

## LABORATORIO 1

1. Implemente la siguiente topología en Packet Tracer. Garantice conectividad completa entre los computadores conectados. No configure VLAN.

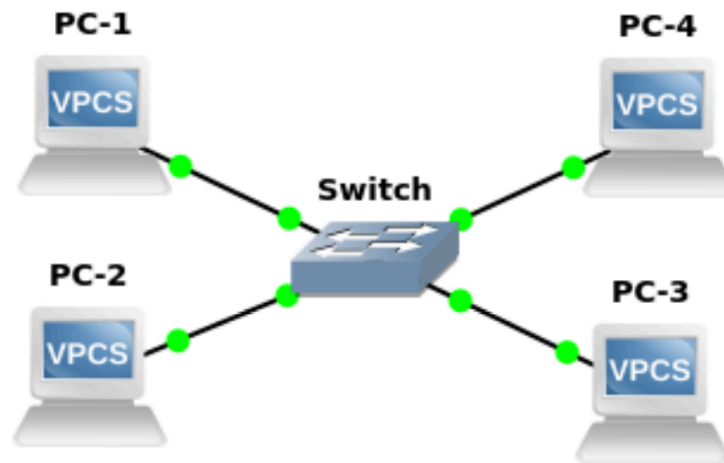


Figure 1: Topología packettracer

- a. Determine la red y las direcciones IP a utilizar

192.168.0.0/24 → Dirección de red  
192.168.0.1 → PC1  
192.168.0.2 → PC2  
192.168.0.3 → PC3  
192.168.0.4 → PC4  
192.168.0.255 → Dirección de broadcast

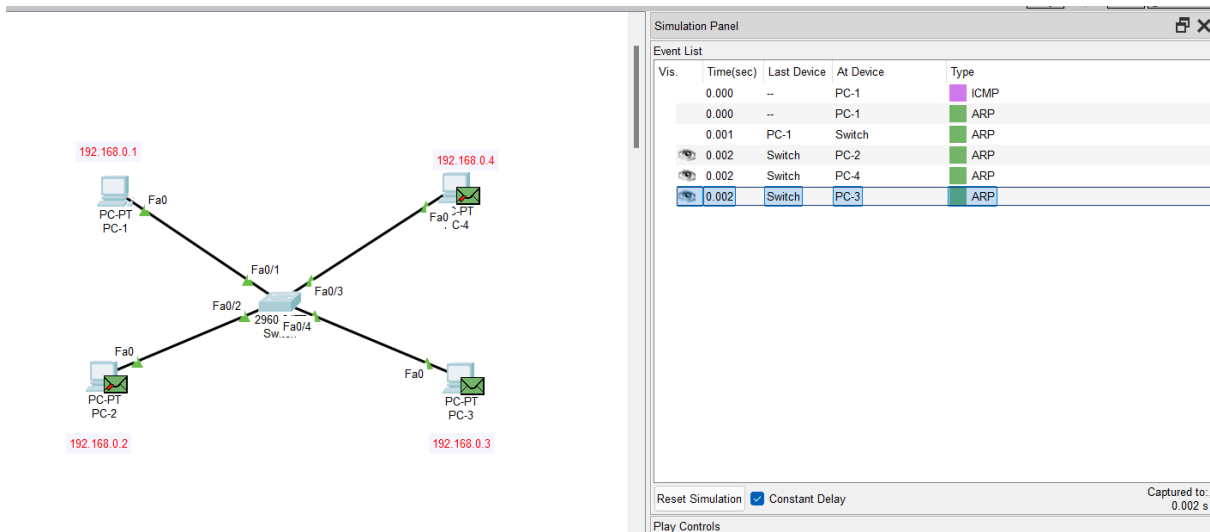
- b. Explique el proceso completo que se realiza, incluyendo los procedimientos en capa 2 (enlace; acceso al medio) y capa 3 (red; que la información llegue de la fuente al destino sin problemas), al generar un ping de un computador a otro.

Se genera una petición desde PC1 que tiene como destino PC3, la tabla de direcciones MAC está vacía en el switch, por lo que este no conoce qué equipo está en qué enlace.

```
Switch>show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -

```

Tras realizar el ping, el switch envía el paquete a todos los equipos (ya que no conoce el equipo con la MAC destino) y solo lo acepta el equipo a quien va dirigido.



En este momento solo se conoce la dirección MAC de PC1.

PC3 devuelve la petición a PC1 a través del switch y este como ya tiene a PC1 en su tabla, lo redirige sin problemas. La dirección MAC de PC3 queda registrada en la tabla en este momento.

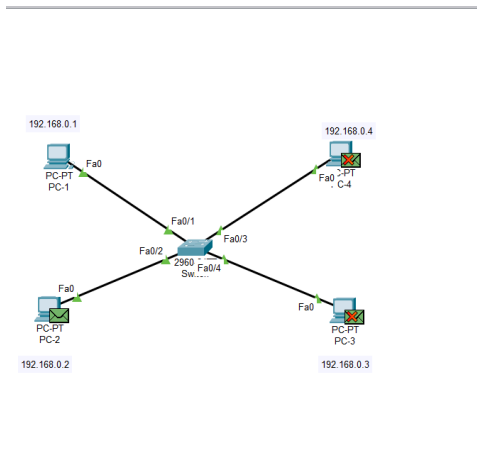
Vlan	Mac Address	Type	Ports
1	0005.5eaa.2a92	DYNAMIC	Fa0/4
1	00e0.a357.ad33	DYNAMIC	Fa0/1

- Reinicie el conmutador y explique, paso a paso, cómo se llena la tabla de correspondencia entre direcciones MAC y puerto del conmutador. Para esto genere tráfico desde un computador a otro y revise inmediatamente la tabla. Repita este procedimiento hasta que se completen todas las entradas posibles de la tabla.

