UNIVERSIDAD DE TARAPACÁ

FACULTAD UNIVERSITARIA DE INGENIERÍA

Departamento de Ingeniería en Computación e Informática

Laboratorio 1: “VLAN y protocolo 802.1Q”

Autores Mino Burgos
Iván Cardemil
Curso Laboratorio de redes
Profesor Diego Aracena

Arica, 01 de septiembre de 2019.

Tabla de contenidos

1. Introducción

Con el objetivo de poner en práctica nuestro conocimiento adquirido en el área de la comunicación de datos y redes es necesario experimentar con el uso de dispositivos intermedios en ambientes reales (no simulados). Pero antes de cometer la acción descrita, es de importancia estudiar cuales son los protocolos que actúan en la transmisión de información. Para efectos de este laboratorio, se pondrá énfasis en el protocolo 802.1 Q.

Una vez realizado el estudio, el equipo de trabajo deberá realizar la caracterización de los diferentes dispositivos intermedios que están presente en el laboratorio, este paso es necesario, ya que permite descartar a aquellos equipos que no cuentan con los requisitos suficientes para satisfacer los requerimientos relacionados a los casos propuestos en las actividades.

Seleccionado los dispositivos, el equipo deberá realizar las configuraciones solicitadas en el laboratorio y utilizar diversas herramientas para comprobar el correcto flujo de datos y, además, la obtención de mediciones que serán de ayuda a la hora de sacar conclusiones de las experiencias realizadas.

2. Objetivos

2.1. Propósitos del documento

El siguiente documento busca exponer de forma clara y ordenada el resultado de la investigación realizada sobre el protocolo 802.1 Q, y a partir de eso, describir de forma detallada el desarrollo de las actividades propuestas.

2.2. Objetivo general

Investigar sobre el protocolo 802.1 Q y configurar VLANs utilizando los dispositivos intermedios disponibles en el laboratorio, para entender de mejor forma su funcionamiento.

2.3. Objetivos específicos

- Estudiar los aspectos teóricos del protocolo 802.1 Q y el método de VLAN.
- Investigar y caracterizar los dispositivos medios a utilizar.
- Diseñar la topología de la red a armar.
- Armar y configurar la red con los dispositivos del laboratorio.
- Asociar los resultados obtenidos con el contenido teórico.

3. Desarrollo

3.1. Marco teórico

3.1.1. ¿Qué son las VLANS?

Las VLAN son una tecnología que permite segmentar la red de manera lógica. Actúa a nivel de la capa 2 (enlace de datos) del modelo OSI.

El hecho de segmentar la red, es de utilidad para garantizar la igualdad de características en el ámbito de la seguridad y el ancho de banda. Además, permite dar solución al problema que nace a partir de la expansión de las organizaciones que poseen un sistema de red interno, ya que el administrador de red podrá crear grupos de dispositivos conectados a la red de forma lógica que actúan como si estuvieran en una red independiente.

Las VLAN se pueden clasificar de la siguiente forma:

- Por puerto: en esta configuración el administrador de red debe especificar cuáles son los puertos que pertenecerán a cada VLAN, por lo que los miembros de cada VLAN solo tendrán acceso a ella si es que están conectados en el puerto apropiado. Esto generará un inconveniente, y es que si un miembro desea moverse (físicamente) se deberá reconfigurar la VLAN.
- Por direcciones MAC: Se asignan los hosts de la VLAN en función de la dirección MAC. A diferencia de la clasificación por puertos, si el usuario cambia de localización, no se debe configurar nuevamente la VLAN. La desventaja es que la asignación de host se debe realizar uno a uno.
- Por protocolo.
- Por direcciones de subred.
- Por niveles superiores.

3.1.2. Protocolo 802.1 Q

Es un protocolo que emplea un mecanismo que permite a múltiples redes compartir el mismo medio físico, sin problemas entre ellas.

El protocolo propone añadir 4 bytes al encabezado Ethernet original en lugar de encapsular la trama original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

Como se puede apreciar en la siguiente figura, la VLAN tag se inserta en la trama entre el campo longitud y dirección fuente. Los primeros dos contienen el tipo de tag y los dos últimos poseen:

- Los primeros 3 bits corresponde a el nivel de prioridad.
- El siguiente bit posee el campo Canonical Format Indicator (CFI) usado para indicar la presencia de un campo Routing Information Field (RIF).
- El resto de bits son el VLAN Identifier (VID) que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.

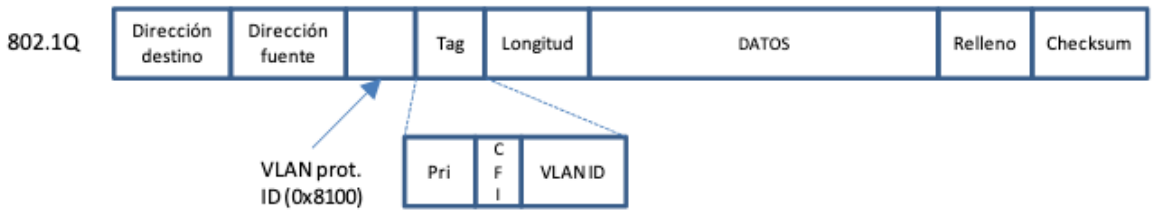


Ilustración 1 Representación de la trama. Fuente: Universitat Politecnica de Valencia.

