

UNIVERSIDAD DE TARAPACÁ



**DEPARTAMENTO DE INGENIERÍA CIVIL EN COMPUTACIÓN
E INFORMÁTICA**

EUIIIS

Área de Ingeniería en Computación e Informática



LABORATORIO 1: Laboratorio de redes

Autor: Leonel Alarcón Bravo
Gonzalo Vega
Curso: Laboratorio de redes
Profesor: Diego Aracena Pizarro

ARICA, 01 de Septiembre 2019

Contenidos

SECCIÓN	PÁGINA
I. INTRODUCCIÓN	3
II. OBJETIVOS	4
2.1 PROPÓSITO	4
2.2 OBJETIVO GENERAL	4
2.3 OBJETIVOS ESPECÍFICOS	4
III. DESARROLLO	5
3.1 Protocolo 802.1Q	5
3.1.1 Formato de la trama del Protocolo 802.1Q	5
3.2 Creando Vlan	6
3.3 Creando Vlan incorporando RouterBoard	9
3.4 Vlan Curso	13
CONCLUSIÓN	18
REFERENCIAS	19

I. INTRODUCCIÓN

El problema abordado consta de analizar e implementar un tipo de red de área local, en este caso una VLAN, realizar diversos testeos a la red creada para verificar el estado de su comunicación. Para ello, se estudiaron tanto las herramientas como conceptos necesarios para entender la situación y dar respuesta a las actividades solicitadas.

En primer lugar, vamos a empezar por saber qué son. Del inglés Virtual LAN (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch. Podría decirse que cada una de estas redes agrupa los equipos de un determinado segmento de red. Crear estas particiones tiene unas ventajas bastante claras a la hora de administrar una red. Es por esto último que el Laboratorio número 1 de la asignatura solicita varias actividades que nos servirá para implementar lo teóricamente aprendido y realizar o ejecutar varios aspectos de este para así ponerlo en práctica.

Los datos, información y citación han sido recolectadas de los capítulos correspondientes a VLAN de los libros de Fred Halsall y J. Kurose entregados por el profesor además de diferentes fuentes en la web. De manera que el documento entrega un conocimiento previo en cuanto a la actividad solicitada para luego enfocarse en los diferentes resultados de ellos.

II. OBJETIVOS

2.1 PROPÓSITO

El propósito del documento es presentar el trabajo realizado y los resultados obtenidos para los enunciados propuestos que corresponden al primer laboratorio.

2.2 OBJETIVO GENERAL

El objetivo general del trabajo es poder realizar un estudio inicialmente teórico sobre las redes de área local (LAN) continuando con el uso de las VLAN armando redes incorporando a ellas y realizando pruebas de las actividades solicitadas.

2.3 OBJETIVOS ESPECÍFICOS

Los objetivos específicos del trabajo son:

- Analizar los aspectos teóricos del protocolo 802.1Q
- Utilizar los libros de Fred Halsall y j. Kurose para adquirir conocimientos sobre VLAN
- Comprobar la compatibilidad de los Switch del laboratorio con VLAN
- Armar una VLAN
- Demostrar y explicar la comunicación entre switches independientes
- Configurar las VLAN creadas y realizar pruebas de conectividad
- Incorporar RouterBoard a las actividades realizadas
- Crear una VLAN con otra grupo de trabajo y realizar las pruebas de conectividad
- Utilizar software (Wireshark), comandos, etc. para demostrar lo desarrollado

III. DESARROLLO

3.1 Protocolo 802.1Q

Este protocolo es una variación al estándar de Ethernet. El 802.1Q fue diseñado para desarrollar un mecanismo que permita a múltiples redes con interconectadas con puentes o switches compartir el mismo medio físico sin problemas de interferencia entre las redes que comparten el medio. Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Permite identificar a una trama como proveniente de un equipo conectado a una red determinada.

Una trama perteneciente a una VLAN sólo se va a distribuir a los equipos que pertenezcan a su misma VLAN, de forma que se separan dominios de broadcast.