Se reinicia la tabla de direcciones MAC con el comando clear mac address-table.

```
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----
1       0000.0000.0000   DYNAMIC Fa0/1
```

Se hace el ping desde PC1 hasta PC2, por lo que la petición viaja desde PC1 hasta el switch, este como no conoce en qué estación está la MAC de destino, inunda con el paquete por todos los puertos.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC-1	ICMP
	0.000	--	PC-1	ARP
	0.001	PC-1	Switch	ARP
	0.002	Switch	PC-2	ARP
	0.002	Switch	PC-4	ARP
	0.002	Switch	PC-3	ARP

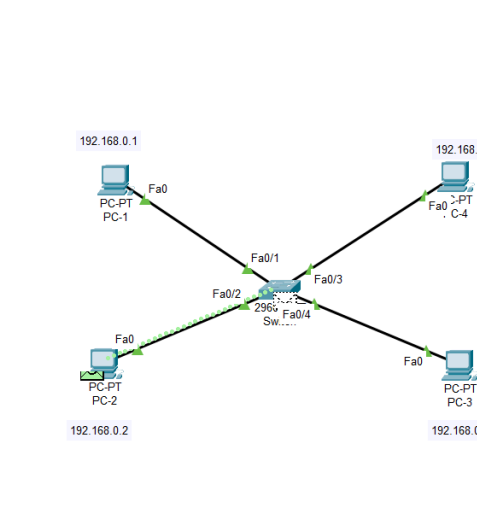
Reset Simulation ☒ Constant Delay Captured to... 0.002 s

Play Controls

Para este punto, en la tabla de direcciones solo está PC1

```
Vlan    Mac Address      Type    Ports
-----
1       00e0.a357.ad33   DYNAMIC Fa0/1
```

Así, PC2 responde el ping, el paquete ya viene desde PC2 hasta el switch, que lo enviará hacia PC1 ya conociendo su dirección MAC.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC-1	ICMP
	0.001	PC-1	Switch	ICMP
	0.002	Switch	PC-2	ICMP
	0.002	Switch	PC-4	ICMP
	0.002	Switch	PC-3	ICMP
	0.003	PC-2	Switch	ICMP
	0.004	Switch	PC-1	ICMP

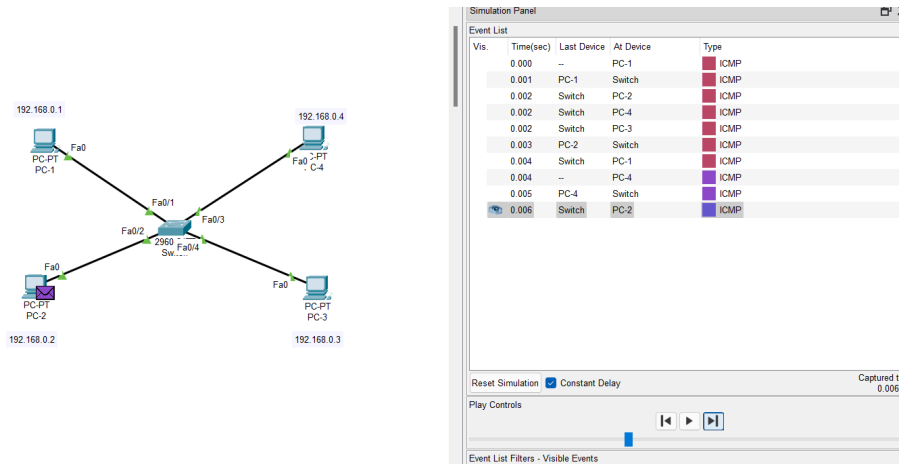
Reset Simulation ☒ Constant Delay Captured to... 0.004 s

Play Controls

De este modo, la dirección MAC de PC2 se agrega a la tabla.

Vlan	Mac Address	Type	Ports
1	0006.2a4e.3b1c	DYNAMIC	Fa0/2
1	00e0.a357.ad33	DYNAMIC	Fa0/1

Ahora, se hará un ping desde PC4 hasta PC2.



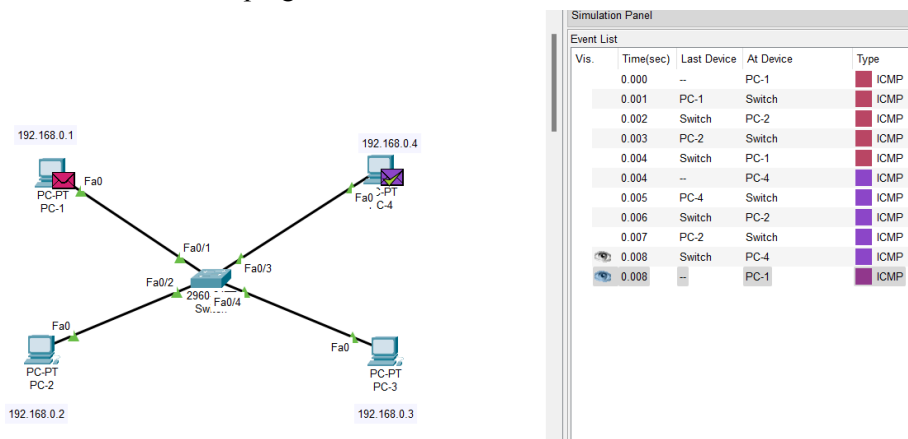
Se envía directamente sin inundar, ya que el switch sabe dónde está el equipo con la MAC de PC2.

La tabla se actualiza con la dirección de PC4.

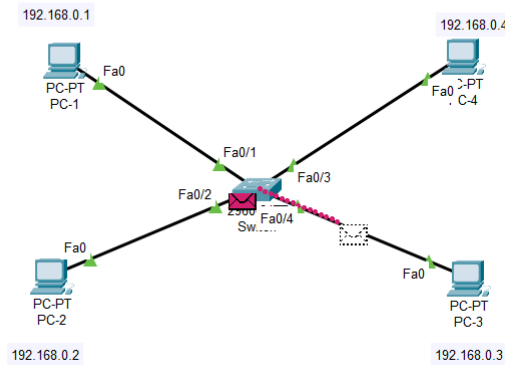
Vlan	Mac Address	Type	Ports
1	0006.2a4e.3b1c	DYNAMIC	Fa0/2
1	00d0.976b.3c42	DYNAMIC	Fa0/3
1	00e0.a357.ad33	DYNAMIC	Fa0/1

Switch#

Finalmente, se hace un ping desde PC1 hasta PC3.



