAQ>.

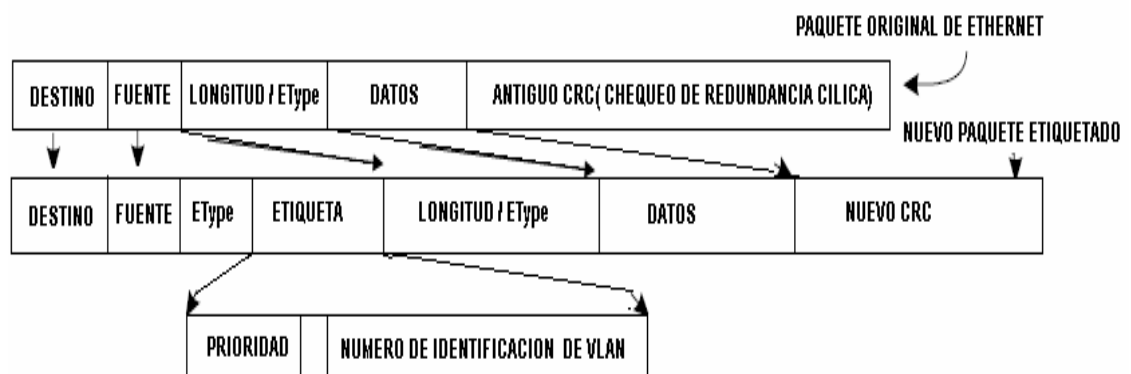
<sup>2</sup> Figura tomada de <http://monografia/investigacion/D-Link TechSupport - FAQ>.

### 802.1Q ENVIO DE PAQUETES



El tipo Ether y el Identificador de VLAN son insertados después de la dirección MAC fuente, pero antes del tipo Ether/longitud originales o Control de enlace lógico. Debido a que el paquete es ahora más grande que el que era originalmente, el chequeo de redundancia cíclica (CRC) debe ser recalculado como se muestra en la figura 10.

Figura 10. Inserción de Etiqueta IEEE 802.1Q.<sup>1</sup>



<sup>1</sup> Figura tomada de <http://monografia/investigacion/D-Link TechSupport - FAQ>.

### 3. PLANTILLA DE PRÁCTICAS DE LABORATORIO

En este capítulo se muestran los aspectos relevantes en la formación de las diferentes prácticas de laboratorio, como lo son su formato general, la cantidad y características de los equipos disponibles, asignación de acuerdo a las estaciones de trabajo disponible por práctica y el tiempo estimado por cada una de las prácticas a desarrollar.

#### 3.1. FORMATO GENERAL

Cada una de las prácticas tendrá los siguientes parámetros generales para su implementación y desarrollo los cuales se explicarán en detalle.

En la tabla 1, podremos ver los aspectos o parámetros que conllevará cada una de las prácticas planteadas.

Tabla 1. Formato general de la plantilla de prácticas de laboratorio

<b>Formato General de la Plantilla de Laboratorio</b>	
NOMBRE DE LA PRACTICA:	
TIEMPO ESTIMADO:	
OBJETIVO GENERAL:	
OBJETIVOS ESPECIFICOS:	
CONOCIMIENTOS PREVIOS Y MARCO TEORICO:	
EQUIPO REQUERIDO:	
SUGERENCIAS Y RECOMENDACIONES:	

PROCEDIMIENTO:
BIBLIOGRAFÍA:

A continuación se explica cada ítem del contenido de la plantilla de forma general,

- a. TÍTULO: Nombre específico de la práctica a desarrollar.
- b. TIEMPO: Es el tiempo que se tiene estimado para el desarrollo y ejecución de la práctica.
- c. OBJETIVO GENERAL Describe la meta global de la práctica a implementar.
- d. OBJETIVOS ESPECIFICOS: Plantea los puntos claves a lograr.
- e. CONOCIMIENTOS PREVIOS Y MARCO TEORICO: Teoría que el estudiante debe conocer para poder ejecutar correctamente la práctica.
- f. EQUIPO REQUERIDO: Todos los elementos (equipos, cableado, instrumentos, extras) necesarios para llevar acabo la práctica con las especificaciones y referencias de cada uno.
- g. SUGERENCIAS Y RECOMENDACIONES: Sugerencias y pistas que pueden ayudar al estudiante a agilizar la práctica o a solventar

inconvenientes que se puedan presentar.

- h. **PROCEDIMIENTO:** Pasos detallados en orden a seguir para la ejecución de la práctica.
- i. **BIBLIOGRAFÍA:** Son los textos, revistas, artículos, medios magnéticos, ponencias en las cuales el estudiante podrá indagar sobre algún tema o equipo para resolver dudas e inquietudes durante y después del desarrollo de la práctica.

### 3.2. EQUIPOS DISPONIBLES

Para el desarrollo de cada una de las prácticas de laboratorio se cuentan con los siguientes equipos y salas de laboratorios<sup>1</sup>:

- a. **Salas de Laboratorios:** como aulas o salones clase para el desarrollo de las diferentes prácticas se tienen los siguientes salones:
  - Laboratorio de Redes (salón 201) y Laboratorio de la Especialización (salón 205)

Estos se encuentran ubicados en el segundo nivel del Edificio de Eléctrica Antigua, de Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones de la Universidad Industrial de Santander.

---

<sup>1</sup> Ver Anexo F.

b. **Switches:** para la implementación de cada una de las prácticas se trabajaran los siguientes switches:

- Switch 3com 3226, este equipo se encuentra instalado en el rack ubicado en el salón 205, del edificio de eléctrica antigua. Para conocer más sobre este equipo como sus características y comandos favor remitirse al anexo A.
- Switch Avaya CAJUN P333R, este switch se encuentra instalado dentro del rack con inventario número 49350 ubicado en el laboratorio de redes del edificio de eléctrica antigua; sus parámetros, comandos y características se pueden observar en el anexo B.
- Switch D-LINK DES-3326, este switch se encuentra instalado dentro del rack con inventario número 61278 ubicado en el laboratorio de redes del edificio de eléctrica antigua, cada uno de los parámetros, comandos y características pueden verse en el anexo C.

c. **Equipos de Computo:** ó estaciones de trabajo para el desarrollo de las prácticas de laboratorio planteadas; son un total de treinta y dos (32) PC, los cuales se encuentran ubicados de la siguiente forma:

- Laboratorio de redes, en este salón se encuentran 16 equipos de cómputo o estaciones de trabajo referenciados con calcomanía de inventario número 56410 al 56425 de la Universidad Industrial de Santander respectivamente.
- Laboratorio de la especialización, en este salón encontraremos 18 a 20 equipos de cómputo o estaciones de trabajo referenciados con calcomanía de inventario número 56315 al 56317, del 56405 al 56420 de la Universidad Industrial de Santander respectivamente.

Las características más relevantes de los equipos de cómputo son las siguientes:

- Procesador Intel Pentium 4 CPU 2.40Ghz
- Disco duro: 30 Gbytes.
- Memoria Ram: 512 Mhz.
- Unidad de CD-ROM
- Unidad Disco de 3 y ¼
- Puertos USB: 6 puertos.
- Interface Ethernet 10/100/1000.
- Sistema Operativo Microsoft Windows XP Professional y Linux Fédora Core 4.

### **3.3. Distribución de Prácticas de laboratorio vs. Equipos disponibles**

Las prácticas a implementar en los laboratorios son la configuración de VLAN por puerto y por protocolo para cada uno de los switches anteriormente descritos.

Cada una de ellas tendrá un tiempo aproximado de desarrollo de una hora (1) y treinta (30) minutos. Las prácticas van dirigidas a un total estimado de treinta (30) estudiantes, los cuales serán reasignados por medio de grupos de máximo tres (3) estudiantes por cada grupo, y desarrollarán las tres prácticas haciendo uso de los switches descritos anteriormente.

Las prácticas a implementar con cada uno de los switches son: la configuración de VLAN por puerto o capa 2 y la configuración de VLAN por protocolo o capa 3. Cada práctica requiere el uso de 3 equipos de cómputo o estaciones de trabajo por grupo; los cuales se organizarán de la siguiente forma:

- Laboratorio de redes; se ubicaran un total de cinco (5) grupos de trabajo.
- Laboratorio de la especialización; se ubicaran un total de seis (6) grupos de trabajo.

Es de aclarar que cada estación de trabajo o equipo de cómputo debe estar conectado a la red LAN de cada salón donde se encuentre ubicado por medio de un patch cord certificado.

## **4. PRÁCTICAS DE LABORATORIO**

En este capítulo se conocerá el contenido de las prácticas de laboratorio; y adicionalmente su orden de desarrollo. Para cada una de las prácticas se muestra el esquema de red y se hace una pequeña descripción de los pasos que el estudiante debe seguir para completar la práctica de manera correcta y precisa obteniendo los resultados sugeridos.

### **4.1. LABORATORIO DE CONFIGURACIÓN DE VLAN CON SWITCH D-LINK DES-3326SR**

#### **4.1.1. Título**

Creación de VLAN empleando el Switch D-Link DES - 3326SR

#### **4.1.2. Objetivo General**

Crear y configurar VLAN en capa 2 (por puerto) y capa 3 (por IP) utilizando el Switch D-Link DES - 3326SR

#### **4.1.3. Objetivos Específicos**

- Familiarizarse con los equipos a utilizar en el desarrollo de la práctica.
- Disponer y adecuar cada equipo a utilizar en el desarrollo de la práctica.
- Realizar la conexión entre el switch y la estación de trabajo verificando el acceso y comunicación entre estos.
- Configurar VLAN en el switch.
- Comprobar la comunicación entre cada una de las estaciones de trabajo dentro de las VLAN creadas.

#### **4.1.4. Conocimientos Previos y Marco Teórico**

- Asignación y configuración de direcciones IP.
- Protocolo RIP.
- Comandos de consola para Switch D-Link DES - 3326SR

### **VLAN**

Los grupos de trabajo en una red se han identificado por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador.

Como consecuencia lógica de la forma tradicional de crear grupos de trabajo, estos grupos comparten el ancho de banda disponible y los dominios de broadcast, así como los problemas que se ocasionan por la dificultad de gestión cuando se producen cambios en los miembros del grupo. Y también la limitación geográfica que supone que los miembros de un determinado grupo de trabajo deben estar situados de forma continua, por su conexión al mismo segmento de la red o concentrador.

Los esquemas de una Red Virtual de Área Local (VLAN) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de forma lógica, en lugar de física.

La tecnología de las VLAN se basa en el empleo de Switches, en lugar de Hubs o Concentradores, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI<sup>1</sup> y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente.

Entre las ventajas más importantes de las VLAN tenemos:

- Sus esquemas proporcionan medios adecuados que ayudan a la solución de problemas permitiendo realizar una agrupación lógica.
- Su tecnología se basa en el empleo de switches, a cambio de Hubs o concentradores, obteniendo de tal forma mayor control inteligente del trafico de la red.
- Su área de trabajo se encuentra en la capa 2 y en la capa 3 del modelo OSI, lo que permite generar mayor eficiencia en toda la red.

---

<sup>1</sup>OSI, modelo de referencia de Interconexión de Sistemas Abiertos

Como principales razones para establecer una red VLAN son la reducción de costos, la facilidad de cambios en la red, mayor seguridad de la red y un mayor control de tráfico de la red

## **ESTÁNDAR IEEE 802.1Q**

Este estándar<sup>1</sup> define la arquitectura para las redes de área local unidas virtualmente, también define los servicios provistos en las VLAN y los protocolos y algoritmos involucrados en la provisión de estos servicios.

Cuando se trabaja con una VLAN no es raro que se presente una situación en que los miembros este ubicados lejos físicamente entre si, los paquetes entre los miembros tendrán que pasar por más de un switch diferente y a veces cubrir grandes distancias, en estos casos es necesario que las tramas lleven un identificador especial o “etiqueta” que le permita a cada switch por donde pasan saber a que VLAN pertenece el paquete y enviarlo adecuadamente.

Este estándar define la estructura que debe llevar la “etiqueta” (tagged) de VLAN que llevarán las tramas de Ethernet.

Para el caso en que todos los miembros de una VLAN estén conectados al mismo Switch no se hace necesario emplear las etiquetas (untagged) puesto que el mismo switch mapea internamente las VLAN que tenga definidas con sus respectivos miembros.

## **PROTOCOLO RIP**

---

<sup>1</sup> Tomado de IEEE Std 802.1Q™, 2003 Edition , IEEE Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks

En inglés **RIP** es Routing Information Protocol que quiere decir Protocolo de Información de Enrutamiento, es un protocolo de pasarela interior que es empleado por los enrutadores para intercambiar información sobre las redes IP

RIP utiliza UDP para enviar sus mensajes y el puerto 520.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. Esta distancia se denomina métrica.

### **En el Switch D-LINK**

Cuando se asignan puertos a una VLAN en el DES 3326SR existen 4 atributos que pueden dársele a un puerto: **Non-Member** que indica que el puerto no es miembro de la VLAN, **Tagged** el puerto es miembro y emplea la etiqueta del estándar 802.1Q para los paquetes que viajen entre terminales de la VLAN, **Untagged** indicando que el puerto siendo miembro de la VLAN no emplea la etiqueta del estándar para marcar las tramas y finalmente **Forbidden** que indica que el puerto no pertenece a la VLAN y además no podrá nunca llegar a ser miembro en forma dinámica.

#### **4.1.5. Equipo Requerido**

- Tres (3) computadores con puerto serial y tarjeta LAN, donde al menos uno de ellos tenga software de hyperterminal.
- UN (1) Switch D-Link DES 3326SR.
- Patch Cord RJ45 de 3 y 6 metros de longitud.
- Cable de consola para el Switch

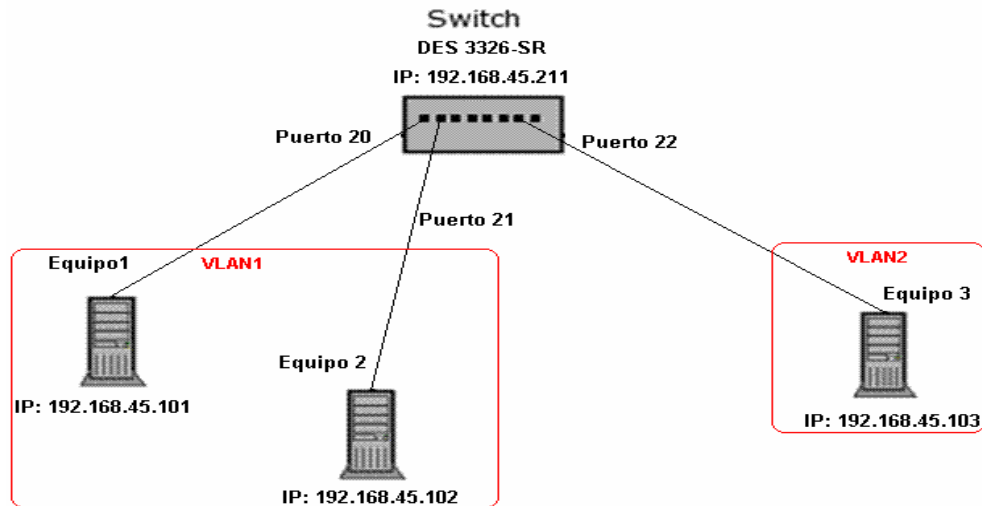
#### **4.1.6. Sugerencias y Recomendaciones**

- Para la creación de una VLAN en el Switch, tenga en cuenta que este trae por defecto una VLAN, y todos sus puertos pertenecen a ella; se recomienda no trabajar en la VLAN por defecto.
- Por defecto el Switch tiene asignada la dirección IP 10.90.90.90 con máscara de subred (mask) 255.0.0.0, se sugiere cambiarla por consola a una dirección que se encuentre dentro de la red que muestra la figura 7. (en el caso de que el dispositivo sea reiniciado)
- Cuando se encuentra trabajando el Switch en ambiente Telnet o línea de comandos CLI (Command Line Interface), en caso de olvidar un comando específico o su sintaxis; digite el comando "?" el cual le visualizará en forma de lista todos y cada uno de los comandos de trabajo del Switch.
- Si usted no sabe u olvida los parámetros requeridos de cada comando, digite el comando en la CLI, la cual le ofrecerá una lista de los posibles parámetros a utilizar con el comando digitado.

#### **4.1.7. Procedimiento**

La figura 11, permite visualizar la conexión física de los elementos que van a ser utilizados durante el desarrollo de la práctica:

Figura 11. Conexión del Switch D-Link DES3326SR y estaciones de trabajo.



**Nota:** Las direcciones IP de los equipos, los números de puertos y los nombres asignados a las VLAN aquí indicados corresponden a un ejemplo y caso particular, si el procedimiento es llevado a cabo por más de un grupo, el coordinador de esta práctica deberá asignar direcciones y puertos a cada grupo con el fin de evitar conflictos de IP y de uso de puertos.

Se debe realizar una conexión entre el switch D-Link DES 3326SR con una estación de trabajo o computador por medio de la consola (puerto serial) con la cual se inicia la configuración inicial.

#### I. Configuración del Switch D-Link DES3326SR por consola:

Cuando se inicializa la comunicación con el Switch podrá observar la siguiente línea, la cual indica que existe comunicación entre el Switch y la estación de trabajo

```
DES-3326SR:4#
```

El comando de configuración de la dirección IP del Switch para acceder ya sea por ambiente Web o por consola es:

```
config ipif System ipaddress
```

Quedando de la siguiente forma:

```
DES-3326SR:4#config ipif System ipaddress 192.168.45.211/255.255.255.0
```

Como se aprecia, al comando le asignamos una dirección IP junto con una máscara (esta puede ser modificada a gusto del practicante o tutor).

Otra manera de asignarle dirección IP de configuración al Switch es:

```
DES-3326SR:4#config ipif System ipaddress 192.168.45.211/24
```

Observe que en este comando no se digita la máscara de subred como tal sino el número en bits correspondiente.

Una vez hecho este paso debe aparecer en la línea de consola la siguiente confirmación la cual informa que los cambios se efectuaron correctamente.

```
Success
```

Si desea verificar la comprobación de cambios realizados al Switch digite el siguiente comando:

```
DES-3326SR:4#show ipif
```

show ipif permite visualizar la comprobación de los cambios de la siguiente forma:

#### IP Interface Settings

Interface Name:	System
IP Address:	192.168.45.211 (MANUAL)
Secondary:	False
Subnet Mask:	255.255.255.0
VLAN Name:	default
Admin. State:	Enabled
Link Status:	Link UP
Member Ports:	1-26

Total Entries: 1

Ahora emplear el comando **show switch** y verificar que características exhibidas son diferentes a las que presenta el comando **show ipif**?

Cuál es la dirección MAC del switch?

Cuál es su IP de puerta de salida?

A que velocidad trabajan los puertos?

Realizado este paso se debe retirar el cable de conexión al Switch del puerto serial, logrando de esta forma la conexión de este ultimo con las estaciones de trabajo por el cable de la red LAN.

Desde otras estaciones de trabajo podemos ver el acceso sea por Telnet o por Web al Switch D-Link DES 3326SR como se muestra en la figura 12 y 13 respectivamente.

Figura 12. Acceso al Switch ambiente Telnet

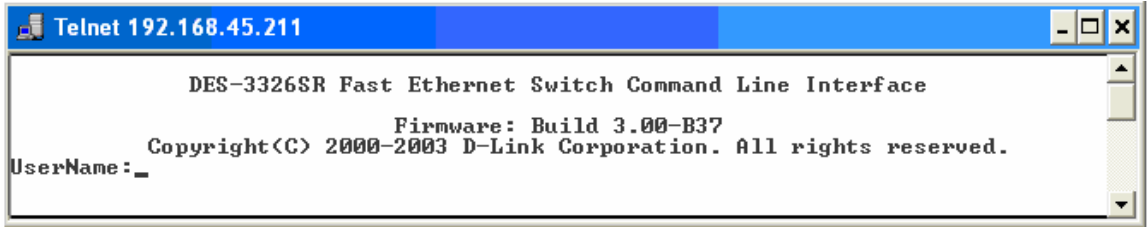
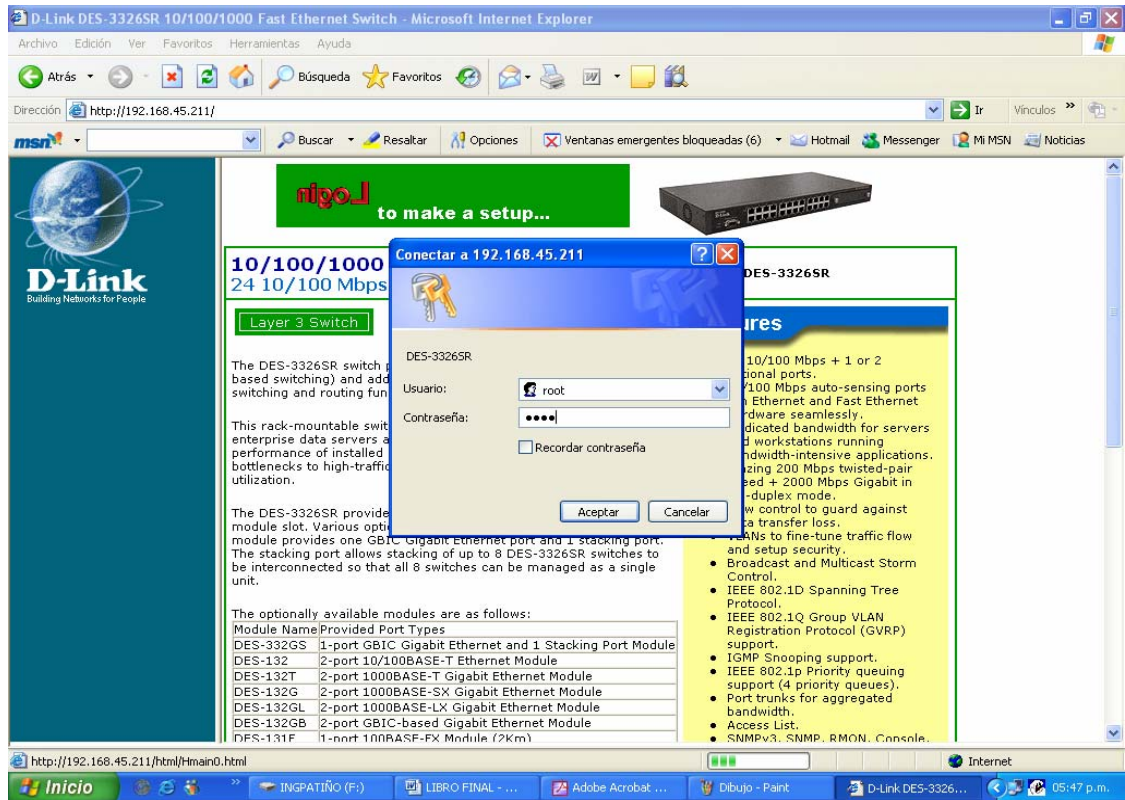


Figura 13. Acceso al Switch ambiente Web



El siguiente paso es digitar en el navegador la dirección asignada al switch, <http://192.168.45.211>, y en la parte superior escoger LOGIN.

