****

**Facultad de Ingeniería**

Departamento de Ingeniería en Computación e Informática



**Estudio del Protocolo 802.1Q y VLAN**

**“Laboratorio 1”**

**Autores**: Juan Copia

Daniela Oñate

Huber Ticona

**Curso**: Laboratorio de Redes

**Profesor**: Diego Aracena

Arica, 01 de septiembre 2019

# Tabla de Contenido

[1 Tabla de Contenido 2](#_Toc18264827)

[2 Historial de Cambios 4](#_Toc18264828)

[3 Introducción 5](#_Toc18264829)

[4 Objetivos 6](#_Toc18264830)

[4.1 Propósito 6](#_Toc18264831)

[4.2 Objetivo General 6](#_Toc18264832)

[4.3 Objetivos Específicos 6](#_Toc18264833)

[4.4 Suposiciones y restricciones 7](#_Toc18264834)

[5 Desarrollo 8](#_Toc18264835)

[5.1 Características de los recursos usados 8](#_Toc18264836)

[5.1.1 Computadores 8](#_Toc18264837)

[5.1.2 Switch y router 9](#_Toc18264838)

[5.2 Estudio del Protocolo 802.1Q 10](#_Toc18264839)

[5.3 Trabajo con Switch 10](#_Toc18264840)

[5.4 Implementación y configuración de equipos 11](#_Toc18264841)

[5.5 Pruebas y Resultados 13](#_Toc18264842)

[5.5.1 Ping en la misma VLAN 13](#_Toc18264843)

[5.5.2 Ping entre distintas VLAN 14](#_Toc18264844)

[5.6 MikroTik RouterBoard 17](#_Toc18264845)

[5.7 Implementación y configuración de equipos 17](#_Toc18264846)

[5.8 Pruebas y Resultados 18](#_Toc18264847)

[5.8.1 Ping en la misma VLAN 18](#_Toc18264848)

[5.8.2 Ping entre distintas VLAN 18](#_Toc18264849)

[5.9 VLAN Curso 21](#_Toc18264850)

[5.1 Implementación y configuración de equipos 21](#_Toc18264851)

[5.1 Pruebas y Resultados 22](#_Toc18264852)

[5.1.1 Ping 23](#_Toc18264853)

[6 Conclusión. 27](#_Toc18264854)

[7 Bibliografía 28](#_Toc18264855)

# Historial de Cambios

|  |  |  |  |
| --- | --- | --- | --- |
| FECHA | VERSIÓN | DESCRIPCIÓN | AUTOR(ES) |
| 29/08/2019 | 1.0 | Estudio del protocolo 802.1Q | Juan Copia  Daniela Oñate  Huber Ticona |
| 30/08/2019 | 1.1 | Objetivos y comienzo de desarrollo | Juan Copia  Daniela Oñate  Huber Ticona |
| 31/08/2019 | 1.2 | Desarrollo y descripción del trabajo realizado | Juan Copia  Daniela Oñate  Huber Ticona |
| 01/09/2019 | 1.3 | Introducción y Conclusión  Últimos detalles | Juan Copia  Daniela Oñate  Huber Ticona |

# Introducción

En el siguiente informe se describen los pasos realizados para la creación de redes VLAN, es decir redes independientes sobre una misma red física con el objetivo de lograr un aislamiento entre ciertas redes y una conexión entre otras a través de enlaces troncales. Para ello se tuvo que utilizar con soporte del protocolo 802.1Q que es el que permite el funcionamiento de esta tecnología. En primer lugar, se procedió a realizar una investigación sobre los conceptos de VLAN y del protocolo nombrado, luego se implementaron las VLAN en un switch, en un routerboard, y finalmente la conexión entre 2 VLAN de distintos switch.

# Objetivos

## Propósito

La importancia de tener las redes separadas es algo muy importante para tener una infraestructura segura y así evitar tráfico no deseado a determinadas zonas de nuestra red.

Una mala infraestructura podría ocasionar que cualquier host acceda a los datos de otros hosts en una misma red y dependiendo de cada empresa u organización estas podrían verse afectadas mediante el robo de información, daño a equipos, etc.

Debido a esto en este laboratorio se estudiarán los aspectos teóricos del protocolo 802.1Q y su potencial aplicable a una organización, que desee implantar una red LAN en su organización.

## Objetivo General

El objetivo de este experimento es demostrar cómo se logra la conexión entre varios hosts en una misma VLAN y en distintas VLAN, además que estas se vean como switch independientes.

## Objetivos Específicos

* Segmentar una LAN en 2 o más VLAN usando switch.
* Segmentar una LAN en 2 o más VLAN usando el Mikrotik RouterBoard como switchr.
* Hacer una VLAN de Curso entre 2 o más switch.

## Suposiciones y restricciones

* Se debe utilizar los switches y RouterBoard disponibles en la sala azufre.
* Se debe terminar en un plazo de 3 semanas.

# Desarrollo

## Características de los recursos usados

### Computadores

|  |  |
| --- | --- |
| Nombre | Descripción |
| Computador Lenovo Y730 | **Procesador**  Intel Core i7 8750H (2200 MHz - 4100 MHz)  **RAM**  16GB DDR4 (2666 MHz)  **Almacenamiento**  HDD 1TB (7200rpm)  SSD 128GB  **Tarjetas de video**  Intel UHD Graphics 630 (Integrada)  NVIDIA GeForce RTX 2070 Max-Q (8GB)  **Sistema Operativo**  Microsoft Windows 10 Home |
| Computador HP | **Procesador**  Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz  **RAM**  8GB DDR4 (2666 MHz)  **Almacenamiento**  HDD 1TB (5200rpm)  **Tarjetas de video**  Intel UHD Graphics 520 (Integrada)  **Sistema Operativo**  Microsoft Windows 10 Home |
| Computador Asus | **Procesador**  Intel(R) Core(TM) i7- 6500U @2.50GHz  **RAM**  8GB DDR4 (2666 MHz)  **Almacenamiento**  HDD 1TB (5200rpm)  **Tarjetas de video**  Intel UHD Graphics 5000 (Integrada)  NVIDIA GeForce 940M (2GB)  **Sistema Operativo**  Microsoft Windows 10 |

Tabla nro. 1 “Características de Computadores”

### Switch y router

|  |  |
| --- | --- |
| Nombre | Descripción |
| DGS-1216T | 16-Port 10/100/1000Mbps Gigabit Ethernet + 2-Port Mini GBIC Web-Smart Switch.  Capacidad de intercambio: 32 GPS.  Rango Máximo de reenvío:  10M: 14,880 pps.  100M: 148,809 pps.  1G: 1,488,095 pps.  Modo de reenvío: Store-and-forward.  Memoria de buffer: 512K.  SDRAM: 8M Bytes. |
| MikroTik RB1100AHx2 | Tiene trece puertos individuales Gigabit Ethernet, dos puertos, cinco grupos de interruptores, e incluye capacidad de Ethernet bypass. 2 GB de RAM SODIMM están incluidos, hay una ranura para tarjeta microSD, un beeper y un puerto serial. |

Tabla nro. 2 “Características de Switch y Router”

## Estudio del Protocolo 802.1Q

El protocolo IEEE 802.1Q, permite a múltiples redes (VLAN) compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

Un conmutador (switch inteligente o routerboard actuando como switch) compatible con redes VLAN permite definir múltiples redes de área local virtuales sobre una única infraestructura de red de área local física.