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

3.1.1 Formato de la trama del Protocolo 802.1Q

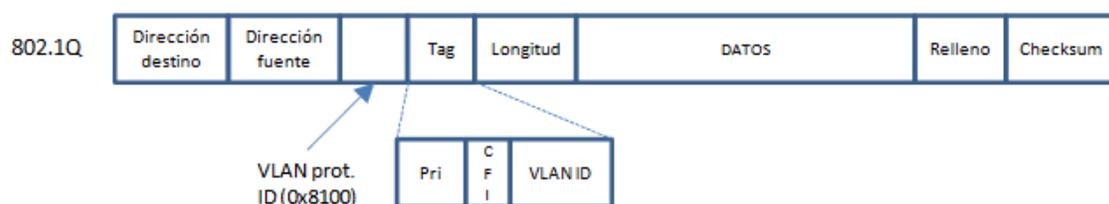


Figura 1. Trama 802.1Q

En la Figura 1, los primeros 2 bytes del VLAN tag consisten en el tipo de tag de 802.1Q y siempre está puesto a 0x8100. Los últimos 2 bytes contienen la siguiente información:

– Los primeros 3 bits son el campo Prioridad de Usuario que pueden ser usados para asignar un nivel de prioridad.

- El próximo bit es el campo Indicador de formato canónico (CFI en inglés) usado para indicar la presencia de un campo de información de enrutamiento.
- Los restantes 12 bits son el Identificador VLAN que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.

3.2 Creando VLAN

En esta ocasión se usó un Switch modelo Des-3028 para llevar a cabo la creación de las diferentes Vlans dentro del mismo switch, para ello en primer lugar se modificó la dirección IP del computador para poder acceder a la interfaz del Switch.

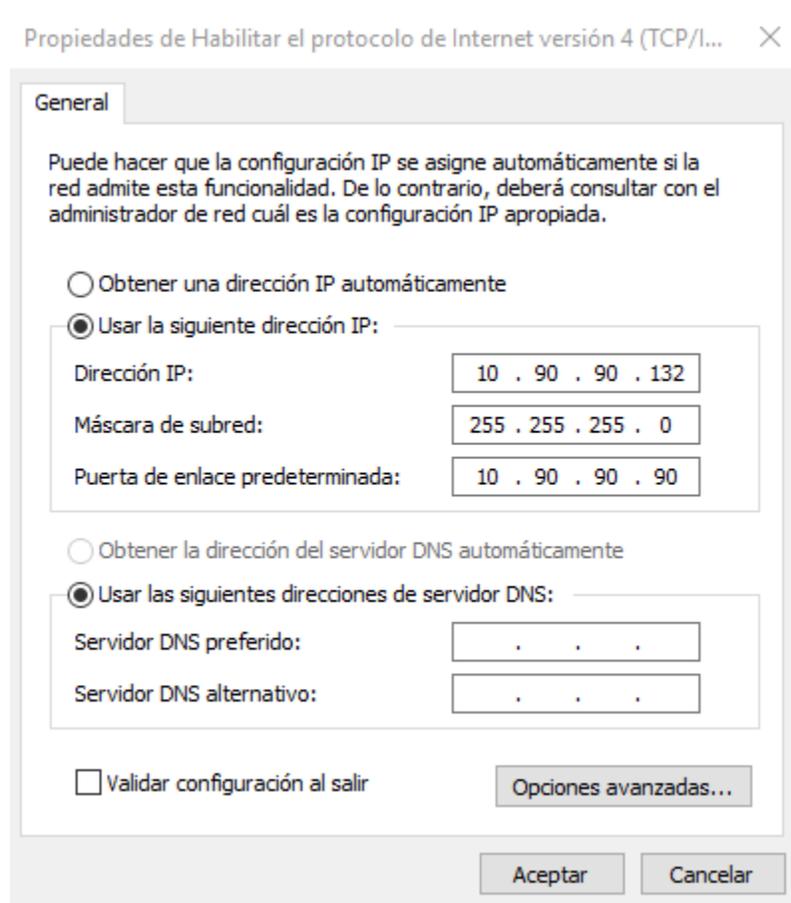


Figura 2. Configuración de dirección IP

Con las configuraciones realizadas como se ve claramente en la Figura 2, se tuvo acceso a la interfaz del Switch DES-3028 para que de esa forma se puedan crear las Vlan correspondientes.