En la parte superior se puede apreciar un mapa con los puertos que forman parte del switch. Qué signo nos indica que un puerto esta activo?

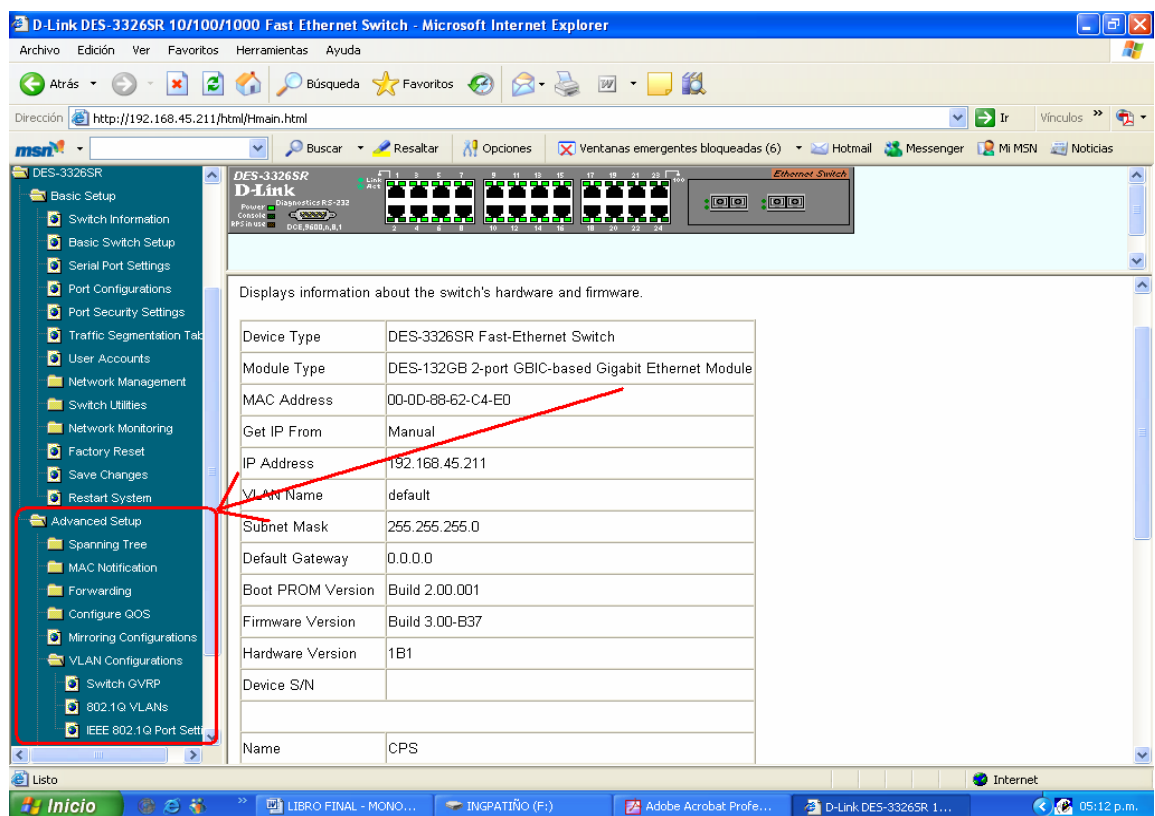
Que sucede cuando se presiona el Mouse sobre un puerto en el mapa?.

Una vez en la página de inicio de la administración del switch se puede proceder a crear las VLAN nuevas.

## II. Creación de VLANS

- a. En el menú de la izquierda derivada de la opción **DES-3326SR** se abre la opción **advanced setup**, dentro de esta se abre la opción **VLAN configurations**, como se muestra en la figura 14.

Figura 14. Acceso al las opciones de VLAN en el switch



Dentro de **VLAN configurations** se escoge **802.1Q VLAN**. Entonces en la pantalla principal se puede apreciar la única VLAN por defecto a la cual pertenecen todos los puertos del switch como lo muestra la figura 15.

Que indican las letras "U" debajo de los números de los puertos?

Figura 15. Vista de la VLAN por defecto del switch D-Link DES3326SR

**802.1Q VLANs**

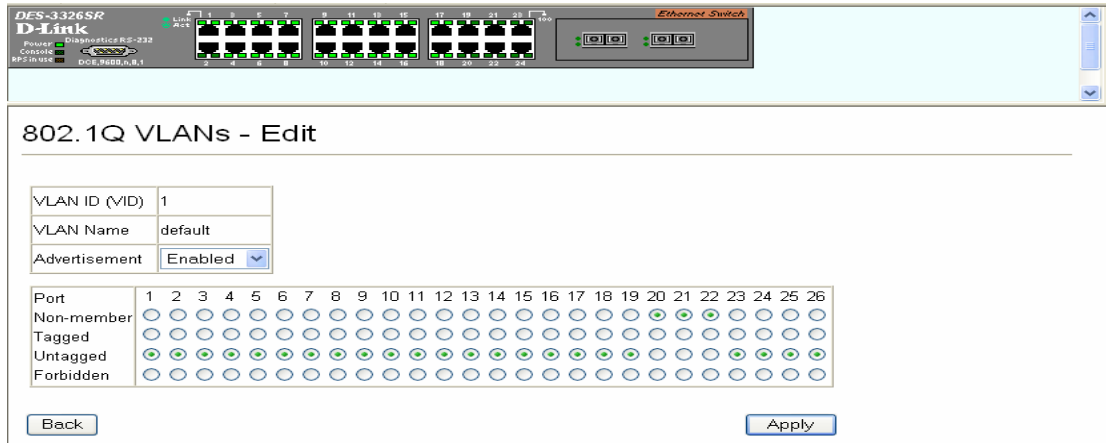
Configure 802.1Q VLANs by assigning ports a membership status.  
Tagged ports can belong to more than one 802.1Q VLAN.

Total Entries: 1

VLAN ID (VID)	VLAN Name	Advertisement	Members					
			1 to 8	9 to 16	17 to 24	25	26	
<input checked="" type="radio"/> 1	default	Enabled	UUUUUUUU	UUUUUUUU	UUUUUUUU	U	U	

b. Se selecciona la VLAN existente y luego se hace clic en **Edit**, se llegará a la imagen mostrada en la figura 16.

Figura 16. Edición de VLAN para switch D-Link DES3326SR



Aquí observará que todos los puertos pertenecen en modo “untagged” a la VLAN por defecto, los puertos seleccionados para esta práctica deben cambiarse de “untagged” a “non-member” para sacarlos de la VLAN por defecto, como se muestra en la figura 11, luego se debe presionar en Apply. Cual es la diferencia entre colocar el puerto Untagged a Tagged?, afecta eso en algo la VLAN que se trabaja?

Figura 17. VLAN por defecto editada para switch D-Link DES3326SR

## 802.1Q VLANs

Configure 802.1Q VLANs by assigning ports a membership status. Tagged ports can belong to more than one 802.1Q VLAN.

Total Entries: 1

[New](#) [Edit](#) [Delete](#)

	VLAN ID (VID)	VLAN Name	Advertisement	Members
				1 to 8 9 to 16 17 to 24 25 26
<input type="radio"/>	1	default	Enabled	UUUUUUUU UUUUUUUU UU--UU U U

- c. Se hace clic en New para crear una VLAN nueva, en seguida aparecerán las opciones de creación de VLAN nueva, se le puede dejar el numero ID como automático o simplemente colocar “2”, luego escribir el nombre (VLAN2) y se deben agregar los puertos que van a pertenecer a esta VLAN (se colocan como untagged los puertos 20 y 21 ( o los puertos seleccionados según el diseño ) ) como se aprecia en la figura 18; luego hacer clic en el botón Apply.

Figura 18. Creación de VLAN para switch D-Link DES3326SR

### 802.1Q VLANs - Add

VLAN ID (VID)	<input type="text" value="2"/> <input type="checkbox"/> Auto Assign
VLAN Name	<input type="text" value="VLAN2"/>
Advertisement	<input type="button" value="Enabled"/>

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Non-member	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Tagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Ahora aparecerá en el cuadro principal las VLAN existentes en el switch indicando que puertos pertenecen a ellas; y se repite el procedimiento de creación de VLAN para crear la VLAN3 y asignarle el puerto 22. Al final de esta acción debe observar lo siguiente: (ver Figura 19)

Figura 19. Nueva lista de VLAN creadas en el switch D-Link DES3226SR

	VLAN ID (VID)	VLAN Name	Advertisement	Members					
				1 to 8	9 to 16	17 to 24	25	26	
<input type="radio"/>	1	default	Enabled	UUUUUUUU	UUUUUUUU	UUUUUUUU	U	U	
<input type="radio"/>	2	VLAN2	Enabled	-----	-----	UUUUUU	-	-	
<input type="radio"/>	3	VLAN3	Enabled	-----	-----	UUUUUU	-	-	

Se pueden salvar los cambios para que en el caso de que el switch se apague, estos se reflejen en el sistema del switch. Para esto, se abre en el menú izquierdo **Basic setup** y se selecciona en este la opción **save changes**.

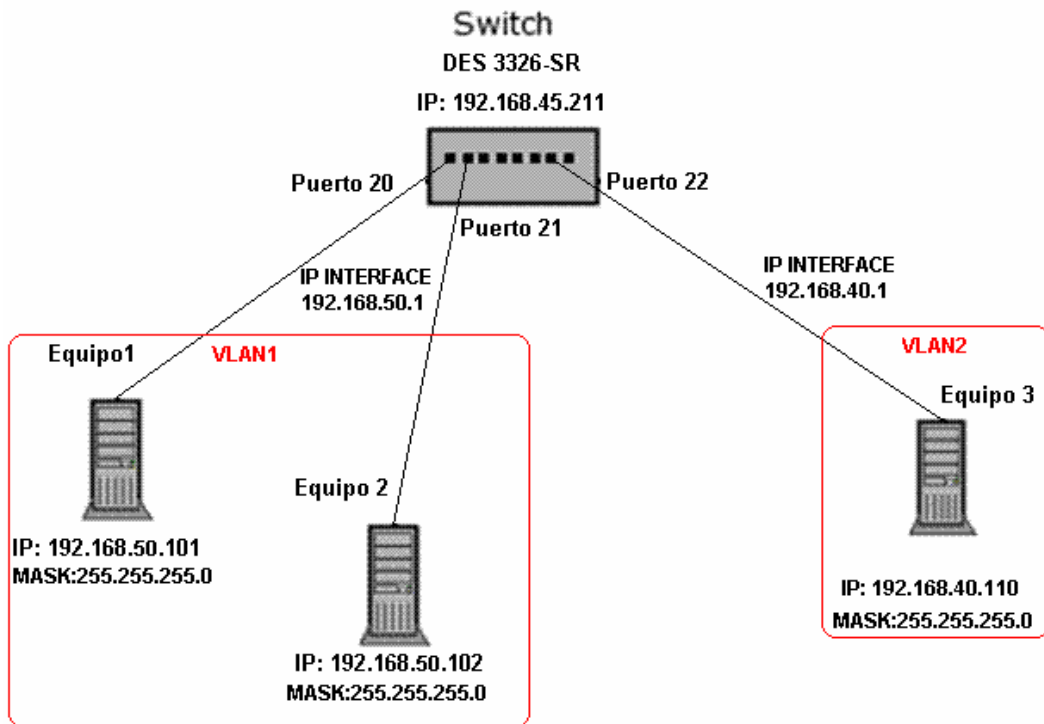
Una vez configuradas las VLAN, se procede a hacer pruebas de comunicación entre los computadores para verificar que solo pueden verse aquellos que pertenezcan a la misma VLAN. Se puede emplear el comando “ping” para esta operación.

➤ Trabajo en capa 3.

Ahora sin cambiar las conexiones físicas ni hacer ningún cambio en las configuraciones hechas en el switch, se reconfigurarán las direcciones IP de cada computador y sus máscaras de subred de acuerdo a la figura 17.

Con esto se pretende separar las dos VLAN en dos subredes distintas, la subred 192.168.50.0/24 y la subred 192.168.40.0/24, estas subredes manejarán las puertas de enlace con las direcciones 192.168.50.1 y 192.168.40.1 respectivamente, estas direcciones de puerta de enlace se deben configurar en cada equipo de acuerdo a la subred a la que pertenezca según la figura 20.

Figura 20. Reconfiguración de las direcciones IP para el switch D-Link DES3326SR.



**Nota:** Las direcciones IP de los equipos, los números de puertos y los nombres asignados a las VLAN aquí indicados corresponden a un ejemplo y caso particular, si el procedimiento es llevado a cabo por más de un grupo, el coordinador de esta práctica deberá asignar direcciones y puertos a cada grupo con el fin de evitar conflictos de IP y de uso de puertos.

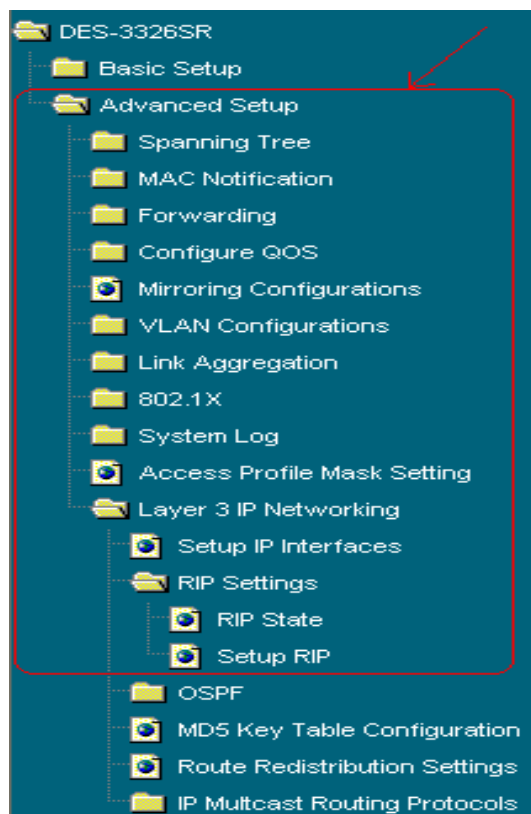
A cada VLAN le corresponde una subred, la puerta de enlace de la subred será asignada a la interfaz que identificará la VLAN dentro del switch. Quedando claro que para la VLAN1 la interfaz es 192.168.50.1 que a su vez es la puerta de enlace de la subred 192.168.50.0/24, así como para la VLAN2 la interfaz es 192.168.40.1 que a su vez es la puerta de enlace de la subred 192.168.40.0/24.

### III. Enrutamiento de VLAN en capa 3

Se accesa con el usuario administrador al switch por Web.

- a. En el menú de la izquierda derivada de la opción **DES-3326SR** se abre la opción **advanced setup**, dentro de esta se abre la opción **Layer 3 IP Networking**, y luego seleccionar la opción **RIP settings** como se muestra en la figura 21. Que quiere decir R.I.P?

Figura 21. Acceso al las opciones de capa 3 en el switch D-Link DES3326SR



- b. Seleccione **RIP state** para ingresar al recuadro del Estado del protocolo RIP, acá se debe habilitar el protocolo RIP seleccionando “Enabled” en la casilla “RIP Status” y luego hacer clic en el botón “Apply” de acuerdo a la figura 22.

Cuál es la utilidad del protocolo RIP?

Figura 22. Habilitación del protocolo RIP en el switch D-Link DES3326SR

## RIP Status

---

Globally enable or disable RIP for the switch.

RIP Status

Apply

- c. En el menú izquierdo se selecciona por **Advanced setup / Layer 3 IP networking** la opción **set up IP interfaces**. Se podrá apreciar un listado con las interfaces actuales en el switch y se deberá encontrar solo una que es la interfaz por defecto llamada "System". Figura 23.

Que es una interfaz en un switch y cual es su utilidad?

Figura 23. Listado de interfaces en el switch D-Link DES3326SR

## IP Interface Settings

Configure an IP interface for each existing 802.1Q VLAN.

Total Entries: 1

	Interface Name	IP Address	Subnet Mask	VLAN Name	Active	Members
						1 to 8 9 to 16 17 to 24 25 26
<input type="radio"/>	System	192.168.45.211	255.255.255.0	default	Yes	MMMMMMMM MMMMMMMM MMMMMMMM M M

- d. Se procede a crear una interfaz por cada VLAN que se tiene, haciendo clic en el botón “New”.

Para cada interfaz nueva se deben ingresar los datos del nombre de la interface, su dirección IP (la puerta de enlace de la subred respectiva), con la máscara de subred y la VLAN a la que esta conectada la interfaz, mostrada en la figura 24.

Figura 24. Creación de una interfaz nueva para el switch D-Link DES3326SR

## IP Interface Settings - Add

Interface Name	INTER1																									
IP Address	192	.	168	.	50	.	1																			
Subnet Mask	255	.	255	.	255	.	0																			
VLAN Name	VLAN1																									
Active	Yes <input type="button" value="v"/>																									
<input type="checkbox"/> Secondary																										

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Member	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Dando clic en “Apply” se crea la nueva interfaz.

Ahora en la lista de **set up interfaces** se pueden ver todas las interfaces creadas, cada una con la VLAN asociada, su dirección IP (gateway) y sus puertos respectivos; como se ilustra en la figura 25.

Figura 25. Nuevo listado de interfaces en el switch D-Link DES3326SR

## IP Interface Settings

Configure an IP interface for each existing 802.1Q VLAN.

Total Entries: 3

	Interface Name	IP Address	Subnet Mask	VLAN Name	Active	Members							
						1	to 8	9	to 16	17	to 24	25	26
<input type="radio"/>	INTER2	192.168. 40. 1	255.255.255. 0	VLAN2	Yes					M			
<input type="radio"/>	System	192.168. 45.211	255.255.255. 0	default	Yes	M	M	M	M	M	M	M	M
<input type="radio"/>	INTER1	192.168. 50. 1	255.255.255. 0	VLAN1	Yes					M			

- e. Se selecciona por **Advanced setup / Layer 3 IP networking /RIP settings / Setup RIP** para llegar al menú de configuración del protocolo RIP para las interfaces, se debe observar un listado con las interfaces existentes y sus configuraciones, luego se observa que para todas las interfaces el estado (State) es habilitado (Enabled), de ser el caso contrario, se debe seleccionar la interfaz que esté deshabilitada y presionar el botón “edit” allí se entra a un menú que permite habilitar el RIP para la interfaz seleccionada. Ver figura 26 y 27.

Figura 26. Listado de las interfaces y su estado en el switch D-Link DES3326SR

## RIP Interface Settings

Configure RIP for each defined IP interface.  
The global flag must be enabled before the individual interface settings have value.

Total Entries: 3

	Interface Name	IP Address	Tx Mode	Rx Mode	Auth.	State
<input type="radio"/>	INTER2	192.168. 40. 1	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	System	192.168. 45.211	Disabled	Disabled	Disabled	Enabled
<input type="radio"/>	INTER1	192.168. 50. 1	Disabled	Disabled	Disabled	Enabled

Figura 27. Menú de edición de las interfaces en el switch D-Link DES3326SR

## RIP Interface Settings - Edit

Interface Name	INTER1
IP Address	192 . 168 . 50 . 1
Tx Mode	Disabled <input type="button" value="v"/>
Rx Mode	Disabled <input type="button" value="v"/>
Authentication	Disabled <input type="button" value="v"/>
Password	<input type="text"/>
State	Enabled <input type="button" value="v"/>

- f. En el menú izquierdo se selecciona **Advanced setup / Layer 3 IP networking / IP Multicast Routing Protocols / Static Router Port settings**, en el se pueden apreciar las rutas estáticas de multicast, en este momento no debe haber ninguna ruta definida como se muestra en la figura 28.

Qué es una ruta estática y cuál es su propósito?

Figura 28. Listado de VLAN con sus puertos asignados a rutas estáticas en el switch D-Link DES3326SR

## Static Router Port Settings

---

Statically configure how multicast packets are routed.

Total Entries: 11

	VLAN Name	Router Port			
		1 to 8	9 to 16	17 to 24	25 26
<input type="radio"/>	default	-----	-----	-----	- -
<input type="radio"/>	VLAN1	-----	-----	-----	- -
<input type="radio"/>	VLAN2	-----	-----	-----	- -

- g. Seleccionar una de las VLAN creadas, se presiona el botón “Edit” y luego se entra a un menú que permite asignar los puertos que se deseen a la ruta de la VLAN seleccionada. A cada VLAN se le deben asignar sus puertos respectivos como se muestra en la figura 29.

Figura 29. Edición de los puertos para rutas estáticas en el switch D-Link DES3326SR

## Static Router Port Settings - Edit

---

VLAN Name

Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26  
Member

Regresando al listado de rutas estáticas de multicast se deben observar los puertos habilitados para las rutas en cada VLAN. La figura 30, permite visualizar los cambios realizados. Explicar por qué se hace esto con Multicast?