Los hosts de una VLAN se comunican entre ellos, como si solo ellos estuvieran conectados al conmutador.

En una VLAN basada en puertos, el administrador de red divide los puertos o interfaz en grupos, donde cada grupo es una VLAN y de esta forma se limita el tráfico del conmutador ya que un host perteneciente a una VLAN solo puede enviar paquetes a otro host de la misma VLAN.

## Trabajo con Switch

El objetivo de este segmento consiste en lograr conectar 4 computadores a un mismo switch, pero en puertos procedentes a distintas VLAN. En principio se conectaron 2 equipos a la VLAN 100 y 2 equipos a la VLAN 101 de manera que los equipos pertenecientes a la misma VLAN tienen conexión entre sí, pero no con los equipos de la otra VLAN. Sin embargo, como este es un escenario de pruebas, para lograr esto, se procedió a crear un enlace troncal entre ambas VLAN, lo que permitió la comunicación entre equipos de diferentes VLAN.

## Implementación y configuración de equipos

En primer lugar, se realizó la configuración del switch con los parámetros que muestran en la figura 1.

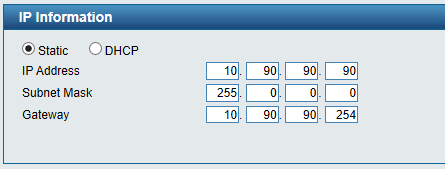


Figura nro. 1 “Información IP del Switch”

Según las indicaciones del manual del Switch, también se procedió a activar “Jumbo Frame”.

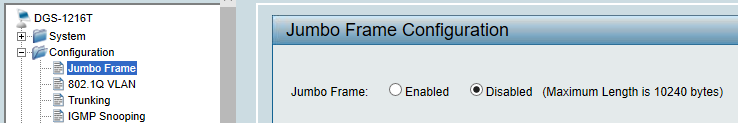


Figura nro. 2 “Configuración Jumbo Frame”

Una vez hecho esto, Se procede a configurar los computadores a conectar, asignando IPs estáticas a cada uno de ellos con la máscara de red correspondiente.

Cada computador deberá tener las siguientes Ips:

* PC1 – 10.90.90.91
* PC2 – 10.90.90.92
* PC3 – 10.90.90.93
* PC4 – 10.90.90.94

Además de ponerles como máscara de subred: 255.0.0.0.

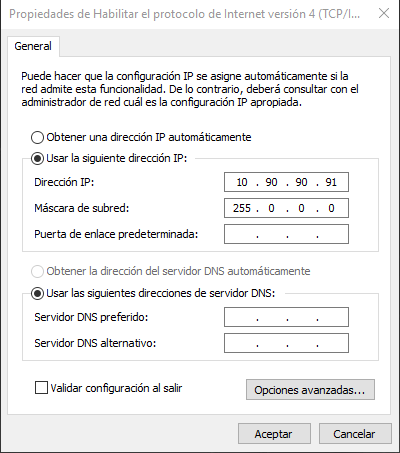


Figura nro. 3 “Configuración Computador”

Una vez realizado todos los pasos anteriores, podremos ingresar al Switch y creas las VLAN correspondientes dadas en la guía.

Inicialmente, el switch contaba con una VLAN por defecto que abarcaba todos sus puertos, esta fue eliminada y se crearon dos VLAN, la 100 que abarca los puertos 01, 02, 05 y 06, y la VLAN 101 que abarca los puertos 03, 04, 07, 08.

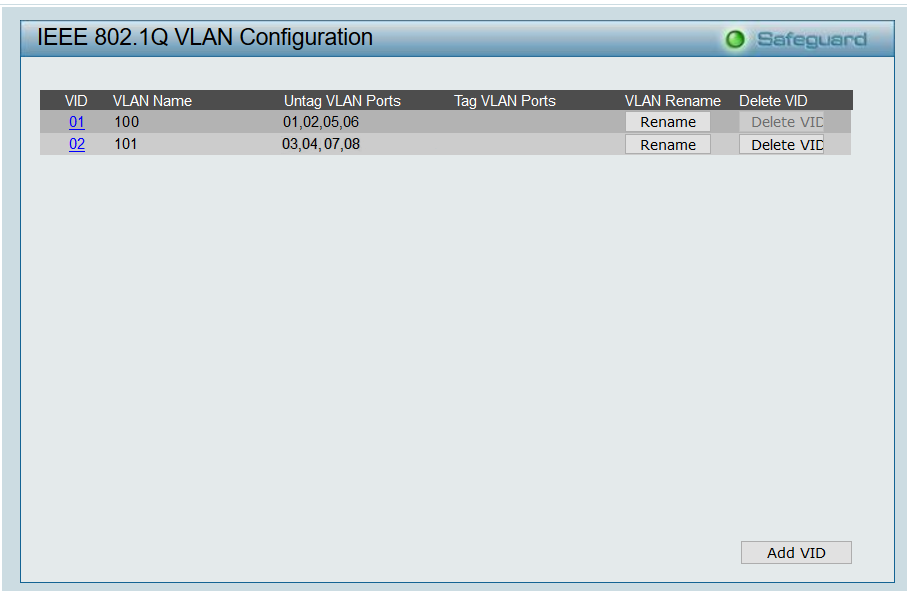


Figura nro. 4 “Configuración VLAN”

Una vez realizado este procedimiento, se se realizaron pings a los distintos computadores conectados en la red, tanto dentro de la misma VLAN como entre ellas.