El switch envía el paquete directamente a PC3, ya que sus otros “enlaces” no tienen la MAC de este.



Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC-1	ICMP
	0.001	PC-1	Switch	ICMP
	0.002	Switch	PC-2	ICMP
	0.003	PC-2	Switch	ICMP
	0.004	Switch	PC-1	ICMP
	0.004	--	PC-4	ICMP
	0.005	PC-4	Switch	ICMP
	0.006	Switch	PC-2	ICMP
	0.007	PC-2	Switch	ICMP
	0.008	Switch	PC-4	ICMP
	0.008	--	PC-1	ICMP
	0.009	PC-1	Switch	ICMP
	0.010	Switch	PC-3	ICMP

PC3 responde y se agrega su dirección a la tabla, completándola.

Vlan	Mac Address	Type	Ports
1	0005.5eaa.2a92	DYNAMIC	Fa0/4
1	0006.2a4e.3b1c	DYNAMIC	Fa0/2
1	00d0.976b.3c42	DYNAMIC	Fa0/3
1	00e0.a357.ad33	DYNAMIC	Fa0/1

- d. Explique claramente cómo utiliza el conmutador la tabla mencionada en el punto anterior para facilitar el intercambio de información.

El switch recoge información de los equipos que hacen una primera petición y también recoge la información de quienes responden tras inundar, ya que solo responderá el equipo a quien va dirigido el paquete. Así para una próxima petición, el switch puede descartar aquellos enlaces con direcciones MAC que ya conoce y que no son el destino del paquete.

¿Es posible tener más de una MAC asociada a uno de los puertos? Si la respuesta es afirmativa, señale un escenario donde se pueda presenciar esto.

No tendría sentido que un puerto tenga más de una MAC, pues esta hace referencia a un código único de cada equipo o estación y tener dos equipos conectados a un mismo puerto entorpece o inhibe la comunicación.

¿Es posible tener una misma MAC asociada a dos puertos diferentes del conmutador?

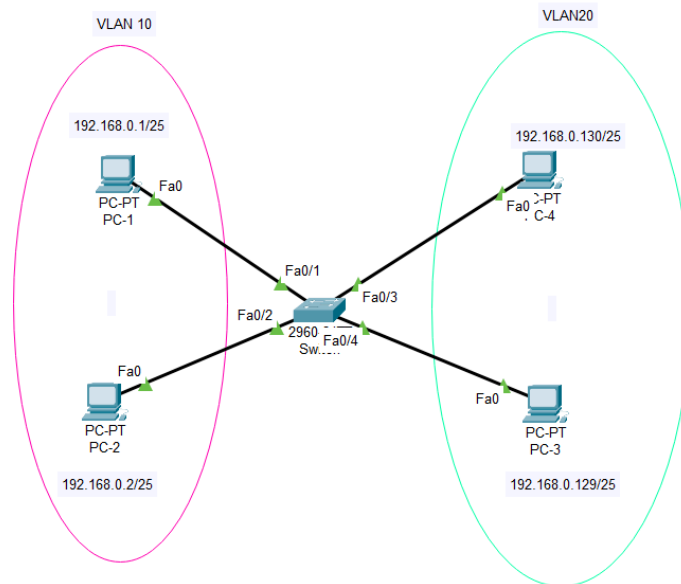
Indique, si es posible, una situación donde se pueda evidenciar esto.

No, ya que generaría problemas al momento de recibir o enviar información, pues el switch no sabría qué puerto tomar y se daría la pérdida de información.

- e. Consulte sobre la posibilidad de asociar una dirección MAC de manera estática a un puerto del conmutador. ¿Cuál es la utilidad de hacer esto?

Establecer de manera manual las direcciones MAC a sus respectivos puertos en un switch permite garantizar seguridad de que ningún otro equipo intente conectarse a la red a través de un puerto del switch.

2. Sobre la topología anterior, cree dos VLAN y asocie dos puertos conectados a cada una de ellas



- a. Determine la(s) red(es) y las direcciones IP a utilizar. ¿Cambia algo respecto al escenario anterior? ¿Por qué?

2 subredes → 1 bit				red 1 para VLAN 10	
192.168.0.0	0000000	→	192.168.0.0/25	255.255.255.128	
192.168.0.1	0000000	→	192.168.0.128/25	255.255.255.128	
128 direcciones = 2 <sup>7</sup>				red 2 para VLAN 20	

VLAN 10

PC1 → 192.168.0.1/25

PC2 → 192.168.0.2/25

VLAN 20









PC3 → 192.168.0.129/25

PC4 → 192.168.0.130/25









Se cambió la máscara, ya que se implementó un bit del cuarto octeto para el subnetting.

- b. Revise la conectividad. Indique qué equipos pueden conectarse y porqué.

La conexión entre equipos de la misma red funciona.

Fire	Last Status	Source	Destination	Type	Color	1
	Successful	PC-1	PC-2	ICMP		
	Successful	PC-4	PC-3	ICMP		
	Successful	PC-1	PC-1	ICMP		
	Successful	PC-3	PC-4	ICMP		

La conexión entre equipos de diferentes redes no funciona, pues pertenecen a dos dominios de broadcast diferentes y el switch no está configurado para el tráfico entre diferentes redes.

Fire	Last Status	Source	Destination	Type	Color
	Failed	PC-1	PC-3	ICMP	
	Failed	PC-2	PC-4	ICMP	
	Failed	PC-3	PC-2	ICMP	
	Failed	PC-4	PC-1	ICMP	

- c. Describa el proceso completo que realiza un computador al generar un ping hacia un computador en otra VLAN. Considere un primer escenario donde exista un gateway por defecto configurado y otro donde no se haya asociado.

Al hacer un ping desde un puerto que está asociado a una VLAN A con destino un puerto asociado a una VLAN B sin tener una configuración adecuada de gateway, no se obtendrá comunicación, pues el switch reenvía el paquete por todos los puertos asociados a la VLAN de origen del paquete (VLAN A en este caso) pero no considera los puertos asociados a otras VLAN.

