UNIVERSIDAD DE LOS ANDES

DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

LABORATORIO #5: Administración de switches y VLANS

ISIS 3204 - INFRAESTRUCTURA DE COMUNICACIONES

Nathalia Quiroga

Grupo 7

David Quiroga 202310820

Nicolas Gonzalez 202310041

Samuel Rodríguez Torres 202310140

2025-20

Contenido

1. Actividad 6.1: Funcionamiento de la red

a. Sub-interfaces y comandos

Para verificar el buen funcionamiento de la red, primero se sugiere esta sección a modo de entendimiento de la topología utilizada y los comandos de configuración de los diferentes dispositivos que la componen.

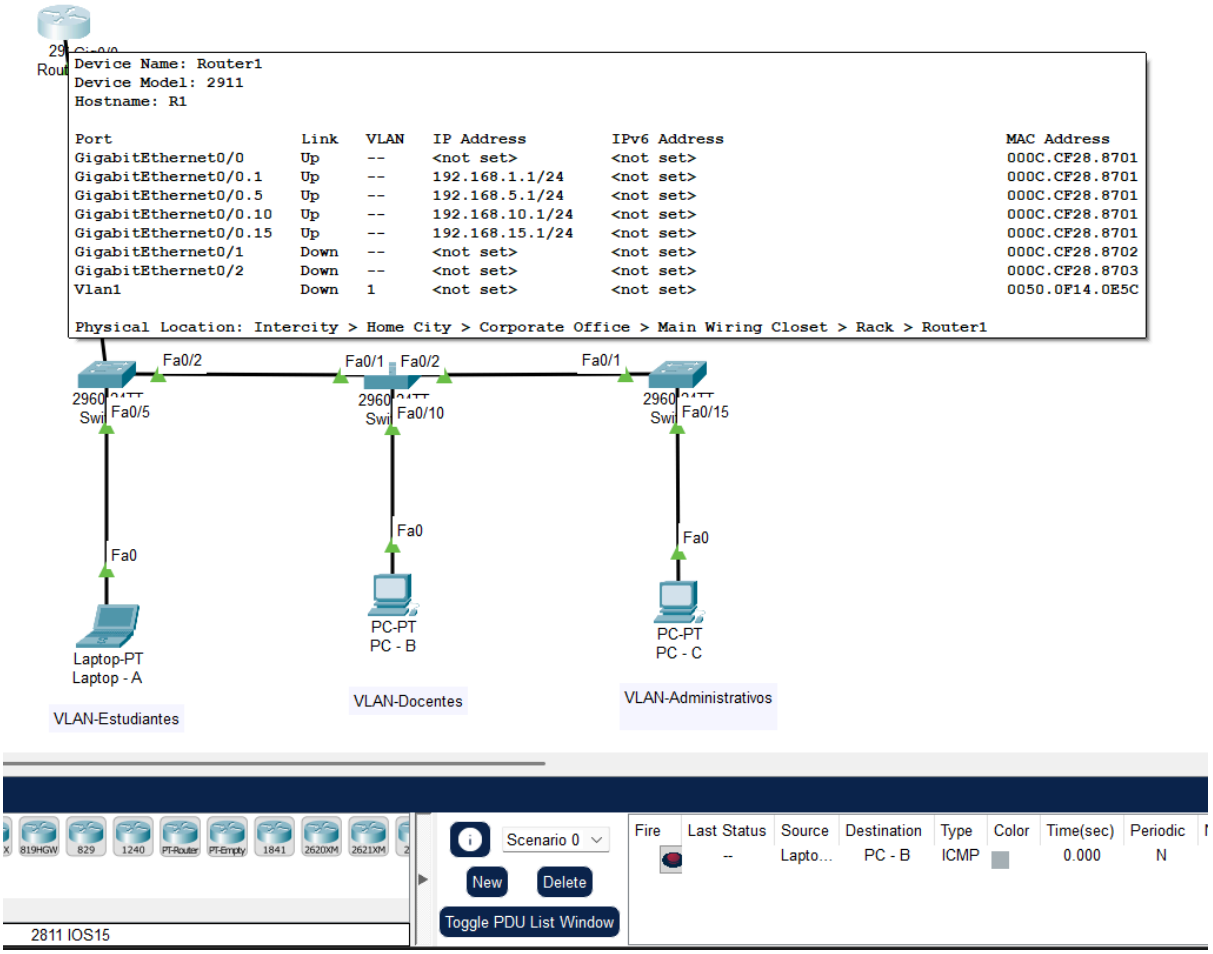


Imagen 1: Topología descrita en la guía del laboratorio.

En la imagen 1, se muestra la implementación de la topología mostrada en la guía del laboratorio en el programa de cisco packet tracer en una de las máquinas del grupo. Dentro de las instrucciones, hay varios comandos para configurar un router-on-stick, y varias VLAN, que como se ve en la imagen, corresponden a una diferente para estudiantes, docentes y administradores. Solo se necesita de un único cable y una única interfaz en el router gracias a su configuración router-on-stick que nos permite virtualizar las interfaces, creando para este caso la g0/0.1, g0/0.5 y g0/0.10. Esta conexión se hace al Switch 1 posicionando a este como el switch principal que debe tener las conexiones troncales a los demás switches y el puente central de todas las VLAN.

En este sentido, PC-a y Switch1 hacen parte de la VLAN de estudiantes (VLAN 5), PC-b y Switch 2 hacen parte de la VLAN de docentes (VLAN 10) y el PC-c y el Switch 3 hacen parte de la VLAN de administradores (VLAN 15). Los switch se encuentran conectados mediante trunk y para la interfaz donde se conecta el respectivo PC se hace mediante el modo access como se puede ver en la siguiente imagen para el Switch 2:

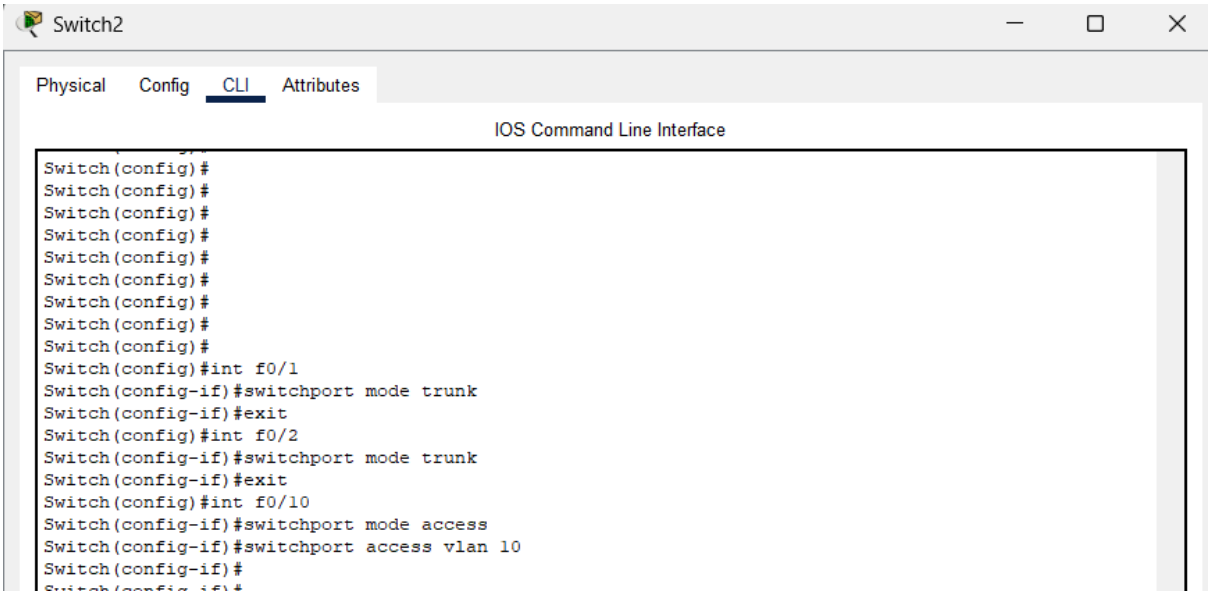


Imagen 2: Configuración del modo trunk y access en el switch 2.