## Pruebas y Resultados

### Ping en la misma VLAN

Para poder corroborar si las VLAN se encuentran funcionando de manera correcta, se procede a realizar ping en ellas.

Como se puede ver en las figuras 5 y 6 a continuación, se hace ping desde el PC2 al PC1 y PC 3 en la VLAN 100, en este proceso, se puede observar la cantidad de bytes por respuesta y el tiempo de vida del paquete enviado.

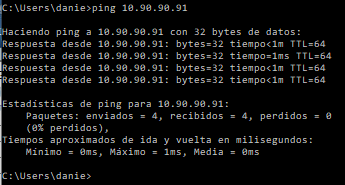


Figura nro. 5 “Ping PC2 a PC1”

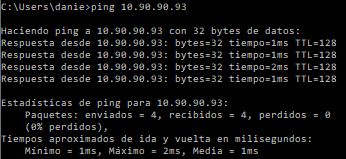


Figura nro. 6 “Ping PC2 a PC3”

Al igual que en las anteriores capturas, la siguiente muestra un ping hecho del PC2 al PC4, el primero se ha cambiado de VLAN, para poder comprobar que la VLAN 101 también funciona de manera correcta.

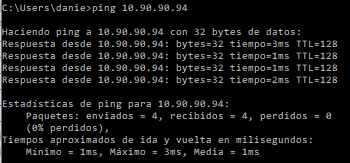


Figura nro. 6 “Ping PC2 a PC4”

### Ping entre distintas VLAN

Los pings realizados entre equipos pertenecientes a distintas VLAN fallaron, un comportamiento esperado ya que es el propósito de una VLAN, este es, crear redes independientes dentro de una misma red física.

Los mensajes que se pueden ver cuando se realizan estos Ping suelen decir “Red de destino inaccesible”, lo que significa que no existe ninguna ruta al destino o “Ha terminado el tiempo de espera para esta solicitud”, que quiere decir que el tiempo límite entre host a host fue superado por lo que existe un error en la conexión.

Sin embargo, para lograr la conexión entre estos equipos y como parte del proceso de aprendizaje dentro del laboratorio, fue necesario realizar un enlace troncal, que consiste en un puente de comunicación entre ambas redes.

Como muestra la figura 7 a continuación, se designó un puerto de cada VLAN para realizar el enlace troncal, puerto 02 para la 100, y puerto 07 para la 101. Finalmente se conectaron ambos puertos a través de un cable de red para hacer efectiva la conexión.

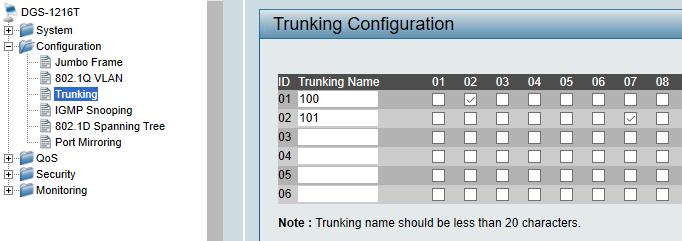


Figura nro. 7 “Configuración Troncal”

Una vez hecho este procedimiento, se realizan ping entre distintos equipos como se puede ver en las figuras 8, 9 y 10, desde el PC2 que se encuentra en la VLAN 100 al igual que PC1, y a PC3 y PC4 que se encuentran en la VLAN 101

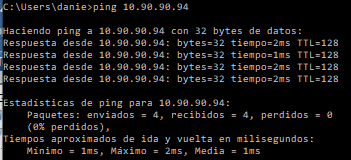


Figura nro. 8 “Ping PC2 a PC4”

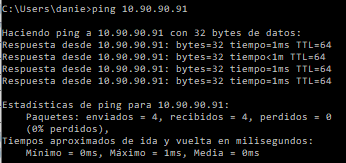


Figura nro. 9 “Ping PC2 a PC1”

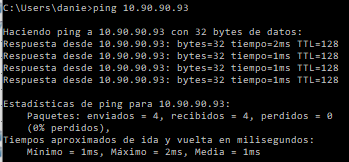


Figura nro. 10 “Ping PC2 a PC3”

## MikroTik RouterBoard

En este apartado se realizarán las VLAN mediante el uso del router MikroTik, donde se observará la conexión entre 2 host en una misma VLAN y luego entre 2 host en distintas VLAN, para ello se crearán 2 puentes donde a cada puente se le asignarán 5 puertos y luego se procederá a realizar las conexiones entre estos.

## Implementación y configuración de equipos

Para comenzar, el Router fue modificado a su estado inicial de fábrica, de esta manera, debíamos trabajar desde cero con él, cambiando todos los ajustes necesarios.

El procedimiento de configuración del RouterBoard, consistió, al igual que el switch, en cambiar la IPs y sub mascara en la que trabaja. No se procede a configurar los PC, ya que se está utilizando las mismas Ips anteriores, sólo se cambió el elemento de trabajo principal de conexión, switch router.

Luego de esto se crearon 2 puentes 100 y 101 como se muestra en la figura 11, y luego se les asignaron puertos a dichos puentes. Al puente 100 se le asignaron los puertos 1, 2, 3, 4 y 5, y por otro lado al puente 101 se le asignaron los puertos 6, 7, 8, 9 y 10. De esta forma se crearon implícitamente 2 VLAN 100 y 101

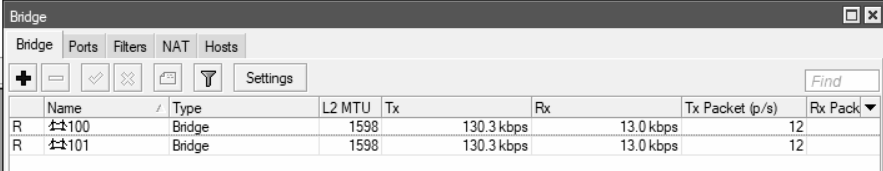


Figura nro. 12 “Configuración de Puentes”

## Pruebas y Resultados

### Ping en la misma VLAN

Para corroborar que los puentes realizados estén funcionando de manera correcta, se procedió a comprobar la conexión entre 2 PC ubicados en la misma VLAN, en este caso la VLAN asociada al puente 100 (figura 13):

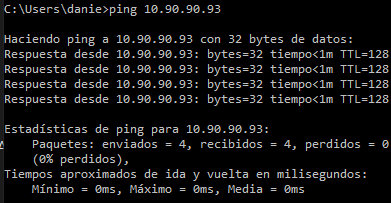


Figura nro. 13 “Ping PC2 a PC3”

### Ping entre distintas VLAN

Al ser dos puentes distintos, la conexión o cualquier tipo de Ping entre ellas, está destinada a fracasar, esto se debe que, aunque estén conectadas físicamente al mismo conmutador (router), cada VLAN solo puede comunicarse con hosts de una misma VLAN.