Total Entries:2

Static VLANs Entry Settings

Add New 802.1Q VLAN

Static VLANs Entry

VLAN ID	VLAN Name	Ports	Modify	Delete
1	default	1-7	<input type="button" value="Modify"/>	<input type="button" value="X"/>
2	Vlan100	8-14	<input type="button" value="Modify"/>	<input type="button" value="X"/>

Figura 3. Vlan creadas

En primer lugar se tomó la Vlan 1 como la Vlan 101, y como se aprecia en la imagen está configurada de tal forma que toma desde los puertos 1 al 7, por otro lado, la Vlan 100 se configuró como la segunda vlan, y va desde los puertos 8 al 14 así de esa forma tenemos creadas 2 Vlan en un mismo switch.

En este caso, la Vlan 1 es la que posee acceso a internet. Luego en la siguiente imagen se muestra como se realizaron las conexiones físicamente dentro del dispositivo.



Figura 4. Conexiones dentro del switch.

A continuación, con las siguientes configuraciones ya listas tanto por fuera como dentro del switch, se realizó ping para corroborar que ambos PC's conectados al switch dentro de la misma Vlan 1 tuvieran conexión entre ellas. Cabe mencionar, que el PC1 está en el puerto 2 y el PC 2 está en el puerto 3, en el puerto 1 del switch está conectada al internet del laboratorio para tener así acceso a esta.

Con todo lo mencionado anteriormente, al hacer ping entre los computadores se mostró el siguiente resultado.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Usuario>ping 10.90.90.133

Haciendo ping a 10.90.90.133 con 32 bytes de datos:
Respuesta desde 10.90.90.133: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 10.90.90.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

Figura 5. Ping en una misma Vlan

Según los resultados apreciados en la figura 5, se ve claramente que si se logró realizar un ping a la maquina 10.90.90.133 la cual es el PC 2 dentro de la Vlan 1.

Para la siguiente actividad se realizó el mismo proceso anterior, solo que esta vez se cambió el PC 2 a la Vlan 2 configurada anteriormente, quedando de la siguiente manera.



Figura 6. Conexiones en Vlan distintas.

Nuevamente se realizó ping entre ambas máquinas para comprobar si se establece una conexión entre ellas, el resultado esperado es que no haya conexiones entre ellas debido a que está en distintas VLANs y por Protocolo 802.1Q.



Figura 9. Fotografía de la RouterBoard 1100 Mikrotik con ambos computadores en la misma bridge.

Con todo lo realizado anteriormente, al hacer ping entre los computadores se mostró el siguiente resultado.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 10.90.90.133

Haciendo ping a 10.90.90.133 con 32 bytes de datos:
Respuesta desde 10.90.90.133: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.90.90.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
```

Figura 10. Captura del resultado al hacer ping entre ambas computadoras.

Según los resultados apreciados en la figura 10, se ve claramente que si se logró realizar un ping a la maquina 10.90.90.133 la cual es el PC 2 y pertenece al mismo bridge.

Para la siguiente actividad se realizó el mismo proceso anterior, solo que esta vez se cambió el PC 2 al segundo bridge, quedando de la siguiente manera.



Figura 11. Fotografía de RouterBoard 1100 Mikrotik con ambos computadores en distintas bridge.

Con todo lo realizado anteriormente, al hacer ping entre los computadores se mostró el siguiente resultado.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 10.90.90.133

Haciendo ping a 10.90.90.133 con 32 bytes de datos:
Respuesta desde 10.90.90.132: Host de destino inaccesible.

Estadísticas de ping para 10.90.90.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
```

Figura 12. Captura del resultado al hacer ping entre ambas computadoras en distintas bridge.