3.2. VLAN Switch

3.2.1. Descripción del Switch utilizado

Para realizar la experiencia, el equipo utilizó el Switch de marca D-Link de serie DES-3526 que posee las siguientes características:

Tabla 1 Caracterización de Switch utilizado.

Nombre	DES-3526
Sub-tipo	Fast Ethernet
Puertos	24 puertos Fast Ethernet 2 puertos Gigabit
RAM	16 MB
Fabricante	D-Link

3.2.2. Topología de la red

En el desarrollo de la actividad el equipo diseñó la red que se puede apreciar en la siguiente figura. La red está compuesta por un Switch DES-3526 con soporte del protocolo 802.1Q y dos hosts cuyo sistema operativo es Windows 10. Para conectar los dispositivos se utilizaron cables de par trenzado directos.

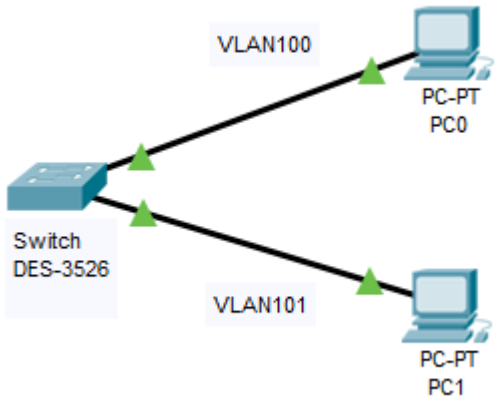


Ilustración 2 Diseño de la red armada. Elaboración propia.

En la siguiente tabla se puede muestra la dirección IPv4 asignada de forma estática a cada Host.

Tabla 2 Dirección IP de cada host

Identificación del Host	Dirección IPv4
PC0	10.90.90.91
PC1	10.90.90.93

3.2.3. Configuración de VLAN

Para realizar la configuración de la VLAN fue necesario conectar uno de los hosts a un puerto del Switch. A continuación, se debió cambiar la configuración de las propiedades del protocolo IPv4 en el host, con el objetivo de ingresar a la interfaz web del Switch. En la siguiente figura se puede apreciar la configuración utilizada por el equipo:

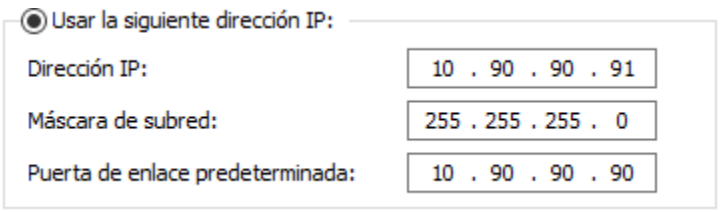


Ilustración 3 Configuración del host

En la interfaz web del Switch, se crearon las VLAN a partir de lo solicitado en el laboratorio, por lo que se realizó la configuración de la siguiente tabla:

Tabla 3 Asignación de puertos VLAN

VLAN	Puertos
VLAN 100	1, 2, 5 y 6
VLAN 101	3, 4, 7 y 8

Una vez dentro de la interfaz web de configuración del Switch, se presenta el siguiente resumen, que nos permite modificar elementos como la IP del dispositivo, la máscara de red, la puerta de enlace predeterminada, entre otros.

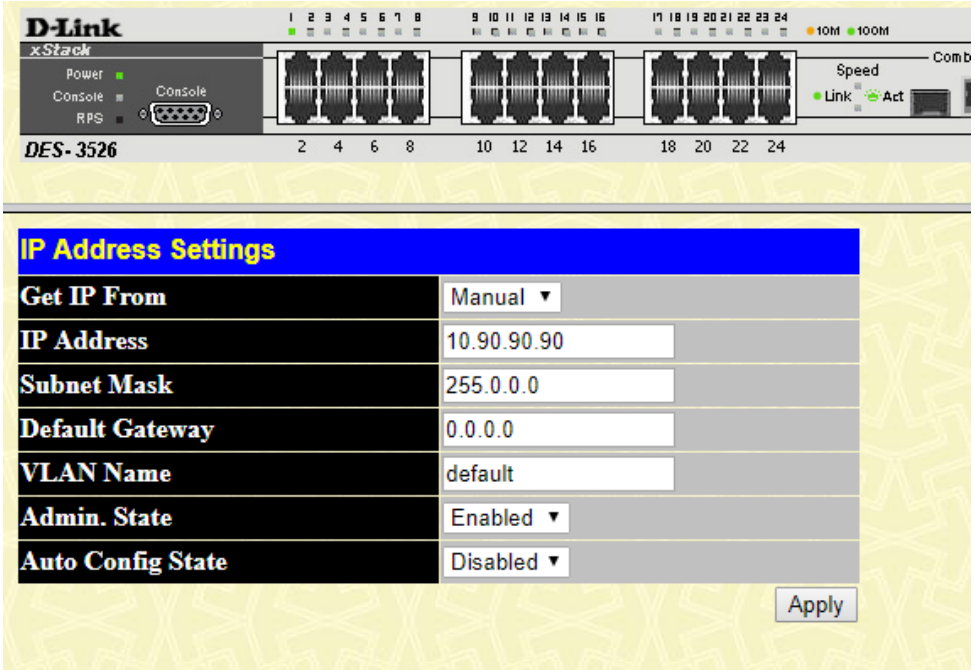


Ilustración 4 Interfaz de ajustes de dirección de Switch

En el menú de configuración se debe ingresar a la sección de VLANs. En esta sección se obtiene una lista de las entradas VLANs creadas con anterioridad, donde podremos modificarlas o eliminarlas (a excepción de la VLAN por default). También está la opción de crear una nueva VLAN, que será la opción que utilizaremos para continuar con el laboratorio.