Para solucionar esto, se implementó un enlace troncal entre ambas VLAN como se ve en la figura 14, esto se hace para que ambas VLAN puedan comunicarse entre sí.

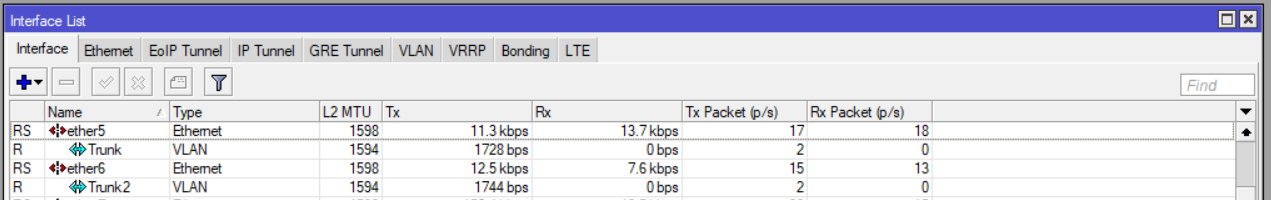


Figura nro. 14 “Enlace Troncal entre puentes”

Una vez configurado el enlace troncal, se procedió a volver a comprobar la conexión entre ambos PC, como se puede observar en la figura 15.

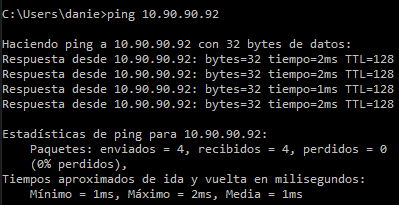


Figura nro. 15 “Ping PC1 a PC2”

Del análisis anterior se realizó un seguimiento de la conexión entre las VLAN mediante whireshark, donde se observa que, al hacer ping, este es realizado por el protocolo ICMP y que la conexión es exitosa. Ver figura 16 y 17.

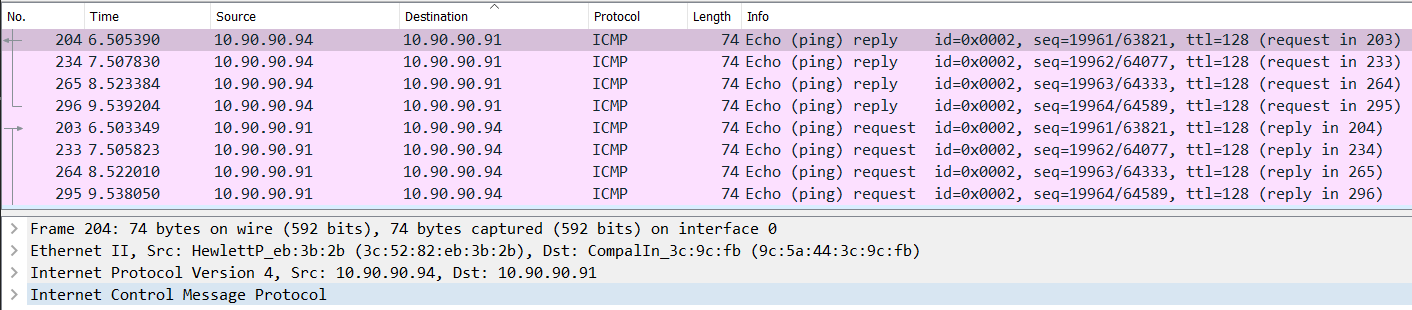


Figura nro. 16 “WireShark”

En la captura anterior, se debe ver los paquetes que fueron enviados de host a hosts, el paquete con dirección fuente 10.90.90.94, que representa al PC4, y su dirección de destino 10.90.90.91, PC1, son los datos correspondientes a los pings realizados, se puede apreciar en que protocolo trabajan, el tiempo exacto que demora cada paquete y además su tamaño.

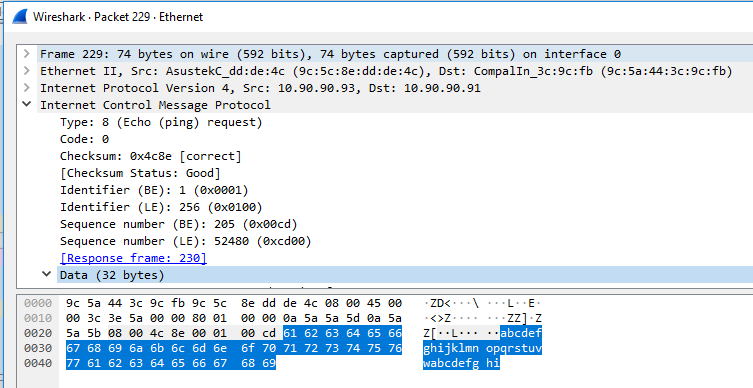


Figura nro. 17 “WireShark”

## VLAN Curso

## Implementación y configuración de equipos

Para este apartado, se realiza una nueva configuración, tanto a PC como Switch que serán usados.

Al primer Switch, le asignamos una VLAN 100 con los puertos 9, 10, 11, 12 ,13, 15 ,15 y 16 (figura 18), mientras que al segundo switch le asignamos dos VLAN 102 y 103 con los puertos 1,2,3,4,5 y 6 para la primer VLAN, 9, 10, 11, 12 ,13, 15 ,15 y 16 para la siguiente (figura 18).