Figura 30. Segundo listado de VLAN con sus puertos asignados a rutas estáticas en el switch D-Link DES3326SR

## Static Router Port Settings

Statically configure how multicast packets are routed.

Total Entries: 11

	VLAN Name	Router Port			
		1 to 8	9 to 16	17 to 24	25 26
<input type="radio"/>	default	-----	-----	-----	- -
<input type="radio"/>	VLAN1	-----	-----	---MM---	- -
<input type="radio"/>	VLAN2	-----	-----	-----M--	- -

Se procede a hacer pruebas de comunicación entre las VLAN, empleando los comandos `ping` y `tracert` entre los equipos pertenecientes a diferentes VLAN para comprobar conectividad y verificar las rutas y saltos que están tomando los paquetes para llegar de un punto al otro.

**Nota:** Si se desea realizar la práctica por medio de la interfaz de línea de comandos en cambio de la interfaz Web; los comandos necesarios se encuentran en el anexo C.

### 4.1.8. Bibliografía

- [www.D-Link.com](http://www.D-Link.com)
- User's Guide DES-3326 24-Port Fast Ethernet Plus 2-Port Gigabit Module Layer 3 Switch.
- [www.wikipedia.com](http://www.wikipedia.com)

## **4.2. LABORATORIO DE CONFIGURACIÓN DE VLAN CON EL SWITCH 3COM 3226**

### **4.2.1. Título**

Creación de VLAN empleando el Switch 3COM 3226

### **4.2.2. Objetivo General**

Crear y configurar VLAN en capa 2 (por puerto) y capa 3 (por IP) utilizando el switch 3COM 3226

### **4.2.3. Objetivos Específicos**

- Familiarizarse con los equipos a utilizar en el desarrollo de la práctica.
- Disponer y adecuar cada equipo a utilizar en el desarrollo de la práctica.
- Realizar la conexión entre el switch y la estación de trabajo verificando el acceso y comunicación entre estos.
- Configurar VLAN en el switch.
- Comprobar la comunicación entre cada una de las estaciones de trabajo dentro de las VLAN creadas.
- Configurar el switch en capa 3 permitiendo el enrutamiento entre VLAN creadas en capa 2.

#### 4.2.4. Conocimientos Previos y Marco Teórico

- Asignación y configuración de direcciones IP.
- Protocolo TCP/IP.
- Comandos de consola para Switch 3COM 3226
- Etiquetado de VLAN

#### VLAN

Los grupos de trabajo en una red se han identificado por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador.

Como consecuencia lógica de la forma tradicional de crear grupos de trabajo, estos grupos comparten el ancho de banda disponible y los dominios de broadcast, así como los problemas que se ocasionan por la dificultad de gestión cuando se producen cambios en los miembros del grupo. Y también la limitación geográfica que supone que los miembros de un determinado grupo de trabajo deben estar situados de forma continua, por su conexión al mismo segmento de la red o concentrador.

Los esquemas de una Red Virtual de Área Local (VLAN) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de forma lógica, en lugar de física.

La tecnología de las VLAN se basa en el empleo de Switches, en lugar de Hubs o Concentradores, de tal manera que esto permite un control mas inteligente del

tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI<sup>1</sup> y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente.

Entre las ventajas más importantes de las VLAN tenemos:

- Sus esquemas proporcionan medios adecuados que ayudan a la solución de problemas permitiendo realizar una agrupación lógica.
- Su tecnología se basa en el empleo de Switches, a cambio de Hubs o concentradores, obteniendo de tal forma mayor control inteligente del tráfico de la red.
- Su área de trabajo se encuentra en la capa 2 y en la capa 3 del modelo OSI, lo que permite generar mayor eficiencia en toda la red.

Como principales razones para establecer una red VLAN son la reducción de costos, la facilidad de cambios en la red, mayor seguridad de la red y un mayor control de tráfico de la red

## **ESTÁNDAR IEEE 802.1Q**

Este estándar<sup>2</sup> define la arquitectura para las redes de área local unidas virtualmente, también define los servicios provistos en las VLAN y los protocolos y algoritmos involucrados en la provisión de estos servicios.

---

<sup>1</sup>OSI, modelo de referencia de Interconexión de Sistemas Abiertos

<sup>2</sup> Tomado de IEEE Std 802.1Q™, 2003 Edition , IEEE Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks

Cuando se trabaja con una VLAN no es raro que se presente una situación en que los miembros este ubicados lejos físicamente entre si, los paquetes entre los miembros tendrán que pasar por más de un switch diferente y a veces cubrir grandes distancias, en estos casos es necesario que las tramas lleven un identificador especial o “etiqueta” que le permita a cada switch por donde pasan saber a que VLAN pertenece el paquete y enviarlo adecuadamente.

Este estándar define la estructura que debe llevar la “etiqueta” (tagged) de VLAN que llevarán las tramas de Ethernet.

Para el caso en que todos los miembros de una VLAN estén conectados al mismo Switch no se hace necesario emplear las etiquetas (untagged) puesto que el mismo switch mapea internamente las VLAN que tenga definidas con sus respectivos miembros.

## **PROTOCOLO RIP**

En inglés **RIP** es Routing Information Protocol que quiere decir Protocolo de Información de Enrutamiento, es un protocolo de pasarela interior que es empleado por los enrutadores para intercambiar información sobre las redes IP

RIP utiliza UDP para enviar sus mensajes y el puerto 520.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. Esta distancia se denomina métrica.

### **4.2.5. Equipo Requerido**

- Tres (3) computadores con puerto serial y tarjeta LAN, donde al menos uno de ellos tenga software de hyperterminal.
- UN (1) Switch D-Link 3COM 3226.

- Patch Cord RJ45 de 3 y 6 pies de longitud.
- Cable de consola para el Switch

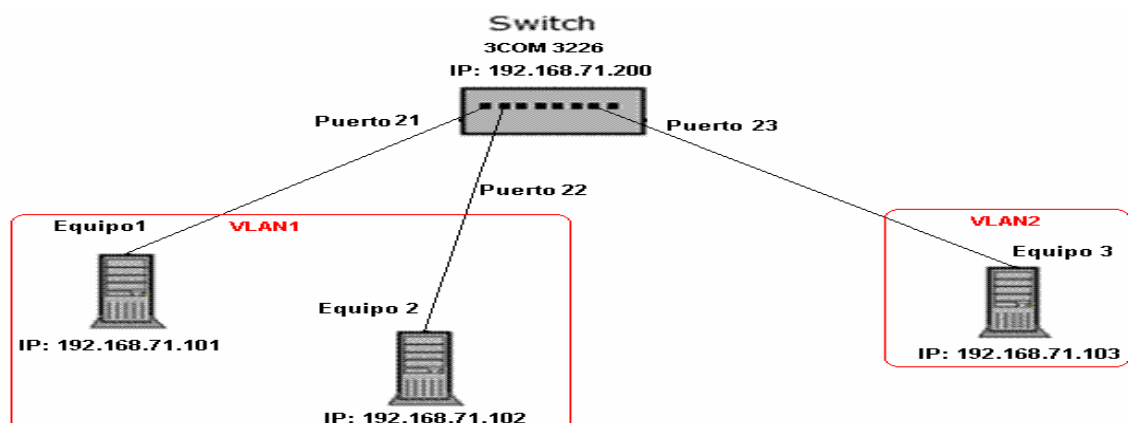
#### 4.2.6. Sugerencias y Recomendaciones

Al conectar los equipos y después de efectuar la configuración de todas las IP y máscaras de subred de los tres (3) computadores y el switch, se recomienda hacer inmediatamente pruebas de conectividad entre todos los computadores y el switch; de esta forma seguir con el desarrollo de la práctica, en caso tal que ningún computador se vea reflejado en la VLAN, revisar las conexiones físicas entre el computador y el puerto, y del puerto al switch.

#### 4.2.7. Procedimiento

La figura 31, nos permite visualizar la conexión física de los elementos que van a ser utilizados durante el desarrollo de la práctica:

Figura 31. Conexión del Switch 3COM 3226 y estaciones de trabajo.



**Nota:** Las direcciones IP de los equipos, los números de puertos y los nombres asignados a las VLAN aquí indicados corresponden a un ejemplo y caso particular,

si el procedimiento es llevado a cabo por más de un grupo, el coordinador de esta práctica deberá asignar direcciones y puertos a cada grupo con el fin de evitar conflictos de IP y de uso de puertos.

Se debe realizar una conexión entre el switch 3COM 3226 con una estación de trabajo o computador por medio de la consola (puerto serial) con la cual iniciaremos la configuración inicial.

¿Que tipo de cable se usa para conectar la salida de la tarjeta de red de cada computador con su respectivo puerto en el switch?

## I. Configuración del Switch 3COM 3226 por consola

Cuando se inicializa la comunicación con el Switch este solicita el Login y una clave. Si es la primera vez que se utiliza el switch el login será admin y la clave ninguna (dar enter) de lo contrario debe solicitarse el usuario y contraseña al administrador del switch.

Ahora se observará una lista de opciones en la figura 32.

Figura 32. Menú inicial de la interfaz de línea de comandos en el Switch 3COM 3226

```
Menu options: -----3Com SuperStack 3 Switch 3226-----
bridge      - Administer bridge-wide parameters
feature     - Administer system features
gettingStarted - Basic device configuration
logout      - Logout of the Command Line Interface
physicalInterface - Administer physical interfaces
protocol    - Administer protocols
security    - Administer security
system      - Administer system-level functions
trafficManagement - Administer traffic management
```

En la interfaz de línea de comandos (CLI) de este switch siempre se puede apreciar un menú donde se ofrecen todas las opciones posibles, los comandos se encuentran distribuidos en forma de árbol, en la figura 32 se aprecia lo que se consideraría la raíz del árbol de comandos con su primer menú; el simplemente debe digitar la opción o comando que desea tomar y seguido se ejecutará el comando o se abrirá la lista de opciones disponibles para dicha opción. En este menú se selecciona (digitando) **gettingStarted**, luego aparecerá un cuadro que se aprecia en la figura 33, donde se solicitan los datos de la IP la máscara de subred y la puerta de salida por defecto para el switch.

Figura 33. Entradas para configuración de IP para el Switch 3COM 3226

```
Select menu option (protocol/ip): basic
Enter configuration method (auto,manual,none)[none]: m
Enter IP Address      [0.0.0.0   ]: 192.168.71.200
Enter Subnet Mask     [255.0.0.0  ]: 255.255.255.0
Enter Default Gateway [0.0.0.0   ]:
Select management VLAN ID (1)[1]: 1

This operation may take up to 30 seconds.
```

Las direcciones IP y las máscaras de subred de los 3 computadores deben ser ajustadas de acuerdo a la conformación de la figura 31 de modo que todos los equipos se encuentren dentro de una misma red.

A partir de este punto, ya es posible acceder a la administración del switch vía Web o por Telnet. En este caso a la dirección IP 192.168.71.200

Al acceder por Telnet se aprecia que la estructura de menú de la interfaz de línea de comandos es la misma que se observó en la consola.

Al ingresar por Web, primero se le solicita al usuario que ingrese el login y la contraseña antes de poder acceder a la página inicial de administración (admin. Y ninguna clave).

Al ingresar a la página principal se debe hacer clic sobre la opción **device view** ubicada en la parte superior izquierda, esto permitirá apreciar el estado actual del switch, su configuración general y un mapa de sus puertos, como se aprecia en la figura 34.


Que sucede cuando se hace clic en la opción “poll Now”?

Figura 34. Vista Web del estado del switch 3COM 3226 y sus puertos.

Summary Device View Help

System  
Bridge  
Feature  
Physical Interface  
Protocol  
Security  
Traffic Management  
Unit 1

**Unit 1**



Polling Interval Poll Now Display Filter Color Key

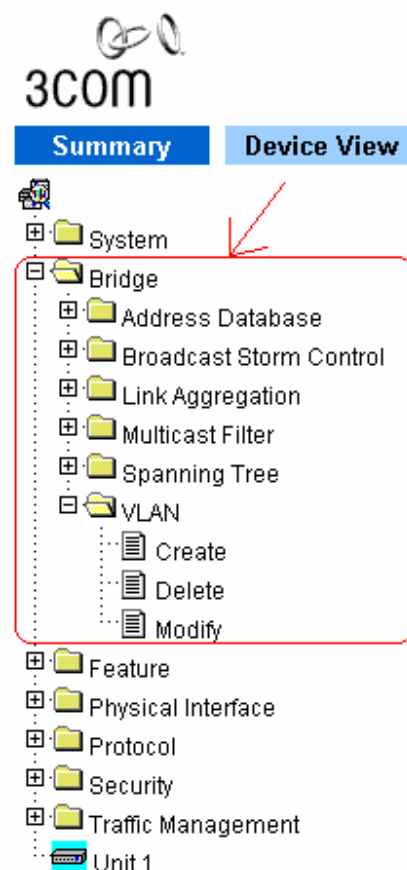
Device Summary : Unit 1	
Name	Lab. Esp. Telecomunicaciones
Type	Switch 3226
Software Version	1.02
Hardware Version	R01
IP address	192.168.71.200
MAC Address	00-0f-cb-a6-df-e0
Boot Version	2.00
Product Number	3CR17500-91
Serial Number	73MF4IBA6DFE0
Up Time	3 days 2 hours 6 minutes

En la parte izquierda se puede apreciar el árbol de opciones y comandos, el cuál es bastante similar en su estructura al árbol encontrado en la línea de interfaz de comandos.

## II. Creación de VLAN

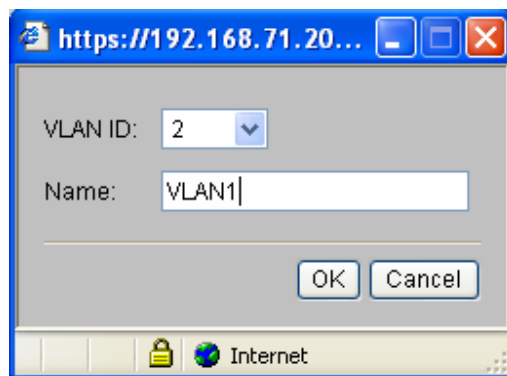
Para la creación de las VLAN, primero, se debe abrir la opción **Bridge** del árbol de opciones de la izquierda, luego se debe abrir la opción **VLAN**, se apreciará las opciones mostradas en la figura 35.

Figura 35. Opciones para trabajar con VLAN en el switch 3COM 3226



Se selecciona **Create**, aparecerá una pequeña ventana donde se solicitará el nombre y el número de identificación de la VLAN nueva, el número puede ser cualquier valor entre 2 y 4094 (ya que la VLAN por defecto a la cual inicialmente pertenecen todos los puertos ya posee el número ID 1), el nombre que se le dará será VLAN1, ver figura 36.

Figura 36. Ventana de creación de VLAN en el switch 3COM 3226



Este procedimiento se repite para crear la VLAN2 cuyo ID será 3

### III. Agregación de puertos

Con las 2 VLAN creadas se procede a agregar los puertos respectivos a cada una, en el menú de **VLAN** se selecciona la opción **modify**

Aparecerá una nueva ventana donde se aprecian todas las opciones necesarias para la edición de cualquier VLAN creada en el switch.

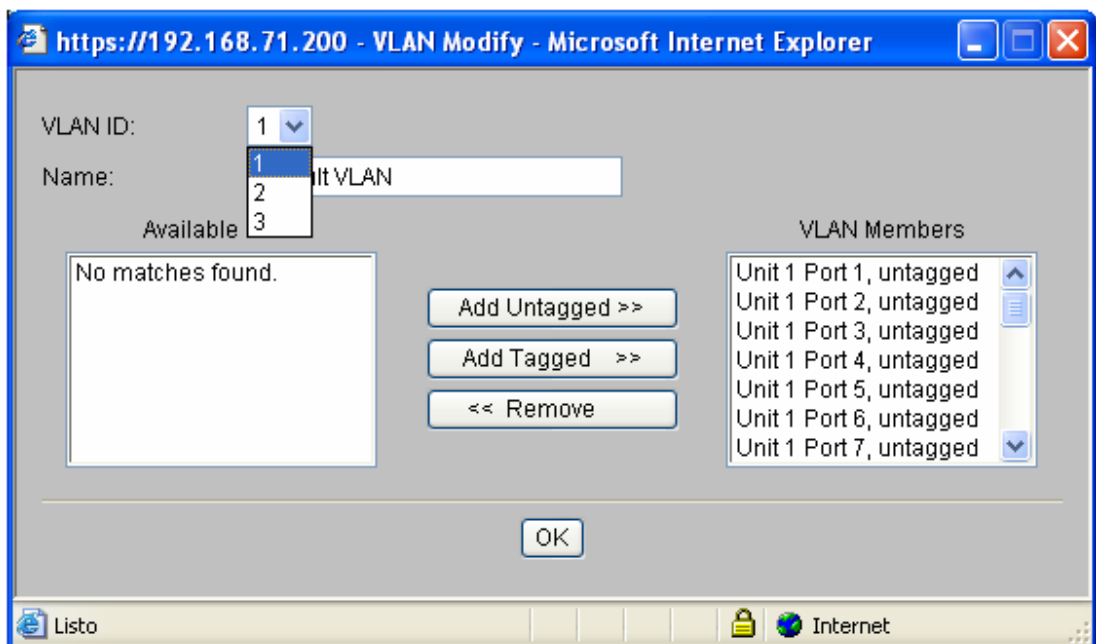
Como se puede apreciar en la figura 37, esta ventana cuenta con un menú plegable que permite seleccionar la VLAN a modificar mostrando la lista de todas las VLAN existentes, tiene un recuadro donde muestra el nombre de la VLAN seleccionada y permite cambiarlo y en la parte inferior están las opciones de los puertos, aquí se le puede agregar o quitar puertos a la VLAN seleccionada, los puertos pueden agregarse como “tagged” o “untagged” a una VLAN.

Cual es la diferencia en que un puerto sea Tagged a Untagged?

Cual es su relación con el protocolo IEEE 802.1 Q?,

Cual es la razón de ser de este protocolo?

Figura 37. Menú de Edición de VLAN en el switch 3COM 3226



Es importante tener claro que Antes de crear las VLAN1 y VLAN2, y existía una VLAN por defecto a la cual pertenecen todos los puertos, para el caso particular de esta VLAN, Intente remover algún puerto de esta VLAN, que sucede?

Luego agregue un puerto a una VLAN nueva e intente removerlo de la VLAN nueva, que sucede?

Para agregar puertos a las VLAN nuevas se debe primero seleccionar la VLAN a modificar en el menú plegable de arriba, luego aparecerán todos los puertos existentes en el switch en el cajón marcado como "Available" (disponibles), se seleccionan de este cajón el puerto que se quiere añadir y se hace clic sobre el botón "Add untagged", entonces en el cajón de la derecha marcado como "VLAN Members" aparecerá el puerto agregado como "untagged". Sería mejor hacer este procedimiento empleando la opción de tagged?, por que?

Se procede a agregar los puertos a cada VLAN de acuerdo al montaje de la figura 37.

**NOTA:** Siempre que se selecciona una VLAN diferente a la VLAN por defecto, aparecerá en el cajón "Available", todos los puertos existentes en el switch independientemente de si estos pertenecen a otra VLAN sea una nueva o la VLAN por defecto, si por ejemplo se le indica a la ventana agregar un puerto a la VLAN2 y si este puerto ya estaba asignado a la VLAN1, el switch automáticamente eliminará el puerto seleccionado de la VLAN1 y se lo asignará a la VLAN2, importante tener esto en cuenta para evitar errores en la asignación de puertos.

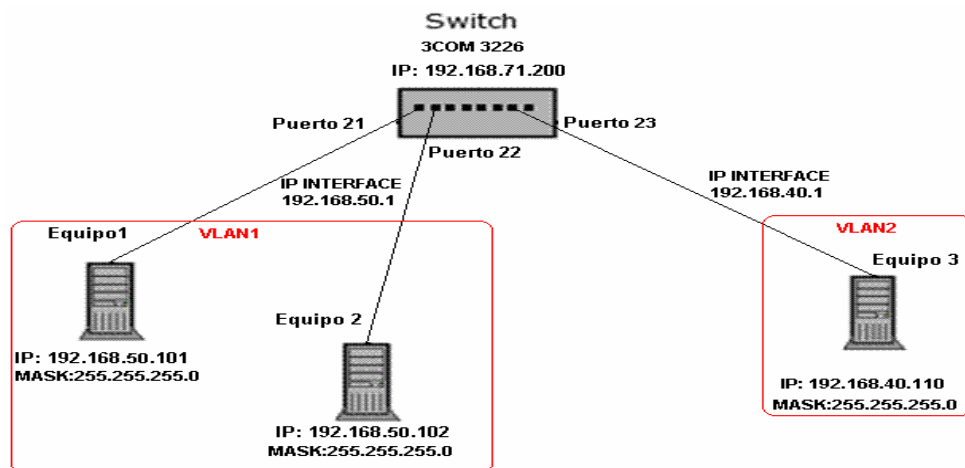
#### IV. Comprobación de comunicación de Equipos en la VLAN.

- a. Se procede a hacer pruebas de comunicación entre los computadores, para verificar que solo pueden verse aquellos que pertenezcan a la misma VLAN, se puede emplear el comando “ping” para esta operación.

Sin cambiar las conexiones físicas ni hacer ningún cambio en las configuraciones hechas en el switch, se reconfigurarán las direcciones IP de cada computador y sus máscaras de subred de acuerdo a la figura 38.

Con esto se pretende separar las dos VLAN en dos subredes distintas, la subred 192.168.50.0/24 y la subred 192.168.40.0/24, estas subredes manejarán las puertas de enlace con las direcciones 192.168.50.1 y 192.168.40.1 respectivamente, estas direcciones de puerta de enlace se deben configurar en cada equipo de acuerdo a la subred a la que pertenezca de acuerdo a la figura 34.