Un gateway permite conexión entre redes, por lo que al ser configurada adecuadamente, sí se podría hacer un ping desde una VLAN A hasta una VLAN B. En este caso, la dirección MAC de destino será la del gateway por defecto.

- d. Revise la tabla de correspondencia entre MAC y puerto. ¿Qué diferencias encuentra frente al caso donde no se tienen VLAN configuradas?

Vlan	Mac Address	Type	Ports
10	0001.c705.cbc0	DYNAMIC	Fa0/1
10	000b.be6e.e977	DYNAMIC	Fa0/2
20	0010.11d3.45ce	DYNAMIC	Fa0/3
20	00d0.5864.25ee	DYNAMIC	Fa0/4

Cada puerto ya no pertenece a la VLAN por defecto que es la 1, ahora cada puerto está asociado a su respectiva VLAN, ya sea la 10 o la 20.



- e. Consulte y configure lo necesario para administrar el conmutador vía telnet. Asocie la interfaz virtual de la VLAN de administración a una VLAN diferente a la VLAN por defecto y a las dos VLAN anteriormente creadas. Debe administrar el conmutador desde un computador conectado a la VLAN de administración. Explique

3. Sobre la topología anterior adicione un conmutador como muestra la figura 2. En este caso, los computadores 1, 2 y 4 pertenecen a una VLAN y los 3 y 5 a otra VLAN. El computador Admin pertenece a una VLAN distinta a las anteriores, que será la VLAN utilizada para administrar remotamente los conmutadores de la topología.

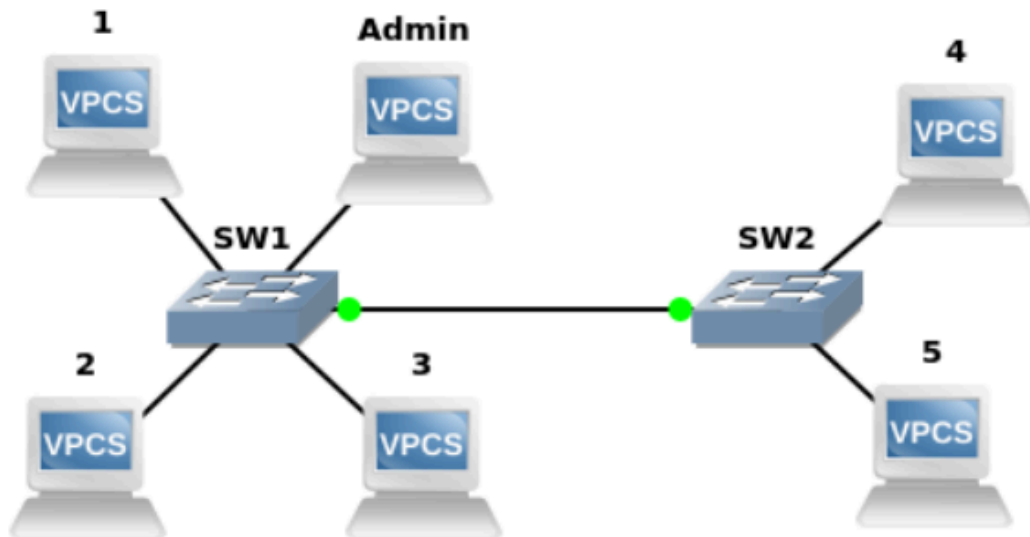


Figure 2: Topología packettracer

- a. Configure inicialmente los puertos tipo acceso. Indique entre qué equipos existe conectividad y por qué. ¿A qué VLAN pertenece el puerto que conecta ambos conmutadores?

Los puertos que conectan a los switches entre sí pertenecen a la VLAN por defecto, que es la VLAN 1.

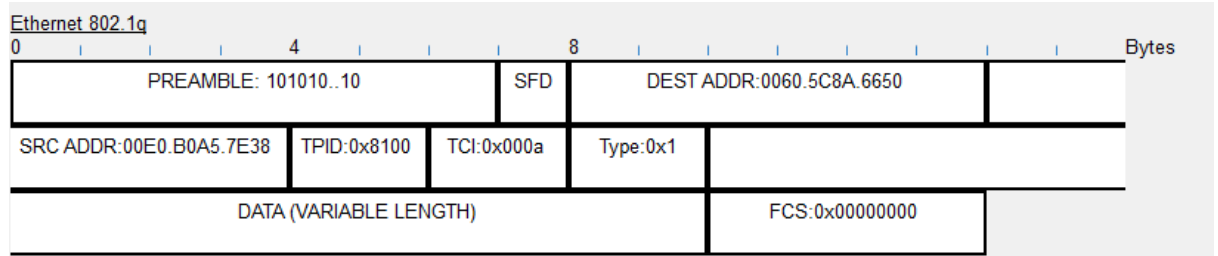
- b. Configure el puerto entre conmutadores para que lleve tráfico de varias VLAN. Explique cómo se identifica el tráfico asociado a cada VLAN en dicho enlace.

El tráfico que entra a un switch entra sin una etiqueta, pero al salir de este, en su trama Ethernet se identifica la información que le fue otorgada a modo de etiqueta de información de VLAN.

Paquete antes de pasar por el switch:

EthernetII					Bytes	
0	4	8				
PREAMBLE: 101010...10		SFD	DEST ADDR: 0060.5C8A.6650			
SRC ADDR: 00E0.B0A5.7E38		TYPE: 0x0800		DATA (VARIABLE LENGTH)	FCS: 0x00000000	