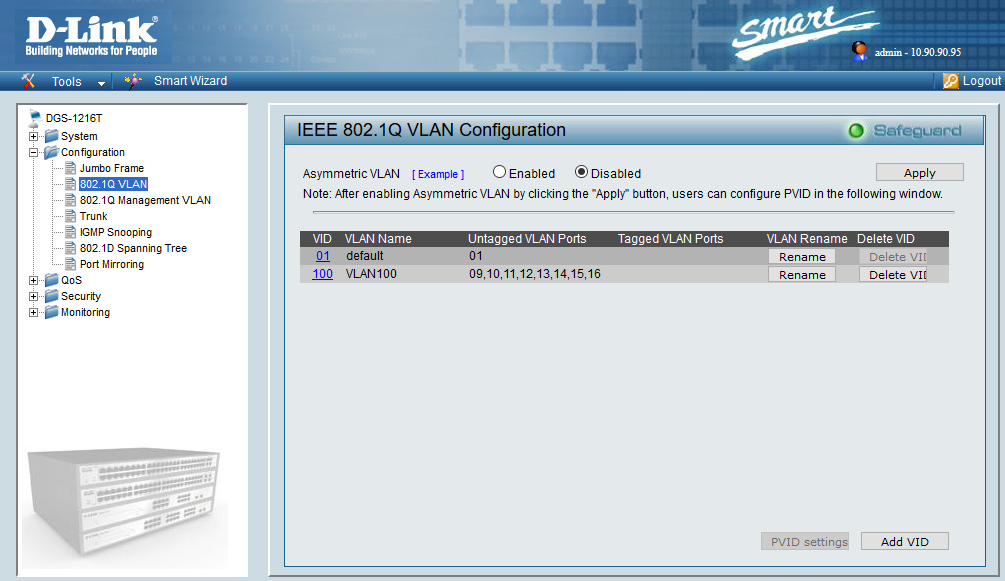


Figura nro. 18 “VLAN 100”

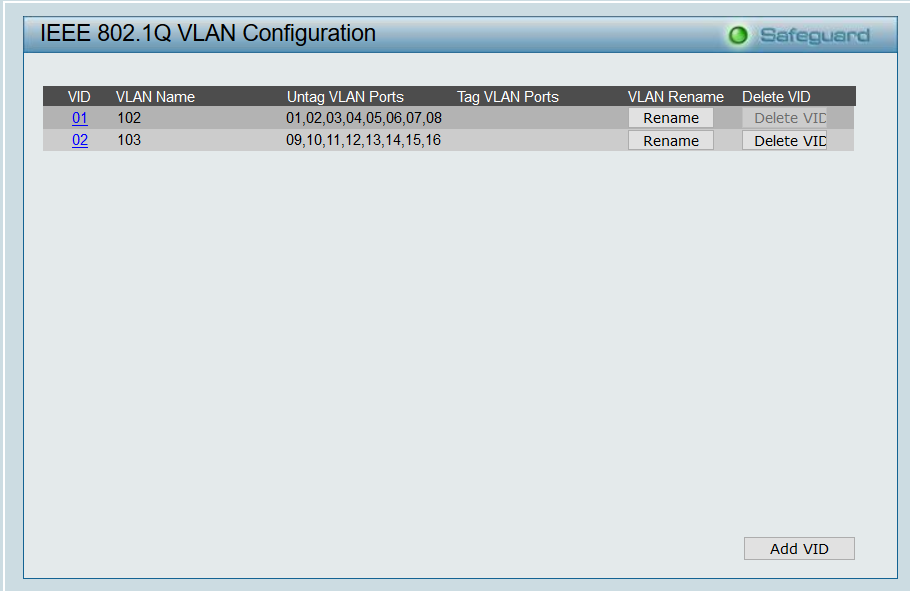


Figura nro. 19 “VLAN 102, VLAN 103”

Además de esto, se configuran los PC con las siguientes direcciones IP:

PC en VLAN 100

* PC1 – 10.90.90.94
* PC2 – 10.90.90.96

PC en VLAN 102 y 103

* PC3 – 10.90.90.92
* PC4 – 10.90.90.93

## Pruebas y Resultados

El objetivo de realizar una red curso, es poder conectarnos e ingresar a la red del otro, es aquí donde finalmente, se puso a prueba los enlaces troncales aprendidos en las prácticas anteriores, ya que si se desea tirar un ping de una a VLAN a otra nose podría.

Para esto, y como se ve en la figura 20 y 21, se realizan los enlaces troncales correspondientes a través de a interfaz de cada switch.

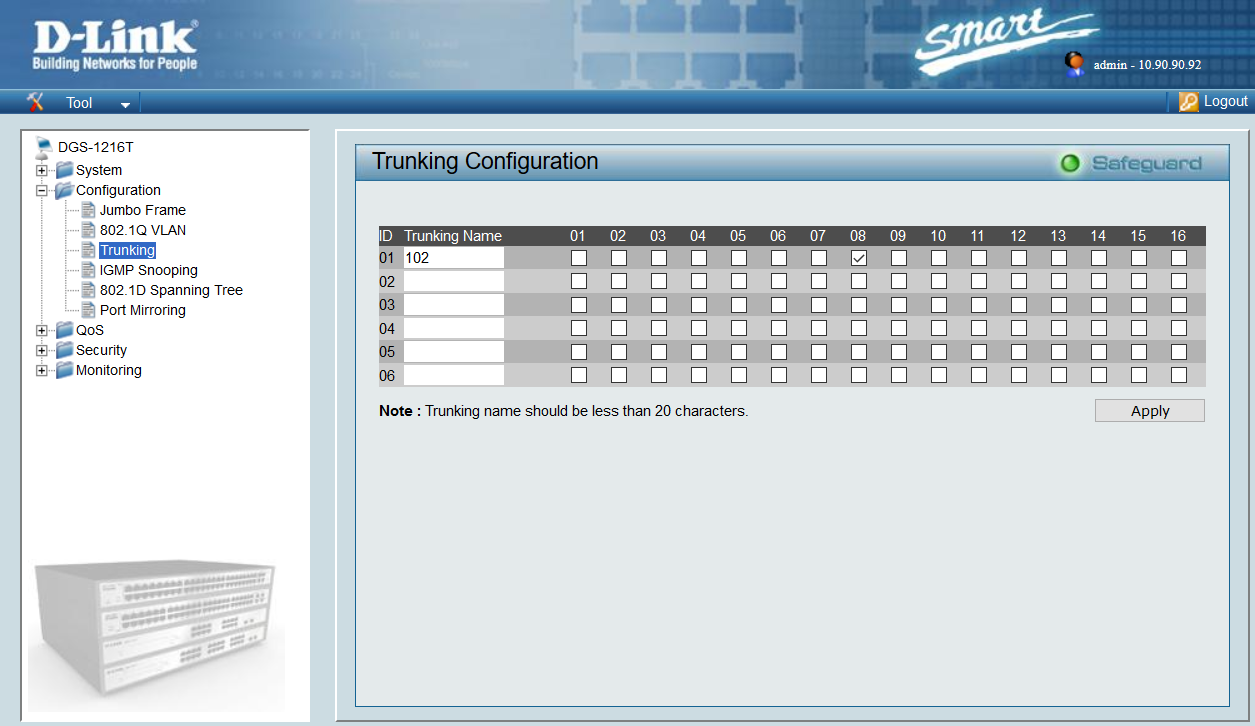


Figura nro. 20 “Enlace Troncal VLAN 102”