Figura 38. Reconfiguración de las direcciones IP para el switch 3COM 3226.



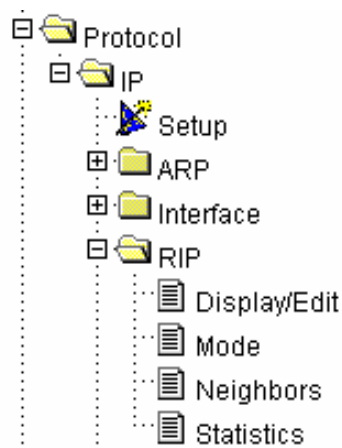
**Nota:** Las direcciones IP de los equipos, los números de puertos y los nombres asignados a las VLAN aquí indicados corresponden a un ejemplo y caso particular, si el procedimiento es llevado acabo por mas de un grupo, el coordinador de esta práctica deberá asignar direcciones y puertos a cada grupo con el fin de evitar conflictos de IP y de uso de puertos.

A cada VLAN le corresponde una subred, la puerta de enlace de la subred será asignada a la interfaz que identificará la VLAN dentro del switch. Quedando claro que para la VLAN1 la interfaz es 192.168.50.1 que a su vez es la puerta de enlace de la subred 192.168.50.0/24, así como para la VLAN2 la interfaz es 192.168.40.1 que a su vez es la puerta de enlace de la subred 192.168.40.0/24.

### b. Enrutamiento de VLAN en capa 3

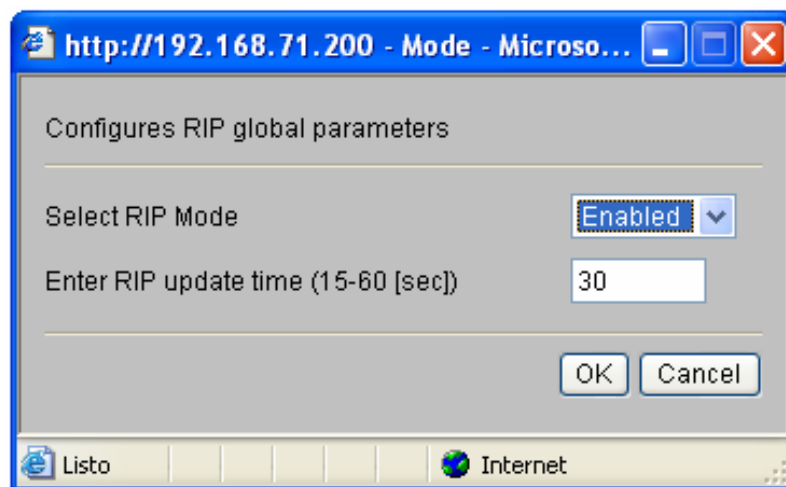
Primero se procede a habilitar el protocolo RIP, para ello en el menú de la izquierda, se debe seleccionar la opción **Protocol**, Luego se abre la opción **IP**, dentro de esta se encuentra la opción **RIP** la cuál se abre igualmente y mostrando las opciones que se aprecian en la figura 39.

Figura 39. Ruta para acceder a las opciones de RIP en el switch 3COM 3226



Se selecciona la opción **Mode** que abre un cuadro de dialogo que permite habilitar el protocolo **RIP**, se verifica que este habilitado, de no estarlo simplemente se hace el ajuste respectivo. Ver la figura 40.

Figura 40. Cuadro de dialogo para habilitar RIP en el switch 3COM 3226.



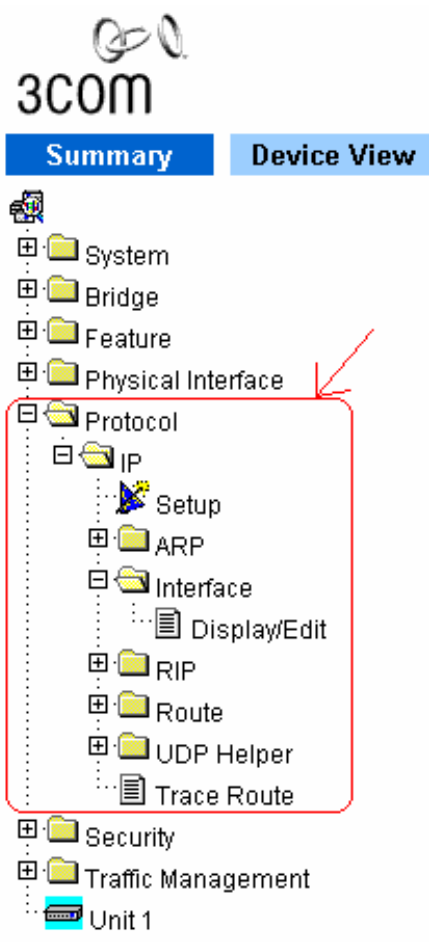
Agregación de interfaces.

Se accede al administrador del switch por Web.

Para crear las interfaces; en el menú izquierdo se abre la opción **Protocol**, de esta se abre la opción **IP**, y ahí se abre la opción **Interface** y aparecerá un último comando **Display/Edit** como se aprecia en la figura 41.

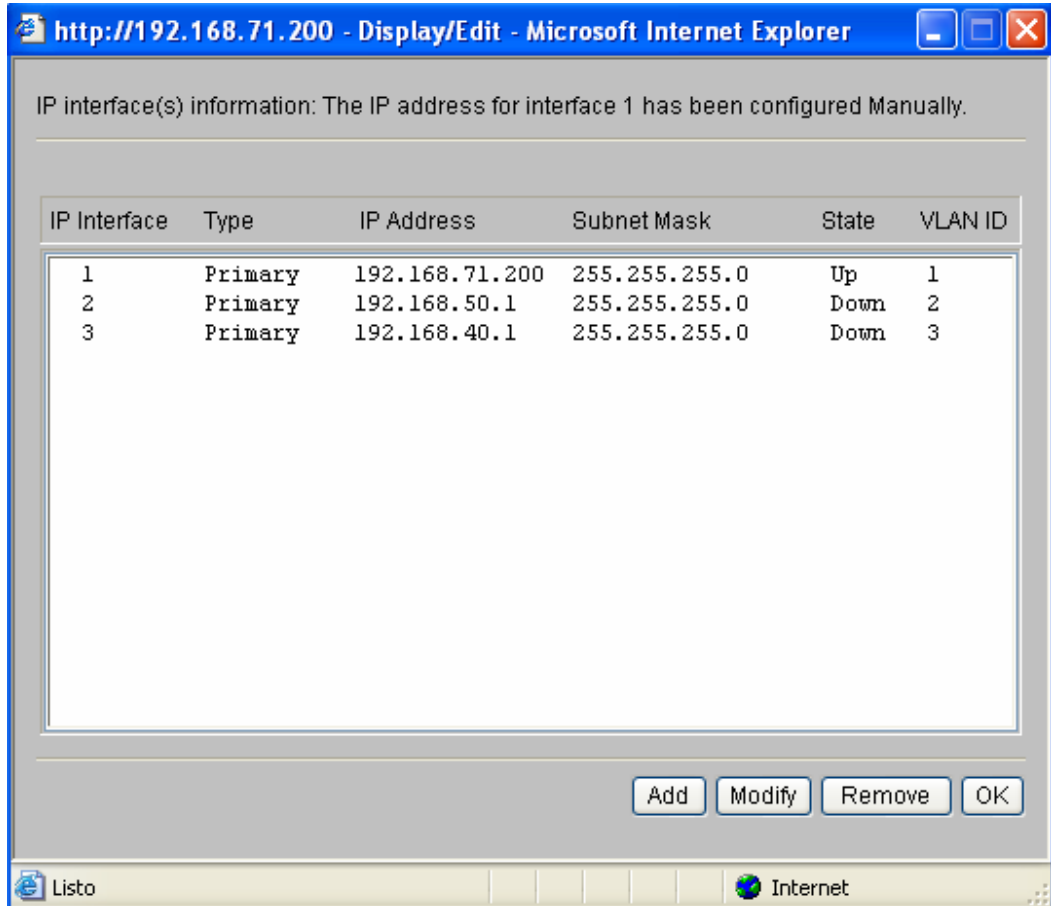
Cual es la función de una interfase de un switch en capa 3?

Figura 41. Ruta para acceder al comando de edición de interfaces IP en el switch 3COM 3226.



Al seleccionar el comando `Display/Edit` se abrirá una ventana en la cuál aparecerá una lista de las interfaces existentes en el switch y en la parte inferior aparecen las opciones de `Add` (**añadir interfaz**), `modify` (**editar interfaz**), `Remove` (**borrar interfaz**) y `OK` (**aceptar**), como se puede apreciar en la figura 42.

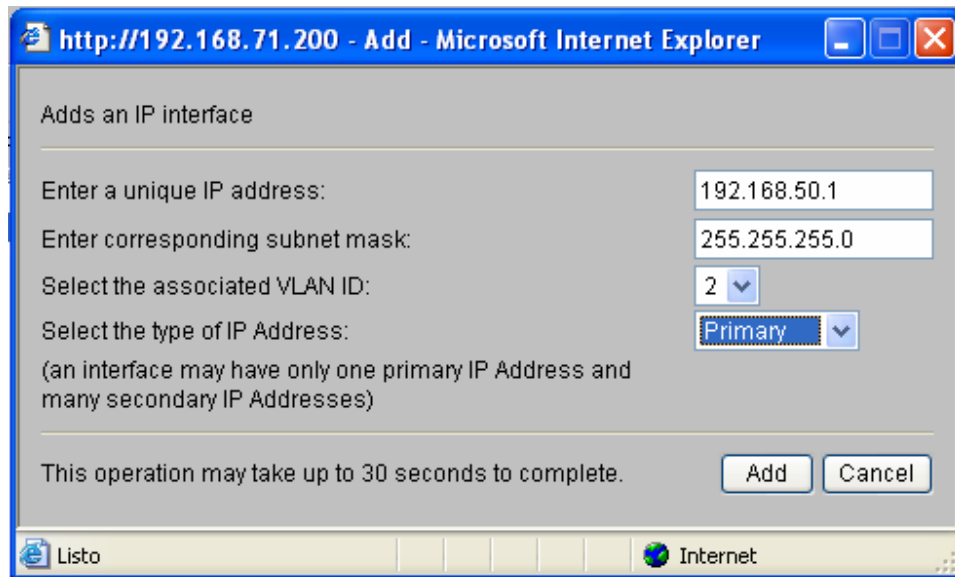
Figura 42. Ventana de interfaces en el switch 3COM 3226.



Se hace clic en la opción **Add**, y se abrirá una nueva ventana para la creación de la interfaz nueva, acá se deben ingresar todos los parámetros necesarios para este procedimiento, se debe dar la dirección IP de la interfaz respectiva, la máscara de subred, la VLAN asociada y finalmente colocar el tipo de IP como primaria. Como se puede apreciar en la figura 43.

Cual es la diferencia entre la IP primaria y la secundaria?

Figura 43. Ventana de creación de interface en el switch 3COM 3226.



Para cada interfaz a crear se lleva acabo este procedimiento

En la ventana de interfaces se puede verificar que todas las interfaces están creadas y que tienen las configuraciones correctas.

**c. Pruebas de verificación.**

Desde el equipo de una VLAN se hace un Tracert a un equipo de otra VLAN y se verifica cuantos saltos se dan y por donde pasa el paquete, también se puede emplear el comando ping para verificar la comunicación entre equipos de diferente VLAN.

**Nota:** Si se desea realizar la práctica por medio de la interfaz de línea de comandos en cambio de la interfaz Web; los comandos necesarios se encuentran en el anexo A.

#### **4.2.8. Bibliografía**

- [www.3com.com/prods/es\\_LA\\_AMER](http://www.3com.com/prods/es_LA_AMER).
- "3com *Transcend* VLANs", <http://www.3com.com/nsc/200375.html>.
- Super Stack® 3Switch 3226 and Switch 3250 Implementation Guide

#### **4.3. LABORATORIO DE CONFIGURACIÓN DE VLAN CON SWITCH AVAYA Cajun P333R.**

##### **4.3.1. Título**

Creación de VLAN empleando Switch AVAYA cajun P333R.

##### **4.3.2. Objetivo General**

Crear y configurar VLAN en capa 2 (por Puerto) y capa 3 (por IP) utilizando el switch Avaya Cajun P33R.

##### **4.3.3. Objetivos Específicos**

- Familiarizarse con los equipos a utilizar en el desarrollo de la práctica.
- Disponer y adecuar de cada equipo a utilizar en el desarrollo de la práctica.
- Realizar la conexión entre el switch y la estación de trabajo verificando el acceso y comunicación entre estos.
- Configurar VLAN en el switch.

- Comprobar la comunicación entre cada una de las estaciones de trabajo dentro de las VLAN creadas.
- Configurar el switch en capa 3 permitiendo el enrutamiento entre VLAN creadas en capa 2.

#### **4.3.4. Conocimientos Previos y Marco Teórico**

- Asignación y configuración de direcciones IP.
- Protocolo TCP/IP.
- Comandos de consola para Switch AVAYA Cajun P333R

#### **VLAN**

Los grupos de trabajo en una red se han identificado por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador.

Como consecuencia lógica de la forma tradicional de crear grupos de trabajo, estos grupos comparten el ancho de banda disponible y los dominios de broadcast, así como los problemas que se ocasionan por la dificultad de gestión cuando se producen cambios en los miembros del grupo. Y también la limitación geográfica que supone que los miembros de un determinado grupo de trabajo deben estar situados de forma continua, por su conexión al mismo segmento de la red o concentrador.

Los esquemas de una Red Virtual de Área Local (VLAN) proporcionan los medios adecuados para solucionar la problemática por medio de la agrupación realizada de forma lógica, en lugar de física.

La tecnología de las VLAN se basa en el empleo de Switches, en lugar de Hubs o Concentradores, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo

OSI<sup>1</sup> y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente.

Entre las ventajas más importantes de las VLAN tenemos:

- Sus esquemas proporcionan medios adecuados que ayudan a la solución de problemas permitiendo realizar una agrupación lógica.
- Su tecnología se basa en el empleo de switches, a cambio de Hubs o concentradores, obteniendo de tal forma mayor control inteligente del tráfico de la red.
- Su área de trabajo se encuentra en la capa 2 y en la capa 3 del modelo OSI, lo que permite generar mayor eficiencia en toda la red.

Como principales razones para establecer una red VLAN son la reducción de costos, la facilidad de cambios en la red, mayor seguridad de la red y un mayor control de tráfico de la red

## **ESTÁNDAR IEEE 802.1Q**

Este estándar<sup>2</sup> define la arquitectura para las redes de área local unidas virtualmente, también define los servicios provistos en las VLAN y los protocolos y algoritmos involucrados en la provisión de estos servicios.

Cuando se trabaja con una VLAN no es raro que se presente una situación en que los miembros este ubicados lejos físicamente entre si, los paquetes entre los miembros tendrán que pasar por más de un switch diferente y a veces cubrir grandes distancias, en estos casos es necesario que las tramas lleven un

---

<sup>1</sup>OSI, modelo de referencia de Interconexión de Sistemas Abiertos

<sup>2</sup> Tomado de IEEE Std 802.1Q™, 2003 Edition , IEEE Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks

identificador especial o “etiqueta” que le permita a cada switch por donde pasan saber a que VLAN pertenece el paquete y enviarlo adecuadamente.

Este estándar define la estructura que debe llevar la “etiqueta” (tagged) de VLAN que llevarán las tramas de Ethernet.

Para el caso en que todos los miembros de una VLAN estén conectados al mismo Switch no se hace necesario emplear las etiquetas (untagged) puesto que el mismo switch mapea internamente las VLAN que tenga definidas con sus respectivos miembros.

## **PROTOCOLO RIP**

En inglés **RIP** es Routing Information Protocol que quiere decir Protocolo de Información de Enrutamiento, es un protocolo de pasarela interior que es empleado por los enrutadores para intercambiar información sobre las redes IP

RIP utiliza UDP para enviar sus mensajes y el puerto 520.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. Esta distancia se denomina métrica.

**TRUNKING<sup>1</sup>**: El Trunking es una función para conectar dos switches o routers, del mismo modelo o no, mediante 2 cables en paralelo en modo Full-Duplex. Así se consigue un ancho de banda del doble para la comunicación entre los switches. Esto permite evitar cuellos de botella en la conexión de varios segmentos y servidores. El protocolo es 802.1q.

## **TRUNK para Avaya**

---

<sup>1</sup> Definición tomada de [http://es.wikipedia.org/wiki/Trunking\\_\(red\)](http://es.wikipedia.org/wiki/Trunking_(red))

En el switch Avaya, el atributo “trunk” pertenece a los puertos y este define si un puerto tiene habilitado o no el etiquetado para VLAN de los paquetes que viajan por dicho puerto.

#### **4.3.5. Equipo Requerido**

- Tres (3) computadores con puerto serial y tarjeta LAN, donde al menos uno de ellos tenga software de hyperterminal.
- UN (1) Switch AVAYA cajun P333R
- Patch Cord RJ45 de 3 y 6 pies de longitud.
- Cable de consola para el Switch

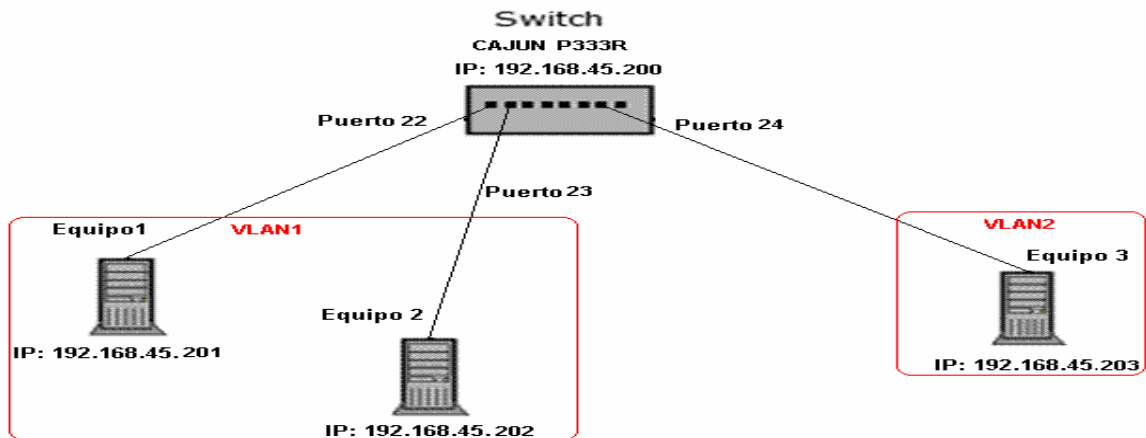
#### **4.3.6. Sugerencias y Recomendaciones**

Teniendo en cuenta que el Switch Avaya se encuentra desconectado de la LAN y los equipos del aula, se recomienda pre-configurar la dirección de IP del switch antes de la práctica para que le sea posible a cualquier equipo del aula acceder al Terminal de línea de comandos por Telnet, sin olvidar efectuar las conexiones necesarias en el rack para que los equipos puedan comunicarse correctamente con los puertos del switch Cajun P333R

#### **4.3.7. Procedimiento**

Primero se deben conformar los equipos de acuerdo a las conexiones mostradas en La figura 44, y asignar las direcciones IP indicadas para que todos pertenezcan a la misma subred:

Figura 44. Conexión del Switch Avaya Cajun P333R y estaciones de trabajo.



**Nota:** Las direcciones IP de los equipos, los números de puertos y los nombres asignados a las VLAN aquí indicados corresponden a un ejemplo y caso particular, si el procedimiento es llevado a cabo por más de un grupo, el coordinador de esta práctica deberá asignar direcciones y puertos a cada grupo con el fin de evitar conflictos de IP y de uso de puertos.

Uno de los computadores será conectado al switch por su puerto serial para hacer la configuración inicial del Cajun P333R por consola.

- I. Conexión y configuración por consola.
  - a. Al ingresar al administrador del switch por consola, se solicita un usuario y contraseña, en este caso se suministra como Login "root" y como contraseña "root" para poder acceder al sistema del switch.
  - b. Asignar una dirección IP a la interfaz del switch, esto se hace mediante el comando

```
red_avaya-1(super)# set interface inband 1 192.168.45.200 255.255.255.0
```

Como de ilustra en la figura 45.

Figura 45. Ejecución del comando set interface en el CAJUN P333R

```
red_avaya-1(super)# set interface inband 1 192.168.45.200 255.255.255.0  
Management VLAN number set to 1  
Interface inband IP address set.  
You must reset the device in order for the change to take effect.  
red_avaya-1(super)#
```

Después de dar este comando, el switch debe ser reseteado para que el cambio se aplique al dispositivo.

- c. Verificar que los cambios han tomado efecto, se puede revisar la interfaz con el comando:

```
Red avaya-1(super)# show interface
```

Y se podrá apreciar la siguiente respuesta en la pantalla de la consola mostrada en la figura 46.

Figura 46. Respuesta al comando show interface en el switch Cajun P333R

```
red_avaya-1(super)# show interface  
Interface Name      VLAN   IP address      Netmask  
-----  
inband              1      192.168.45.200 255.255.255.0  
ppp disabled       1      0.0.0.0         0.0.0.0  
red_avaya-1(super)# _
```

## II. Acceso y configuración vía Telnet.

Una vez hecho este paso, ahora es posible conectarse vía Telnet al switch con cualquier equipo que se encuentre en la misma LAN como se observa en la figura 47.

Figura 47. Ingreso al switch Cajun P333R por TELNET

```
Welcome to P333R
SW version 3.12.0

Login: root
Password:
Password accepted.

red_avaya-1(super)#
```

- a. Se procede a la creación de VLAN, mediante el uso del comando `set vlan`, a este comando se le ingresan dos parámetros, primero el número de ID de la VLAN que se crea y luego el nombre que se le va a asignar a la VLAN. Ver figura 48.