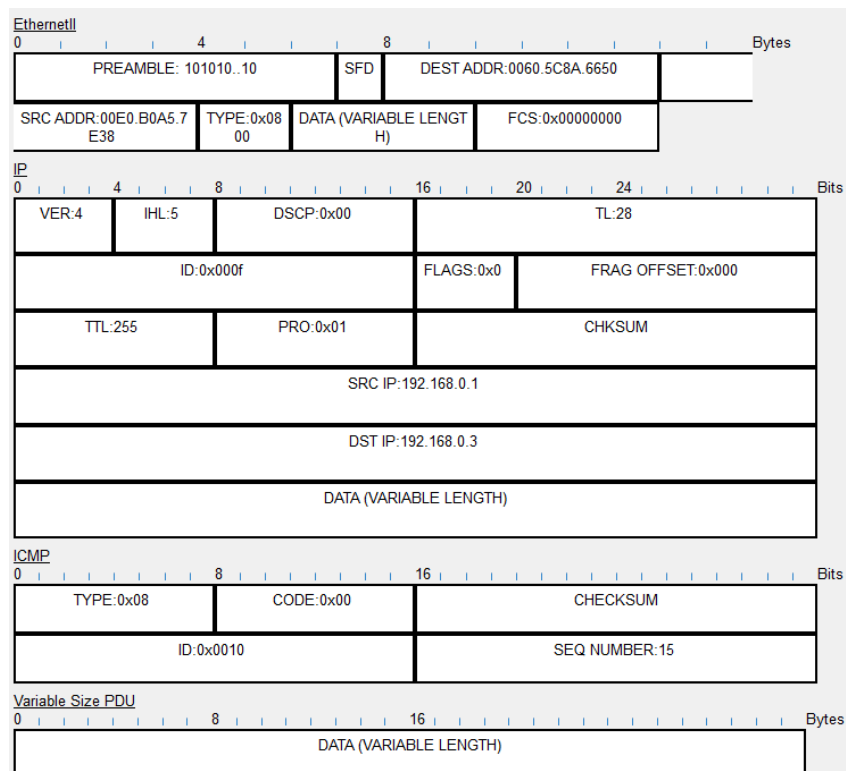
Paquete luego de salir del switch:



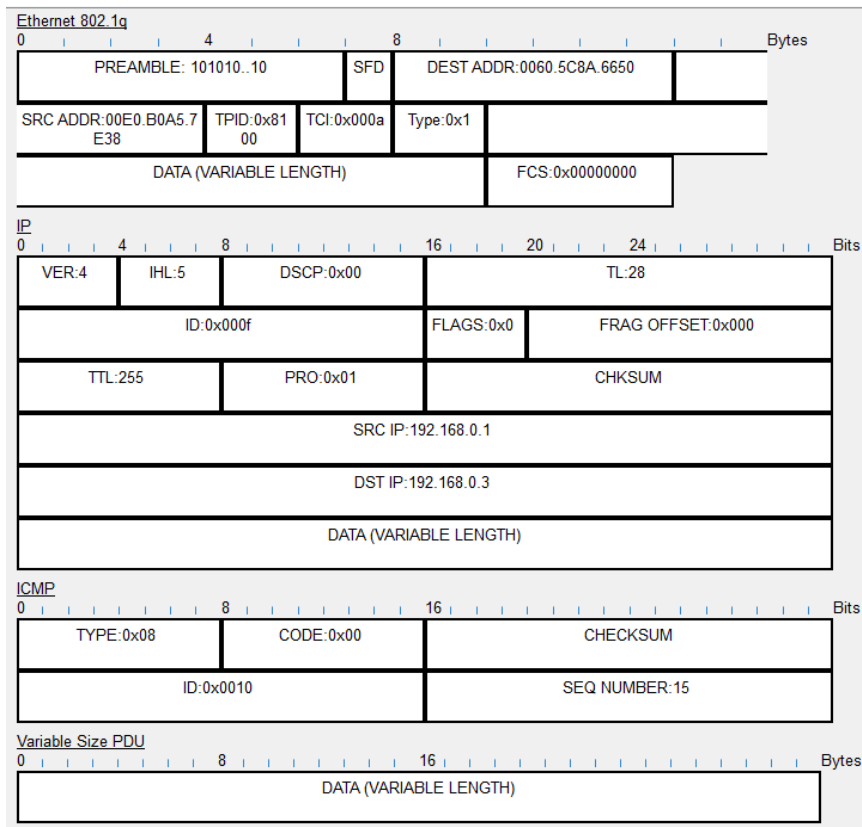
- c. Realice un ping entre los equipos 1 y 4. Explique el proceso completo de agregación y remoción de etiquetas durante el transporte de la trama. También explique los procedimientos asociados a ARP.

Ambos equipos pertenecen a la VLAN 10, por lo que anticipadamente, se sabe que habrá conectividad al haber predispuesto los switches para este tipo de tráfico.

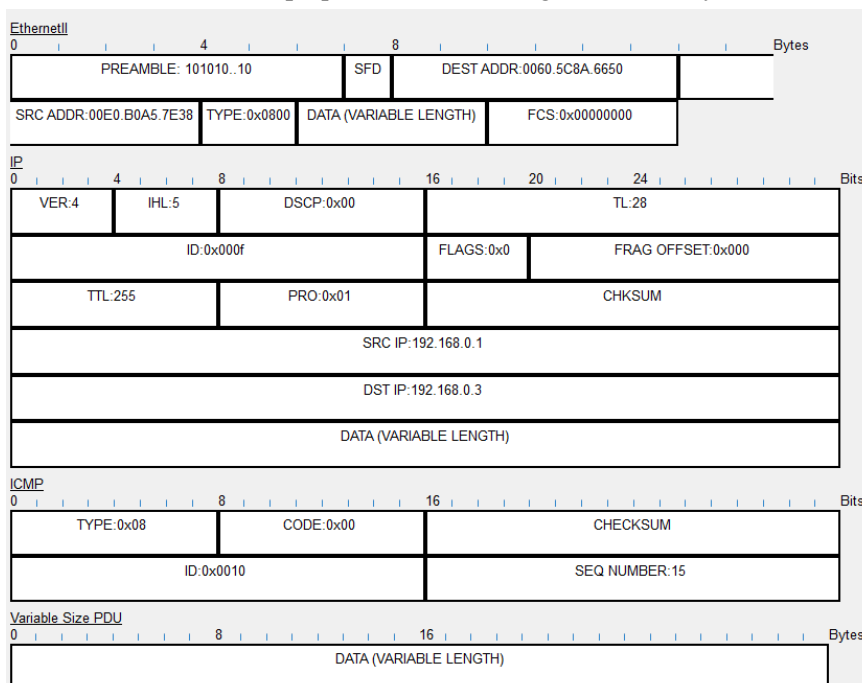
Este es el contenido del paquete al salir de PC1 y al entrar al primer switch:



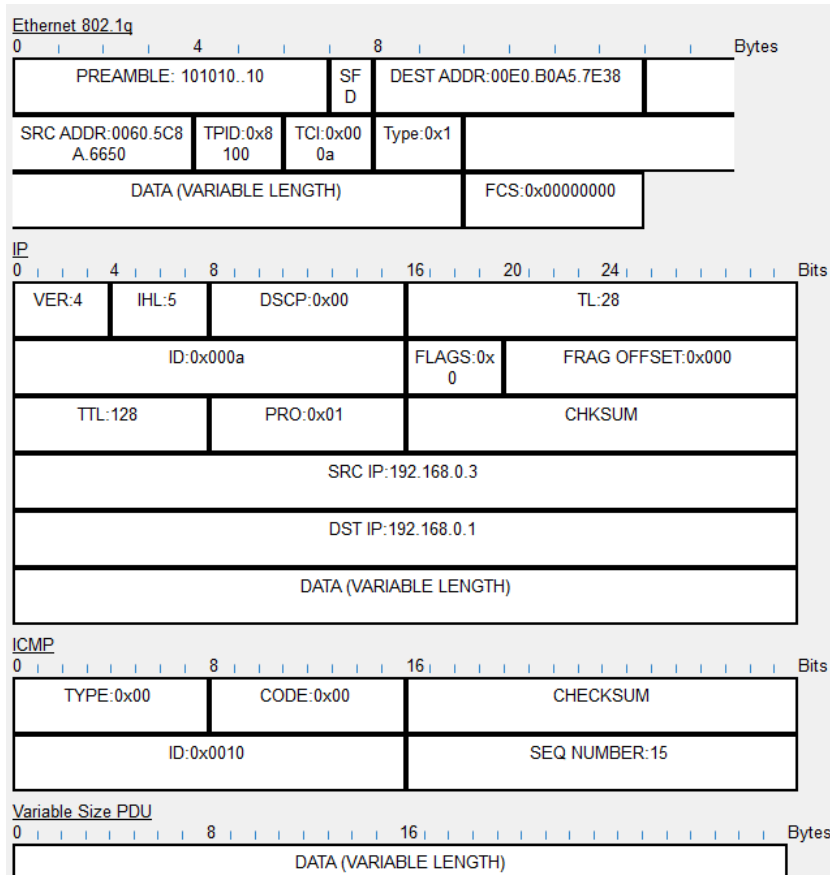
Este es el contenido del paquete al salir del primer switch y entrar al segundo switch:



Este es el contenido del paquete al salir del segundo switch y entrar al PC4:



Este es el contenido del paquete al salir del PC4:



Para este paquete, cambi3 su IP source y destino.

Y en general, al salir de un switch, se generan unas etiquetas TPID y TCI.

**TPID:** Es un campo de 16 bits que indica que el paquete lleva una etiqueta VLAN.

**TCI:** Contiene la informaci3n de la VLAN, y est3 compuesto por tres subcampos:

- **PRI (Priority Code Point):** 3 bits para la prioridad del paquete.
- **DEI (Drop Eligible Indicator):** 1 bit que indica si el paquete puede ser descartado en situaciones de congesti3n.
- **VID (VLAN Identifier):** 12 bits que identifican el n3mero de VLAN a la que pertenece el paquete.

- Revisa la tabla de asociaci3n entre MAC y puerto de ambos conmutadores despu3s de probar la conectividad entre los equipos de las mismas VLAN. ¿Qu3 direcciones MAC est3n asociadas al puerto que conecta ambos conmutadores?

Primer switch:

```
Switch>show mac address-table
```

Mac Address Table

Vlan	Mac Address	Type	Ports
-----	-----	-----	-----
1	00d0.ba02.1018	DYNAMIC	Fa0/24
10	0001.424c.c7de	DYNAMIC	Fa0/2
10	0060.5c8a.6650	DYNAMIC	Fa0/24
10	00e0.b0a5.7e38	DYNAMIC	Fa0/1
30	00e0.f79b.1dbb	DYNAMIC	Fa0/24
30	00e0.f7e9.633b	DYNAMIC	Fa0/11

Segundo switch:

```
Switch>show mac address-table
```

Mac Address Table

Vlan	Mac Address	Type	Ports
-----	-----	-----	-----
1	00e0.b063.e9c6	DYNAMIC	Fa0/24
10	0001.424c.c7de	DYNAMIC	Fa0/24
10	0060.5c8a.6650	DYNAMIC	Fa0/1
10	00e0.b063.e9c6	DYNAMIC	Fa0/24
10	00e0.b0a5.7e38	DYNAMIC	Fa0/24
20	00e0.b063.e9c6	DYNAMIC	Fa0/24
30	00e0.b063.e9c6	DYNAMIC	Fa0/24
30	00e0.f79b.1dbb	DYNAMIC	Fa0/12
30	00e0.f7e9.633b	DYNAMIC	Fa0/24