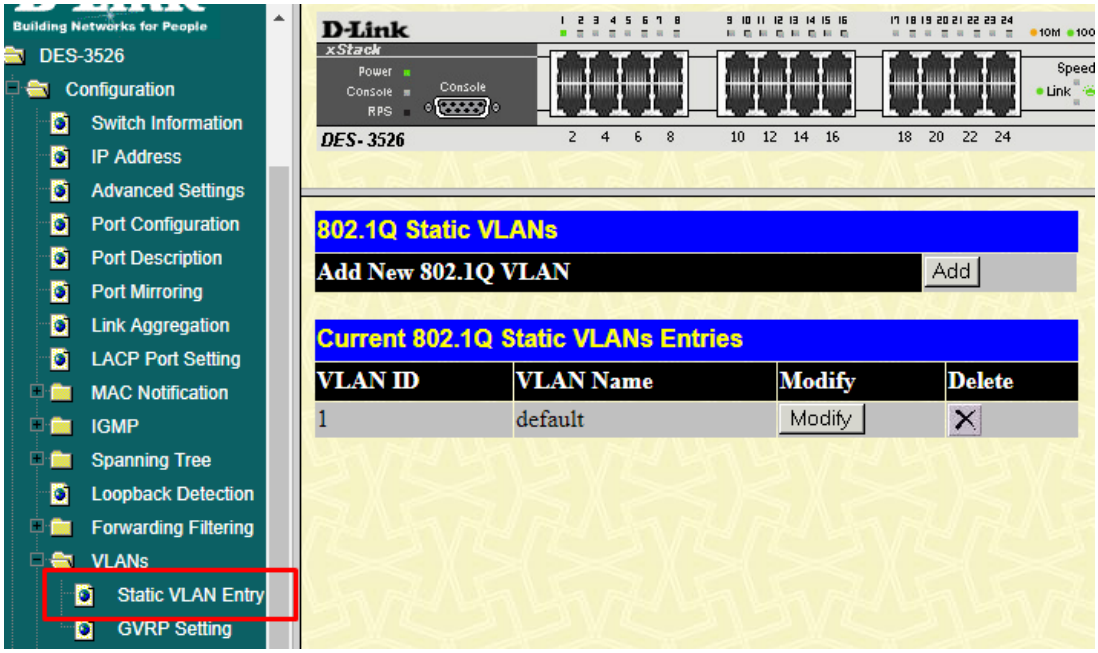


Ilustración 5 Interfaz de gestión de VLAN

Seleccionada la opción de agregar una VLAN, deberemos ingresar una identificación y un nombre. Luego, podremos seleccionar qué puertos van a formar parte de la VLAN.
Para lograr esto se deben cumplir con dos condiciones:

- El puerto no debe ser utilizado por alguna VLAN creada con anterioridad.
- El puerto que se va a utilizar debe tener marcada la casilla de Egress.