Figura 48. Creación de las VLAN con el comando `set vlan` en el CAJUN P333R

```
red_avaya-1(super)# set vlan 2 name vlan2
VLAN ID 2 is named vlan2.
red_avaya-1(super)# set vlan 3 name vlan3
VLAN ID 3 is named vlan3.
red_avaya-1(super)#
```

- b. Luego se procede a verificar la existencia de las VLAN creadas mediante el comando `show vlan` como se observa en la figura 49.

Figura 49. Aplicación del comando `show vlan` en el CAJUN P333R

```

red_avaya-1(super)# show vlan
VLAN ID Vlan-name
-----
1      default
2      vlan2
3      vlan3

red_avaya-1(super)# _

```

Se puede apreciar la existencia de la vlan 1 que por defecto posee todos los puertos del switch cuando no existe ninguna otra vlan con Puertos asignados.

- c. Asignación de puertos; se asignan los puertos a cada VLAN de acuerdo a la configuración dispuesta en la figura 50, con el comando `set port vlan`.

Figura 50. Uso del comando `set port vlan` en el CAJUN P333R

```

red_avaya-1(super)# set port vlan 2 1/22-23
VLAN 2 modified.
VLAN Mod/Ports
-----
2 1/12,22

VLAN 2 modified.
VLAN Mod/Ports
-----
2 1/12,22-23
red_avaya-1(super)# set port vlan 3 1/24
VLAN 3 modified.
VLAN Mod/Ports
-----
3 1/5-6,10,16-17,24,102
red_avaya-1(super)#

```

A este comando se le ingresan tres parámetros, primero el número de ID de la vlan a la que se le asignan los puertos, luego el número del módulo al que se le asignaran los puertos y después del “/” los puertos que se le asignan a la vlan.

Cuántos módulos tiene el switch ¿en que afecta emplear diferentes módulos a las VLAN?

- d. Verificación, procedemos a verificar que los puertos quedaron asignados a la VLAN correspondiente se emplea el comando `show port .`, el cual se muestra en la figura 51.

Figura 51. Empleo del comando show port en el Cajun P333R

```

red_avaya-1(super)# show port
Port Name Status Vlan Level Neg Dup. Spd. Type
-----
1/1 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/2 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/3 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/4 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/5 NO NAME no link 3 0 enable full 100M 10/100Base-Tx
1/7 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/8 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/9 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/10 NO NAME no link 3 0 enable full 100M 10/100Base-Tx
1/11 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/12 NO NAME no link 2 0 enable full 100M 10/100Base-Tx
1/13 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/14 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/15 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/16 NO NAME no link 3 0 enable full 100M 10/100Base-Tx
1/17 NO NAME no link 3 0 enable full 100M 10/100Base-Tx
1/18 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/19 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/20 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
1/21 NO NAME no link 1 0 enable full 100M 10/100Base-Tx
--type q to quit or space key to continue--
1/22 NO NAME no link 2 0 enable full 100M 10/100Base-Tx
1/23 NO NAME no link 2 0 enable full 100M 10/100Base-Tx
1/24 NO NAME no link 3 0 enable full 100M 10/100Base-Tx
1/51 NO NAME no link 1 0 enable full 1G 1000Base-Sx
1/102 lag no link 3 0 enable full 100M LAG of 10/100Base
-T
red_avaya-1(super)#

```

En la columna VLAN se puede apreciar a que VLAN pertenece cada puerto, que quiere decir “no link” en la columna de status?

- e. Para grabar los cambios efectuados, las VLAN creadas y sus nuevos puertos asignados, se debe ingresar al modo router mediante el comando `session router`, una vez en el modo router se debe correr el comando `copy running-config startup-config` para que los cambios sean guardados. Ver figura 52.

Figura 52. Guardado de cambios en el Cajun P333R

```
red_avaya-1(super)# session router
Router-1(super)# copy running-config startup-config
Beginning copy operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show copy status' command
Router-1(super)# _
```

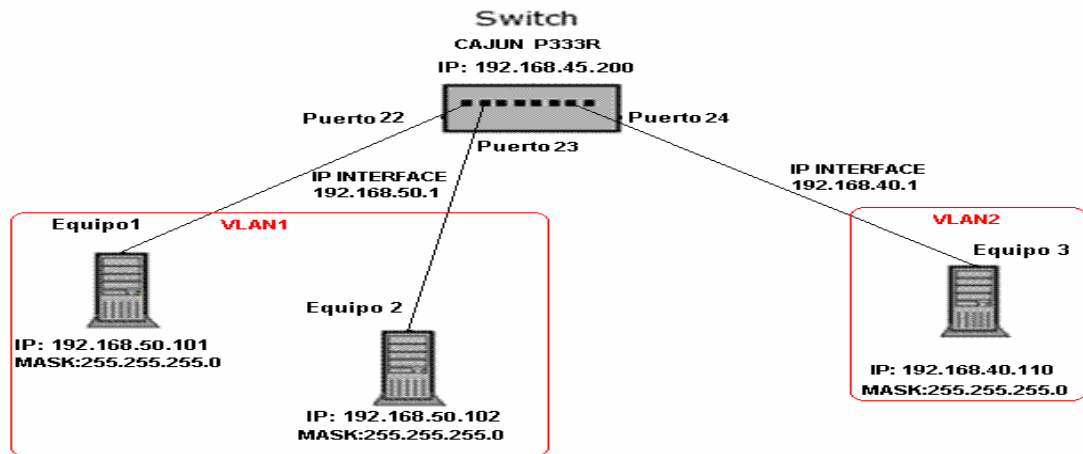
Se procede a hacer pruebas de comunicación entre los computadores, para verificar que solo pueden verse aquellos que pertenezcan a la misma VLAN, se puede emplear el comando “ping” para esta operación.

➤ Trabajo en capa 3

- f. Sin realizar cambios en las conexiones físicas ni hacer ninguna modificación en las configuraciones hechas en el switch, se reconfiguraran las direcciones IP de cada computador y sus máscaras de subred de acuerdo a la figura 44.

Con esto se pretende separar las dos VLAN en dos subredes distintas, la subred 192.168.50.0/24 y la subred 192.168.40.0/24, estas subredes manejarán las puertas de enlace con las direcciones 192.168.50.1 y 192.168.40.1 respectivamente, estas direcciones de puerta de enlace se deben configurar en cada equipo de acuerdo a la subred a la que pertenezca de acuerdo a la figura 53.

Figura 53. Reconfiguración de las direcciones IP para el switch Avaya Cajun P333R.



**Nota:** Las direcciones IP de los equipos, los números de puertos y los nombres asignados a las VLAN aquí indicados corresponden a un ejemplo y caso particular, si el procedimiento es llevado a cabo por más de un grupo, el coordinador de esta práctica deberá asignar direcciones y puertos a cada grupo con el fin de evitar conflictos de IP y de uso de puertos.

A cada VLAN le corresponde una subred, la puerta de enlace de la subred será asignada a la interfaz que identificará la VLAN dentro del switch. Quedando claro que para la VLAN1 la interface es 192.168.50.1 que a su vez es la puerta de enlace de la subred 192.168.50.0/24, así como para la VLAN2 la interface es 192.168.40.1 que a su vez es la puerta de enlace de la subred 192.168.40.0/24. Ver figura 51.

Estando conectado al switch, en la línea de comandos se dará el comando `session router` para entrar en el modo de enrutador de el switch. Ver figura 54.

Figura 54. Entrada al modo enrutador en el Switch Cajun P333R.

```

Welcome to P333R
SW version 3.12.0
red_avaya-1(super)# session router
Router-1(super)# _

```

Una vez en el modo enrutador se empleará el comando `interface` para crear las interfaces requeridas, en este caso una por cada VLAN, es importante destacar que el comando `interface` tiene doble propósito, el de crear y también el de acceder a una interfaz que ya este creada. Ver figura 55.

Figura 55. Creación de interfaces en el Switch Cajun P333R.

```
Router-1(super)# interface INTER2
Done!
Router-1(super-if:INTER2)# interface INTER3
Done!
Router-1(super-if:INTER3)#
```

El comando `exit` se emplea para salir de una interfaz o también para salir del modo enrutador y entrar en la línea principal de comandos, ahora se empleara `exit` para salir de la última interfaz creada.

Sin salir de el modo enrutador se aplicará el comando `set vlan` se crearán las VLAN necesarias para esta práctica, estas VLAN son ahora de capa3 y pueden tener el mismo o diferente nombre o identificador que las primera VLAN creadas que corresponden a capa 2. Ver figura 56.

Por que pueden tener el mismo nombre?

Son las mismas VLAN que se crearon al principio? que pasa con estas nuevas VLAN?

Figura 56. Creación de las VLAN en el modo enrutador en el Switch Cajun P333R.

```

Router-1(super)# set vlan 2 name VLAN2
Done!
Router-1(super)# set vlan 3 name VLAN3
Done!

```

Ahora con las interfaces y las VLAN creadas se procederá a configurar las interfaces, para esto primero se accede a la interface con el comando **interface**, dentro de la interfaz se emplea el comando **ip address** para configurar la dirección IP de la interfaz y su respectiva máscara de subred y luego se empleará el comando **ip vlan** con el número de ID de una VLAN para asociar la VLAN a esta interfaz. Ver figura 57.

Figura 57. Configuración de las interfaces en el Switch Cajun P333R.

```

Router-1(super)# interface INTER2
Done!
Router-1(super-if:INTER2)# ip address 192.168.50.1 255.255.255.0
Done!
Router-1(super-if:INTER2)# ip vlan 2
Done!
Router-1(super-if:INTER2)# interface INTER3
Done!
Router-1(super-if:INTER3)# ip address 192.168.40.1 255.255.255.0
Done!
Router-1(super-if:INTER3)# ip vlan 3
Done!
Router-1(super-if:INTER3)#

```

Nuevamente se emplea **exit** para salir de la última interfaz y ahora se empleará el comando **show ip route** para verificar la existencia de las interfaces, sus direcciones y VLAN asociada así como sus máscaras de subred, tal como se observa en la figura 58.

Por que no se le asignaron puertos a estas nuevas VLAN?

Figura 58. Listado de las interfaces en el Switch Cajun P333R.

```

Router-1(super-if:INTER3)# exit
Router-1(super)# show ip route
Showing 2 rows
  Network          Mask           Interface      Next-Hop       Cost  TTL  Source
-----
192.168.40.0      255.255.255.0  INTER3        192.168.40.1   1    n/a  LOCAL
192.168.50.0      255.255.255.0  INTER2        192.168.50.1   1    n/a  LOCAL
Router-1(super)# _

```

Se guardan los cambios en el modo enrutador como se muestra en la figura 59.

Figura 59. Segundo guardado de cambios en el Cajun P333R

```

Router-1(super)# copy running-config startup-config
Beginning copy operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show copy status' command
Router-1(super)# _

```

Ahora se procede a hacer pruebas: desde el equipo de una VLAN se hace un Tracert a un equipo de otra VLAN y se verifica cuantos saltos se dan y por donde pasa el paquete, también se puede emplear el comando ping para verificar la comunicación entre equipos de diferente VLAN.

Cuantos saltos se debería esperar que ocurran y por que?. Verificar utilizando el comando Tracert

#### g. Creación de VLAN entre dos Switch.

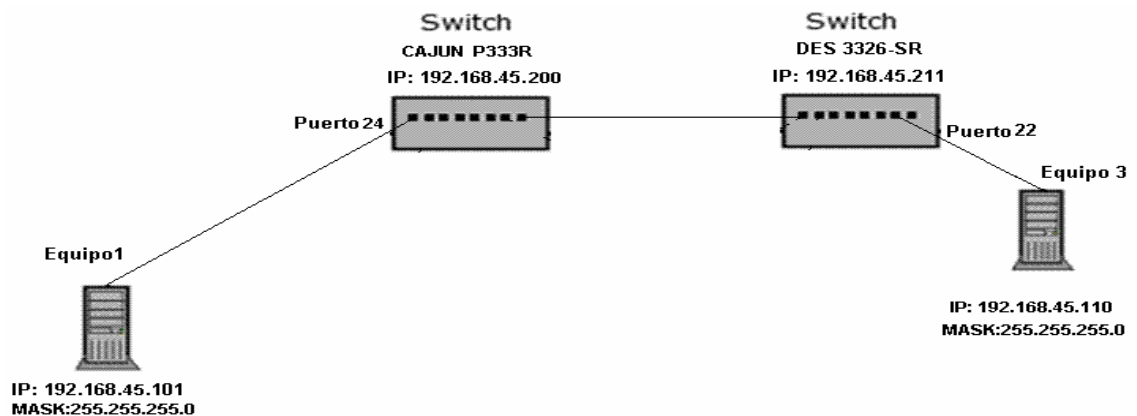
Como punto adicional se propone crear una VLAN que se extienda a más de un switch.

Para esto se emplearán el switch DES3326SR D-LINK y el CAJUN P333R de Avaya, los cuales se encuentran ubicados en un mismo rack, permitiéndonos facilidad y ahorro de tiempo.

Para esta parte se deben conectar dichos switches de modo que se puedan comunicar, para esto se conectará un puerto libre de el DES3326 con un puerto del CAJUN P333R empleando un patch cord directo.

Para esta parte se emplearan solamente dos computadores con los dos switches que irán conectados de acuerdo a la figura 60.

Figura 60. Conexiones para prueba de VLAN inter switches.



Ahora se entra al administrador del DES 3326SR por Web y se realizan las siguientes configuraciones:

En el menú de la izquierda derivada de la opción **DES-3326SR** se abre la opción **advanced setup**, dentro de esta se abre la opción **VLAN configurations**, se escoge **802.1Q VLAN** para entrar al menú de las VLAN, luego se seleccionan las dos VLAN creadas y se borran una a una empleando el botón “**delete**”.

Ahora se va a crear una nueva VLAN que se llamará vlan3 y se le colocará como ID el número 3 (importante por que se debe hacer igual en el switch Avaya) y se le asignará un solo puerto como “tagged”(uso del el estándar IEEE 802.1Q), el puerto 22. Ver figura 61.

Que pasa si se le asigna el puerto como “untagged”?

Figura 61. Creación de la VLAN3 para la prueba inter switches

802.1Q VLANs - Add

---

VLAN ID (VID)	<input type="text" value="3"/> <input type="checkbox"/> Auto Assign
VLAN Name	<input type="text" value="vlan3"/>
Advertisement	<input type="button" value="Enabled"/> ▾

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
Non-member	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Se verifica la creación de la VLAN y sus puertos en el menú principal de VLAN. Ver figura 62.

Figura 62. Verificación de la VLAN3 para prueba inter switches.

802.1Q VLANs

---

Configure 802.1Q VLANs by assigning ports a membership status.  
Tagged ports can belong to more than one 802.1Q VLAN.

Total Entries: 2

	VLAN ID (VID)	VLAN Name	Advertisement	Members
<input type="radio"/>	1	default	Enabled	1 to 8 9 to 16 17 to 24 25 26
<input type="radio"/>	3	vlan3	Enabled	-----T-- - -

Ahora se procede a conectarse al AVAYA a su línea de comandos:

Primero se va a verificar el estado de configuración de los puertos mediante el comando `show trunk`. Ver figura 63.

Figura 63. Verificación de los puertos del Avaya con comando `show trunk`  
`red_avaya-1(super)# show trunk 1/1-24`

```

1/19 off  statically bound          1    1
-----
Port  Mode  Binding mode          Native vlan  Vlans allowed on trunk
-----
1/20 off  statically bound          1    1
-----
Port  Mode  Binding mode          Native vlan  Vlans allowed on trunk
-----
1/21 off  statically bound          1    1
-----
Port  Mode  Binding mode          Native vlan  Vlans allowed on trunk
-----
1/22 off  statically bound          2    2
-----
Port  Mode  Binding mode          Native vlan  Vlans allowed on trunk
-----
1/23 off  statically bound          2    2
-----
--type q to quit or space key to continue--
Port  Mode  Binding mode          Native vlan  Vlans allowed on trunk
-----
1/24 off  statically bound          3    3

```

Se aprecia que todos los puertos tienen el modo “Mode” en off, esto indica que no están habilitados para emplear el estándar IEEE 802.1Q

Para habilitar un puerto al estándar se debe emplear el comando `set trunk` (figura 64) de la siguiente forma:

Figura 64. Empleo del comando set trunk para habilitar el estándar IEEE 802.1Q en el puerto 24 del switch CAJUN P333R.

```
red_avaya-1(super)# set trunk 1/24 dot1q
Dot1Q VLAN tagging set on port 1/24.
red_avaya-1(super)#
```

Se verifica si existe la vlan3, de no ser así se crea mediante el comando `set vlan` (ver figura 65).

Figura 65. Creación de la vlan3 en el CAJUN P333R.

```
red_avaya-1(super)# set vlan 3 name vlan3
VLAN ID 3 is named vlan3.
red_avaya-1(super)#
```

Se configure la vlan3 para que tenga asignado el Puerto 24 con el comando `set port vlan` (ver figura 66).

Figura 66. Asignación del puerto 24 al CAJUN P333R

```
red_avaya-1(super)# set port vlan 3 1/24
VLAN 3 modified.
VLAN Mod/Ports
-----
 3 1/5-6,10,16-17,24,102
red_avaya-1(super)#
```

Ahora se debe verificar que los dos computadores se encuentran en la misma VLAN mediante pruebas con el comando ping

#### 4.3.8. Bibliografía

- User's Guide CAJUN P333R STACKABLE 3RD LAYER SWITCH.
- [http://support.avaya.com/elmodocs2/cajun/cajun\\_documentation/P330/routing-redis.pdf](http://support.avaya.com/elmodocs2/cajun/cajun_documentation/P330/routing-redis.pdf).
- IEEE Std 802.1Q™, 2003 Edition
- [www.D-Link.com](http://www.D-Link.com)
- User's Guide DES-3326 24-Port Fast Ethernet Plus 2-Port Gigabit Module Layer 3 Switch

## CONCLUSIONES Y OBSERVACIONES

- Con la elaboración de cada una de las prácticas de laboratorio, observamos el amplio potencial de trabajo ofrecido por los dispositivos no solo en la

creación y configuración de VLAN, si no, también con otras aplicaciones que ellos nos ofrecen con relación a redes de datos.

- Las VLAN, tienen un alto grado de importancia no solo en el área de formación académica, si no, en el momento que se utilicen o apliquen en el área comercial y laboral, las cuales le facilitan a los empresarios tener una mayor cobertura de aplicabilidad, permitiéndoles tener un alto grado control de los departamentos a interactuar ahorrando grandes cantidades de dinero.
- El desarrollo de este trabajo, permitió afianzar los conocimientos adquiridos durante las diferentes etapas y procesos de la Especialización, logrando despejar aquellas dudas o inquietudes surgidas durante dicho lapso tiempo.
- Es importante comprender el significado y aplicaciones del switch, del protocolo TC/IP; conocimientos de cableado estructurado, permitiendo de una manera u otra la facilidad del análisis, creación de redes ya sean tipo LAN, MAN, WAN como lo VLAN, ya que estas ultimas es la tendencia de configuración de redes a nivel mundial.
- Con el desarrollo de las prácticas de laboratorio planteadas, se espera que los estudiantes den importancia relativamente alta al tema de las VLAN, ya que observamos el movimiento y las directrices que ha tomado el mundo con respecto a las telecomunicaciones, va dirigido a esta nueva generación de configuración de redes.
- Tener seguridad en los conocimientos y habilidades adquiridas en el transcurso de la especialización, permitirá de manera segura y eficaz la ejecución y solución de las practicas planteadas.

## BIBLIOGRAFÍA

- Revista RED; La comunidad de expertos en redes, Junio 2001 Edición 129.
- Sistema de comunicaciones Electrónicas; Tomasy, Editorial Prentice Hall, Segunda edición.
- [www.3com.com/prods/es\\_LA\\_AMER](http://www.3com.com/prods/es_LA_AMER).
- Diccionario El Pequeño Larousse Ilustrado, Edición 2005, Pág. 569.
- Enciclopedia Encarta2005, Microsoft Corporation.
- [http://support.avaya.com/elmodocs2/cajun/cajun\\_documentation/P330/routing-redis.pdf](http://support.avaya.com/elmodocs2/cajun/cajun_documentation/P330/routing-redis.pdf).
- <http://es.wikipedia.org/wiki/Switch>.
- <http://es.wikipedia.org/wiki/VLAN>.
- <http://es.wikipedia.org/wiki/Concentrador>
- [http://monografia/investigacion/D-Link TechSupport – FAQ](http://monografia/investigacion/D-Link_TechSupport_-_FAQ).
- IEEE Std 802.1Q™, 2003 Edition
- [www.D-Link.com](http://www.D-Link.com)
- [http:// monografia/redes virtuales](http://monografia/redes_virtuales).
- Revista Microbyte N° 130, Junio 1996, artículo:" VLANs, Redes Virtuales", Págs. 26, 27, 28.
- "3com *Transcend* VLANs", <http://www.3com.com/nsc/200375.html>.
- User's Guide DES-3326 24-Port Fast Ethernet Plus 2-Port Gigabit Module Layer 3 Switch.
- Super Stack® 3Switch 3226 and Switch 3250 Implementation Guide.

- <http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=107715&temp.bucketID=160257>.
- <http://www.jegsworks.com/lessons-sp/lesson7/lesson7-3.htm>.
- [http://ramcir\\_cjm.tripod.com/codigo.htm](http://ramcir_cjm.tripod.com/codigo.htm)

## **ANEXO A. SWITCH 3COM – 3226**

### **1. CARACTERÍSTICAS**

#### **1.1. FÍSICAS**

##### **1.1.1. Dimensiones**

- Altura: 45 mm
- Ancho: 440 mm
- Profundidad: 252 mm
- Peso: 4.3 Kg.

#### **1.2. PUERTOS**

En este switch vemos la siguiente asignación de puertos:

- 24 puertos de auto detección 10BASE-T/100BASE-TX2.

- 2 Puertos de propósito dual que soportan conexiones 10BASE-T/100BASE-TX/1000BASE-T o puertos SFP que acomodan 1000BASE-SX, 1000BASE-LX o 1000BASE-LH70.