Según los resultados apreciados en la figura 12, se ve claramente que no se logró realizar un ping a la maquina 10.90.90.133 la cual es el PC 2 y pertenece al otro bridge.

Para la siguiente y última actividad se realizó el mismo proceso anterior, solo que esta vez además de que cambió el PC 2 al segundo bridge, también se hizo un bridge entre bridges con un cable rj45 cruzado estableciendo una conexión entre ellos quedando de la siguiente manera.



Figura 13. Fotografía de RouterBoard 1100 Mikrotik con ambos computadores en distintas bridge y con un bridge entre ellos.

Con todo lo realizado anteriormente, al hacer ping entre los computadores se mostró el siguiente resultado.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 10.90.90.133

Haciendo ping a 10.90.90.133 con 32 bytes de datos:
Respuesta desde 10.90.90.133: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.90.90.133:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

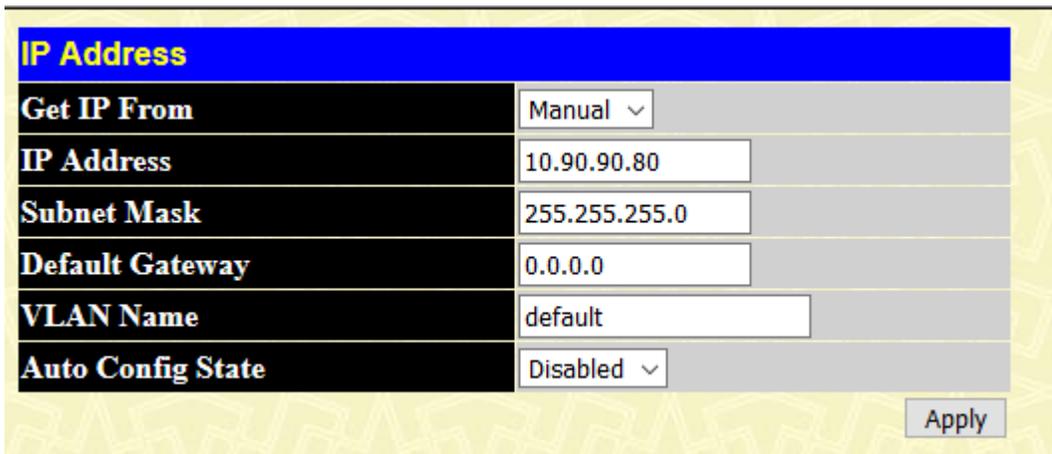
Figura 14. Captura del resultado al hacer ping entre ambas computadoras en distintas bridge pero además de tener otro bridge entre ellos.

Según los resultados apreciados en la figura 14, se ve claramente que si se logró realizar un ping a la maquina 10.90.90.133 la cual es el PC 2, esto fue posible gracias al bridge extra que se implementó entre ambas permitiendo así su conexión.

3.4 Vlan Curso

Para comenzar esta sección del laboratorio se tuvo que llegar a un acuerdo con el grupo contiguo para determinar cuáles serán las direcciones a usar por cada grupo en cada PC y switch con el objetivo de no causar ningún error al realizar la actividad.

Mencionado lo anterior se llegó al acuerdo de que nuestro Switch DES-3028 tendrá una dirección IP de "10.90.90.80" y el grupo con los que realizaremos Vlan curso tendría una IP en su switch de "10.90.90.90". Así, se ingresó a la interfaz del switch para cambiar dicha dirección.



IP Address	
Get IP From	Manual
IP Address	10.90.90.80
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
VLAN Name	default
Auto Config State	Disabled

Apply

Figura 15. Cambio de dirección IP Switch DES-3028

Luego cambiando la dirección de la switch se procedió a cambiar las direcciones IP de las máquinas a utilizar, en este caso para nuestro grupo se usó la dirección "10.90.90.81" y "10.90.90.82" para el PC 1 y el PC 2 respectivamente. Por otro lado, el grupo contrario usó direcciones "10.90.90.91" y "10.90.90.92".