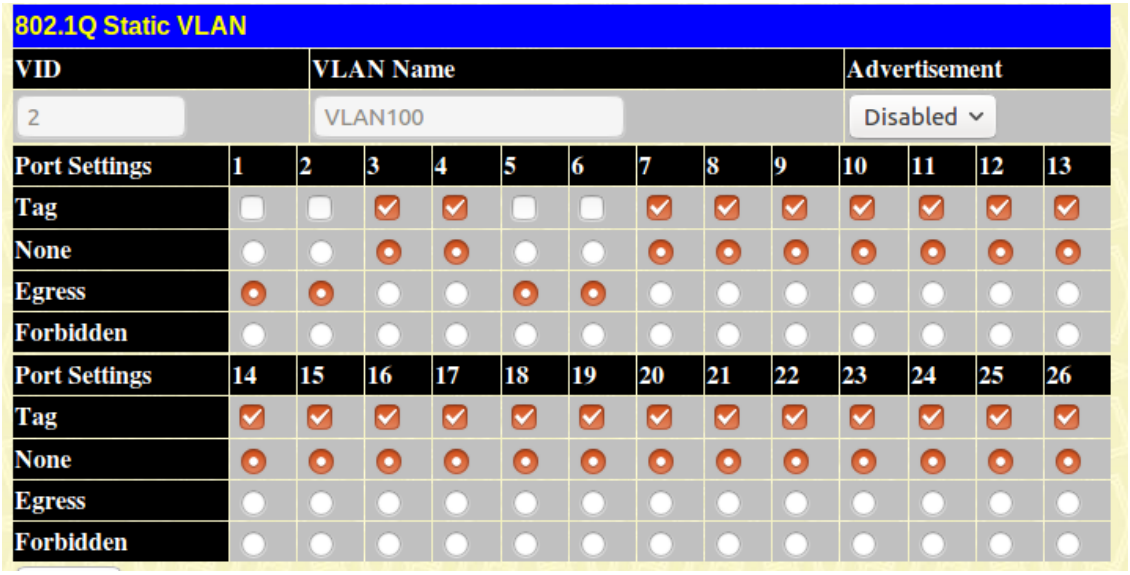


Ilustración 6 Proceso de creación de la VLAN 100

3.2.4. Pruebas de conectividad

3.2.4.1. Equipos en una misma VLAN

Para probar el funcionamiento de la red se realizó un ping entre host, lo que demostró que la red creada está funcionamiento como corresponde. Esto se puede observar en la siguiente figura, ya que el resumen de la consola arroja que los cuatro paquetes enviados al host de destino fueron recibidos de forma satisfactoria. Además, la figura presenta la configuración de red del host emisor (PC0) de los paquetes.

```
Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::616f:b794:ac64:46c7%16
   Dirección IPv4. . . . . . . . . . . . . . : 10.90.90.91
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.90.90.90

Adaptador de LAN inalámbrica Wi-Fi:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

C:\Users\mipc>ping 10.90.90.93

Haciendo ping a 10.90.90.93 con 32 bytes de datos:
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.90.93:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ilustración 7 Ping desde PC0 hacia PC1

Como prueba de conectividad adicional, se utilizó el comando tracert que determinar la ruta que toma un paquete de protocolo de Internet (IP) para alcanzar su destino. En este caso se realizó desde el host PC1 hacia el PC0. Como se puede apreciar en la figura, la transmisión del paquete solo le toma un salto para llegar al host destino, y es que el Switch, que es dispositivo que permite la conectividad entre los host, no aparece en el resumen del comando, y eso se debe a que el Switch trabaja en la capa 2 (enlace de datos), mientras que el comando sigue a los paquetes que fluyen por la capa 3 (capa de red).

```
Traza a la dirección MINO-NOTE [10.90.90.91]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  MINO-NOTE [10.90.90.91]

Traza completa.
```

Ilustración 8 Traza entre PC1 a PC0

3.2.4.2. Equipos en distintas VLAN

3.2.4.2.1. Sin troncal

Una de las pruebas que se realizó, fue el de hacer ping desde un host (PC0) en la VLAN 100 a otro host (PC1) ubicado en la VLAN 101. Como se puede observar en la siguiente figura, el host destino queda en un estado inaccesible. Esto se debe principalmente, a que al momento de segmentar la red no existe un vínculo troncal que permita que los hosts de ambas redes puedan interactuar, es por eso que, al momento de realizar un envío de paquetes, estos no puedan llegar a destino.

```
Adaptador de Ethernet Ethernet 2:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::616f:b794:ac64:46c7%16
   Dirección IPv4. . . . . . . . . . . . : 10.90.90.91
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.90.90.90

Adaptador de LAN inalámbrica Wi-Fi:

   Estado de los medios. . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

C:\Users\mipc>ping 10.90.90.93

Haciendo ping a 10.90.90.93 con 32 bytes de datos:
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.
```

Ilustración 9 Ping con Host inaccesible

3.2.4.2.2. Con troncal

Para abordar el problema del punto anterior, el equipo de trabajo debió integrar un vínculo entre las redes, es por eso que conectó un cable directo entre dos puertos pertenecientes a cada una de las VLAN.

En la siguiente figura se puede apreciar la configuración realizada por el equipo, donde los cables que se presentan con color verde pertenecen a la VLAN 100 y los cables de color azul corresponden a la VLAN 101. Finalmente, el cable de color rojo es el troncal utilizado para conectar a las VLAN que se encuentran conectados a los puertos 2 (VLAN 100) y 8 (VLAN 101).

Ilustración 10 Agregando el troncal en las VLAN

Para comprobar si la conexión propuesta permite la conectividad entre los dispositivos, se realizó un ping entre los dispositivos que se encuentran entre distintas VLAN.

```
C:\Users\mipc>ping 10.90.90.93

Haciendo ping a 10.90.90.93 con 32 bytes de datos:
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.90.93:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Ilustración 11 Comprobación de la conectividad con el troncal

Como prueba adicional se realizó un pathping. Este comando combinado las funcionalidades de el comando ping y tracert. Por lo que realiza una transmisión de paquetes entre un host emisor a un host destino y, además, realiza un trazado de los paquetes enviados por la red. Por lo tanto, como se puede apreciar en la siguiente imagen, solo le tomó un salto al paquete llegar hasta el host destino. Además, se puede observar que un 100% de los paquetes fueron enviados.

```
C:\Users\mipc>pathping 10.90.90.93

Seguimiento de ruta a DESKTOP-6KUH5S4 [10.90.90.93]
sobre un máximo de 30 saltos:
  0  Mino-Note [10.90.90.91]
  1  DESKTOP-6KUH5S4 [10.90.90.93]

Procesamiento de estadísticas durante 25 segundos...
             Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                          Mino-Note [10.90.90.91]
                               0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  DESKTOP-6KUH5S4 [10.90.90.93]
```

Ilustración 12 Pathping para comprobar conexión y obtener la traza

3.3. VLAN Router

3.3.1. Descripción del Router utilizado

Para continuar con la experiencia fue necesario cambiar el Switch por un MikroTik RouterBoard RB1100AHx2 que posee las siguientes características:

Tabla 4 Caracterización del RouterBoard

Nombre	RouterBoard RB1100AHx2
Sistema operativo	RouterOS
Puertos	13 puertos Fast Ethernet
RAM	1 GB
Almacenamiento	128 MB
Fabricante	MikroTik

3.3.2. Topología de la Red

Al igual que en la topografía anterior, se tienen dos hosts con Windows 10, pero en este caso, es reemplazado el Switch por un RouterBoard 1100, por lo que se tiene la siguiente topografía.