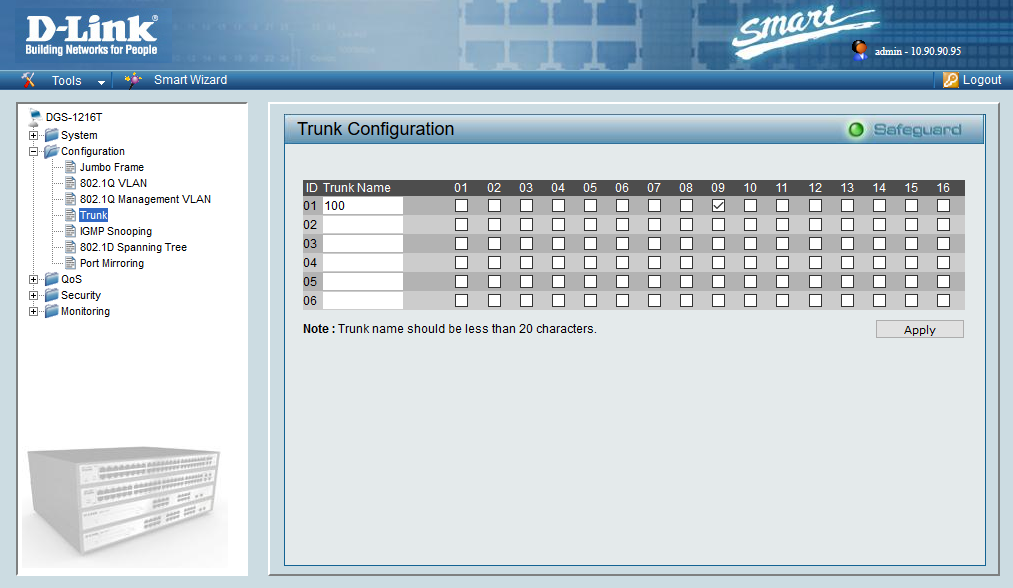


Figura nro. 21 “Enlace Troncal VLAN 100”

### Ping

Con la configuración anterior lista, se puede realizar ahora Ping de la VLAN 102 a la VLAN 100, figuras 22 y 23.

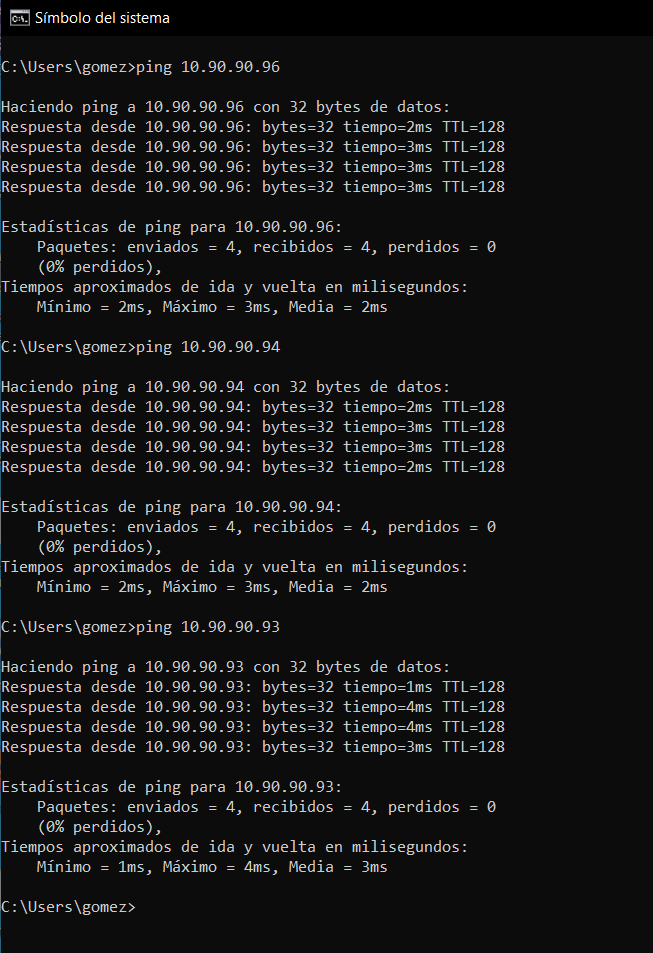


Figura nro. 21 “Ping PC3 a PC2”

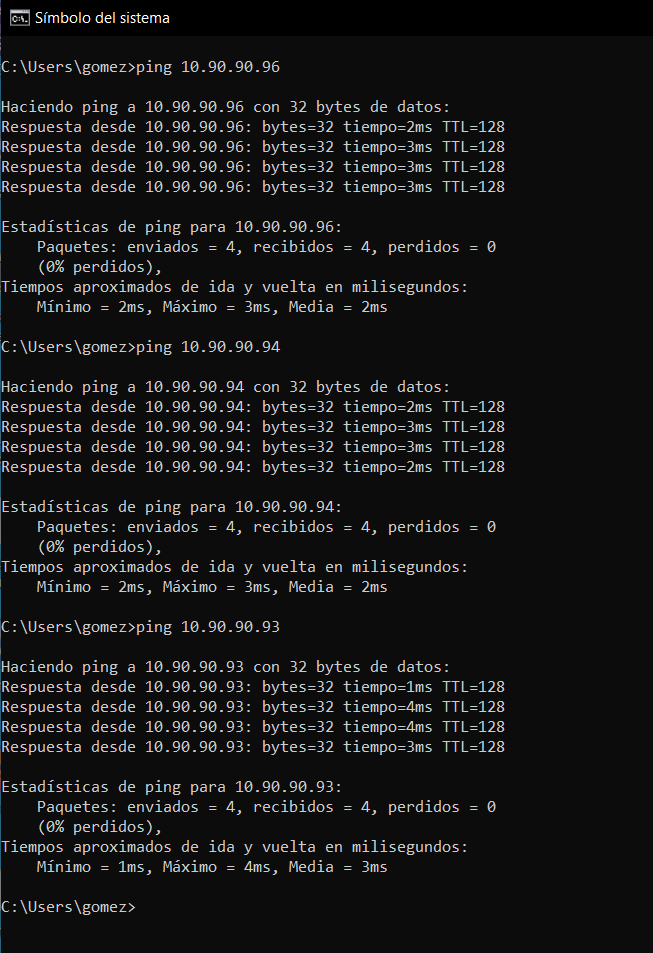


Figura nro. 21 “Ping PC3 a PC1”

Este siguiente ping se ha realizado dentro de la misma VLAN, figura 21.