4. Agregue un tercer conmutador a la topología y los equipos indicados, según la siguiente figura:

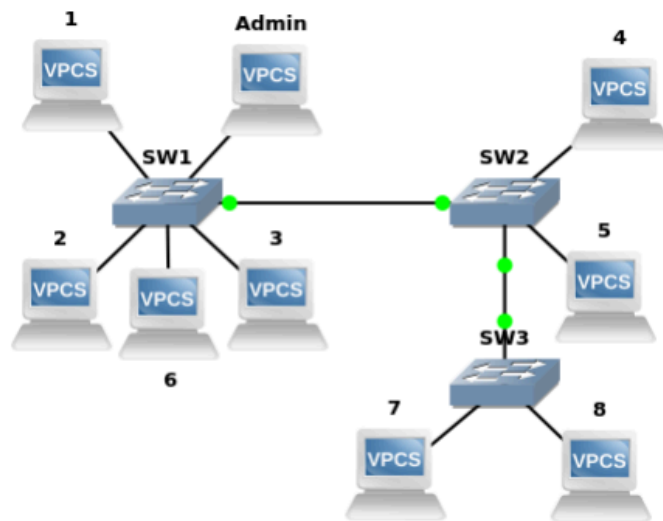
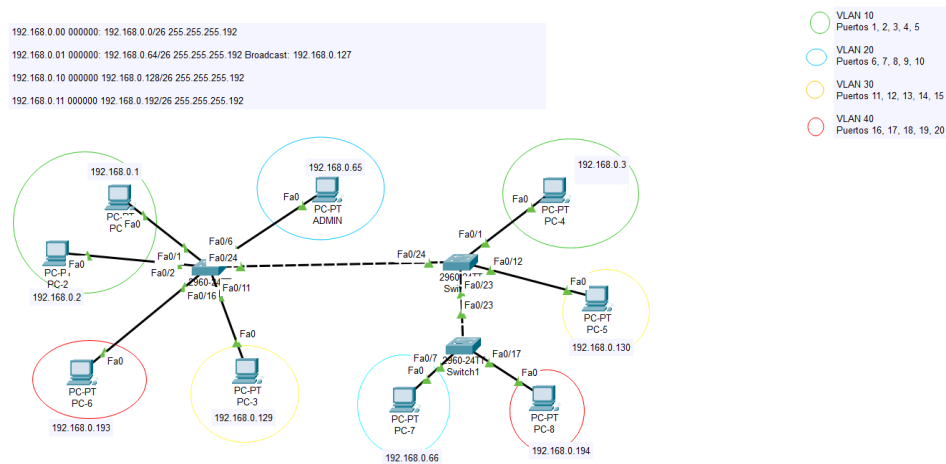


Figure 3: Topología packettracer

- a. Cree una nueva VLAN en la topología y asocie a dicha VLAN los equipos 6 y 8. Agregue el equipo 7 a la VLAN de administración.



- b. Explique el tratamiento que se debe dar al tráfico sin etiquetas en los enlaces troncales. Consulte la utilidad de la VLAN nativa y señale la diferencia con la VLAN de administración. Defina la VLAN a la que pertenecen los equipos 6 y 8 como nativa.

Si en mi sistema, tengo todas las VLAN configuradas adecuadamente en cada uno de los switches y al generar tráfico, los switches etiquetan este tráfico con la VLAN a la que pertenecen, no habría ningún problema. La VLAN nativa se define como aquella VLAN que

atraviesan los enlaces troncales sin ninguna etiqueta VLAN. Por lo que, si en mi sistema todos los paquetes se etiquetan con la información de su respectiva VLAN y se da el caso de un paquete sin etiqueta, se le atribuye su pertenencia a esta VLAN nativa.

La VLAN de administración es de hecho, una VLAN generada con un número propio, tal como se hizo con las demás.

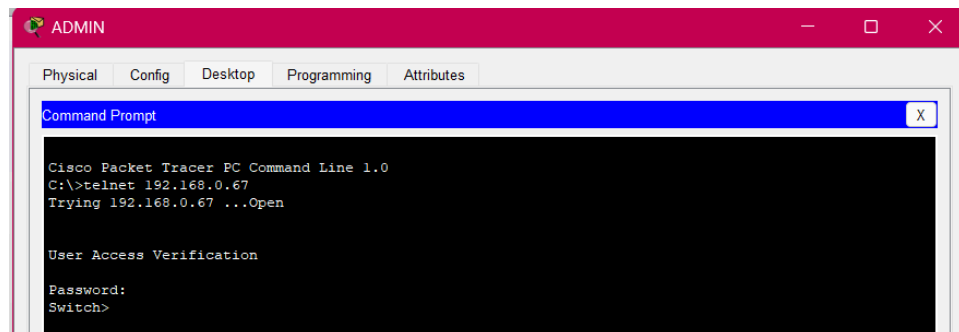
c. Consulte la posibilidad de permitir solo el tráfico de algunas VLAN a través de los enlaces troncales. Permita a través de los enlaces troncales solamente las VLAN creadas en la topología.

d. Finalmente, configure lo necesario para garantizar conectividad entre los equipos de la misma VLAN. Desde los equipos 7 y Admin se deben administrar a través de telnet todos los conmutadores de la topología.

1. Se debe de garantizar conectividad ip entre el pc y los switches para hacer telnet, por lo que los switches y el pc deben estar en la misma VLAN.
2. Se agregan los 3 switches a la VLAN 20 con ips 192.168.0.67, 192.168.0.68, 192.168.0.69 para SW1, SW2 y SW3 respectivamente.
3. Se agrega la configuración adecuada para telnet, incluyendo una contraseña