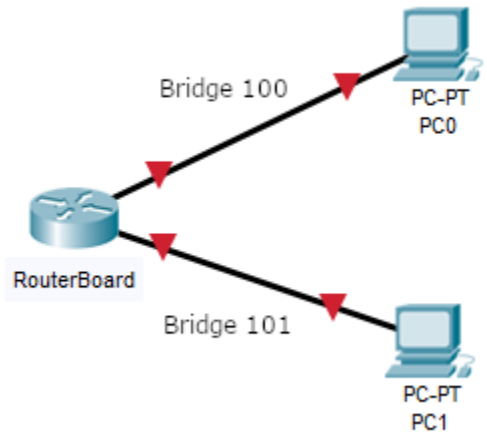


Ilustración 13 Diseño de la red armada. Elaboración propia.

Tabla 5 Dirección IP de cada host

Identificación de Host	Dirección IPv4
PC0	10.90.90.91
PC1	10.90.90.93

3.3.3. Configuración de VLAN

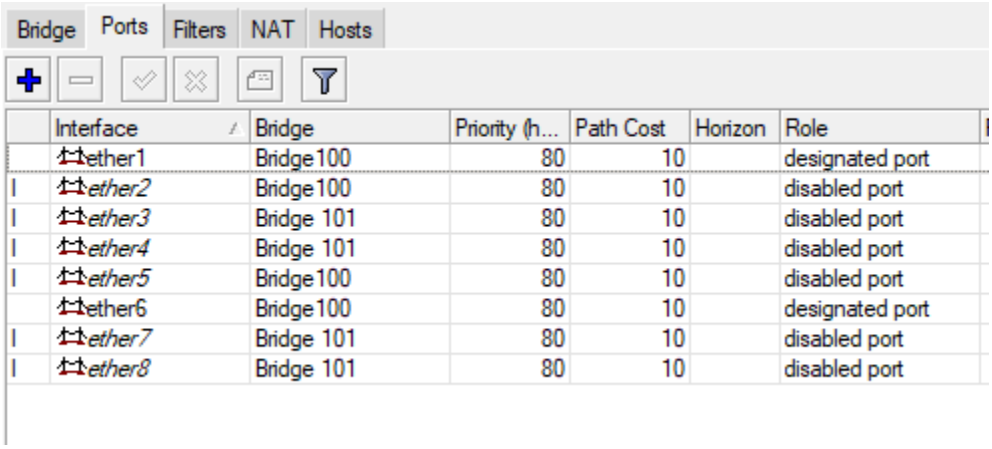
Para realizar la configuración es necesario conectar un puerto del RouterBoard a un host con un cable directo. Para acceder a la interfaz de configuración del dispositivo intermedio se utilizó el programa Winbox. Esta herramienta permite realizar configuraciones a través de una interfaz gráfica amigable para los usuarios.

Antes de crear las VLAN 100 y 101, se debieron crear los puentes de red o bridge, que nos permitirá segmentar la red en dos grupos de interfaces, tal como se muestra en la siguiente tabla:

Tabla 6 Asignación de cada puerto a los Bridge

Bridge	Puertos
Bridge 100	1, 2, 5 y 6
Bridge 101	3, 4, 7 y 8

De la anterior tabla se realizó la configuración en el RouterBoard que se puede apreciar en la siguiente figura, donde destaca el campo de Interface que corresponde al puerto ethernet asociado a uno de los Bridge; el campo Bridge nos ayuda a identificar el puente de red que se está utilizando; finalmente el campo Role nos revela cuales son los puertos que están siendo utilizados, en el caso de la actividad realizada, el equipo utilizó el puerto uno y seis.



Interface	Bridge	Priority (h...	Path Cost	Horizon	Role
ether1	Bridge100	80	10		designated port
ether2	Bridge100	80	10		disabled port
ether3	Bridge 101	80	10		disabled port
ether4	Bridge 101	80	10		disabled port
ether5	Bridge100	80	10		disabled port
ether6	Bridge100	80	10		designated port
ether7	Bridge 101	80	10		disabled port
ether8	Bridge 101	80	10		disabled port

Ilustración 14 Asignación de los puertos en el RouterBoard

A continuación, se crearon las VLAN 100 y 101, cuya interfaz se debió asociar a los Bridge creados con anterioridad.

Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	VLAN ID	Interface
VLAN100	VLAN	1500	1594	0 bps	0 bps	0	0	1	Bridge100
VLAN101	VLAN	1500	1594	0 bps	0 bps	0	0	2	Bridge 101