### **1.3. INTERFACES**

Utiliza conectores RJ-45 para los puertos 10/100 y 10/100/1000; para los SFPs depende del módulo SFP específico.

### **1.4. PARA CAPA 2**

Completa tasa de no bloqueo en todos los puertos Ethernet; auto negociación de full/half duplex y de control de flujo; filtrado multicast de capa 2; soporte al estándar 802.1Q para VLAN, al estándar 802.1p para priorización de tráfico, IGMP snooping.

### **1.5. PARA CAPA 3**

Rutas estáticas; Rutas dinámicas de capa3 RIP.

Entre las capacidades de capa 3 cabe destacar el enrutamiento del tráfico segmentado localmente en el closet de cableado, sin necesidad de enviar el tráfico al centro de la red para el enrutado. A través del el soporte al enrutamiento dinámico (RIP) presenta más ventaja a trabajar con rutas estáticas, con reconfiguración automática cuando hay cambios de topología en la red.

Las características de seguridad incluyen las listas de control de Acceso y Log-In a la red del estándar IEEE 802.1X. La administración del switch se hace a través de sesiones de SSL (HTTPS) y SSH, múltiples dispositivos pueden ser administrados por medio del supervisor de red 3Com.

### **1.6. CARACTERÍSTICAS ADMINISTRABLES**

El software de administración permite cambiar el estado por defecto de algunas características del switch, las cuales son:

### **1.6.1 Enlaces Agregados**

Son conexiones que permiten a los dispositivos comunicarse usando múltiples enlaces en paralelo. Este switch soporta un link agregado usando los puertos 10/100/1000 y SFP (puertos 25 y 26 del switch). El link agregado provee dos beneficios: incrementan potencialmente el ancho de banda de una conexión y además proveen redundancia.

El switch implementa el estándar 802.3ad para la agregación de enlaces.

### **1.6.2. Auto-negociación**

Esta permite a los puertos auto negociar la velocidad del puerto, el modo dúplex (solo a 10 Mbps y a 100 Mbps) y el flujo de control. Cuando la auto negociación está habilitada (por defecto lo esta), un puerto “informa” sus máximas capacidades – estas capacidades son por defecto los parámetros que proveen el máximo desempeño soportado por el puerto.

Los puertos SFP no soportan auto negociación de velocidad de puerto. Los puertos operando a 1000 Mbps solo soportan el modo full dúplex.

### **1.6.3. MDI/MDI-X Automático**

Permite a los puertos detectar cuando ellos están conectados a un computador o a otro switch y configurarse adecuadamente, eliminando la necesidad de uso de cables cruzados.

#### **1.6.4. Duplex**

El modo Full duplex permite recibir y transmitir paquetes simultáneamente y duplica el throughput (tasa máxima de transmisión) de un enlace.

#### **1.6.5. Control de flujo**

Todos los puertos del switch soportan control de flujo, el cual es un mecanismo que minimiza la pérdida de paquetes durante periodos de congestión en la red. El control de flujo emplea en los puertos su operación en modo half Duplex, y es implementado utilizando el estándar de la IEEE 802.3-2002 (incorporando el 802.3x) en puertos operando en modo full duplex.

#### **1.6.6. Salvado de configuración y restauración**

Estos permiten guardar la configuración del switch en un servidor remoto, o restaurarla en el switch tomando el archivo de un servidor remoto. La información de configuración es guardada en un archivo de texto ASCII.

Toda la información de configuración que puede ser ajustada empleando la interface de línea de comandos del switch es guardada y restaurada. (La información de passwords y administración de IP no será guardada en el archivo de configuración).

Es necesario tener acceso de nivel administrativo de lectura/escritura para poder guardar y restaurar la configuración del switch.

Consideraciones a tener en cuenta:

- Se recomienda resetear el switch a sus ajustes por defecto de fábrica antes de restaurar una configuración en él. El switch se puede resetear empleando el comando **system control initialize** en la interface de línea de comandos o con la opción System>Control>initialize en la interface Web.
- La configuración solo puede ser restaurada en un dispositivo que tenga las mismas conexiones físicas que se encontraban cuando la configuración fue guardada inicialmente. La operación de restauración no será exitosa si la configuración física del dispositivo es diferente.
- La configuración del switch solo puede ser restaurada o guardada por un solo usuario a la vez.
- Cuando se emplea el guardado de configuración y la restauración de la misma, se recomienda que los enlaces agregados sean configurados de una de dos maneras: Mediante agregaciones manuales con el protocolo de configuración de enlace agregado (LACP) deshabilitado en los puertos que van a ser manualmente ubicados en el enlace agregado. O con agregaciones automáticas LACP- entonces, con LACP habilitado en todos los puertos y los enlaces agregados son creados automáticamente. El enlace agregado debe estar habilitado y el protocolo de árbol de spanning también.
- Cuando se restaura una configuración en una unidad en un enlace agregado, la comunicación con esa unidad puede ser perdida debido a que la operación de restauración deshabilita los puertos de enlace agregado. La comunicación sobre los enlaces agregados es restablecida cuando la operación de restauración ha sido completada.

#### 1.6.7. Filtrado de multicast

Permite al switch enviar tráfico de multicast a solamente las estaciones de destino que son parte de un grupo predefinido de multicast, en lugar de difundir este tráfico por toda la red.

El sistema de filtrado de multicast soportado por el switch emplea IGMP (protocolo de administración de grupos en Internet) escaneando para detectar la estaciones destino en cada grupo multicast al cual el tráfico multicast debe ser enviado.

#### **1.6.8. Protocolo de árbol de expansión rápida**

Conocido como (RSTP) este es un sistema basado en puente que hace a la red más resistente a las fallas de enlace y también provee protección de los loops en la red (una de las mayores causas de las tormentas de broadcast).

RSTP permite implementar caminos alternativos para el tráfico de red en el caso de una falla de camino y emplea un proceso de detección de enlace para:

- Descubrir la eficiencia de cada camino.
- Habilitar el camino más eficiente.
- Deshabilitar los caminos menos eficientes.
- Habilita uno de los caminos menos eficientes si el camino más eficiente falla.

RSTP es una versión mejorada de STP (Protocolo de árbol de expansión) y es completamente compatible con los sistemas STP. RSTP puede restaurar una conexión de red más rápido que STP. RSTP puede detectar si esta conectado a un dispositivo de legado STP que solo soporte es estándar STP IEEE 802.1D y automáticamente se ajustará a STP para ese puerto. RSTP comprende es estándar IEEE std 802.1w-2001.

#### **1.6.9. Base de datos del switch**

Es una parte integral del switch y es empleado por el switch para determinar si un paquete debe ser enviado, y a cual puerto debe ser transmitido el paquete si va a ser enviado.

#### **1.6.10. Priorización de tráfico**

Esta capacita al switch a proveer priorización de clases de servicio en la red. El tráfico puede ser priorizado en la red para asegurar que la información prioritaria sea transmitida con un atraso mínimo.

#### **1.6.11. Limitación de tasa**

Es la restricción al ancho de banda o a una sección de la red. Limitando la tasa del tráfico de red se reduce el estrés en su red y, cuando se usa con priorización de tráfico, asegura que el tráfico importante no sea retenido cuando la red está ocupada.

#### **1.6.12. RMON (Monitoreo Remoto)**

Monitoreo Remoto es una característica estándar industrial para el monitoreo de tráfico y la recolección de estadísticas de red. El software del switch continuamente recolecta las estadísticas sobre los segmentos de la LAN que están conectados al el switch. Si se tiene una estación de administración con una aplicación de administración RMON, el switch puede transferir estas estadísticas a la estación cuando se le requiera o cuando un umbral predefinido es excedido.

#### **1.6.13. Control de tormenta de broadcast**

Sistema que monitorea el nivel de tráfico de broadcast en el puerto, si este tráfico se eleva a un número predefinido de tramas por segundo (umbral), el tráfico de

broadcast en el puerto es bloqueado hasta que el nivel de tráfico de broadcast caiga por debajo de el umbral. Este sistema previene el exceso de tráfico de broadcast que puede resultar de equipos en la red que estén fallando o estén mal configurados.

#### **1.6.14. VLAN**

Siendo una LAN Virtual un grupo flexible de dispositivos que pueden ser ubicados en cualquier parte de una red y que se comunican como si estuviesen en el mismo segmento físico. Con las VLAN, se puede segmentar la red sin estar restringido a las conexiones físicas que es la limitación tradicional del diseño de redes.

#### **3.1.1.5.15. Configuración de IP automática**

El switch puede tener su información de IP automáticamente configurada usando un servidor DHCP. Alternativamente, se puede configurar manualmente la información de IP.

#### **1.5.16. Seguridad del puerto**

El switch soporta varios modos de seguridad, los cuales pueden ser ajustados a un puerto individual o a un rango de puertos. Entre esos modos están:

- **Sin seguridad**

La seguridad del puerto es deshabilitada y todo el tráfico de red es enviado por el puerto sin restricciones.

➤ **Seguro**

Todas las direcciones que han sido agregadas al puerto hasta el momento se hacen permanentes. Cualquier paquete que tenga una dirección de fuente que no este incluida en el puerto será descartado.

➤ **Entrada a la Red**

Las conexiones son solamente permitidas en un puerto solo si el cliente ha sido autenticado por un servidor RADIUS.

#### **1.6.17. Enrutado de IP.**

Método para distribuir el tráfico a través de una red IP. Es usado para unir las LAN a la capa de red (la capa 3 del modelo OSI). El switch esta optimizado para configuraciones edge de capa3 y tiene solo funcionalidad limitada como switch principal.

#### **1.6.18. Enrutado dinámico.**

Permite al switch ajustar automáticamente los cambios en la topología de red o tráfico.

#### **1.6.19. Protocolo de información de enrutamiento (RIP).**

Este es un protocolo de enrutamiento dinámico que permite al switch ajustarse automáticamente a los cambios en la topología o el tráfico de la red. Las rutas son calculadas entre las redes de manera automática.

#### **1.7. Software de administración.**

El software de administración ofrece dos interfaces diferentes: La interface Web y la interface de línea de comandos.

### 1.7.1. Operaciones de la interface Web.

A continuación veremos cada una de las operaciones y cual función desempeña por medio de la interface Web:

<b>Operación</b>	<b>Función</b>
System Getting Started	Guía al usuario por la configuración inicial del switch.
System Console Setup	Configura la velocidad de un Puerto consola.
System Control Initialize	Inicializa el switch a su configuración de fabrica.
System Control Reboot	Resetea el Switch.
System Control	Actualiza el software en el switch.
System Management	Cambia la información de configuración del Switch.
System Telnet Connect	Comienza una sesión de Telnet al switch en una ventana aparte.
System Backup Configuration Save	Guarda la configuración actual en un archivo.
System Backup Configuration Restore	Recupera la configuración de un archivo.

Bridge Address Database Add	Añade una dirección a la Base de Datos.
Bridge Address Database Find	Muestra la ubicación de una dirección MAC.
Bridge Address Database Remove	Borra una dirección de la base de Datos.
Bridge Address Database Statistics	Muestra el sumario de la base de datos de direcciones.
Bridge Address Database Summary	Muestra todas las direcciones que están guardadas vs. un Puerto o enlace agregado en particular.
Bridge Link Aggregation Modify Add Port	Añade un Puerto a un enlace agregado.
Bridge Link Aggregation Modify Admin State	Cambia el estado de un enlace agregado.
Bridge Link Aggregation Modify Remove	Borra un Puerto de un enlace agregado.
Bridge Link Aggregation Summary	Lista todos los enlaces agregados del switch.
Bridge VLAN Create	Crea una VLAN nueva.
Bridge VLAN Delete	Borra una VLAN existente.
Bridge VLAN Modify	Modifica los puertos pertenecientes a una VLAN.
Protocol IP Setup	Configura la información de IP para la unidad.
Protocol IP Interface Display/Edit	Muestra y edita las interfaces IP.

Protocol IP Route Default Gateway	Muestra y cambia el gateway (puerta de salida) por defecto.
Protocol IP Route Display/Edit	Muestra y modifica las entradas de enrutamiento.
Protocol IP Route Find	Encuentra las rutas desarrolladas a las direcciones IP.
Protocol IP Route Flush	Remueve todas las direcciones desarrolladas de la tabla de enrutamiento.
Protocol IP Trace Route	Encuentra la ruta a un dispositivo.

### 1.7.2. Comandos de la interface de línea de comandos

A continuación veremos cada una de las operaciones y cual función desempeña por medio de la interface de línea de comandos:

Comando	Que hace
bridge addressDatabase add	Añade una dirección configurada estáticamente.
bridge addressDatabase find	Encuentra una dirección en la base de datos.
bridge addressDatabase remove	Remueve una dirección de la base de datos.
bridge addressDatabase statistics	Muestra información estadística sobre las direcciones en la base de datos.

bridge addressDatabase summary	Muestra el sumario de las direcciones en la base de datos.
bridge linkAggregation detail	Muestra información detallada sobre un enlace agregado.
bridge linkAggregation modify addPort	Añade un Puerto a un enlace agregado.
bridge linkAggregation modify linkState	Habilita o deshabilita un enlace agregado.
bridge linkAggregation modify removePort.	Remueve un Puerto de un enlace agregado.
bridge linkAggregation summary	Muestra la información sumarial del enlace agregado.
bridge port defaultPriority	Ajusta la prioridad por defecto 802.1D para tramas sin etiqueta.
bridge port detail	Muestra la información detallada de un puerto.
bridge port label	Marca un Puerto con un texto definido.
bridge port summary	Muestra la información sumarial de un puerto.
bridge vlan create	Crea una VLAN.
bridge vlan delete	Borra una VLAN.
bridge vlan detail	Muestra información detallada sobre una VLAN.
bridge vlan modify addPort	Añade un Puerto a una VLAN.

bridge vlan modify name	Nombra una VLAN.
bridge vlan modify removePort	Remueve un Puerto de una VLAN.
bridge vlan summary	Muestra información sumarial sobre la VLAN.
gettingStarted	Guía al usuario durante la configuración inicial del switch
logout	Sale de la interface de línea de comandos.
physicalInterface ethernet detail	Muestra información detallada sobre un puerto Ethernet.
physicalInterface ethernet portCapabilities.	Ajusta las capacidades del puerto.
physicalInterface ethernet portState Ethernet.	Habilita o deshabilita un puerto.
physicalInterface ethernet summary Ethernet.	Muestra el sumario de un Puerto.
protocol ip basicConfig	Lleva a cabo configuración de administración básica de IP.
protocol ip initializeConfig	Resetea la información IP al la de fabricación.
protocol ip interface add	Añade una interface IP al switch.
protocol ip interface modify	Modifica una interface IP existente.
protocol ip interface remove	Remueve una interface IP del switch.

protocol ip interface summary	Muestra el sumario de la información en la interface IP.
protocol ip interface vlanModify	Cambia la VLAN empleada para administrar el switch.
protocol ip ping	Hace ping a dispositivos remotos.
protocol ip route	Añade una ruta estática.
protocol ip route default	Define la ruta por defecto en la tabla de enrutamiento.
protocol ip route find	Encuentra una ruta existente en la tabla de enrutamiento.
protocol ip route flush	Borra todas las rutas enseñadas a la tabla de enrutamiento.
protocol ip route noDefault	Borra la ruta por defecto de la tabla de enrutamiento.
protocol ip route remove	Borra una ruta existente.
protocol ip route summary	Muestra el sumario de la información de la tabla de enrutamiento.
system backupConfig restore	Recupera la configuración del switch de un archivo.
system backupConfig save	Guarda la configuración del switch en un archivo.
system control initialize	Resetea a lo configuración de fabrica.
system control reboot	Lleva a cabo un reinicio del sistema.

system control softwareUpgrade	Ejecuta un programa de actualización de software.
system inventory	Muestra la información del switch.
system management contact	Ajusta el contacto del sistema.
system management location	Ajusta la ubicación del sistema.
system management name	Ajusta el nombre del sistema.
system management password	Ajusta la contraseña del sistema.
system summary	Muestra el sumario de la información del sistema.

## ANEXO B. SWITCH AVAYA Cajun P333R

### 1. Características

#### 1.1. Físicas

##### 1.1.1. Dimensiones

➤ Alto 88mm

- Ancho 482.6 mm
- profundidad 450 mm
- peso 7.5 Kg.

### 1.1.2. Requerimientos de energía alterna – AC

- Voltaje de Entrada: 85 a 265 VAC, 50/60 Hz
- Disipación de potencia: 150 W máximo
- Corriente de entrada: 1.94 A @ 100 VAC  
0.97 A @ 200 VAC
- Corriente pico máximo en entrada: 25 A @ 100 VAC  
50 A @ 200 VAC

### 1.1.3. Requerimientos de energía directa – DC

- Voltaje de entrada: -32 a -72 VDC
- Disipación de potencia: 150 W máximo
- Corriente de entrada: 5.2 A máximo
- Corriente pico máximo de entrada: 50 A máximo

### 1.1.4 Interfaces

- 24 x 10/100BASE-T RJ-45 conectores de puertos.
- RS-232 para Terminal vía conector RJ-45 en el panel frontal.

## 1.2. Estándares a los que obedece

### 1.2.1. IEEE

- IEEE 802.3x Para control de flujo.
- IEEE 802.1Q Para Etiquetado de VLAN y compatibilidad con 802.1p.



- Control de flujo IEEE 802.3x en modo full duplex.

### **1.3.1.3. VLAN**

El switch es completamente compatible con la norma IEEE 802.1Q y puede manejar hasta 3000 VLAN Etiquetadas.

La VLAN Especial (Banda lateral Virtual) para administración provee seguridad física para las aplicaciones claves.

### **1.3.1.4. Múltiples VLAN por puerto**

El switch tiene la habilidad de de configurar múltiples VLAN por puerto (hasta 1000). Los tres modos de enlazar son:

- Enlazado a todos - El puerto es programado para soportar todo la capacidad de 3000 VLAN.
- Enlazado a los configurados - El puerto soporta todas las VLAN configuradas en el Switch o en la pila de Switch.
- Enlazado Estáticamente - El puerto soporta VLAN configuradas manualmente a el.

### **1.3.1.5. VLAN con fuga**

Provee la habilidad de enviar trafico unicast entro dos puertos de VLANs diferentes.

### **1.3.1.6. Clasificación de puertos**

El switch permite clasificar cualquier puerto como regular o importante. Ajustar un puerto a “importante” quiere decir que un mensaje de “trap” para indicar una falla del enlace, puede ser enviada aún si el puerto es deshabilitado. Esta característica es particularmente útil para la aplicación de redundancia en el software, donde es necesario estar informado sobre las fallas de un enlace en el puerto inactivo.

#### **1.3.1.7. Protocolo SNTP**

Soporta el protocolo SNTP sobre el puerto UDP 123. Se puede escoger entre este protocolo de tiempo o el protocolo de tiempo anteriormente soportado sobre el puerto UDP 37.

#### **1.3.1.8. Seguridad para Mac**

Un puerto puede ser definido como seguro para prevenir que este aprenda nuevas direcciones Mac, Si una dirección Mac o estación desconocida intenta acceder el puerto seguro, la solicitud del intruso será enviada a la estación de administración.

#### **1.3.1.9. Grupo de agregación de enlace (LAG)**

El LAG provee un incremento en el ancho de banda y redundancia para aplicaciones críticas de alto ancho de banda tales como los enlace entre pilas de switch y conexiones a los servidores. Se puede elevar el ancho de banda hasta ocho puertos 10/100 Base-Tx, dos puertos 100 Base-FX o 1000BASE-X.

Compartir las cargas asegura que si una de las conexiones de uno de los puertos falla, las otras conexiones asumirán la carga en cantidades iguales. El balanceo de la carga garantiza que la carga de tráfico a cualquier nivel será igualmente dividida entre todos los enlaces agregados.

#### **1.3.1.10. Filtrado de IP multicast**

El multicast IP permite enviar una sola copia de un paquete IP a varios destinos, y pueden ser usados para varias aplicaciones incluyendo video conferencia y video de corrido.

En las LAN, los paquetes Multicast son transmitidos en tramas Multicast MAC. Los switches de LAN tradicionales inundan con estos paquetes Multicast a todas las estaciones en la VLAN. Las funciones de Filtrado de Multicast pueden ser añadidas a los switches de capa 2 para evitar enviar paquetes Multicast a donde no son requeridos. Los switches de capa 2 que son capaces de filtrar el Multicast envían los paquetes de Multicast solo a los puertos que conectan miembros de ese grupo Multicast. Esto esta basado típicamente en espionaje GMRP o CGMP.

#### **1.3.1.11. Seguridad RADIUS**

El servicio de Usuario para Autenticación remota vía telefónica (RADIUS) es un estándar de la IETF (RFC 2138) es un protocolo de seguridad cliente/servidor. La información de seguridad y de entrada es guardada en una ubicación central conocida como el servidor RADIUS. El cliente RADIUS, en este caso el switch, se comunica con el servidor RADIUS para autenticar a los usuarios.

Todas las transacciones entre el cliente RADIUS y el servidor son autenticadas por medio del uso de un “secreto compartido” el cual no es enviado por la red. El secreto compartido es una contraseña de autenticación configurada en ambos, tanto el cliente como el servidor RADIUS. El secreto compartido es guardado como texto simple en el archivo del cliente en el servidor RADIUS, y en la memoria no volátil del switch. Además, las contraseñas de usuario son enviadas entre el cliente y el servidor son encriptadas para incrementar la seguridad.

#### **1.3.1.12. Redundancia de puertos**

Esta puede ser implementada entre dos puertos cualesquiera en la misma pila en el nivel de enlace. Se puede asignar redundancia entre dos enlaces agregados cualesquiera en la pila o entre un LAG y un puerto. Un puerto o LAG es definido como el puerto primario y el otro como el puerto secundario. En el caso de que el enlace del puerto primario falle, el puerto secundario se encarga.