Continuando, ya teniendo listas las configuraciones internas se establecieron las conexiones físicas de los switches de tal forma que los PC's quedarán en una misma vlan en sus respectivos switch y luego establecer una conexión con un cable cruzado entre aquellas vlan de distintos switch. En la siguiente imagen se ve el resultado de las conexiones.

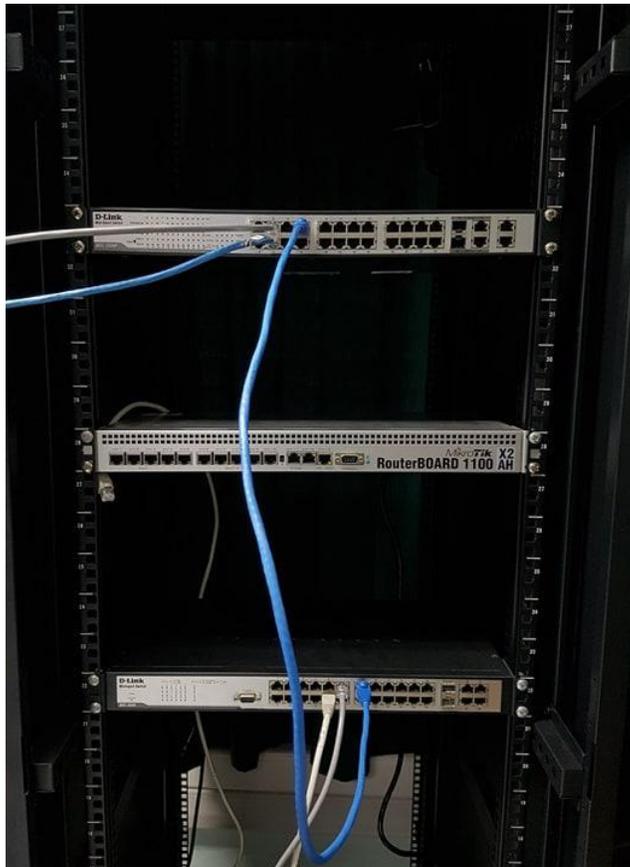


Figura 16. Conexiones entre los switch.

Para un mejor entendimiento, el switch que se posiciona en la parte superior es aquella con dirección “10.90.90.90” y el switch en la parte inferior es la de dirección “10.90.90.80”. Por otro lado, los PC’s “10.90.90.91” y “10.90.90.92” se encuentran en una misma Vlan de su switch (superior), al igual que ocurre con los PC’s “10.90.90.81” y “10.90.90.82” y el objetivo del cable cruzado de color azul es enlazar ambas Vlan de los diferentes switch.

Para comprobar el funcionamiento de las conexiones y configuraciones ya realizadas, se hicieron ping a las distintas máquinas, en primer lugar a las máquinas de una misma vlan en el mismo switch, en este caso entre los PC’s con direcciones IP “10.90.90.81” y “10.90.90.82” obteniendo los resultados mostrados a continuación.

```
C:\Users\Usuario>ping 10.90.90.82

Haciendo ping a 10.90.90.82 con 32 bytes de datos:
Respuesta desde 10.90.90.82: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 10.90.90.82:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

Figura 17. Ping entre máquina de una misma vlan

Al igual que la primera actividad realizada se logró correctamente la conexiones entre ambas máquinas de una misma vlan, a continuación se testeó el ping entre una máquina de la switch contraria, estos son de distintas vlan las cuales que estas últimas están conectadas entre sí por el mismo cable cruzado actuando como puente entre ambas switches.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.10586]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 10.90.90.91

Haciendo ping a 10.90.90.91 con 32 bytes de datos:
Respuesta desde 10.90.90.91: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.90.90.91: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 10.90.90.91:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura 18. Ping entre distintas Vlans

De la misma forma se obtuvieron los resultados esperados, cumpliendo con realizar la Vlan entre dos grupos con diferentes switch.

Por último, se verificaron varios aspectos de esta red como la ruta que toma para llegar de un switch a otro y el tráfico que se encuentra en la misma red, todo con el objetivo de ver cómo es que trabaja la red teniendo este tipo de conexión.