Ilustración 15 Creación de las VLAN y asignación de los Bridge

3.3.4. Pruebas de conectividad

3.3.4.1. Equipos en una misma VLAN

De forma análoga a la actividad anterior con el Switch, se realizó un ping desde el PC0 hacia el PC1 para comprobar la conectividad. Como se muestra en la figura, los paquetes son enviados y recibidos de forma satisfactoria, por lo que queda demostrado la conectividad entre los hosts.

```
C:\Users\mipc>ping 10.90.90.93

Haciendo ping a 10.90.90.93 con 32 bytes de datos:
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.90.90.93: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.90.90.93:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ilustración 16 Pruebas de conectividad entre host

También se realizó el análisis utilizando la herramienta de wireshark, donde se puede observar de mejor forma el intercambio de paquetes entre los hosts. La siguiente figura ayuda a comprobar el correcto funcionamiento de la red creada.

Time	Source	Destination	Protocol	Length	Info
4.860767	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=373/29953, ttl=128 (reply in 8)
4.861434	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=373/29953, ttl=128 (request in 7)
5.865880	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=374/30209, ttl=128 (reply in 12)
5.866820	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=374/30209, ttl=128 (request in 11)
6.871796	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=375/30465, ttl=128 (reply in 15)
6.872338	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=375/30465, ttl=128 (request in 14)
7.885224	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=376/30721, ttl=128 (reply in 18)
7.885737	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=376/30721, ttl=128 (request in 17)

Ilustración 17 Análisis de los pings enviados con Wireshark

3.3.4.2. Equipos en distintas VLAN

3.3.4.2.1. Sin troncal

En esta parte de la actividad, se realizó una prueba de conectividad entre dispositivos finales que se encuentran en distintas VLANS. Esto se puede apreciar en la siguiente figura, donde el PC0 se encuentra conectado al puerto número 1, que está asociado a la VLAN 100 y el PC1 se encuentra en el puerto número 4, asociado a la VLAN 101

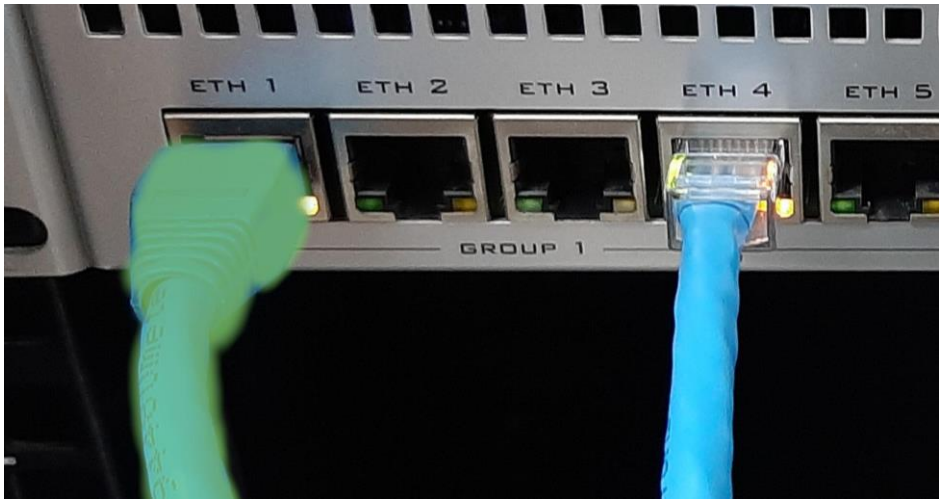


Ilustración 18 Host conectados en distintas VLAN

Descrito el escenario, se procedió a realizar un envío de paquetes desde el PC0 ubicado en la VLAN 100 hacia el PC1 que se encuentra en la VLAN 101, y como se puede apreciar en la figura que enseña el resultado del comando ejecutado en consola, no se pudo acceder al host de destino (PC1). Esto se debe a la ausencia de algún medio que permita establecer la conexión entre ambas redes.

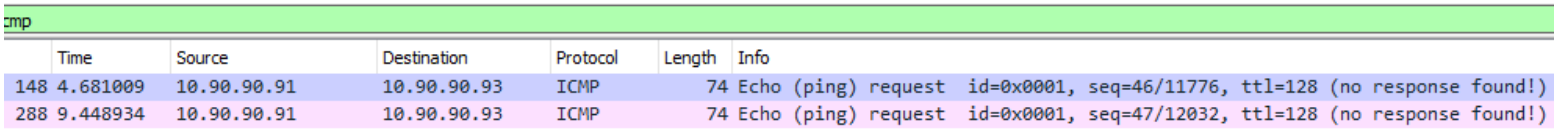
```
C:\Users\mipc>ping 10.90.90.93

Haciendo ping a 10.90.90.93 con 32 bytes de datos:
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.
Respuesta desde 10.90.90.91: Host de destino inaccesible.

Estadísticas de ping para 10.90.90.93:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

Ilustración 19 Prueba de conectividad en distintas VLAN

Realizando el análisis de Wireshark, también se obtiene un mensaje de “no respuesta” al momento de enviar los paquetes al host destino.



cmp

	Time	Source	Destination	Protocol	Length	Info
148	4.681009	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (no response found!)
288	9.448934	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (no response found!)

Ilustración 20 Análisis de los paquetes enviado

3.3.4.2.2. Con troncal

Como se mencionó en el punto anterior, para solucionar problema de conectividad se debió conectar un cable directo en un puerto de cada VLAN, para establecer la conexión que permita el correcto envío/recepción de paquetes. En este caso se conectó el cable que hará de troncal en los puertos 6 y 8. En la siguiente figura se puede observar cómo quedó la configuración en el RouterBoard, donde la VLAN 100 es representada con el color verde, la VLAN 101 con el azul y el cable troncal con el color rojo.

Ilustración 21 Adición de cable troncal entre las VLAN

El siguiente paso fue el de comprobar la conectividad entre los dispositivos, por lo que se realizó un pathping entre el Host que se encuentra en la VLAN 101 hacia el otro host ubicado en la VLAN 100.

```
C:\Users\AICI>pathping 10.90.90.91

Seguimiento de ruta a MINO-NOTE [10.90.90.91]
sobre un máximo de 30 saltos:
  0  DESKTOP-6KUH5S4 [10.90.90.93]
  1  MINO-NOTE [10.90.90.91]

Procesamiento de estadísticas durante 25 segundos...
             Origen hasta aquí   Este Nodo/Vínculo
Salto  RTT    Perdido/Enviado = Pct  Perdido/Enviado = Pct  Dirección
  0                                            DESKTOP-6KUH5S4 [10.90.90.93]
                               0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  MINO-NOTE [10.90.90.91]

Traza completa.
```

Ilustración 22 Pathping entre hosts

Finalmente, se utilizó la herramienta de wireshark para analizar el flujo de los paquetes entre los hosts que se encuentran en diferentes VLAN. Gracias a la incorporación del troncal, la conexión entre host se pudo realizar de forma correcta. Lamentablemente, no se pudo identificar el cabezal que agrega el protocolo 802.1 Q, por lo que se perdió la posibilidad de obtener más información de los paquetes, como, por ejemplo, el identificador único de la VLAN (VID).

Time	Source	Destination	Protocol	Length	Info
3.987333	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=69/17664, ttl=128 (reply in 122)
3.987755	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=69/17664, ttl=128 (request in 121)
4.991171	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (reply in 153)
4.991690	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=70/17920, ttl=128 (request in 152)
5.998227	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 183)
5.998660	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=128 (request in 182)
7.005718	10.90.90.91	10.90.90.93	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (reply in 217)
7.006121	10.90.90.93	10.90.90.91	ICMP	74	Echo (ping) reply id=0x0001, seq=72/18432, ttl=128 (request in 216)

Ilustración 23 Análisis del intercambio de paquetes

3.4. VLAN Curso

3.4.1. Descripción de los dispositivos utilizados

En esta última experiencia debimos coordinarnos con otro grupo para crear una red curso. La red se compuso de cuatro hosts con Windows 10 y dos Switch DES-3526, ya que estos eran los que estaban disponibles en nuestro rack, además de tener el protocolo 802.1Q.

3.4.2. Topología de la red

Para lograr la comunicación entre las redes, se tuvo que conectar ambos Switch con un cable directo en un puerto que esté dentro de cualquiera de las VLAN creada en las anteriores experiencias.

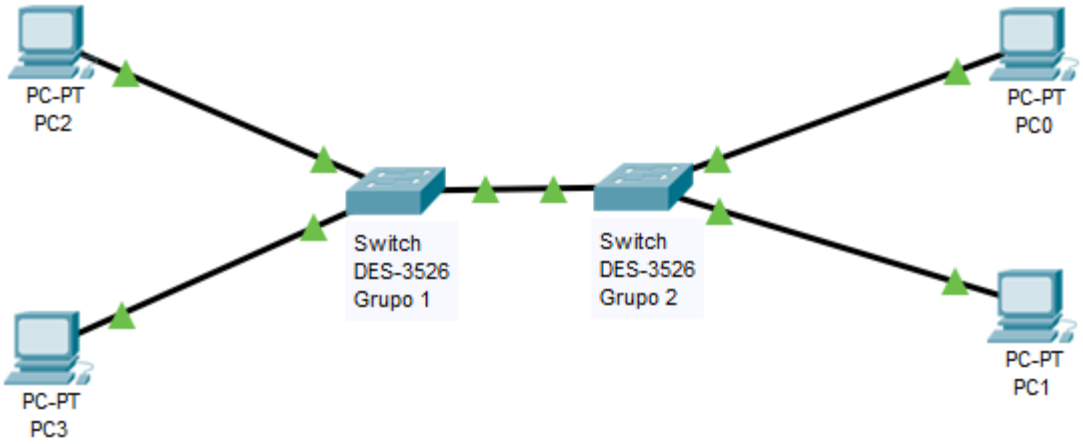


Ilustración 24 Diseño de la red curso

Las direcciones IPv4 asociadas a cada host fueron las siguientes:

Tabla 7 Distribución de direcciones y redes de los hosts.

Grupo	Identificación de Host	Dirección IPv4	VLAN
Grupo 2	PC0	10.90.90.91	100
Grupo 2	PC1	10.90.90.93	101
Grupo 1	PC2	10.90.90.132	100
Grupo 1	PC3	10.90.90.92	101

Un aspecto a tomar en cuenta de esta actividad, es que al momento de crear la VLAN curso, ambos grupos tenían creadas sus respectivas VLAN 100 y 101, además de haber realizada la respectiva conexión con el cable directo como troncal. Esto provocó que todos los hosts puedan interactuar entre sí, a pesar de estar enrolados en VLAN distintas. A continuación, en el siguiente punto se mostrarán los resultados de las pruebas de conectividad.

3.4.3. Configuración física

En la siguiente figura se puede apreciar la configuración realizada por el grupo 1, donde se puede distinguir que su VLAN 100 está asociada al puerto número uno (verde), su VLAN 101 está asociada al puerto cuatro (azul) y que posee un troncal capaz de permitir la comunicación entre host en distintas VLAN. Además, se tiene presente el cable (amarillo) que permite la conectividad entre las redes de cada grupo, cabe mencionar que este cable directo se encuentra conectado en el puerto cinco que es parte de la VLAN 100.