Estas configuraciones se repitieron para todos los switches, routers y PC, siguiendo la guía del laboratorio donde se encuentran los comandos de todos los elementos de la topología.

b. Pruebas de conectividad

Una vez configurada los dispositivos, se empezaron a realizar varias pruebas de conectividad entre los dispositivos como se puede ver a continuación:

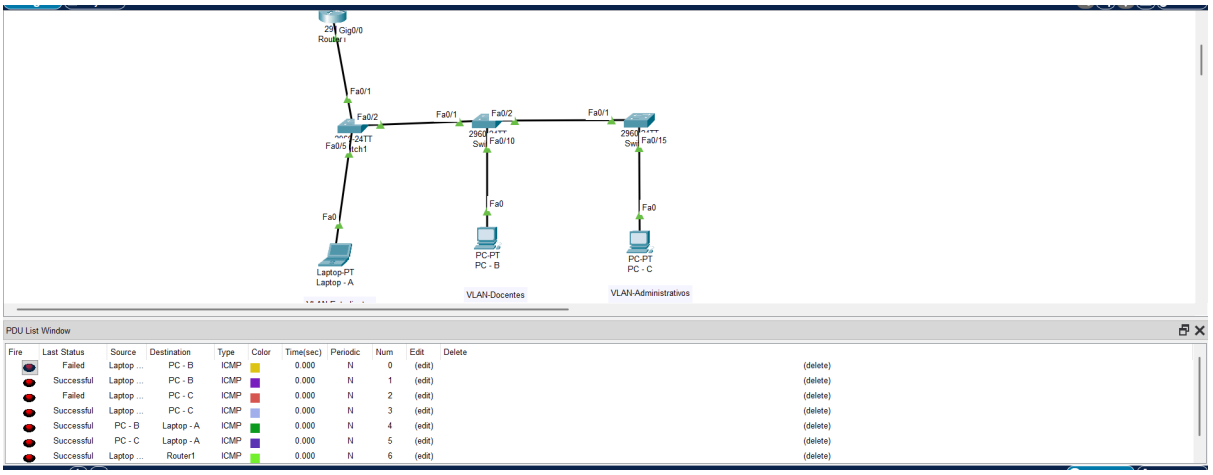


Imagen 3: Pruebas de conectividad entre dispositivos de la topología.

En la imagen se puede ver el origen y el destino de la prueba de conectividad a través de ping. Aunque ambos equipos están conectados a través de la misma infraestructura física cada uno pertenece a una subred distinta, por lo que no pueden comunicarse directamente en capa 2. Al inicio, el primer ping falla porque el router aún no ha resuelto la dirección MAC del equipo destino en la subinterfaz correspondiente a su VLAN. Como las VLAN generan dominios de broadcast separados, el ARP del origen no puede llegar directamente al otro PC. Posterior a esto, se vuelven a hacer los pings que fallaron y se puede ver como ahora si son exitosos y de esta manera, se prosigue con el resto de dispositivos y se puede ver que toda la topología funciona y se pueden comunicar entre estos.

2. Actividad 6.2: Demostración del funcionamiento

A continuación en esta sección se presenta una prueba de conectividad (ping) entre la Laptop-A y el PC-B que permita comprender el funcionamiento de la topología y el camino que siguen los paquetes. Para esto, desde cisco packet tracer y el modo de simulación se vio el paso a paso que siguen los paquetes ICMP para llegar de un extremo al otro.

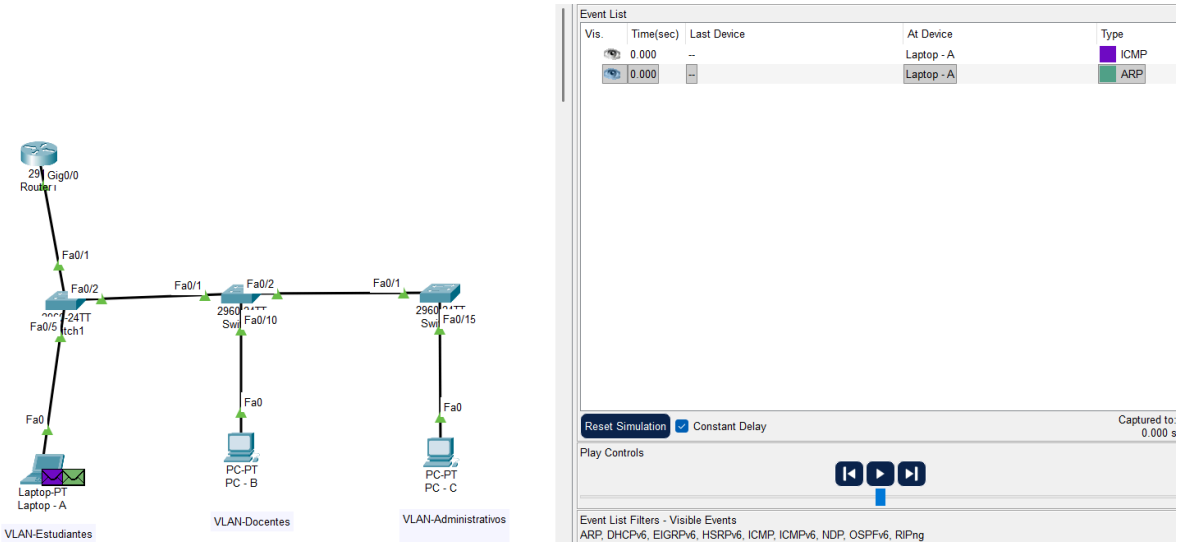


Imagen 4: Inicio del comando ping desde Laptop-A

En la imagen 4 se ve el inicio de la simulación que se llevará a cabo y como se puede ver en la parte derecha, el paquete ICMP corresponde al icono de color morado del lado izquierdo. En este orden de ideas, a continuación se muestra una secuencia de imágenes que busca ilustrar el funcionamiento de la red y el recorrido que debe seguir el paquete:

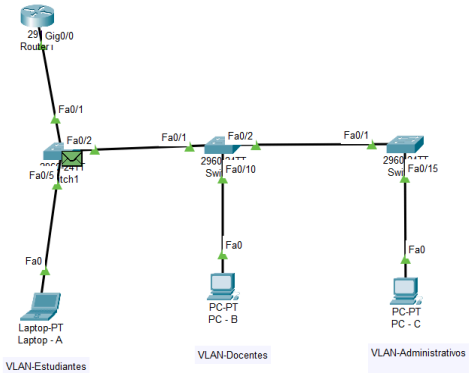


Imagen 5: ICMP de Laptop-A a Switch1

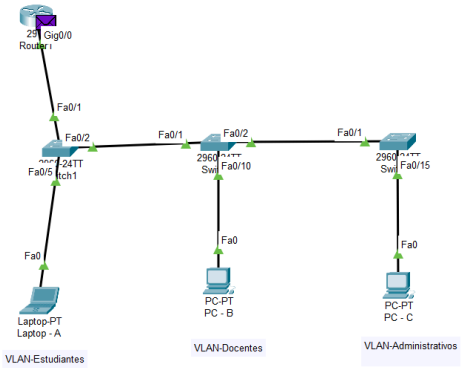


Imagen 6: ICMP de Switch1 a Router1

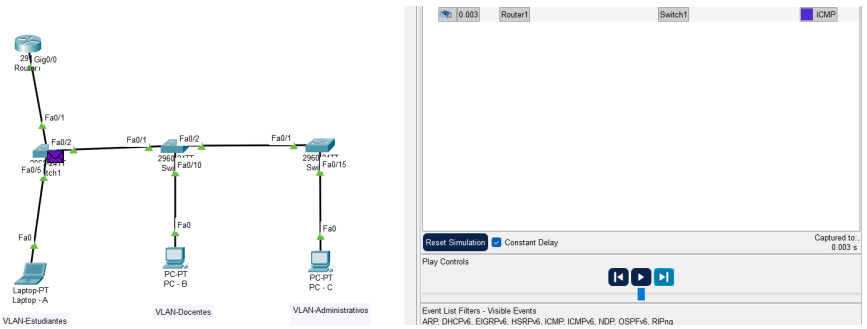


Imagen 7: regreso del ICMP de Router1 a Switch1

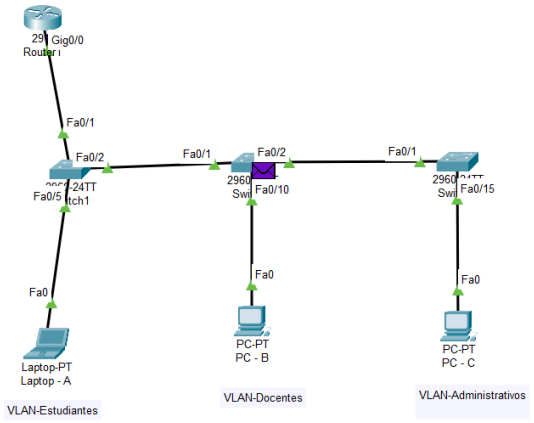


Imagen 8: ICMP de Switch 1 a Switch 2

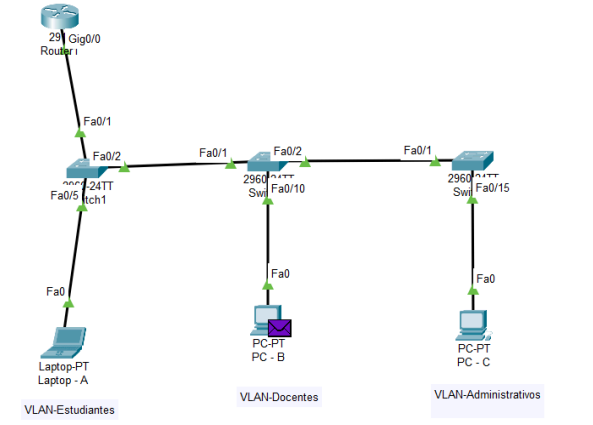


Imagen 9: ICMP de Switch 2 a PC-B

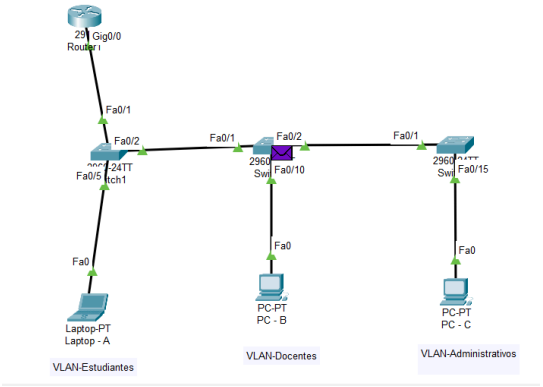


Imagen 10: Reply ICMP de PC-B a Switch 2

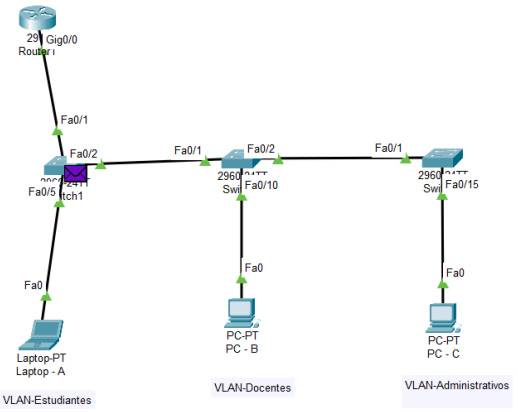


Imagen 11: Reply ICMP de Switch 2 a Switch 1

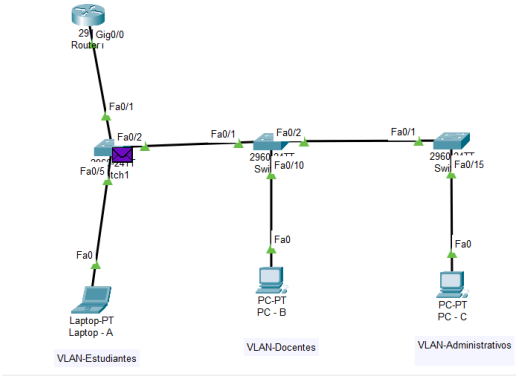


Imagen 12: Reply ICMP de Switch 2 a Switch 1

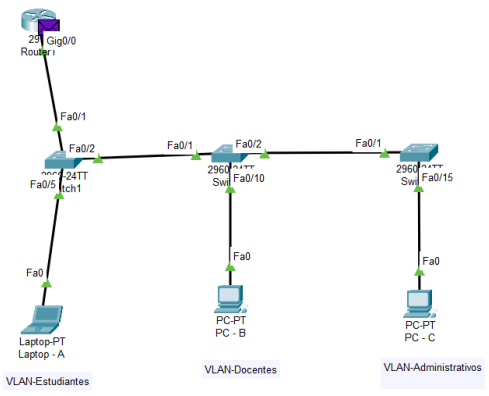


Imagen 13: Reply ICMP de Switch 1 a Router 1

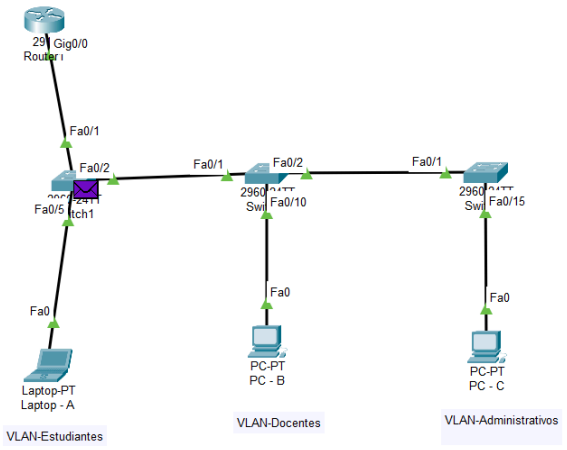


Imagen 14: Reply ICMP de Router 1 a Switch 1 (VLAN 5)