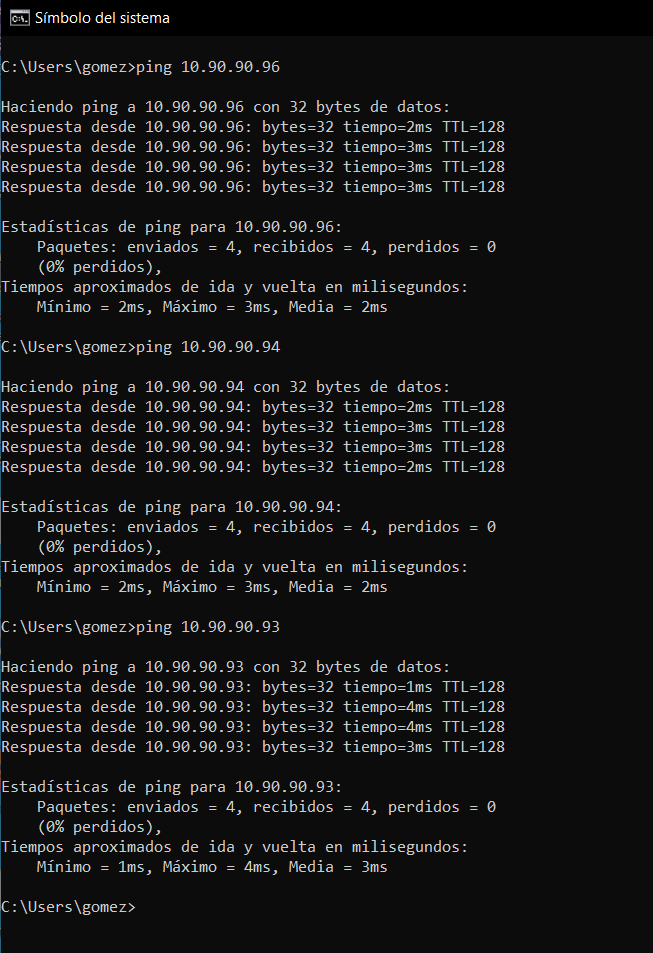


Figura nro. 21 “Ping PC3 a PC4”

De igual manera, esto funciona si realizamos ping en sentido contrario, de VLAN 102 a VLAN 100, figuras 22 y 23.

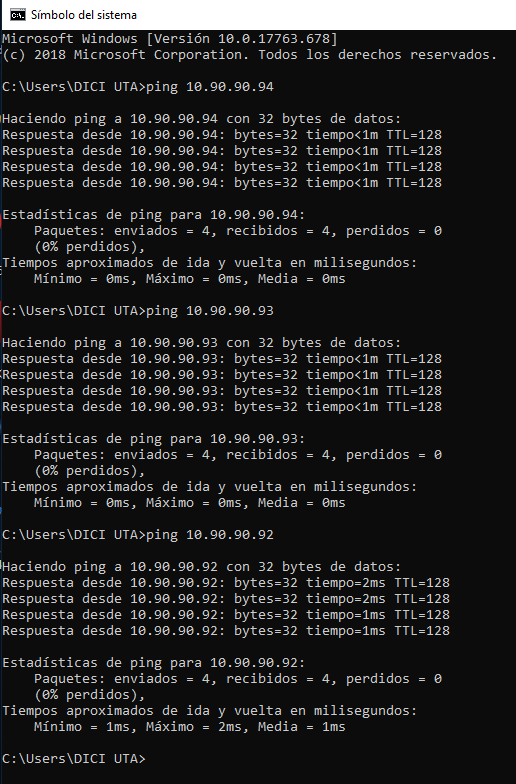


Figura nro. 24 “Ping PC2 a PC4”

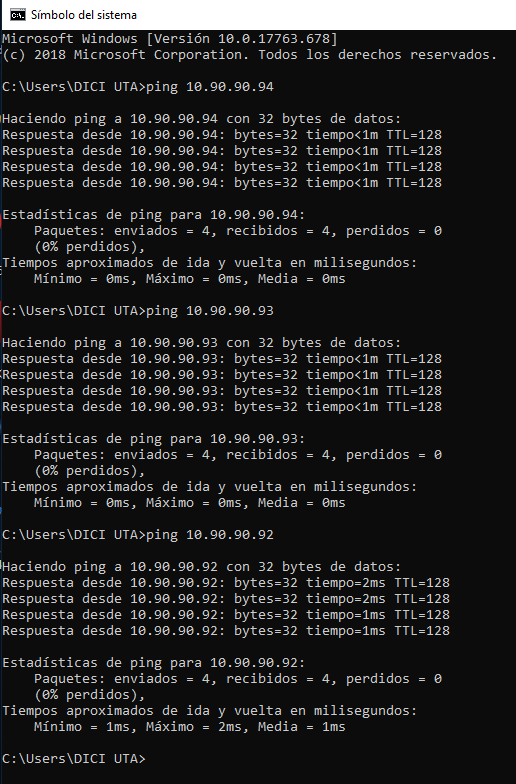


Figura nro. 24 “Ping PC2 a PC3”

Este siguiente ping se ha realizado dentro de la misma VLAN, figura 24.

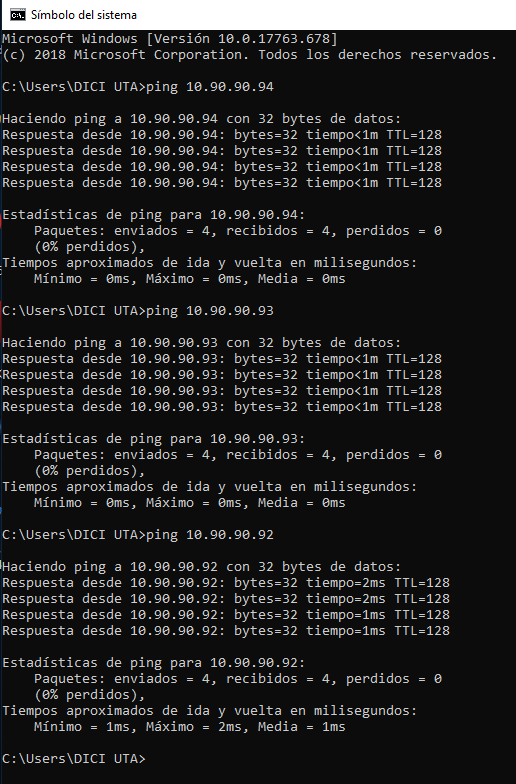


Figura nro. 24 “Ping PC2 a PC1”

Además, para asegurar el recorrido y los saltos que ocurren, se ha hecho un comando tracert, desde VLAN 100 a VLAN 102 y viceversa, como se puede observar en la figura 25 y 26, el máximo de saltos es de 30.