#### **1.3.1.13. Redundancia entre Módulos.**

Esta incluye la funcionalidad de redundancia de todos los puertos. La redundancia ínter modular mantiene la integridad del puerto aún cuando el enlace del puerto primario falla como resultado de una falla del módulo. Si el módulo en el cual el puerto primario que está en una Redundancia de puerto Ínter modular es apagado o removido del dispositivo, el puerto secundario en la Redundancia de puerto Ínter modular se hace cargo. Solo un módulo por pila debe ser ajustado para la Redundancia de Puerto Ínter modular.

#### **1.3.1.14. Redundancia de Pila**

En el caso de que el switch o el enlace octoplanar fallara, la integridad de la pila es mantenida. El enlace roto es superado y la transmisión de datos continúa sin interrupción. La dirección IP de administración para la pila es también preservada para mantener el monitoreo y la administración ininterrumpidas.

#### **1.3.1.15. Intercambio en “Caliente”**

Es posible remover o reemplazar cualquier unidad dentro de la pila sin interrumpir la operación o teniendo que hacer una reconfiguración del nivel de la pila. Se puede por lo tanto adaptar el switch a los requerimientos mientras se esta operando la red y con un tiempo de apagado del switch de segundos a nada.

#### **1.3.1.16. Fuente de Respaldo**

El switch posee un conector para una fuente de potencia de respaldo. Si la fuente de poder interna falla, la fuente de poder alterna automáticamente suministra potencia al switch para evitar la interrupción.

#### **1.3.1.17. Ventiladores**

Los ventiladores de switch tienen sensores integrados que proveen advertencias avanzadas de fallas en los ventiladores por medio del administrador.

#### **1.3.1.18. Redundancia del Agente Administrador de la Red**

Cada modulo Avaya posee un agente SNMP, cualquier módulo en una pila puede servir como el Agente administrador de Red mientras otros actúan como agentes redundantes en standby “caliente”. Si el Agente Administrador que esta activo falla, entonces uno de respaldo es activado instantáneamente.

#### **1.3.1.19. Descarga de Software**

El switch incluye un procedimiento de descarga de software seguro en el cual un código de respaldo esta siempre presente.

### **1.3.2. Capa 3**

#### **1.3.2.1 Modos de operación**

Se cuentan con tres modos de operación (en cada modo, capa 2 siempre esta activa):

- Modo solamente Capa2.
- Modo ruta EZ2 y Capa2.
- Modo enrutador y capa2.

### **1.3.2.2 Envío**

El switch envía paquetes IP entre redes IP. Cuando este recibe un paquete IP por una de sus interfaz, este envía el paquete a través de una de sus interfaces. El switch soporta multiredes, habilitándolo para enviar paquetes entre subredes IP en la misma VLAN así como entre diferentes VLAN. El envío es llevado a cabo usando estándares en los modos enrutador y ruta EZ2.

### **1.3.2.3. Modo Ruta EZ2**

La tecnología del modo emplea la potencia y la simplicidad del hardware para llevar a cabo funciones de switch de capa3 sin la administración superior asociada con los enrutadores regulares.

En el modo ruta EZ2, el desempeño de switch de capa3 esta basado en aprendizaje automático. Esto elimina la necesidad de configurar el switch como una entidad de enrutamiento y elimina las complicaciones asociadas con la configuración de enrutadores regulares.

En este modo, el switch no lleva a cabo ninguna operación de enrutamiento, tales como correr protocolos de enrutamiento o hacer cálculos de rutas intensivas para recursos. Esto hace al switch transparente a otras entidades de enrutamiento en la red.

Este modo permite incrementar el ancho de banda de nivel 3 añadiendo switches adicionales a la pila. Un switch P333R en modo ruta EZ2 puede ser usado para incrementar el desempeño de uno o más enrutadores fuera de la pila y de otro switch en la misma pila operando en modo Enrutador. Múltiples switches en este modo pueden apilarse juntos para incrementar la capacidad de envío de capa 3 de la pila.

En este modo el switch aprende la red dinámicamente y por lo tanto elimina la necesidad de configuración. Sin embargo, has algunos casos especiales donde una mínima configuración es necesaria.

#### **1.3.2.4. Redundancia**

Los protocolos de enrutamiento proveen algún nivel de redundancia por lo general. Sin embargo, las estaciones IP que son configuradas manualmente con una puerta de salida por defecto con una dirección IP no se recuperan de forma natural cuando su puerta de salida falla. Estas estaciones no intentan automáticamente usar otros enrutadores o los switches de capa-3 conectados a la misma subred. Este switch soporta dos protocolos de redundancia de enrutamiento, VRRP y SRRP para resolver este problema.

#### **1.3.2.5. Protocolo de redundancia de enrutador virtual (VRRP)**

VRRP es un protocolo de la IETF diseñado para soportar la redundancia de los enrutadores en la LAN, así como balancear la carga de tráfico. VRRP es transparente a las estaciones host, haciéndolo una elección ideal cuando la redundancia, el balanceo de carga y facilidad de configuración son requeridas.

El concepto relacionado con VRRP es que un enrutador puede dar respaldo a otros, además de llevar acabo sus funciones primarias de enrutamiento. Esta redundancia es alcanzada introduciendo el concepto de enrutador virtual. Un enrutador virtual es una entidad enrutadora asociada con múltiples enrutadores físicos. Las funciones de enrutamiento del enrutador virtual son llevadas a cabo por uno de los enrutadores físicos con el cuál esta asociado. Este enrutador es conocido como el enrutador maestro.

Para cada enrutador virtual, VRRP selecciona un enrutador maestro. Si el enrutador maestro falla, otro enrutador es seleccionado como el maestro.

En VRRP, dos o más enrutadores físicos pueden ser asociados con un enrutador virtual. Ellos no están concientes de que este enrutador es un enrutador virtual y ellos no son afectados cuando un nuevo enrutador toma el rol de enrutador maestro. Esto hace que el VRRP sea completamente ínter operable con cualquier estación host.

El VRRP puede ser activado en una interfaz empleando un solo comando mientras se hagan los ajustes necesarios de los muchos parámetros VRRP.

#### **1.3.2.6. Protocolo de redundancia de enrutador simple (SRRP)**

Este protocolo provee respaldo automático al desempeño del switch de capa 3 para las estaciones IP. Las unidades del switch pueden ser configuradas para respaldarse las unas a las otras de modo que si una falla la otra tomará sus funciones de envío. El switch de respaldo no se encuentra inactivo. Tan pronto como ambas unidades sean funcionales, el tráfico es compartido entre ellas. Los Switch pueden estar en la misma pila o en diferentes. Los switches pueden respaldar otro switch o cualquier otro enrutador.

Un Switch configurado para respaldar otro switch monitorea el estado del otro mediante sondeos a intervalos configurados, y automáticamente detecta cuando el otro falla y cuando este vuelve a estar funcional nuevamente. Cuando se detecta una falla, el switch de respaldo envía un mensaje ARP gratuito que hace que todas las estaciones envíen su tráfico IP a la dirección MAC del switch de respaldo en vez de la dirección MAC de la unidad que esta fallando. Mientras esta este funcionando como un respaldo debido a la falla en el switch principal, el switch de respaldo responde las peticiones de ARP en vez de la unidad principal, dando su propia dirección MAC.

#### **1.3.2.7. Balanceo de carga OSPF**

El Switch soporta el balanceo de carga en capa 3 usando OSPF Multicamino de Costo Equivalente (ECM) y multicamino de rutas estáticas. OSPF y el multicamino estático balancea la carga de envíos de la capa 3 dividiendo el tráfico en varios caminos posibles de costo equivalente, así liberando ancho de banda adicional para tráfico.

#### **1.3.2.8. Política de calidad de servicio (QoS)**

El switch soporta QoS usando múltiples niveles de prioridad y el etiquetado de prioridad IEEE 802.1p para asegurar que los datos y la voz reciban los niveles necesarios de servicio.

El switch puede hacer cumplir la política en los paquetes enrutados (en cada paquete), de acuerdo a cuatro criterios:

- La etiqueta de prioridad IEEE 802.1p en el paquete entrante.
- El Byte diferenciador de servicio (campo TOS) en el encabezado IP del paquete entrante.
- El ajuste de la dirección IP fuente o destino del paquete para ser configurada como una política de prioridad.
- Cual sea el puerto TCP/UDP destino o fuente del paquete, el número siempre estará en un rango predefinido.

Como el Switch es multicapa, está en capacidad de imponer políticas de red centralizadas empleando la aplicación de administración de política central de reglas RealNet de Avaya.

#### **1.3.2.9. Política de control de acceso**

El switch soporta la política de control de acceso. Empleando listas de políticas que contienen tanto reglas de control de acceso como reglas QoS. Las listas de política están ordenadas por indexado de reglas. Las reglas de control de acceso definen como el switch debe manejar los paquetes enrutados.

Hay tres posibles formas de manejar tales paquetes:

- Enviar el paquete (permitir operación).

- Desechar el paquete (Denegar operación).
- Desechar el paquete y notificar a la estación de administración (denegar y notificar).

El switch puede imponer la política de control de acceso en cada paquete enrutado, de acuerdo a los siguientes criterios:

- Concordancia de la dirección IP fuente o destino del paquete con la política de control de acceso configurada.
- Determinar si el número del puerto TCP/UDP fuente o destino del paquete se encuentra dentro del rango predefinido.
- Uso del bit de ACK en el encabezado del TCP.

Las reglas de control de acceso son configuradas empleando la Interface de Línea de Comandos y la aplicación de administración de política central de reglas RealNet.

#### **1.3.2.10. Relevo DHP/BOOTP**

El switch soporta la función del Agente de relevo DHCP/BOOTP. Esta es una aplicación que acepta las peticiones DHCP/BOOTP que son transmitidas en broadcast en una VLAN y las envía a un servidor DHCP/BOOTP que se conecta a otra VLAN o a un servidor que puede ser ubicado a lo largo de uno o mas enrutadores que de otra forma no obtendrían la solicitud por broadcast. El agente de relevo igualmente maneja las respuestas DHCP/BOOTP, transmitiéndolas al cliente directamente o como broadcast, de acuerdo a la bandera en el mensaje de respuesta.

Cuando hay más de una interface IP en una VLAN, el switch elige una de las direcciones IP en esta VLAN cuando atiende la solicitud de relevo de

DHCP/BOOTP. El servidor DHCP/BOOTP entonces usa esta dirección para decidir a cual subred la dirección debería ser asignada.

Cuando el servidor DHCP/BOOTP es configurado par asignar direcciones solo de una subred sencilla entre las diferentes subredes definidas en la VLAN, puede ser necesario configurar el switch con la dirección de relevo en la subred de modo que el servidor DHCP/BOOTP pueda aceptar la solicitud.

El relevo DHCP/BOOTP en el switch es configurable por VLAN y permite especificar dos servidores DHCP/BOOTP. En este caso, se duplica cada solicitud y se envía a ambos servidores. Esto provee redundancia y previene que la falla de un solo servidor bloquee al los hosts de cargar.

El relevo DHCP/BOOTP en el switch puede ser habilitado o deshabilitado

#### **1.3.2.11. Protocolo RIP**

El switch P333R soporta el protocolo de enrutamiento RIP (versiones 1 y 2). El protocolo RIP versión 1 impone algunas limitaciones en el diseño de la red en consideración al diseño de subredes. Cuando se opera RIPv1, no se debe configurar mascarar de subred con longitud variable (VLMS). Cada red IP debe tener una sola mascara, implicando que todas las subredes en una red IP dada son del mismo tamaño. También, cuando se opera RIPv1 no deben configurarse superredes, redes con una mascara más pequeña que la mascara natural de la clase de la dirección.

RIPv2 es una nueva versión del protocolo RIP, que aún no es usada ampliamente pero tiene algunas ventajas sobre RIPv1. RIPv2 resuelve algunos de los problemas asociados con v1. El cambio mas importante es la adición de un campo de mascara de subred que le permite a este protocolo soportar subredes de longitud

variable. También incluye un mecanismo de autenticación similar al empleado en OSPF.

La configuración de la versión RIP 1 o 2, es por interface IP (por defecto es versión1). LA configuración debe ser homogénea en todos los enrutadores en cada subred, no puede haber enrutadores con ambas versiones la RIPv1 y RIPv2 en la misma subred. Sin embargo, se pueden configurar diferentes interfaces IP del switch con diferentes versiones de RIP (mientras todos los enrutadores en la subred sean configurados a la misma versión):

RIPv1 y RIPv2 son considerados el mismo protocolo con consideración a la redistribución a/de OSPF y preferencias de rutas estáticas.

#### **1.3.2.12. Protocolo OSPF**

El switch soporta el protocolo de enrutamiento OSPF. Además puede ser configurado como un Enrutador de frontera de sistema autónomo (ASBR) por medio de la configuración de la redistribución de rutas. El switch puede ser instalado en el área backbone del OSPF (área 0.0.0.0) o en cualquier área OSPF que sea parte de una red de áreas múltiples. Sin embargo, este switch no puede ser configurado para ser un enrutador de frontera de área por si mismo.

Soporta el multicamino de igual costo (ECMP) que permite balanceo de cargas dividiendo el tráfico entre varios caminos equivalentes.

Mientras OSPF puede ser activado con valores por defecto para cada interfaz empleando un solo comando, muchos de los parámetros OSPF son configurables.

#### **1.3.2.13. Rutas Estáticas**

Estas pueden ser configuradas en el switch. Ellas nunca quedan fuera de tiempo, o se pierden al reiniciar el sistema y solo pueden ser removidas por configuración

manual. Al borrar por configuración la interfaz IP se borran las rutas estáticas que empleen esa interfaz.

Una ruta estática se vuelve inactiva si la interfaz sobre la cual esta está definida es deshabilitada. Cuando la interfaz es habilitada, la ruta estática vuelve a estar activa.

Las rutas estáticas solo pueden ser configuradas para destinos remotos, como por ejemplo un destino que solo es alcanzable por medio de otro enrutador en el siguiente salto. El enrutador del siguiente salto debe pertenecer a una de las redes conectadas directamente para las cuales el switch tiene una interfaz IP. Las rutas estáticas locales, aquellas que no necesitan de un salto, no se permiten. Se pueden configurar dos tipos de rutas estáticas, Rutas estáticas de alta preferencia las cuales son preferidas a las rutas aprendidas de cualquier protocolo de enrutamiento y las rutas estáticas de baja preferencia las cuales son usadas temporalmente hasta que la ruta sea aprendida por un protocolo de enrutamiento. Por defecto, una ruta estática tiene preferencia baja.

Las rutas estáticas pueden ser anunciadas por los protocolos de enrutamiento (como RIP y OSPF) bajo redistribución de Ruta.

Las rutas estáticas también soportan el balanceo de cargas de igual forma que OSPF. Una ruta estática puede ser configurada con múltiples próximos saltos de forma que el tráfico sea repartido entre esos próximos saltos.

#### **1.3.2.14. Redistribución de Rutas**

Es la interacción de múltiples protocolos de enrutamiento. OSPF y RIP pueden ser operados concurrentemente en el switch. En este caso, el switch puede ser configurado para redistribuir las rutas aprendidas de un protocolo en el dominio de otro protocolo de enrutamiento. De forma similar, las rutas estáticas pueden ser redistribuidas a RIP y a OSPF. La redistribución de rutas no debe ser configurada descuidadamente, ya que involucra cambios métricos y puede causar

ciclos sin fin en la presencia de otras rutas con esquemas incomparables para la redistribución de rutas y preferencias de rutas.

El esquema del Switch P333R para la traducción métrica en la redistribución de rutas se ve a continuación:

- Estático para la métrica RIP configurable (por defecto 1).
- Métrica interna OSPF N a métrica 1 de RIP.
- Métrica N tipo 1 externa OSPF a métrica 1.
- Métrica N tipo 2 externa OSPF a métrica 1.
- De estático a OSPF externo tipo 2, métrica configurable (por defecto 1).
- Métrica N tipo RIP a OSPF externa tipo 2, métrica N.
- Directo al OSPF externo tipo 2, métrica 1.

Por defecto, el switch no redistribuye las rutas entre OSPF y RIP.

La redistribución de un protocolo al otro puede ser configurada. Las rutas estáticas están por defecto, redistribuidas al RIP y al OSPF. El switch permite al usuario deshabilitar globalmente la redistribución de las rutas estáticas a RIP y deshabilitar globalmente la redistribución de rutas estáticas a OSPF. Además el switch permite al usuario configurarlo en una base por ruta estática, ya sea que el enrutador esta para ser redistribuido a RIP y OSPF y que métrica (Rango de 1–15). El estado por defecto esta en habilitar la ruta a ser redistribuida a una métrica de 1. Cuando las rutas estáticas están redistribuidas a OSPF, ellas están redistribuidas como externas del tipo 2.

#### **1.3.2.15. Preferencias de ruta**

La tabla de enrutamiento puede contener rutas de diferentes fuentes. Las rutas a un cierto destino pueden ser aprendidas independientemente del RIP y el OSPF, y al mismo tiempo, una ruta estática puede también ser configurada hacia el mismo destino. Mientras las métricas son empleadas para escoger entre las rutas del

mismo protocolo, las preferencias del protocolo son empleadas para escoger entre rutas de diferentes protocolos.

Las preferencias solo se aplican a rutas para la misma dirección IP destino y mascara. Ellas no sobrepasan la elección de coincidencia mas larga, de esta forma una ruta por defecto estática de alta preferencia no será preferida sobre una ruta RIP a la subred del destino.

Las preferencias del protocolo están listadas a continuación desde la más a la menos preferida:

1. Local (Red conectada directamente).
2. Estática de alta preferencia (Rutas configuradas manualmente).
3. Rutas internas OSPF.
4. RIP.
5. Rutas externas OSPF.
6. Estática de baja preferencia (Rutas configuradas manualmente).

#### **1.3.2.16. Redifusión de Netbios**

El switch puede ser configurado para relevar los paquetes de broadcast UDP de la netbios. Esta característica es empleada para aplicaciones tales como WINS que emplean el broadcast pero que pueden necesitar comunicarse con las estaciones en las otras subredes o VLAN.

La configuración es llevada a cabo en una base por interfaz. Cuando un paquete de broadcast de netbios llega de una interfaz en la cual la redifusión de broadcast esta habilitada, el paquete es distribuido a todas las otras interfaces configuradas para retransmitir broadcast de netbios.

Si el paquete de netbios es un broadcast dirigido a red, el paquete es relevado a todas las otras interfaces en la lista y la dirección IP de destino de el paquete es reemplazada por la dirección de broadcast de la interfaz apropiada.

Si el paquete de broadcast de netbios es un broadcast limitado, este es relevado a todas las VLAN en las cuales hay interfaces habilitadas de netbios. En ese caso, la dirección IP de destino sigue siendo la dirección de broadcast limitada.

#### **1.3.2.17. Multiredes (Múltiples Subredes por VLAN)**

En el modo Enrutador, la mayoría de las aplicaciones tales como RIP y OSPF, operan por interfaz IP. Otras aplicaciones como VRRP y relevo DHCP/BOOTP operan por VLAN. La configuración de estas aplicaciones es hecha en el modo Interfase. Cuando hay solo una interfaz (subred) por VLAN entonces el comportamiento del sistema es intuitivo ya que una subred y una VLAN son lo mismo.

Si la configuración incluye múltiples interfaces (subredes) por VLAN, la cuestión comienza a complicarse.

Si por ejemplo, hay dos interfaces sobre la misma VLAN y se configura el servidor DHCP en una interfaz, este será usado también para la segunda interfaz sobre la misma VLAN. Este comportamiento puede ser lo menos esperados y en algunos casos erróneo.

Con el fin de prevenir la mala configuración y resultados inesperados, el switch previene la configuración de VLAN orientadas a comandos en una interfaz a menos que el usuario explícitamente requiera usar los nuevos “comandos para habilitar VLAN” CLI.

La configuración de los comandos para habilitar VLAN en una interfaz sobrepasa esta configuración en las otras interfaces que pertenezcan a la misma VLAN.

Esto asegura que los comandos orientados a VLAN puedan ser configurados desde solamente una interfaz.

En el caso de que solo haya una interfaz sobre una VLAN, entonces los comandos orientados a VLAN para esta VLAN pueden ser configurados por medio de la interfaz sin necesidad de hacer uso de los comandos para habilitar VLAN.

### **1.3.2.18. Archivo de Configuración del Enrutador**

Este archivo permite al usuario leer los parámetros de configuración de enrutamiento del switch y guardarlos en un archivo en la estación. Los comandos de configuración de enrutamiento en el archivo están en formato CLI. El usuario puede editar el archivo (de ser necesario) y reconfigurar el switch descargando el archivo de configuración. Aunque el archivo puede ser editado, se recomienda que los cambios que se le hagan al archivo sean muy pocos.

El método de configuración recomendado es empleando el Dispositivo de Administración Cajón View P330 y/o el CLI. Los cambios en el archivo de configuración deben limitarse a aquellos requeridos para ajustar un archivo de configuración que se va pasar de un enrutador a otro.

## **1.4. Comandos relacionados con VLAN**

### **1.4.1. Interfase de línea de comandos – Capa 2**

#### **1.4.1.1. Comandos para nivel de usuario**

##### **1.4.1.1.1. Mostrar Puertos en Modo adjunto a VLAN**

Se emplea este comando para mostrar la información de los puertos en Modo adjunto a la VLAN.

Sintaxis:     **show port vlan-binding-mode**

##### **1.4.1.1.2. Mostrar VLAN**

Este comando se emplea para mostrar las VLANs que se encuentren configuradas en la pila o el switch.

Sintaxis: `show vlan`

#### 1.4.1.1.3. Mostrar VLAN con filtración

Este comando se emplea para mostrar es estado de la VLAN con filtración.

Sintaxis: `show leaky-vlan`

#### 1.4.1.2. Comandos privilegiados

##### 1.4.1.2.1. Limpiar VLAN

Este comando se emplea para borrar una VLAN existente y para regresar los puertos de esta VLAN a la VLAN #1 por defecto. Al borrar una VLAN, todos los puertos asignados a esa VLAN serán asignados a la VLAN por defecto #1.