```

Traza a la dirección DESKTOP-VFEP3PA [10.90.90.91]
sobre un máximo de 30 saltos:

 1      1 ms      1 ms      <1 ms  DESKTOP-VFEP3PA [10.90.90.91]

Traza completa.

```

Figura 19. Traceroute desde PC "10.90.90.81" a PC "10.90.90.91"

Como se puede observar el camino que toma la conexión entre una vlan a otra de diferentes switch es simplemente 1 camino, al cual tampoco se demora un tiempo extendido, se podría decir que la conexión es directa ya que como se ve solo toma un camino para llegar a su destino, además esto tiene sentido ya que al tener la conexión con el cable cruzado se toma como si estuvieran dentro una misma vlan todos los PC's que se usaron par esta actividad.

Time	Time	Source	Destination
5	1.164139	fe80::f921:2d1:59a5...	ff02::16
6	1.165693	fe80::f921:2d1:59a5...	ff02::2
7	1.176004	fe80::f921:2d1:59a5...	ff02::16
8	1.238139	fe80::f921:2d1:59a5...	ff02::fb
9	1.265390	fe80::f921:2d1:59a5...	ff02::fb
10	1.489205	fe80::f921:2d1:59a5...	ff02::fb
11	1.612026	fe80::f921:2d1:59a5...	ff02::16
12	1.739925	fe80::f921:2d1:59a5...	ff02::fb
13	1.940566	fe80::f921:2d1:59a5...	ff02::fb
14	2.028015	fe80::f921:2d1:59a5...	ff02::16
15	2.265296	fe80::f921:2d1:59a5...	ff02::fb
16	2.964428	fe80::f921:2d1:59a5...	ff02::fb
17	3.807816	0.0.0.0	255.255.255.255
18	4.266230	fe80::f921:2d1:59a5...	ff02::fb
19	4.341222	D-LinkIn_90:b7:2f	Broadcast
20	4.841734	D-LinkIn_90:b7:2f	Broadcast
21	4.988357	fe80::f921:2d1:59a5...	ff02::fb
22	5.829572	D-LinkIn_90:b7:2f	Broadcast
23	6.743629	0.0.0.0	255.255.255.255
24	7.291059	fe80::4018:3669:173...	ff02::c
25	7.293901	10.90.90.91	239.255.255.250
26	7.352947	D-LinkIn_90:b7:2f	Broadcast
27	7.389438	fe80::4018:3669:173...	ff02::c
28	7.390508	10.90.90.91	239.255.255.250
29	8.269090	fe80::f921:2d1:59a5...	ff02::fb
30	8.337334	D-LinkIn_90:b7:2f	Broadcast

Figura 20. Tráfico de red entre vlan

Junto con la herramienta Wireshark se puede observar que ocurre variados tráficos de red en este tipo de conexiones, además entre ellas se puede apreciar un broadcasts la cual manda un

mensaje a todos los que se encuentran conectados en la red. Ahora por último se realizó nuevamente un ping para ver como actuaba el tráfico de red al realizar dicho comando.

30	8.757754	D-LinkIn_90:07:2f	Broadcast	ARP	42 Who has 10.90.90.80? Tell 10.90.90.81
31	8.751954	10.90.90.81	10.90.90.91	ICMP	74 Echo (ping) request id=0x0001, seq=127/32512, ttl=128 (reply in 32)
32	8.752742	10.90.90.91	10.90.90.81	ICMP	74 Echo (ping) reply id=0x0001, seq=127/32512, ttl=128 (request in 31)
33	9.337441	D-LinkIn_90:b7:2f	Broadcast	ARP	42 Who has 10.90.90.80? Tell 10.90.90.81
34	9.759599	10.90.90.81	10.90.90.91	ICMP	74 Echo (ping) request id=0x0001, seq=128/32768, ttl=128 (reply in 35)
35	9.760524	10.90.90.91	10.90.90.81	ICMP	74 Echo (ping) reply id=0x0001, seq=128/32768, ttl=128 (request in 34)
36	10.778559	10.90.90.81	10.90.90.91	ICMP	74 Echo (ping) request id=0x0001, seq=129/33024, ttl=128 (reply in 37)
37	10.779478	10.90.90.91	10.90.90.81	ICMP	74 Echo (ping) reply id=0x0001, seq=129/33024, ttl=128 (request in 36)