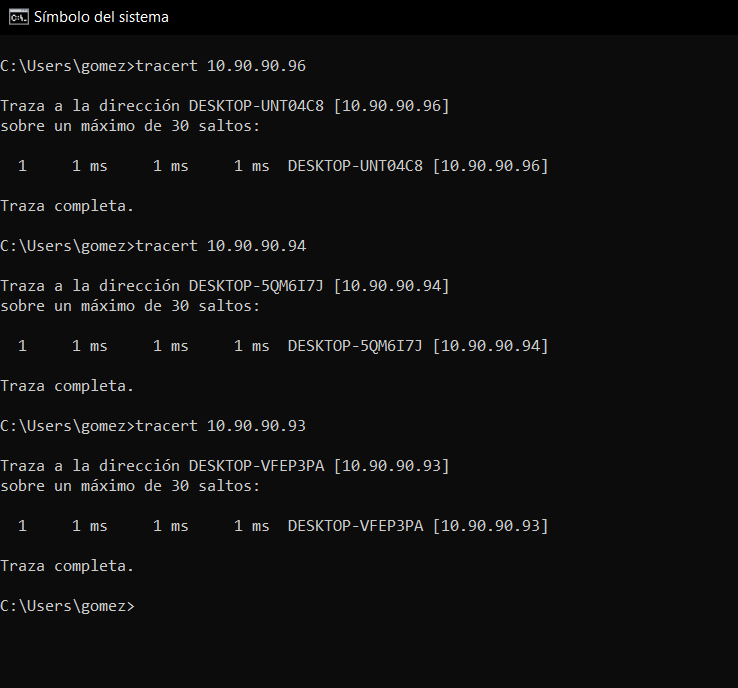


Figura nro. 25 “Tracert VLAN 102 a 100”

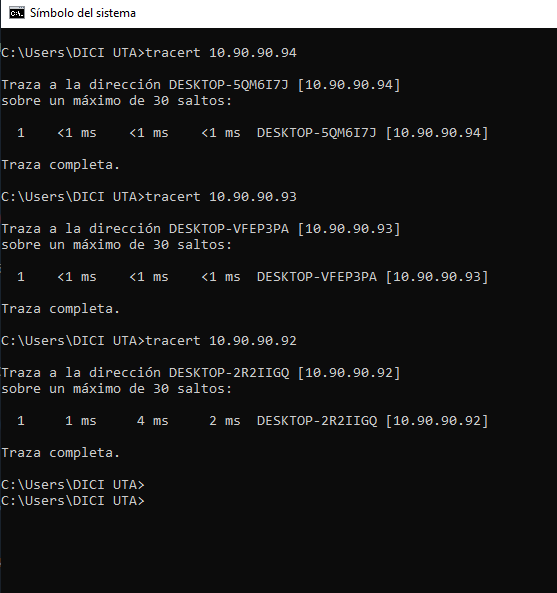


Figura nro. 25 “Tracert VLAN 102 a 102”

Y finalmente, para tener una corroboración de los datos aun más exacta, se realiza un análisis con WireShark de los tracert hechos, figura 26.

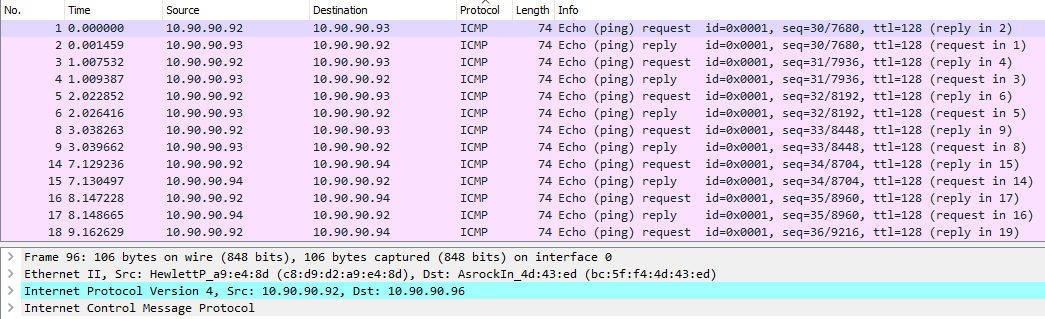


Figura nro. 26 “WireShark”

# Conclusión.

En esta actividad, se pudieron adquirir amplios conocimientos del área de redes de comunicación.

Además, se pudo apreciar, que el hecho de entender y comprender de manera clara tanto los protocolos como el equipamiento a ser usado en los distintos ejercicios prácticos, es de suma importancia, para no incurrir en errores ni echar a perder el material.

Por otra parte, se hizo uso de comandos ya conocidos en cursos anterior, como ping y tracert, además de la herramienta WireShark. Estos nos sirven para poder visualizar de mejor manera los tráficos de paquetes y todo lo que les competa, tiempo de vida, respuesta, otros.

OBS: Efectivo, explica poco el cómo se procedió y que resultados se lograron..

Básico en cuanto a lo teórico sobre el protocolo 802.1Q

Se cumple con todos los puntos de lo solicitado, sin grandes aportes lo descriptivo

Hay aspectos como los troncales tanto en switch como en el routerboard como switch, no se explica, ni tampoco se indica el sentido que tiene en la segmentación de redes

Las conclusiones son muy pobres, más bien comentarios, considerando que habían 5 actividades bien separadas

Se pensó en que iban a sacar partido de las herramientas, pero no se realizaron las descripciones de las muestras

# Bibliografía

|  |  |  |
| --- | --- | --- |
| [1] | Manual Cisco CCNA |  |
| [2] | James F. Kurose & Keith W. Ross (2012) “Computer Networking: A Top Down Approach Featuring the Internet” Alison Wesley, 3rd Edition, England. |  |
| [3] | Fred Halsall, “Computer Networking and the Internet”, 5th edition published 2005 |  |