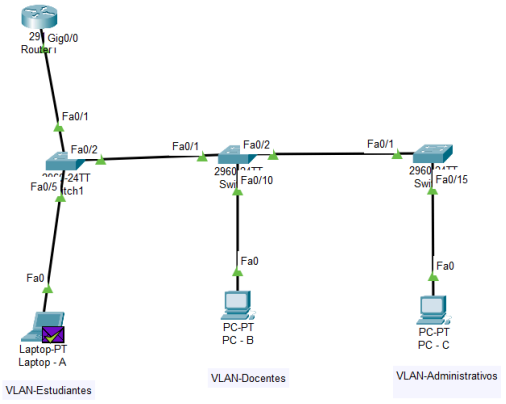
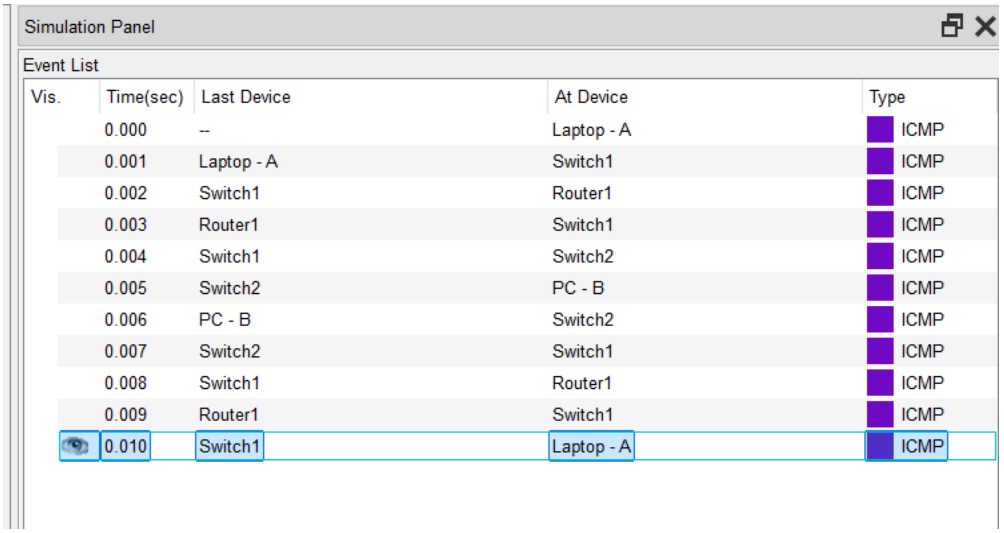


Imagen 15: Reply ICMP de Switch 1 a Laptop - A



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop - A	ICMP
	0.001	Laptop - A	Switch1	ICMP
	0.002	Switch1	Router1	ICMP
	0.003	Router1	Switch1	ICMP
	0.004	Switch1	Switch2	ICMP
	0.005	Switch2	PC - B	ICMP
	0.006	PC - B	Switch2	ICMP
	0.007	Switch2	Switch1	ICMP
	0.008	Switch1	Router1	ICMP
	0.009	Router1	Switch1	ICMP
	0.010	Switch1	Laptop - A	ICMP

Imagen 17: Resumen del curso del paquete ICMP exitoso.

Como se pudo observar, en especial en la imagen 17, el paquete debe ir primero al switch. Esto ocurre en la VLAN 5, asociada a la interfaz física Fa0/5. El switch hace el trabajo de clasificar la trama dentro de su VLAN correspondiente y, al no encontrar la MAC destino dentro de su dominio de broadcast (Están en diferentes redes), detecta que el tráfico debe salir de la subred. Por esta razón, lo redirecciona hacia el router a través del enlace troncal. El router recibe el paquete en la subinterfaz correspondiente a esa VLAN, lo desencapsula, lo enruta y determina la salida adecuada hacia la otra VLAN. Con esta información, regresa el paquete al switch y éste lo reenvía por el troncal hacia el otro switch (al 2), el cual tiene configurada la VLAN 10 de docentes y, finalmente, a través de la interfaz Fa0/10, el paquete llega al PC de destino.

3. Actividad 6.3: Respuesta a las preguntas

1. Realice pings de todo, revise tablas ARP y analícelas. Todo debería funcionar

En la siguiente imagen se pueden apreciar los pings de todo y como la topología funciona, tal y como se había mostrado en secciones anteriores:

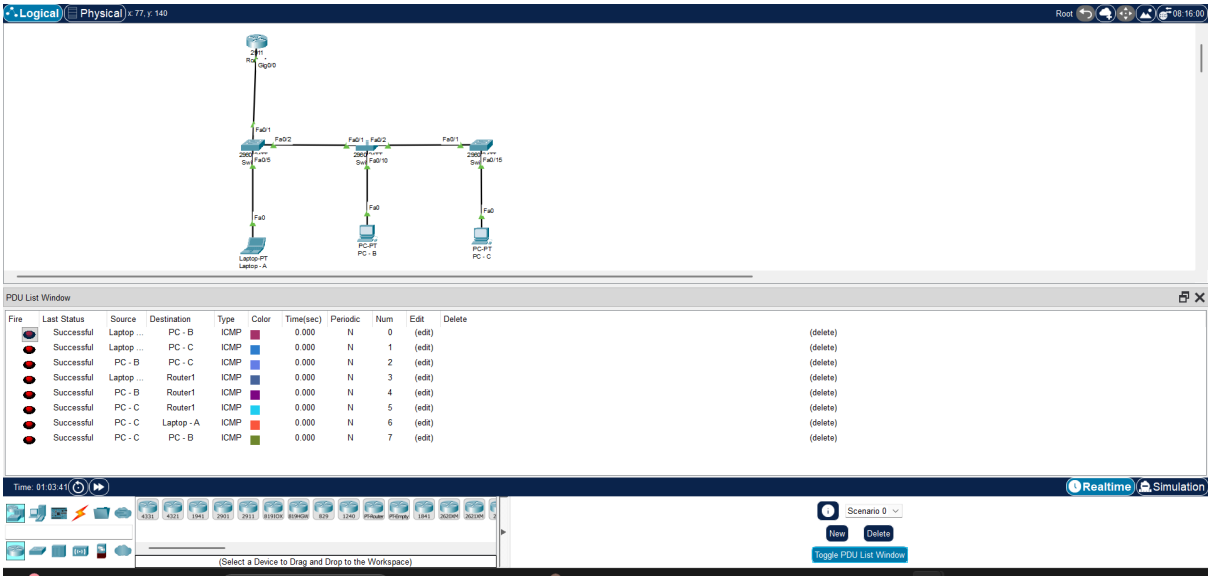


Imagen 18: Pings entre todos los dispositivos

Adicionalmente, en la anterior sección se mencionó que los primeros pings fallan, esto se debe a que los PC están en computadores diferentes, tienen broadcast diferente y una dirección de red diferente, por lo que es necesario asociar la IP a la dirección MAC en la tabla ARP del switch. Esta tabla asocia direcciones IP con la dirección MAC del dispositivo correspondiente, de esta manera los dispositivos pueden enviar tramas a nivel de capa 2 hacia el destino correcto sin necesidad de resolver nuevamente la dirección física mediante ARP, permitiendo una comunicación más rápida y eficiente dentro de la red, sin necesidad de pasar por el router.
En un inicio esta tabla se encuentra vacía por lo que el dispositivo debe mandar un broadcast para obtener una resolución con la MAC del dispositivo con la IP para llenar esta tabla con los dispositivos que se encuentren en la LAN, VLAN para este caso como se puede ver a continuación:

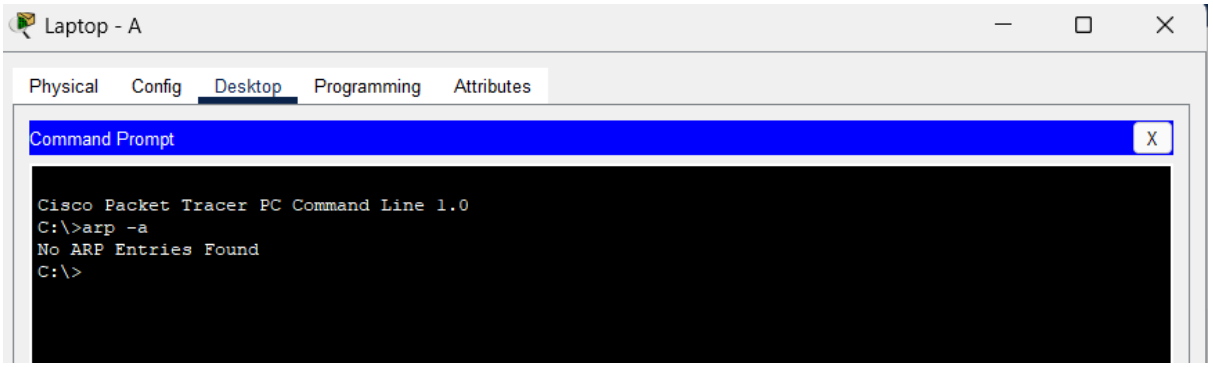


Imagen 19: Tabla ARP de Laptop - A antes de intentar hacer pings.

```
R1#
R1#show ip arp

R1#
```

Copy Paste

Imagen 20: Tabla ARP del Router - 1 antes de intentar hacer pings.