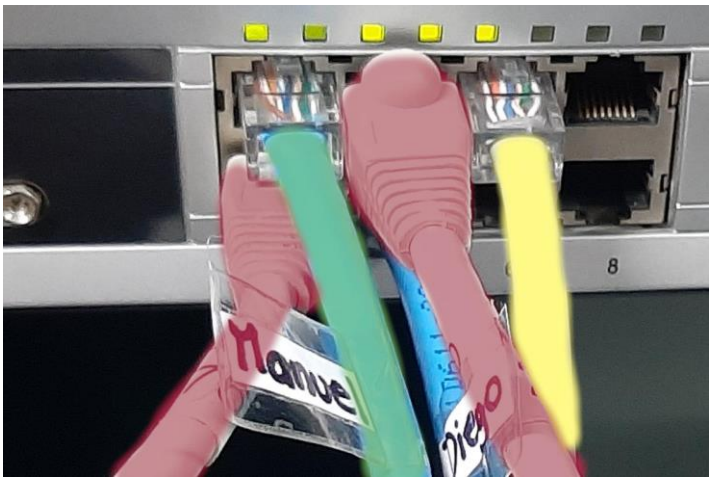


Ilustración 25 Configuración de grupo 1

Continuando con las configuraciones, la siguiente figura describe la realizada por el grupo 2, donde se destaca que el cable encargado de comunicar a las dos redes, también se encuentra en el puerto número cinco, por lo que también sería parte de la VLAN 100.

Ilustración 26 Configuración de grupo 2

Como la configuración de cada grupo cuenta con un cable troncal, esto permitió la comunicación entre host que se encuentran en distintas VLAN de cada dispositivo.

3.4.4. Pruebas de conectividad

Como primera prueba se realizará un ping desde el PC0 del grupo 2 que se encuentra en la VLAN 100, hacia el PC2 que también se ubica en VLAN 100 de su respectivo Switch. Entonces, de la siguiente figura se puede apreciar el correcto funcionamiento de la red, ya que el envío de paquetes se realiza de forma satisfactoria.

Algo interesante que se puede desprender de la siguiente medición es que el tiempo de vida de los paquetes enviados se reducen a la mitad. Esto se contrasta con lo registrado en el escenario donde ocurre el intercambio entre dos hosts conectados en el mismo Switch.

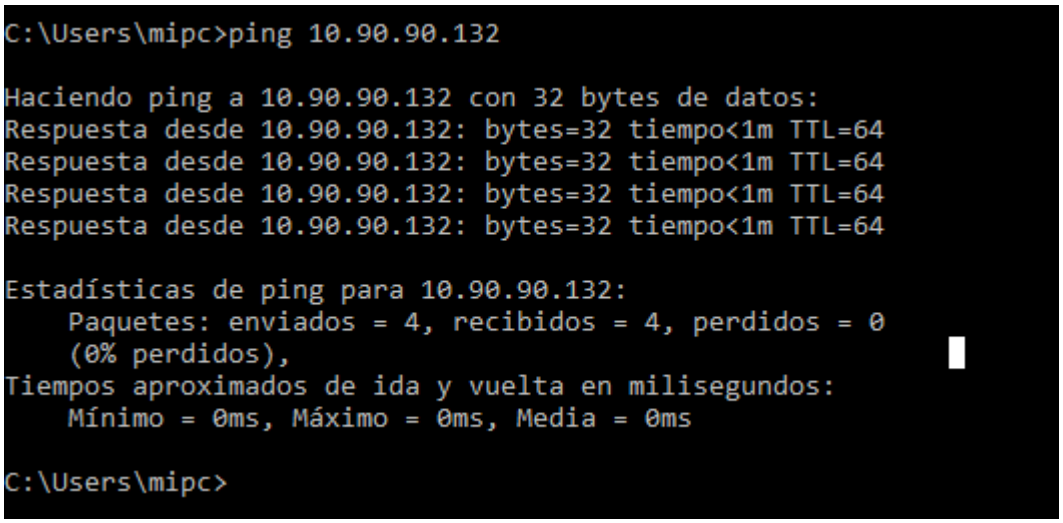


Ilustración 27 Comprobación de conectividad entre redes

4. Conclusiones

En conclusión, de acuerdo a las actividades de investigación y experimentación realizadas, se pudo determinar la importancia de realizar configuraciones de acuerdo a las necesidades de las organizaciones con la finalidad de conservar la integridad y seguridad del flujo de datos, por lo que el uso de técnicas como el VLAN son muy importantes de abordar. Otro punto clave, es la implementación de mecanismos que permitan compartir los dispositivos intermedios de transmisión, por lo que es necesario el estudio y aplicación de protocolos como el 802.1 Q.

Abordando la experiencia práctica del laboratorio, se pudo comprobar los aspectos teóricos que se estudiaron en la primera parte de la actividad, por ejemplo, el intento de comunicación entre host que se encuentren en distintas VLAN sin troncal, donde utilizó herramientas como Wireshark para realizar análisis sobre el no flujo de paquetes. También, se puso en práctica el mecanismo que permitiría el intercambio de paquetes entre host que están en distintas VLAN.

Como actividad complementaria, se diseñó y armó una VLAN curso donde se segmentó la red en dos partes y en dos Switch distintos, y por medio de envío de pings se puedo comprobar su correcto funcionamiento.

Para finalizar, en el desarrollo del laboratorio logramos comprender el cómo es trabajar con instrumentos manufacturados por distintas compañías, lo que nos permite obtener una experiencia más cercana a la que nos podríamos enfrentar en nuestro futuro entorno laboral.

5. Referencias

- EcuRed. 2019. VLAN.
- ServerFault. 2013. Is it possible to include switches in traceroute hops?.
- Universitat Politécnica de Valencia. 2019. Características y configuración básica de VLANs.
- D-Link. 2005. Manual de usuario DES-3526.
- MikroTik. Año. Especificación de RouterBoard RB1100AHx2.