38	11.793214	10.90.90.81	10.90.90.91	ICMP	74 Echo (ping) request id=0x0001, seq=130/33280, ttl=128 (reply in 39)
39	11.794107	10.90.90.91	10.90.90.81	ICMP	74 Echo (ping) reply id=0x0001, seq=130/33280, ttl=128 (request in 38)

Figura 21. Trafico de red al hacer ping a "10.90.90.91"

Ya con este último comando se puede comprobar el funcionamiento de la red al hacer ping entre vlan distintas, pero conectadas entre sí por un cable cruzado actuando así como una sola Vlan. Donde se puede apreciar que el tipo es ICMP y se manda sus respectivos paquetes para establecer la conexión, además cabe destacar que al actuar como una sola Vlan el tiempo de respuesta es casi de inmediato.

CONCLUSIÓN

Para finalizar, las redes son una parte muy importante dentro de la sociedad, porque con ella se agiliza y facilita la comunicación entre distintos usuarios. El haber estudiado y analizado los comandos presentados ayuda a comprender de mejor forma como trabajan las redes, en este laboratorio en específico tuvimos que analizar e implementar redes con nuevos conceptos como la VLAN, Bridges, agregar un RouterBoard, entender por qué haciendo ping se podía establecer la conexión y cuando no. Además de también realizar actividades variadas a ellas como cambiar las computadoras de VLAN, cambiarlas de Bridges, etc.

El conocer los distintos comandos y herramientas aprendidos en asignaturas anteriores realizando talleres y/o laboratorios ha aportado en buen parte al conocimiento y su empleo en la red. Desde un diagnóstico del estado de red, hasta la comprobación de la comunicación entre computadoras. Es importante conocer lo básico acerca del cómo establecer una pequeña red y del cómo estas funcionan. Además de aprender acerca de las distintas herramientas que dispone el Sistema Operativo y terceros como máquinas virtuales, Software de administración, Herramientas de medición, etc.

Además, cabe mencionar que las herramientas estudiadas y utilizadas fueron algo complicadas en su uso o en su comprensión ya que fue nuestra primera experiencia agregando una RouterBoard por ejemplo, pero también fue muy importante su uso ya ayudan a comprender la red que está siendo analizada. Por último, la implementación de un adecuado sistema de redes y la elección de los medios y materiales son factores claves para que todo funcione de la mejor manera posible.

REFERENCIAS

1. Libro “Redes de Computadoras”
 - o James F. Kurose - Keith W. Ross / Quinta edición - Capítulo 5
2. Libro “Comunicacion De Datos, Redes De Computadores Y Sistemas Abiertos”
 - o Fred Halsall / Quinta edición - Capítulo 3
3. Manual de usuario RouterBOARD 1100 Mikrotik
 - o <https://bit.ly/2zKxjil>
2. Canal de “Nestor Cateller” en Youtube / Canal relacionado sobre tecnologías de redes
 - o <https://www.youtube.com/user/necaosdj/videos>

Nota: La estructura y distribución de la tabla de contenido, en su referenciación, tanto del documento general como del índice de figuras en el mismo, se ha basado y seguido según el estándar IEEE 610-12-1990 (“Glossary”). La que provee y muestra una distribución ordenada en la manera de referenciar las figuras y enlazarlas en una tabla de contenido.