Si estas tablas, que representan la situación antes de intentar hacer pings, las comparamos con una situación después de haber logrado hacer un ping exitoso entre los pc nos podremos dar cuenta que las tablas ARP se empiezan a llenar de información como se puede ver a continuación:

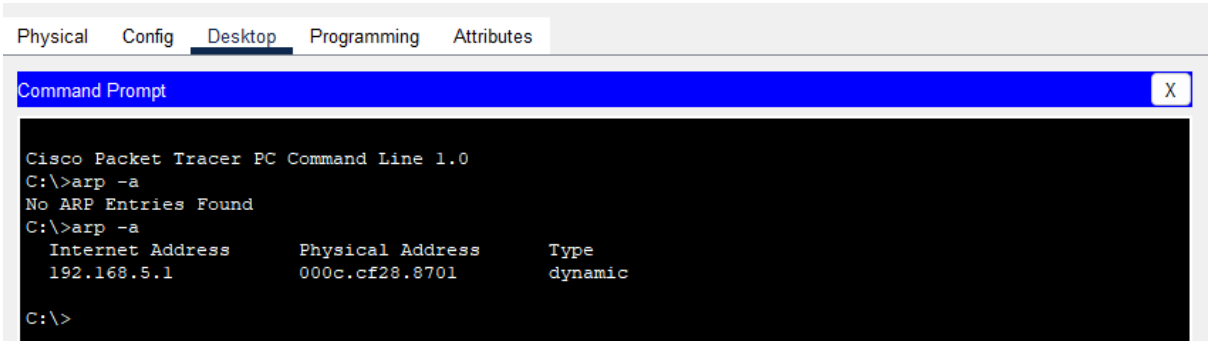


Imagen 21: Tabla ARP de Laptop - A después de hacer pings.

```
R1#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.5.71           0   0060.2F56.01E9  ARPA   GigabitEthernet0/0.5
Internet  192.168.10.71          0   0040.0BDC.BB99  ARPA   GigabitEthernet0/0.10
Internet  192.168.15.71          0   000B.BE9A.21E5  ARPA   GigabitEthernet0/0.15
R1#
```

Imagen 22: Tabla ARP del Router - 1 después de hacer pings.

Estas capturas muestran que la tabla ARP solo se completa con la información de los dispositivos dentro de la misma VLAN y para el caso del router, este únicamente tiene las direcciones IP y MAC de los equipos conectados a cada una de sus subinterfaces. El router no aprende direcciones MAC de dispositivos que estén fuera de su propia LAN o de otras VLAN que no atraviesen una de sus interfaces lógicas, ya que ARP nunca cruza los router y cada tabla ARP corresponde únicamente al dominio de broadcast asociado a cada subred.

2. **En tu red, ¿qué ocurriría si accidentalmente asignarás el comando switchport access vlan 5 en un puerto que actualmente es troncal?**

En primera instancia, el modo “access” está pensado para conectar switches a los hosts finales puesto que solo maneja una VLAN, la vlan 5 en este caso, por lo que al cambiar el troncal por un access se limitaría el uso de la interfaz a unicamente la vlan 5, dejando inhabilitadas la vlan 10 y 15, como se puede ver en la siguiente imagen:

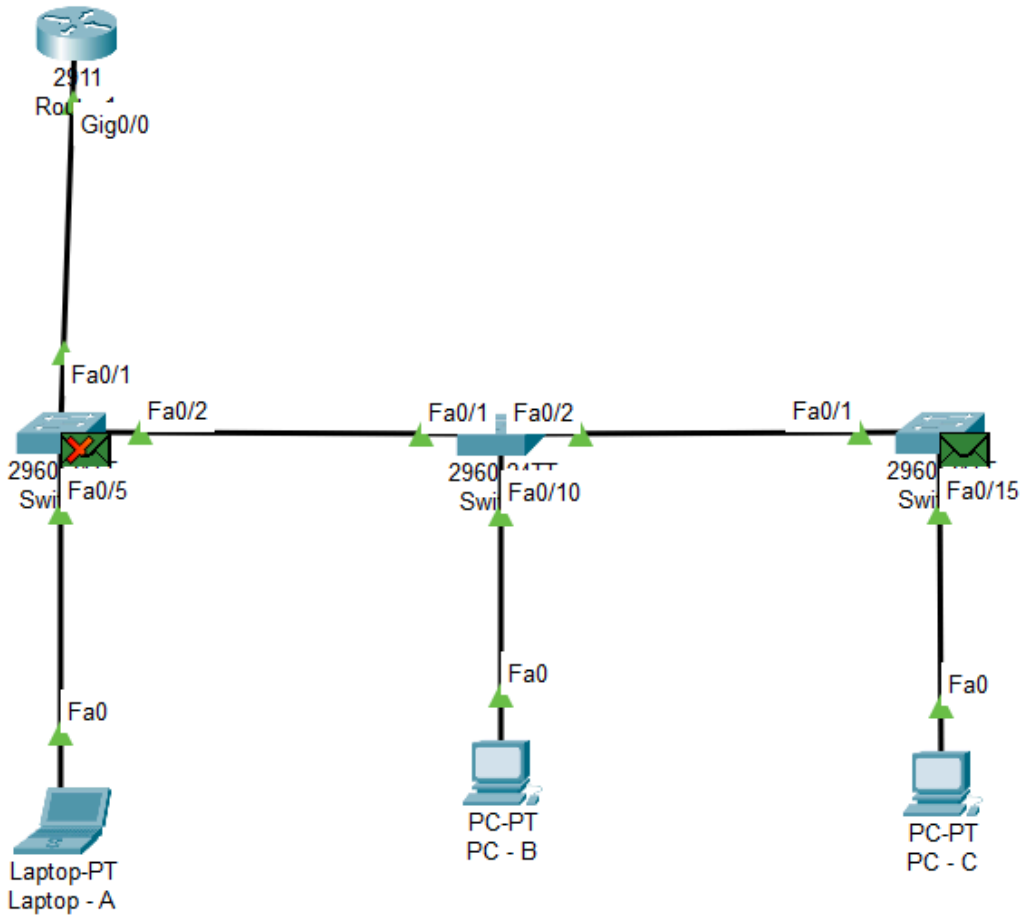


Imagen 23: Falla en ping de PC - B a Laptop - A

Al cambiar el modo troncal a access de Fa0/2, solo se espera tráfico de vlan 5 - estudiantes en la etiqueta 802.1Q, por lo que al llegar una trama de vlan 10 - docentes, esta no será aceptado por el switch y la trama será descartada. Cabe aclarar que al usar el comando: *switchport access vlan 5,* dependiendo de la versión del switch, este también cambiará al modo access sin necesidad del comando *switchport mode access,* cambiando la configuración del switch como se puede ver a continuación.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
5    Estudiantes                      active    Fa0/2, Fa0/5
10   Docentes                         active
15   Administrativos                  active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Imagen 24: Estado actual del switch después del comando *switchport access vlan 5*

3. **Si en R1 en vez de escribir este comando:**
   R1(config-subif)# ip address 192.168.10.1 255.255.255.0
   Se cambiará la máscara por /25. ¿Qué PCs dejarían de funcionar en tu laboratorio y por qué específicamente? Muestre capturas del proceso

Al cambiar la máscara, se reduce la cantidad de host disponibles a la mitad, partiendo la red en: 192.168.10.**0** y 192.168.10.**128.** En este caso, al cambiar la máscara a /25, la red quedaría de la siguiente manera:

```
R1>enab
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.128
R1(config-subif)#exit
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Imagen 25: Configuración del router 1 con la máscara /25.

Estas configuraciones se asocian a la VLAN 10, de manera que la nueva red es la siguiente:

Dirección de red	192.168.10.0
Broadcast	192.168.10.127
Rango de host utilizables	192.168.10.1 - 192.168.10.126

Tabla 1: Características de la red con máscara /25.

Para nuestro caso, grupo 7, sección 1, la dirección IP del PC-B termina en 71, por lo que todo sigue funcionando igual, y esto será así mientras la IP del PC-B esté en el rango de host utilizables. Pero si por el contrario la IP no estuviera en el rango descrito en la tabla 1 como es el caso de la siguiente imagen (26), las conexiones fallarian para llegar a este host y para que este host pueda acceder a su router, ya que IP y gateway están en redes diferentes.

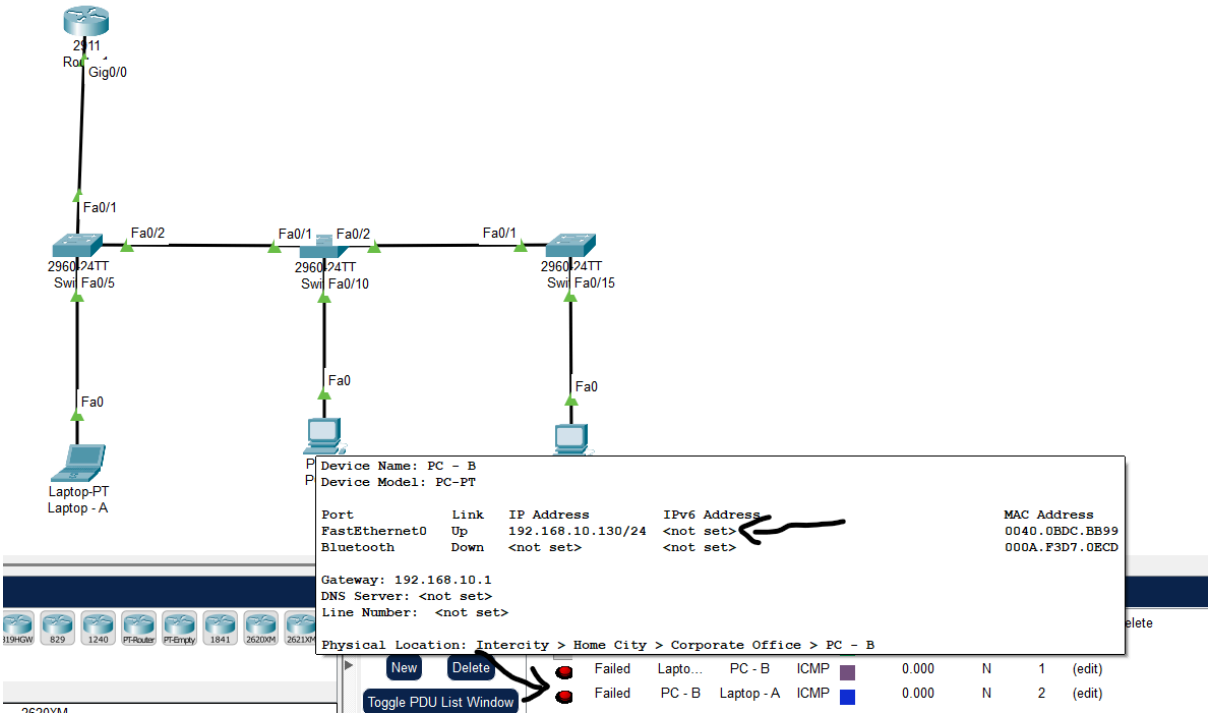


Imagen 26: Cambio de IP en PC-B para mostrar fallas en Pings.

Para estos casos, para que funcione con una máscara de /25, es necesario cambiar el comando por el siguiente:

ip address 192.168.10.129 255.255.255.128

y en la configuración del PC-B asignar esta nueva dirección al gateway.

Cabe resaltar que todo es un escenario explicativo ya que nuestra ip: 192.168.10.71 sigue funcionando con todos los pings como se puede apreciar a continuación:

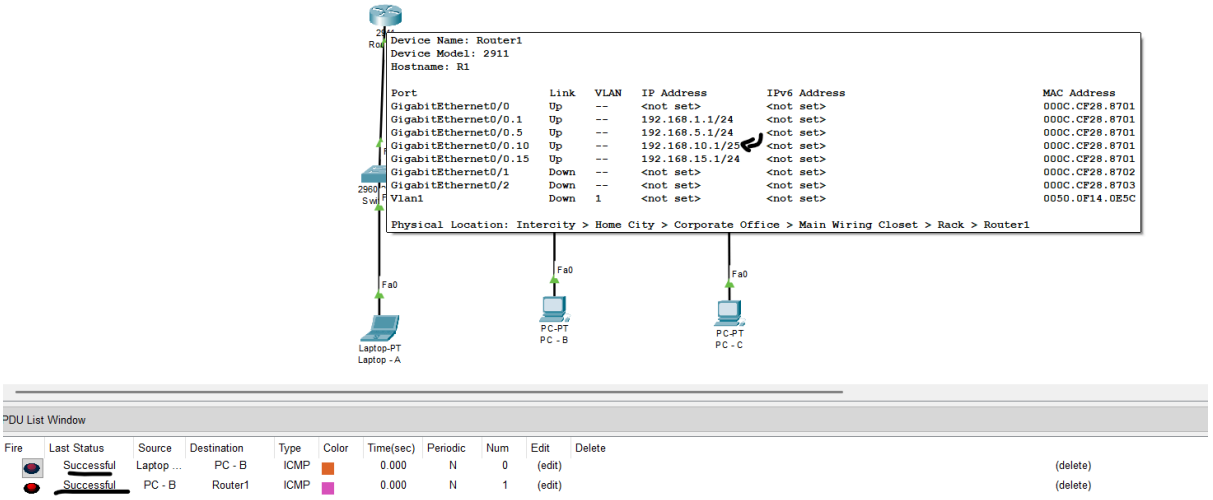


Imagen 27: Buen funcionamiento de la máscara /25 en VLAN 10

4. **Cree una ACL que:**
    - **Permita a VLAN 5 comunicarse con VLAN 10**
    - **Pero bloquee la VLAN 10 hacia la VLAN 5**
    - **Y aún permita que ambas lleguen al gateway de VLAN**

   Explique dónde la aplicó, muestre capturas del proceso y funcionamiento

Un ACL, por sus siglas significa Access Control List, es decir, funciona análogo a un cortafuegos que filtra el tráfico por puertos y por direcciones IP. En este caso, un ACL se puede aplicar tanto a un switch como a un router y dependiendo de la VLAN, bloquea el tráfico que va o que pasa por el dispositivo.

Para este laboratorio, con bloquear la comunicación desde la VLAN 10 hacia la VLAN 5, se cumplen las otras 2 restricciones propuestas, puesto que la llegada al gateway de ambas VLAN es independiente de la conexión entre VLAN 10 y VLAN 5, hacer el bloqueo propuesto satisface esta restricción; al solo bloquear la comunicación en un sentido, la VLAN 5 se podrá seguir comunicando con la VLAN 10 en esa dirección.

Para implementar una ACL, se debe ingresar a la configuración del router on-stick, dispositivo que se encarga de hacer el enrutamiento (y por ende puede filtrar) entre las diferentes VLAN con los siguientes comandos:

```
R1>enab
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#ip access-list extended BLOQUEO_PUNTO4
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int g0/0.5
R1(config-subif)#ip access-group BLOQUEO_PUNTO4 out
R1(config-subif)#exit
R1(config)#
```

Copy Paste

Top

Imagen 28: Comandos para configurar el ACL en el router.

A modo de resumen, los comandos primero crean una lista de acceso en la que se niega el tráfico cuyo origen pertenece a la red de la VLAN 10, utilizando la wildcard correspondiente de la máscara /24. Una vez definida la ACL, esta se aplica a la interfaz asociada a la VLAN 5, indicando que ningún paquete proveniente de dicha red debe salir por esa interfaz. En otras palabras, todo tráfico cuyo origen sea la red de la VLAN 10 será bloqueado cuando intente pasar por la interfaz de la VLAN 5. En la siguiente imagen se ve el total de las listas de acceso en el router, comprobamos que quedó bien configurada:

```
R1#show access-lists
Extended IP access list BLOQUEO_PUNTO4
    10 deny ip 192.168.10.0 0.0.0.255 any
    20 permit ip any any (11 match(es))
```

Imagen 29: show access

Para probar el funcionamiento se realizó una simulación de pings donde el comportamiento corresponde al esperado:

- El ping desde VLAN 5 a VLAN 10 funciona pero el reply desde VLAN 10 a VLAN 5 falla, por ende, el ping total falla.
- Ping entre VLAN 5 y VLAN 15 funciona, ping entre VLAN 10 y VLAN 15 funciona.
- El ping desde VLAN 10 a VLAN 5 falla desde el primer envío de los paquetes ICMP de VLAN 10 a VLAN 5.

Estos resultados se pueden ver en la siguientes imágenes, viendo el estado de los pings y el flujo que siguieron en la simulación:

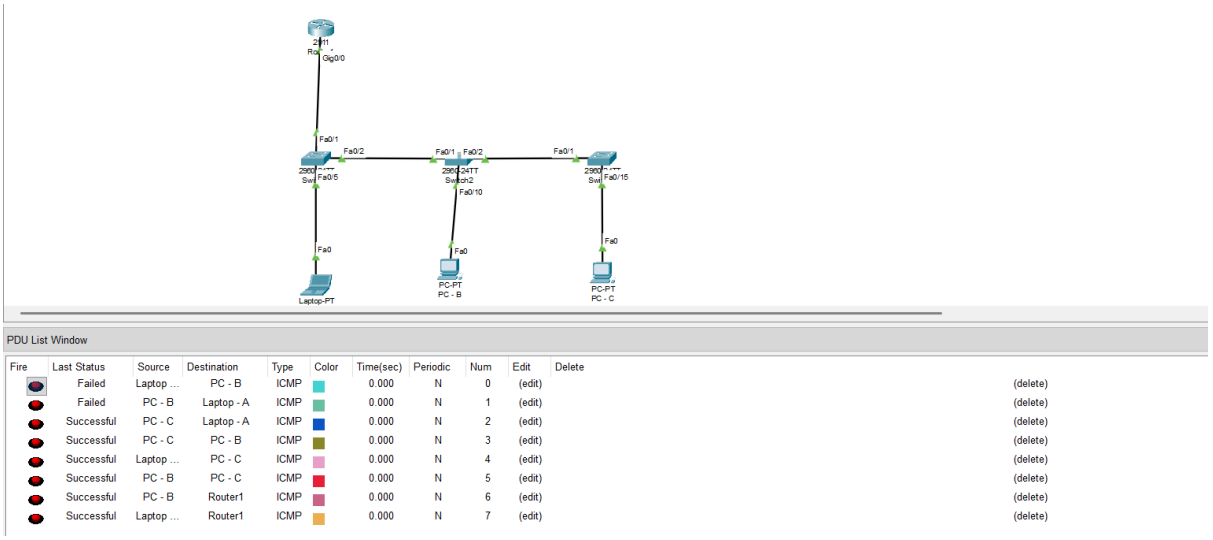


Imagen 30: Pings entre las diferentes VLANs y de VLAN 5, 10 al gateway.

En las siguientes imágenes se ve el tránsito de los paquetes, desde que cada paquete llega al router con la dirección de red de la VLAN 10 (ya sea request o reply), el tráfico se detiene y se demuestra el funcionamiento de la ACL correctamente.

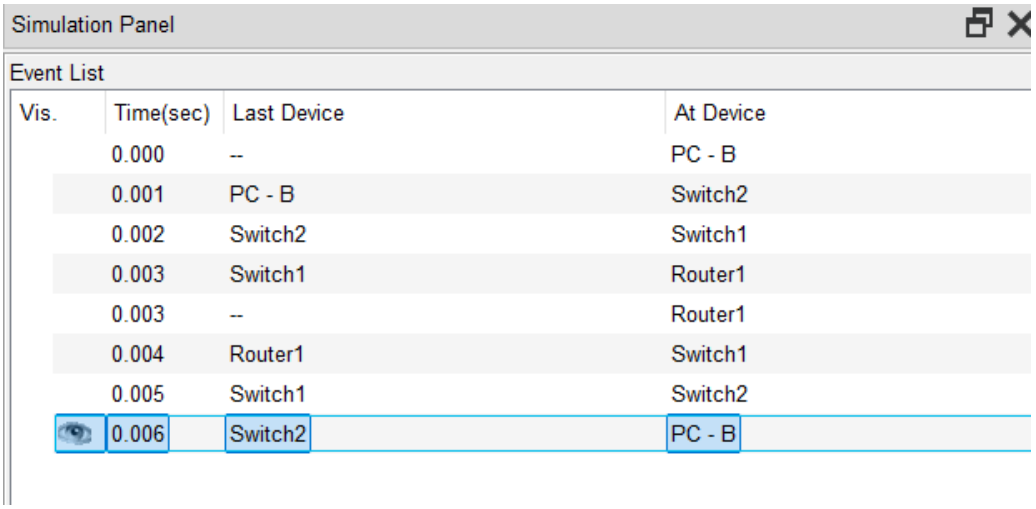


Imagen 31: Ping desde PC-B a Laptop A.

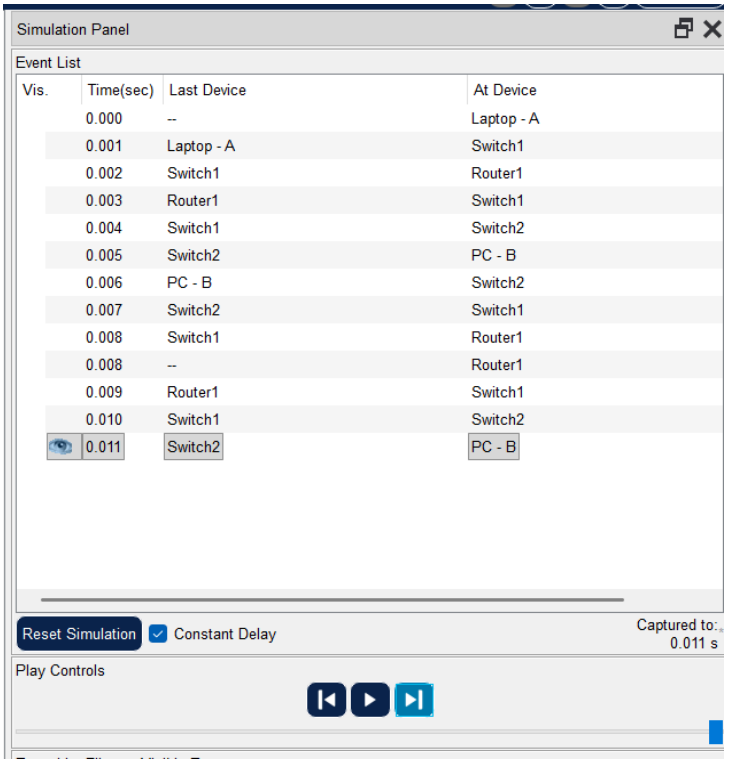


Imagen 32: Ping desde Laptop A a PC-B.

5. **Cambie solo la siguiente línea en el router 1:**

R1(config-subif)# encapsulation dot1Q 10

Por:

R1(config-subif)# encapsulation dot1Q 10 native

- **Muestre la tabla de ARP de VLAN 10 y VLAN 1**
- **Determine si VLAN 10 recibe o envía tráfico como VLAN nativa y explique qué significa esto**
- **Explique exactamente qué está pasando en la conectividad**
- **Revise si alguna VLAN recibe tráfico "erróneo" y por qué.**

En un análisis preliminar, al cambiar esa línea de la configuración, el router dejará de etiquetar las tramas que envía al switch con la VLAN 10, es decir, no se podrá acceder a los dispositivos de la VLAN 10 desde el router. Esto, se debe a que el router envía las tramas sin la etiqueta, pensando que es la VLAN nativa, pero para el switch, la VLAN nativa sigue siendo la VLAN 1 (no se cambió la configuración predeterminada de los switches cisco), por lo que no hay consistencia entre estos y la topología falla para los dispositivos de VLAN 10.

En un primer lugar, las tablas ARP de VLAN 10 y VLAN 1 corresponden a las siguientes imágenes:

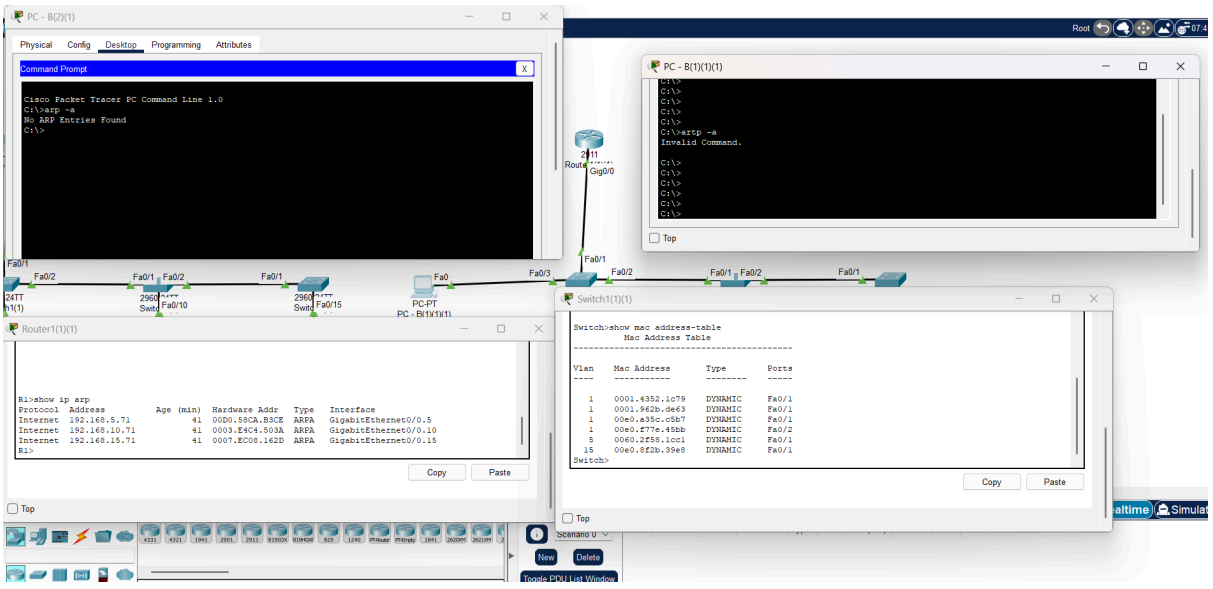


Imagen 33: Tablas ARP del switch 1, router, PC en VLAN 10 y PC en VLAN 1

Como se puede observar en las imágenes, las tablas ARP no tienen entradas pues las VLAN no se pueden conectar, y aunque llegue al router, el paquete reply del ping no se puede completar y por ende los PC no pueden aprender la MAC de su router. Por su parte, en el switch se puede ver que la tabla de direcciones MAC sí está poblada con varias direcciones asociadas a los puertos y a las VLAN correspondientes, lo que indica que el tráfico de capa 2 sigue llegando al switch y éste aprende las MAC de origen, pero esto no garantiza conectividad de capa 3 entre VLAN. En el router, en cambio, al revisar el comando show ip arp solo aparecen entradas para algunas redes y no se observan registros de los

hosts de las VLAN 1 y 10, lo que evidencia que, debido al desajuste de la VLAN nativa en el enlace router–switch, el proceso de ARP nunca se completa para esas VLAN y el gateway no puede resolver sus direcciones MAC ni hacer el enrutamiento inter-VLAN correspondiente.

En segundo lugar, se puede ver con un ping y el modo de simulación, que el ping llega al router, pero en este punto, el router envía las tramas sin la etiqueta correspondiente por lo que el switch envía todo el tráfico nativo a VLAN 1, independientemente si el tráfico original tenía una etiqueta de VLAN 10 o no. Todos los hosts de VLAN 1 recibirán tráfico erróneo correspondiente al enviado para VLAN 10. Para esta parte del laboratorio, se decidió crear un nuevo PC con la finalidad de mostrar los paquetes que llegan a VLAN 1 como se ve a continuación:

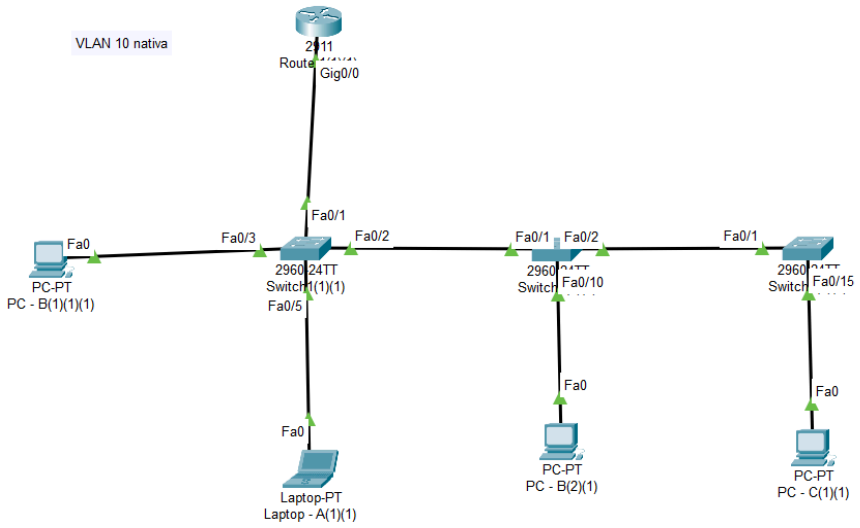


Imagen 34: Topología modificada con PC en VLAN 1.

Esta topología se puede encontrar en el archivo adjunto topologia5.pkt, al hacer esto, se comprobó que un ping entre VLAN 5 y VLAN 15 todavía es posible, pero al intentar interactuar con VLAN 1 o VLAN 10 todos los pings fallan por la siguiente razón:

- VLAN 1: Al comunicarse con VLAN 1, los ICMP se envían desde aquí con la etiqueta para VLAN 1, llegan al switch, al ser la VLAN nativa aquí, las tramas se envían sin ninguna etiqueta y el router sabe que vienen de una VLAN nativa; para el router la VLAN nativa es 10 por lo que concluye que debe meter las tramas en la VLAN 10 y en ese cambio de red, la comunicación con VLAN 1 falla.

- VLAN 10: Para la VLAN 10 la situación es un poco diferente, todo lo tráfico que vaya para la VLAN 10 saldrá del router sin etiqueta, por lo que el switch pensará que es para la VLAN 1 (es la nativa para el switch), por lo que se redireccionará para la VLAN 1 y nunca llegará a su destino en la VLAN 10.

En este sentido, todo el tráfico dirigido a VLAN 10 será recibido por VLAN 1, representando un gran problema para la conectividad y la seguridad de la red.