Sintaxis: `clear vlan <numero de id-vlan> [name <nombre_vlan>]`

El número de VLAN va de 1 a 3071

##### 1.4.1.2.2. Ajustar VLAN de un puerto

Este comando se emplea para definir o ajustar el número de identificación de la VLAN asociada a un puerto específico. El número de identificación de la VLAN debe estar entre 1 y 3071.

Sintaxis:

`set port vlan <numero_VLAN> <numero_módulo>/<numero_puerto(s)>`

#### 1.4.1.2.3. Ajustar puertos en modo adjunto a VLAN

Este comando se emplea para definir el método de adjuntamiento que será empleado por los puertos.

Sintaxis: `set port vlan-binding-mode [lista de puertos] [valor]`

#### 1.4.1.2.4. Ajustar puertos de VLAN estática

Este comando permite estáticamente asignar VLANs a los puertos del switch.

Sintaxis:

```
set port static-vlan [modulo/puerto rango] [numero_vlan]
[modulo/puerto rango] Rango de puertos
```

#### 1.4.1.2.5. Ajustar VLAN de banda interna

Este comando permite ajustar un valor para la VLAN de administración.

Sintaxis: `set inband vlan <valor>`

`<valor>`: un número de VLAN entre 1 y 3071.

#### 1.4.1.2.6. Ajustar VLAN

Este comando permite crear VLANs.

Sintaxis: `set vlan <numero_id_VLAN> [name <nombre_VLAN>]`

#### 1.4.1.2.7. Ajustar VLAN con filtración

Este comando permite definir el modo de VLAN con filtración del switch. En este modo, las pruebas de VLAN son hechas solamente en tramas desconocidas de broadcast y multicast y no en tramas unicast.

Sintaxis: `set leaky-vlan <enable|disable>`

### 1.4.2. Interfase de Línea de Comandos – Capa 3

#### 1.4.2.1. Comandos para VLAN

##### 1.4.2.1.1 Modo usuario

###### 1.4.2.1.1.1. Mostrar VLAN

Comando que permite mostrar las interfaces de capa 2 del enrutador.

Sintaxis: `show vlan [details]`

##### 1.4.2.1.2. Modo configuración

###### 1.4.2.1.2.1. Ajustar VLAN

Comando empleado para crear una interfaz de capa2 en el enrutador.

Sintaxis: `set vlan <numero_ID_VLAN> name <nombre_VLAN>`

#### **1.4.2.1.2.2. Borrar VLAN**

Este comando se emplea para borrar una interfaz de capa 2 del enrutador

Sintaxis: `clear vlan [<Numero_ID-VLAN>] | [name <nombre _VLAN>]`

## **ANEXO C. SWITCH D-LINK DES-3326 SR**

### **1. Características**

#### **1.1. Puertos**

24 puertos 10/100 BASE-T con soporte para hasta 2 puertos adicionales Gigabit Ethernet.

## **1.2. Tamaño de la tabla de direcciones MAC**

8000

## **1.3. Capacidad**

8.8 Gbps

### **3.3.1.4. Método de Transmisión**

Guardar- y- Enviar

## **1.5. VLAN**

Soporta hasta 64 grupos de VLAN estáticos y/o hasta 255 grupos de VLAN dinámicos

### **3.3.1.6. Mecanismo de apilamiento GBIC**

Soporta 8 unidades por pila, Configuración Máxima: (192) puertos 10/100BASE-T, (8) puertos de apilamiento t (8) Ranuras GBIC abiertas.

## **1.7. Ancho de Banda de Apilamiento**

Hasta 1.2Gbps.

## **1.8. Agregación de Enlace**

8 Enlaces por grupo y hasta 8 grupos por pila.

## **1.9. Listas de control de Acceso**

Basadas en Puerto, Campo TOS, campo DiffServ, campo 802.1p, Direcciones MAC, Direcciones IP y/o numero de puerto TCP/UDP.

## **1.10. Control de Ancho de Banda**

El Ancho de banda puede ser limitado en incrementos de 1.0 Mbps.

## **1.11. Protocolos de Enrutamiento**

RIP v1 /v2, OSPF y DVMRP.

## **1.12. Tabla de Direcciones IP**

2000 Entradas IP.

## **1.13. Opciones de interfaces**

### **1.13.1. RJ-45**

10BASE-T, 100BSDL-TX y 1000BASE-T

### **1.13.2. SC**

- 100BASE-FX cable de fibra multimodo; 62.5/125 o 50/125 micrones.
- 1000BASE-SX cable de fibra multimodo; 62.5/125 o 50/125 micrones.
- 1000BASE-LX cable de fibra multimodo; 62.5/125 o 50/125 micrones o cable de fibra de modo simple: 9/125 micrones.

### **1.13.3. GBIC**

Soporte para el Estándar GBIC de 3.3 Voltios

## **1.14. ADMINISTRACIÓN DE RED**

### **1.14.1 Dentro y fuera de la banda**

Telnet, CLI/Consola, RMON, HTTP basado en Web, compatible con SNMPv1 Y Mirroring de Puerto.

### **1.14.2. PROTOCOLO DE RED Y ESTANDARES**

#### **1.14.2.1. IEEE**

82.3 Ethernet, 802.3u Fast Ethernet, 802.1d Árbol de Spanning, 802.1p Etiquetas de prioridad, 802.1q VLAN, 802.1ac Etiquetado de VLAN, 802.1ad Control de Agregación de enlace, 802.3x Control de Flujo y 802.1x Control de Acceso a la Red Basado en Puerto.

#### **1.14.2.2. IEFT**

RFC 1157 SNMP, RFC 1112/2236 IGMPv ½

#### **3.3.1.15. ELECTRICAS**

Alimentación: 100–240 VAC, 50/60/ Hz

#### **1.16. FISICAS Y AMBIENTALES**

##### **1.16.1. Dimensiones**

- Altura: 441 mm.
- Ancho: 210 mm.
- Profundo: 43 mm.
- Peso: 6 Kg.
- Rack de montaje de 19 pulgadas de ancho y 1.0 U de altura.

##### **1.16.2. Temperatura**

- De operación: 0° – 40° C.
- De almacenamiento: –40 a 70 °C
- Humedad en operación: 5% a 95%, RH no condensado.

#### **1.17. CARACTERÍSTICAS ADMINISTRABLES**

##### **1.17.1. Puertos**

- 24 puertos NWay de alto desempeño, todos operando a 10/100 Mbps para conectarse a estaciones finales, servidores y hubs (23 puertos Ethernet UTP MDI-X 10/100 y uno MDI-II/MDI-X. El puerto MDI-X puede ser intercambiado entre dos modos en el panel frontal).
- Todos los puertos puede auto-negociar (NWay) entre 10 Mbps/100 Mbps, half duplex o full duplex y control de flujo para puertos half-duplex.
- Una interface de modulo "slide-in" en el panel frontal para un módulo Gigabit Ethernet de dos puertos 100BASE-SX, 1000BASE-LX, 1000BASE-T o GBIC.
- Puerto de diagnóstico DCE RS-232 (puerto consola) para ajustar y administrar el switch por medio de una conexión a un Terminal de consola o el PC empleando un programa de emulación.

## **1.17.2. Características por capa**

### **1.17.2.1. Capa 2**

- El switch tiene una capacidad de 8.8Gbps.
- Su esquema de funcionamiento es de "guardado y enviado".
- Full y half duplex para conexiones de 10 Mbps y 100 Mbps. El modulo Gigabit Ethernet del puerto frontal opera solamente a full duplex. El Full duplex permite al puerto del switch transmitir y recibir datos, y solo trabaja con conexiones a switches y estaciones finales con capacidad de full duplex.
- Soporta el estándar IEEE 802.3x de control de flujo para puertos con modo full duplex.
- Soporta el control de flujo "Back-Pressure" para puertos con modo half duplex.
- Detección de Auto-polaridad y corrección de polaridad incorrecta en el par trenzado de transmisión y recepción en cada puerto.

- Conforme al estándar IEEE 802.3z para todos los puertos Gigabit (módulo opcional).
- Conforme al estándar IEEE 802.3x para el soporte de control de flujo para todos los puertos Gigabit (módulo opcional).
- Conforme al estándar IEEE 802.3ab para los puertos Gigabit 1000BASE-T (cobre), (módulo opcional).
- Tasa de envío de datos de 14.880 pps por puerto al 100% de velocidad del cable para una velocidad de 10 Mbps.
- Tasa de envío de datos de 140,880 pps por puerto al 100% de velocidad del cable para una velocidad de 100 Mbps.
- Tasa de filtrado de datos elimina todos los paquetes erróneos, dañados, etc. A 14,880 pps por puerto al 100% de la velocidad del cable para una velocidad de 10Mbps.
- Tabla de entrada de direcciones MAC activa de 8000 por cada switch con aprendizaje y envejecimiento automático (10 a 9999 segundos).
- Buffer de 16MB por switch.
- Filtrado de tormenta de Multicast y Broadcast.
- Soporta puerto espejo.
- Soporta Trunking de puerto - hasta seis grupos de trunk (cada uno contiene hasta 8 puertos) pueden ser ajustados.
- Soporta el Árbol de expansión para el estándar 802.1D
- Soporta el espionaje IGMP.
- Soporta el Multicast de capa 2- GMRP (Protocolo de Registro Multicast GARP)

### 1.17.2.2. Capa 3

- Envío de IP por Cable.
- Desempeño del switch para IP en capa 3 basado en Hardware.
- Tasa de envío de paquetes de 6.6 Mpps.
- Tabla de entrada con 2000 direcciones IP activas.
- Soporta RIP (Protocolo de Información de Enrutamiento), versión I y II.
- Soporta OSPF (Primer camino más corto abierto).
- Soporta MD5 y autenticación por paquete de password OSPF.

- Soporta IP versión 4.
- IGMP versiones 1 y 2 (RFC 1112 y RFC 2236).
- Soporta el Modo Denso de PIM.
- Soporta DVMRP.
- Soporta multi-redes IP.
- Soporta defragmentación de paquetes IP.
- Soporta el pathfinder (buscador de caminos) MTU.
- Soporta la trama de apoyo 802.1D.

## 2. COMANDOS DE LA INTERFACE DE LÍNEA DE COMANDOS

Tener en cuenta que:

- Los paréntesis angulares “< >”, encierran un valor o variable que debe ser especificado por el usuario.
- Los paréntesis cuadrados “[ ]”, encierran un valor o conjunto de argumentos requeridos. Pueden especificarse uno o más valores o argumentos.
- El slash “/”, separa dos o mas elementos mutuamente excluyentes en una lista – uno de los cuales debe ser ingresado.
- Las llaves “{ }”, encierran un valor o un conjunto de argumentos opcionales.

### 2.1. Comandos básicos del switch

- `create account [admin/user] <nombre_usuario>`

Propósito: Se emplea para crear cuentas de usuario

- `config account < nombre_usuario >`

Propósito: Permite configurar cuentas de usuario.

- `Delete account <nombre_usuario>`

Propósito: Borra una cuenta de usuario existente.

- `show account`

Propósito: Muestra las cuentas de usuario

- `show session`

Propósito: Muestra la lista de los usuarios que se encuentran en sesión

- `show switch`

Propósito: Muestra la información del switch

- `show serial_port`

Propósito: Muestra la configuración del Puerto serial.

- `config serial_port baud_rate [9600/19200/38400/115200]  
auto_logout [never/2_minutes/5_minutes/10_minutes/15_minutes]`

Propósito: Configurar el puerto serial

- `enable clipaging`

Propósito: Empleado para detener los pantallazos de la consola cuando el comando show muestra mas de una página.

- `disable clipaging`

Propósito: deshabilita la acción del comando `enable clipaging`

- `enable telnet <numero_puerto_tcp >`

Propósito: Permite la comunicación con el modulo de administración del switch empleando protocolo Telnet.

- **disable telnet**

Propósito: Deshabilita el protocolo Telnet en el switch.

- **enable web < numero\_puerto\_tcp >**

Propósito: Habilita la administración basada en http para el switch

- **disable web**

Propósito: Deshabilita la administración basada en http para el switch

- **save**

Propósito: Salva los cambios en la configuración del switch a la RAM no volátil.

- **Reboot**

Propósito: Reinicia el switch.

- **reset {config/system}**

Propósito: Se emplea para devolver el switch a su configuración de fábrica.

- **Login**

Propósito: Empleado para que un usuario ingrese iniciando sesión en la consola del switch.

- **Logout**

Propósito: Empleado para que el usuario termine su sesión en la consola del switch

## 2.2. COMANDOS DE LOS PUERTOS DEL SWITCH

- `config ports <Lista_puertos/all (todos) > speed [auto/10_half/10_full/100_half/100_full/1000_half/1000_full] learning [enabled/disabled] state [enabled/disabled]`

Propósito: configure los ajustes del Puerto Ethernet del switch

- `config port_security < Lista_puertos >/all admin_state [enabled/disabled] max_learning_addr <1-10> lock_address_mode [DeleteOnTimeout/DeleteOnReset]`

Propósito: permite configurar los ajustes de seguridad de los puertos.

- `show ports <portlist/all>`

Propósito: Muestra la configuración actual de un rango de puertos.

- `Show port_security`

Propósito: muestra la configuración de seguridad de los puertos.

## 2.3. COMANDOS DE VLAN

- `create vlan <nombre_vlan> tag <vlan_id> advertisement`

Propósito: Permite crear una VLAN en el switch

- `delete vlan <vlan_name>`

Propósito: Borra una VLAN previamente configurada en el switch

- `config vlan <nombre_vlan> add [tagged/untagged/forbidden]  
delete <lista_puertos> advertisement [enabled/disabled]`

Propósito: Permite adicionar puertos adicionales a una VLAN previamente configurada

- `config gvrp <portlist> all state [enabled/disabled]  
ingress_checking [enabled/disabled]`

Propósito: Permite configurar GRPV en el switch

- `enable gvrp`

Propósito: Habilita el GRPV en el switch

- `disable gvrp`

Propósito: Deshabilita el GRPV en el switch

- `show vlan <nombre_vlan>`

Propósito: Muestra la configuración de VLAN en el switch

- `show gvrp <lista_puertos>`

Propósito: Muestra el estado del GRPV para un Puerto listado en el switch

## 2.4. COMANDOS DE LA INTERFASE IP

- `create ipif <ipif_name> <network_address> vlan <vlan_name>  
state [enabled/disabled]`

Propósito: Se emplea para crear una interfaz IP en el switch

- `delete ipif <nombre_interfaz_ip> all`

Propósito: Borra una interfaz ip previamente configurada en el switch

- `config ipif System vlan <nombre_vlan> ipaddress  
<dirección_red> state [enabled/disabled] bootp dhcp`

Propósito: permite configurar la interfaz IP del sistema

- `enable ipif <nombre_interfaz_ip> all`

Propósito: Habilita una interfaz IP en el switch

- `disable ipif <ipif_name> all`

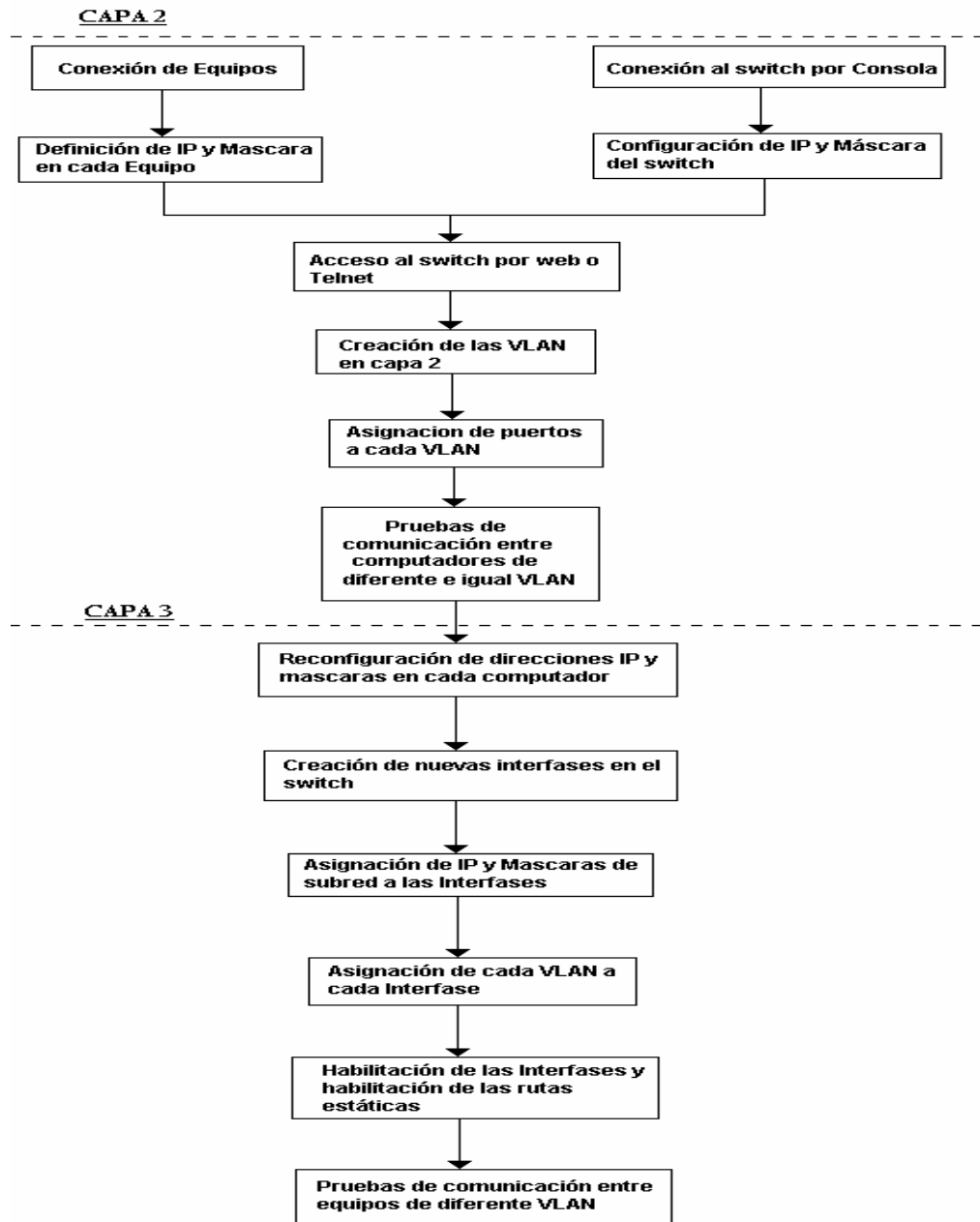
Propósito: Deshabilita una interfaz IP en el switch

- `show ipif <ipif_name>`

Propósito: Muestra la configuración de una interfaz IP en el switch

## ANEXO D. FLUJOGRAMA PRÁCTICAS DE LABORATORIO

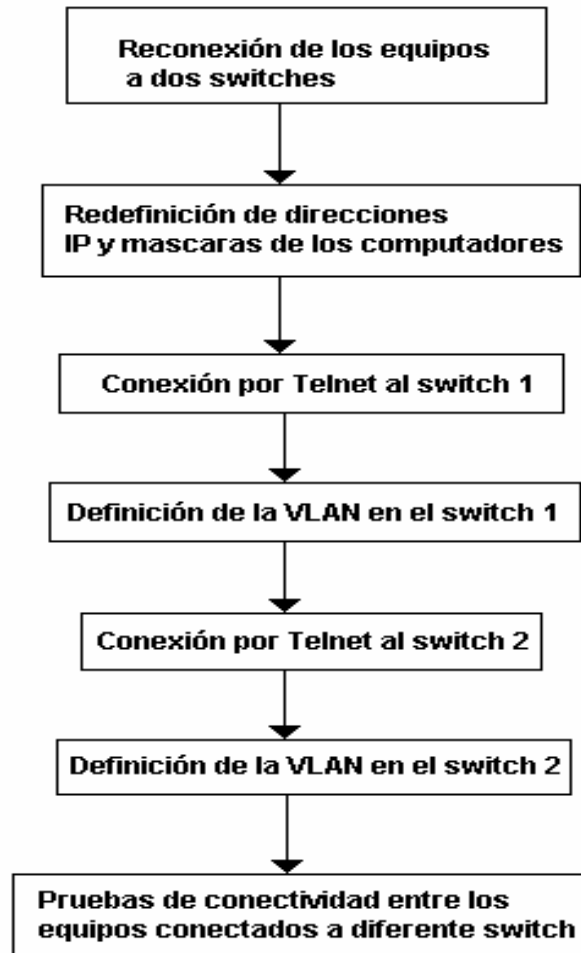
Creación de VLAN en un Switch:



Creación de VLAN entre dos Switches:

## VLAN INTER SWITCHES

---



## ANEXO E. EQUIPOS UTILIZADOS EN EL DESARROLLO DE LAS PRÁCTICAS DE LABORATORIO.

### Laboratorios y Equipos de Computo.

#### ➤ Laboratorio de Redes



Lado Derecho



Lado Izquierdo

#### ➤ Laboratorio de la Especialización

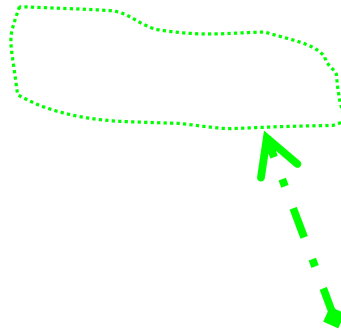


Panorámica del salón y ubicación de los PC.

### Switches y Rak

- Switch D-Link Des3326SR y Switch Avaya Cajun P333R





Switch D-Link Des 3326SR

Switch Avaya Cajun P333R

Ubicación: Laboratorio de Redes

➤ Switch 3Com 3226





**Switch 3Com 3226**

**Ubicación: Laboratorio de la Especialización.**