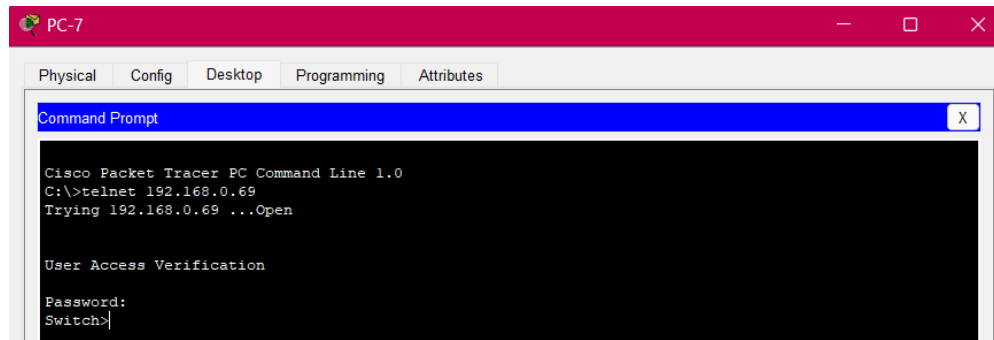
```
Switch(config)#line
% Incomplete command.
Switch(config)#line ?
<0-16>  First Line number
console Primary terminal line
vty     Virtual terminal
Switch(config)#line
% Incomplete command.
Switch(config)#line vty 0 15
Switch(config-line)#password viernes
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

4. Se verifica a través del PC de administración el acceso en este caso a SW1.



También se verifica el acceso desde PC-7 al SW3.



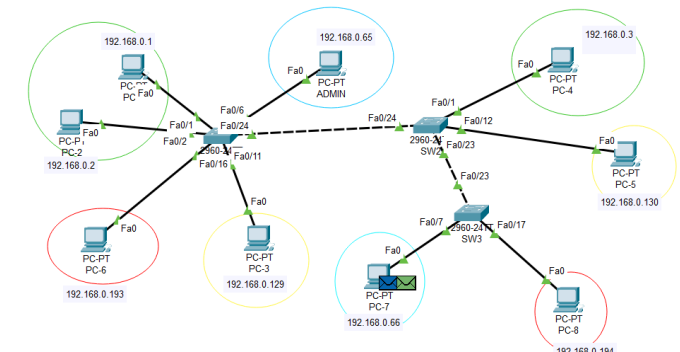


- e. Señale el camino que sigue una trama que encapsula un ping que va desde el equipo 1 hasta la SVI (interfaz de administración) del conmutador 3.

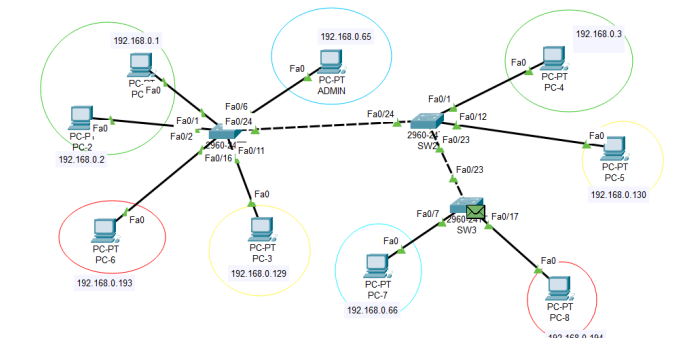
Como no hay un gateway configurado en PC-1, el paquete no sale siquiera del mismo, por lo que genera un error y no puede llegar a su destino.

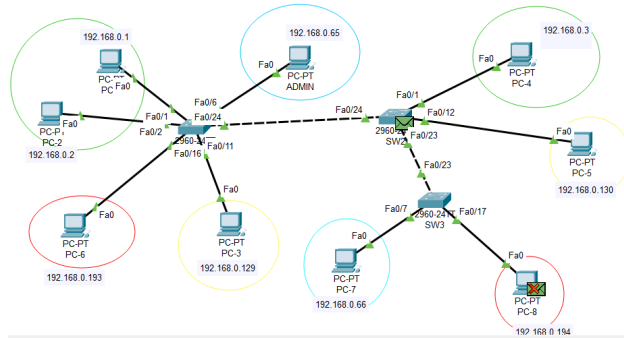
- f. Señale el camino que sigue una trama que encapsula un ping que va desde el equipo 7 hasta la SVI (IP del switch) del conmutador 1. Adicionalmente, explique en qué partes del recorrido se adiciona o se remueve la etiqueta asociada a la VLAN correspondiente.

1. Se genera el ping en PC-7



2. Llega al SW3 y este inunda a sus puertos en busca de la MAC destino.

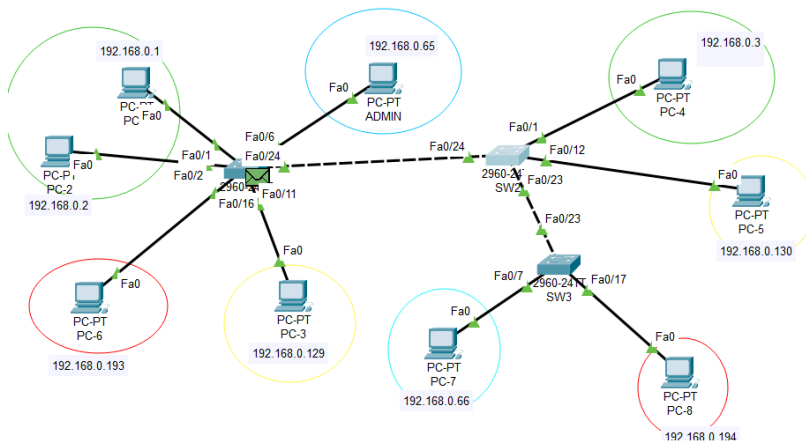




- El paquete desde SW2 va directamente hasta SW1 ya que su tabla MAC tiene algunas direcciones que indican por cuales puertos no inundar.

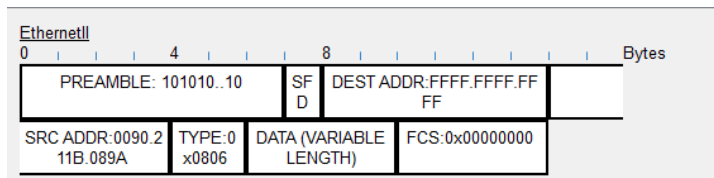
SW1#show mac address-table  
Mac Address Table

Vlan	Mac Address	Type	Ports
1	0090.2b12.1717	DYNAMIC	Fa0/23
1	00e0.a30b.ee27	DYNAMIC	Fa0/24
20	000b.bece.149b	DYNAMIC	Fa0/24
20	0090.211b.089a	DYNAMIC	Fa0/23

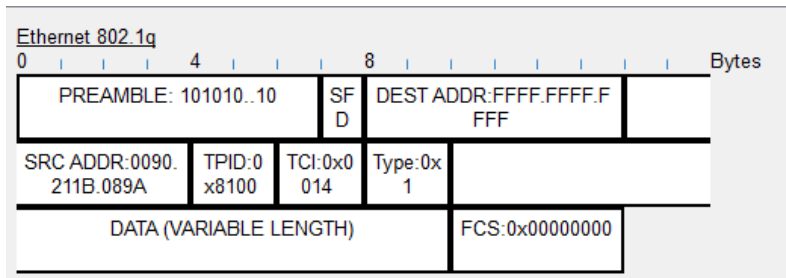


La primera etiqueta se genera cuando el paquete de entrar a SW3, sale.

En esta parte al entrar a SW3 y salir de PC-7 no lleva las etiquetas TPID y TCI:



Al salir de SW3 para entrar a SW2 lleva ya estas etiquetas de identificación de VLAN:



Estas etiquetas se mantienen en el trayecto entre SW2 y SW1:

