**Laboratorio 09. RECO-02**

Jefer Alexis González Romero

**Introducción**

En este laboratorio, daremos continuidad a la configuración básica de switches que vimos en el laboratorio anterior. Repasaremos la asignación de nombres, mensajes del día, sincronización de la pantalla y bloqueo de la búsqueda de comandos en un servidor externo. Esta configuración nos ayudará en la creación de una red de área local (LAN) y a adentrarnos más en su infraestructura. Además, utilizaremos un sniffer para capturar paquetes y examinar los frames Ethernet, lo que nos proporcionará un mayor conocimiento sobre su estructura.

Durante la configuración de las redes LAN, nos enfocaremos en la configuración de las redes de área local virtual (VLAN). Prestaremos atención a aspectos como el ID y nombre de las VLAN, el modo de asociación de VLAN para los puertos y la forma en que se asigna una VLAN a cada uno.

Adicionalmente, llevaremos a cabo un montaje utilizando Cisco Packet Tracer, donde analizaremos el comportamiento de la red y reforzaremos el protocolo ARP, junto con el formato de los frames Ethernet. Realizaremos envíos de paquetes entre hosts, partiendo de una tabla de ARP vacía y culminando con la configuración de tres VLAN.

**Desarrollo del tema**

**Marco teórico**

Para comprender lo que se va a trabajar es necesario tener presentes unos conceptos, en primer lugar, una red de área local (**LAN)**, son redes contenidas en una ubicación pequeña, normalmente dentro del mismo edificio (Clodflare, s.f.)​. Estas redes se pueden dividir en red de área local virtual (**VLAN**), las cuales son redes que nos permiten crear redes lógicamente independientes dentro de la misma red física, haciendo uso de **switches,** dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (Redes Telemáticas, 2013).

El protocolo de la capa de red que repasaremos es **ARP,** el cual convierte dinámicamente las direcciones de Internet en las direcciones de hardware exclusivas de las redes de área local ​ (IBM, 2021).Tanto para la configuración de la LAN y para el protocolo ARP se analizará **el frame Ethernet**, tienen información de control sobre los datos, información sobre las direcciones de origen y destino de los envíos y un registro de los datos enviados (Geyma, 2021)​. Este análisis se hará en la herramienta **Wireshark,** herramienta para capturar y analizar paquetes de datos intercambiados por medio de protocolos web (Keepcoding, 2022).

Además, realizaremos montajes simulados a través de **Cisco Packet Tracer**, una herramienta que nos ayuda a diseñar redes y realizar simulaciones, que además nos permiten ver cómo los dispositivos interactúan entre sí (Cisco Networking Academy, s.f.).

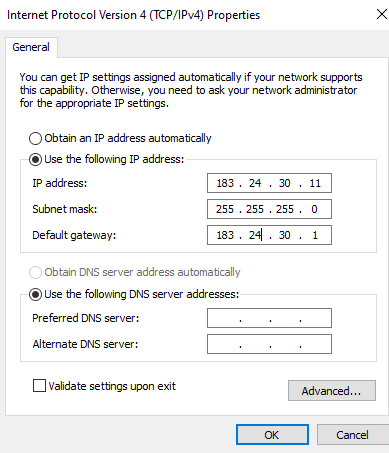
**Uso y aplicaciones**

**Instalación de software**

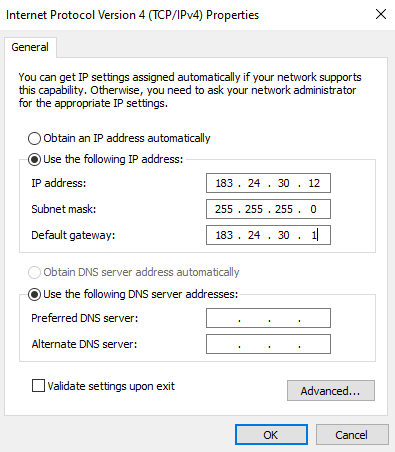
1. **Configuración básica del switch**

* Configure los equipos con la ip 183.24.30.0/24 y un consecutivo que sea el número del equipo del Laboratorio.

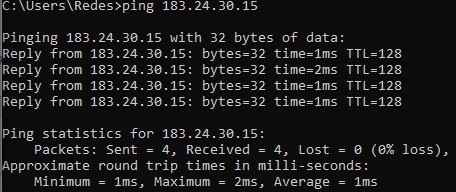
Computador 11



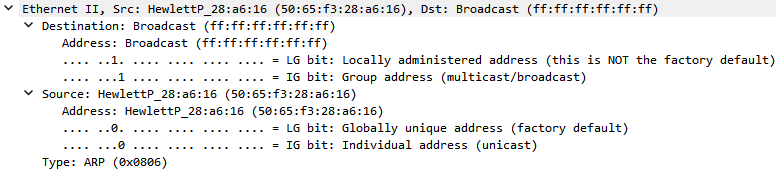
Computador 12



* Verifique conectividad entre los computadores usando el comando ping.

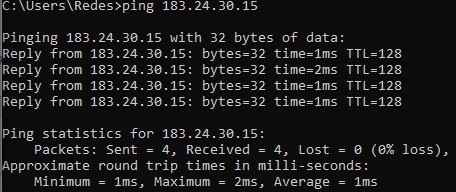


* Usando Wireshark capture un paquete y revise el frame Ethernet. Verifique estructura del frame, direcciones MAC, control de errores, etc.

****

Los campos que nos dan en el frame de Ethernet son la dirección MAC de origen que es HewlettP\_28:a6:16 y la dirección del dispositivo de destino que en este caso como aún no sabemos la dirección MAC de destino se hace una petición con el protocolo ARP y esta es enviada a la dirección broadcast (ff:ff:ff:ff:ff:ff). Además de las direcciones nos dan el protocolo que está encapsulado en la carga útil, en este caso es ARP (0x0806). Por último, el control de errores que Wireshark ya no lo muestra predeterminadamente porque no siempre se presenta en la captura. El FCS (Frame Check Sequence) es llenado por el host de envío, en el caso de Ethernet, con el algoritmo de CRC (Cyclic Redundancy Check), este es formado por 4 Bytes

* Interconecte los montajes de todo el grupo y verifique que se vean entre ellos haciendo uso del comando ping



1. **Configuración básica del switch**

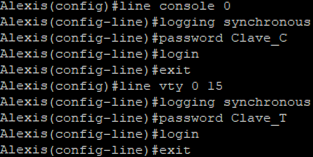
* Nombre del switch: NombreEstudiante.



* Mensaje del día: “Uso exclusivo para estudiantes de RECO – Lab9”



* Sincronización de pantalla y claves de acceso al equipo.





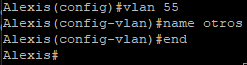
1. **Configuración de VLAN**

* Configure dos VLANs1

1. sistemas à VLAN\_ID 50 (marco circular azul)

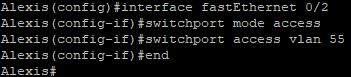


1. otros à VLAN\_ID 55 (marco circular verde)



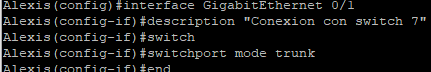
* Configure los computadores pares en la VLAN sistemas, los computadores impares en la VLAN otros.



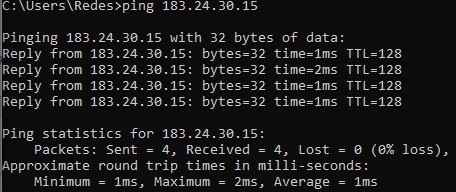


* Configure en enlace entre los switches para que permita la conexión de VLANs (Pista: ¿Qué son los enlaces troncales?, ¿para qué se usan?)

Un enlace truncal es un enlace punto a punto entre dos dispositivos de red que llevan mas de una VLAN. Un enlace truncal de VLAN amplía las VLAN através de toda la red.

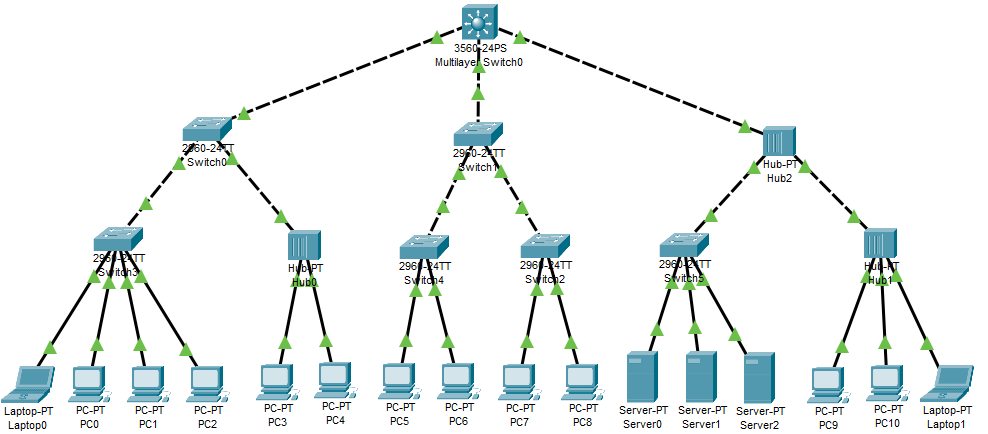


* Verifique conectividad.



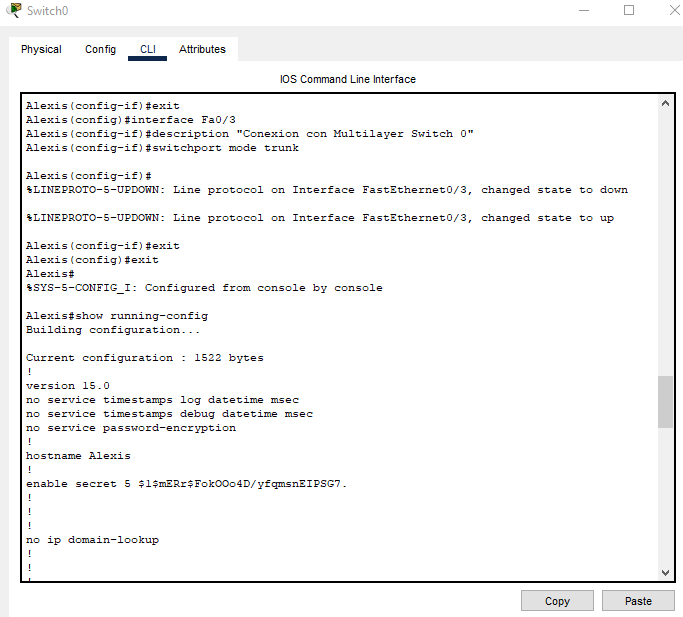
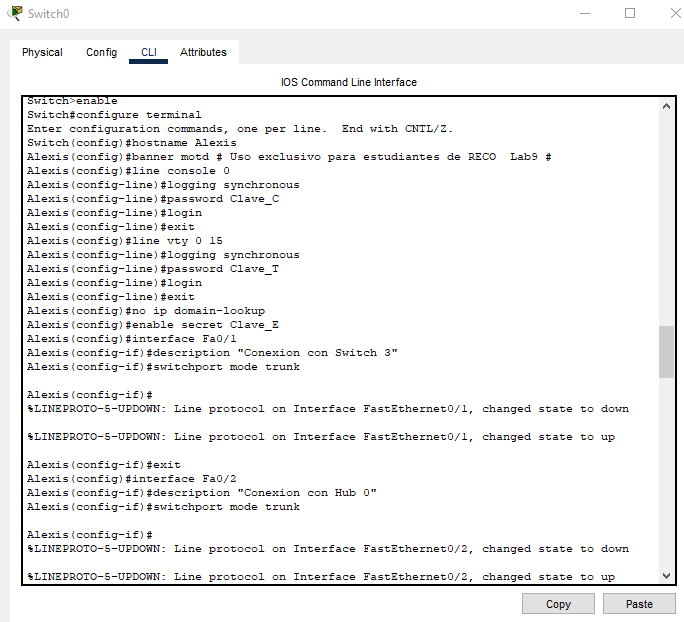
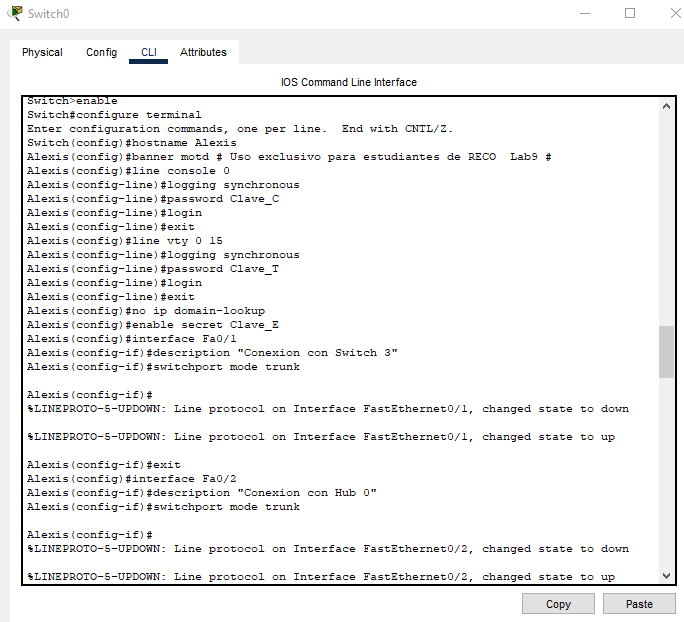
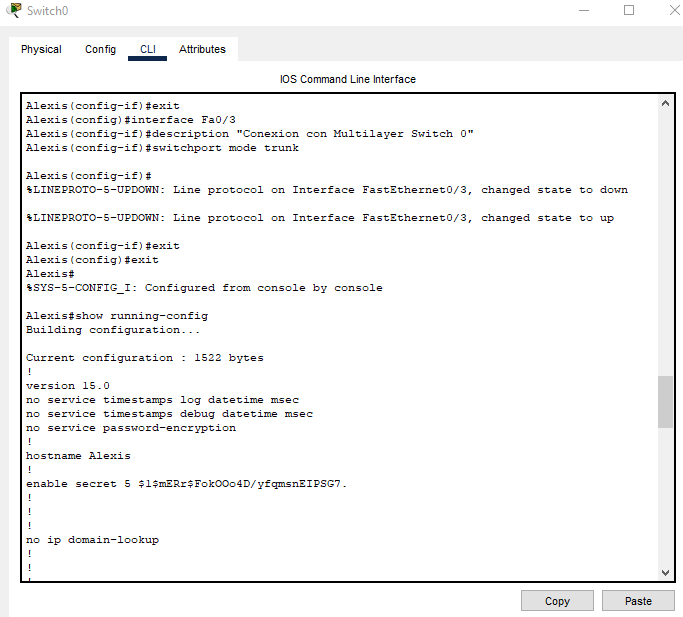
**Simulación**

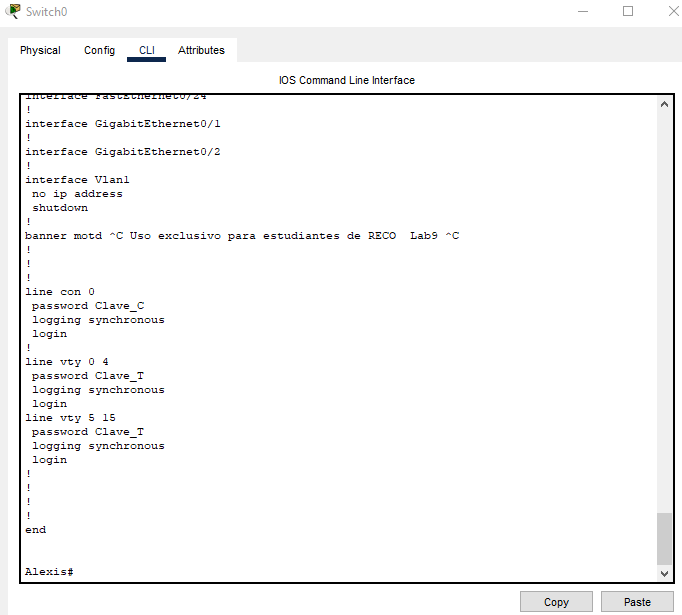
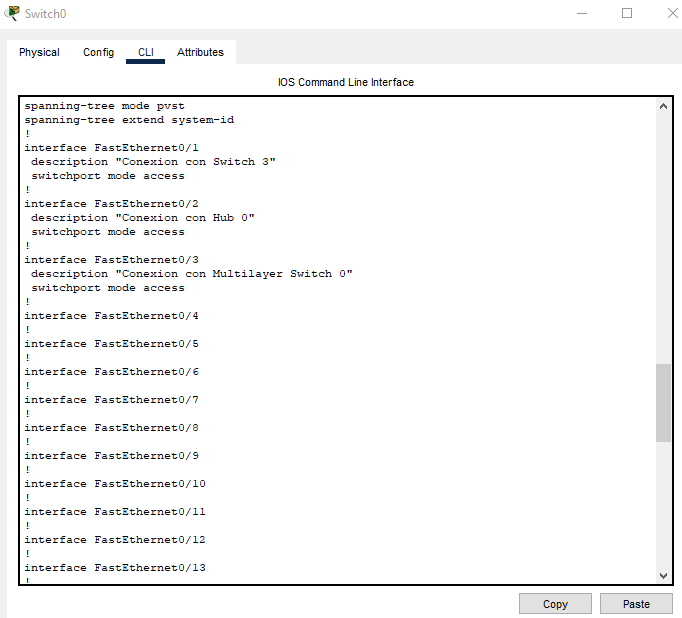
1. **Redes de switches más grandes**



* Realice la configuración básica a TODOS de los switches

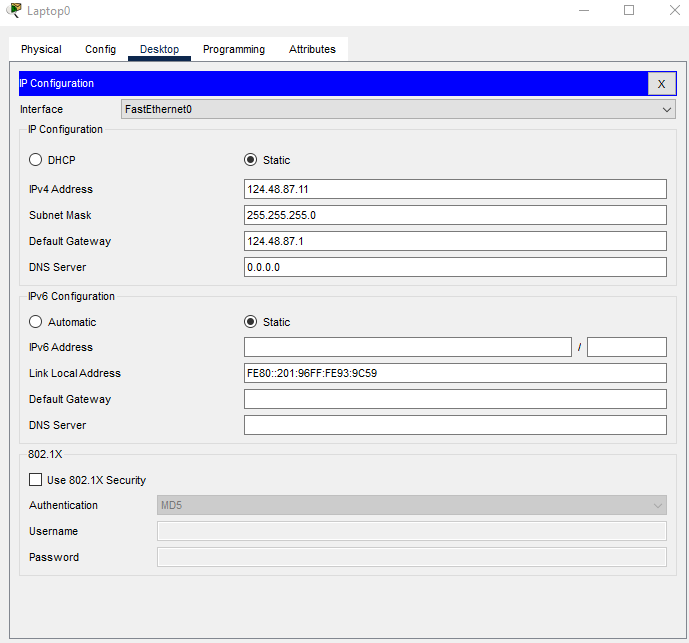
Se configuran los nombres, mensajes del día, sincronización de la pantalla y bloqueo de la búsqueda de comandos en un servidor externo y las interfaces de los switches con su respective descripción.



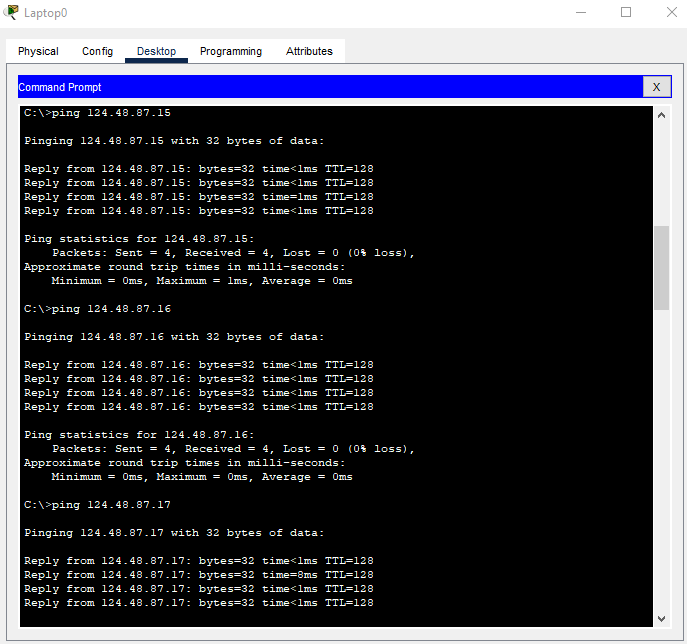
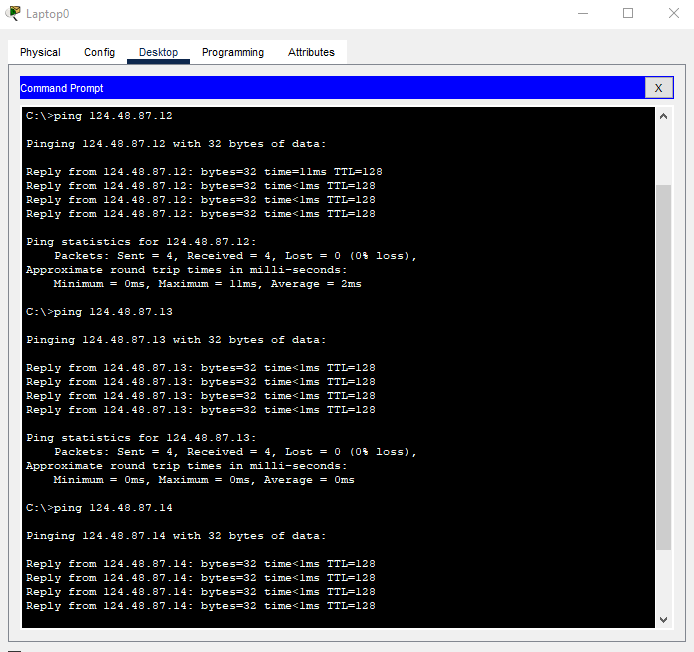
* Configure los computadores y servidores con la información que se indicada a continuación:

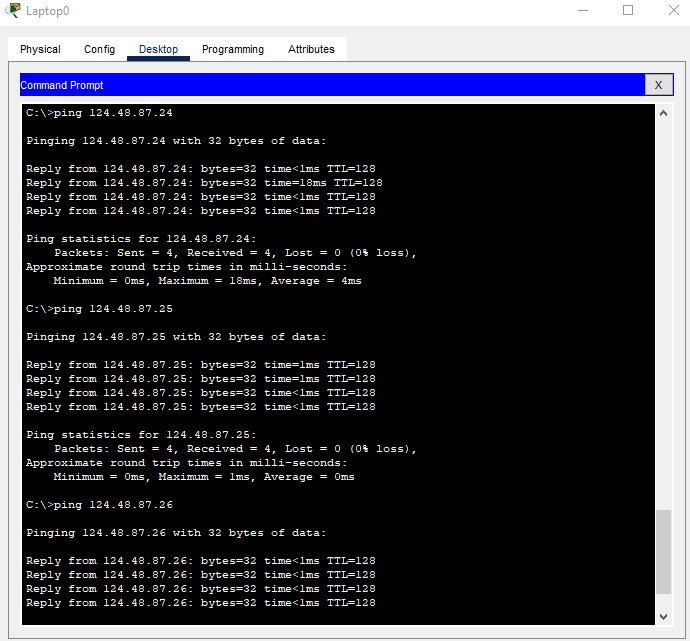
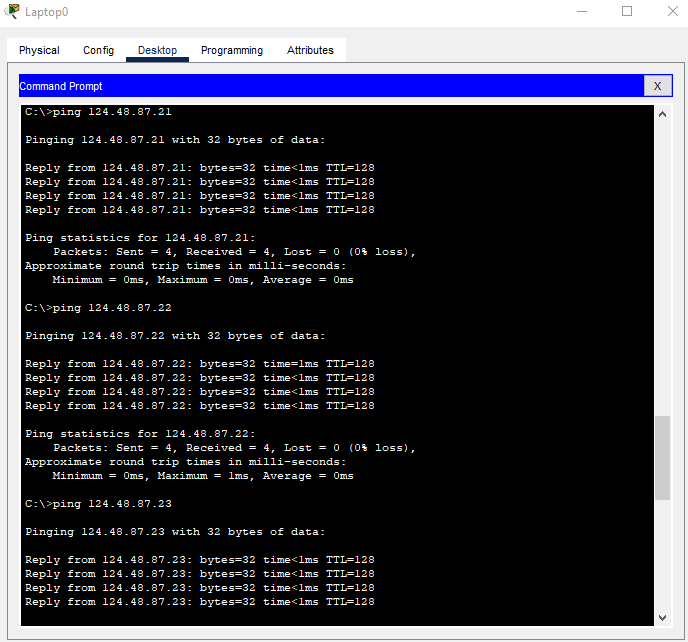
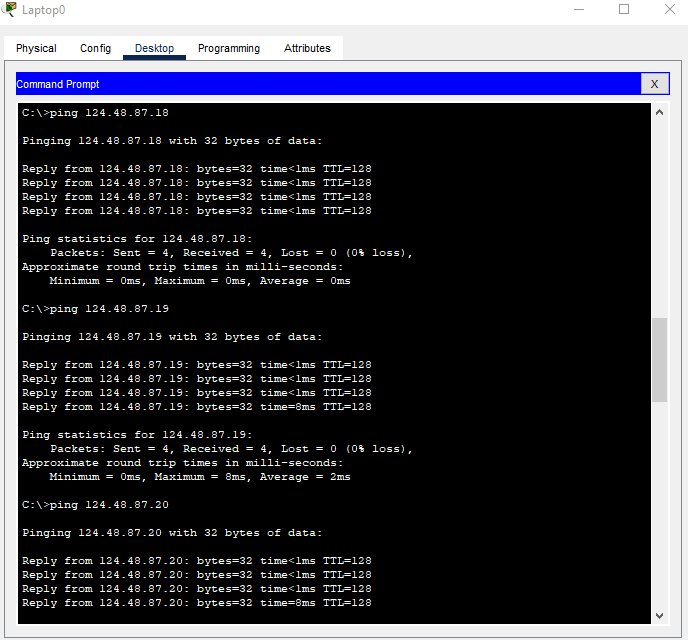
En cada computador, laptop y servidor se le asigna una dirección IP, se le ingresa su mascara y el gateway.



* Revise conectividad entre los equipos

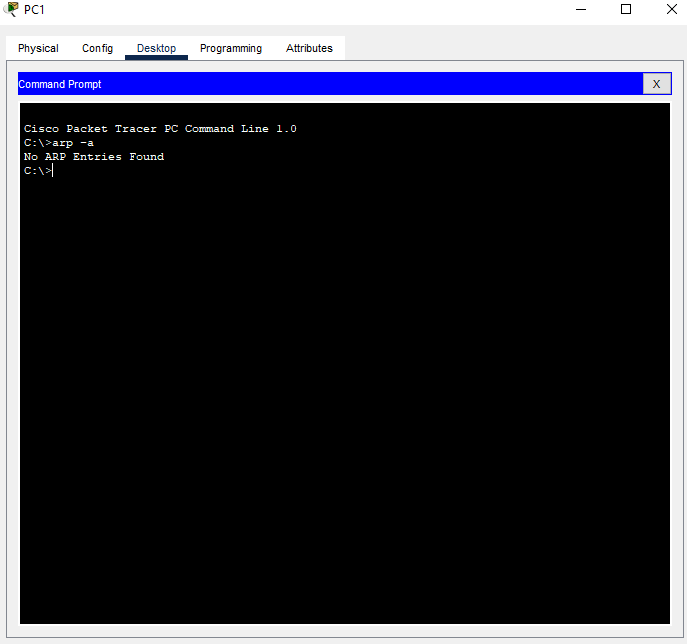
Se realiza ping a todos los dispositivos desde la Laptop 0 para comprobar la conexión.



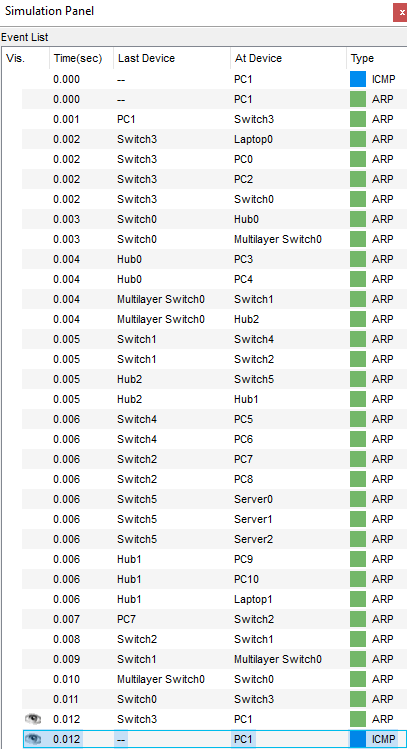
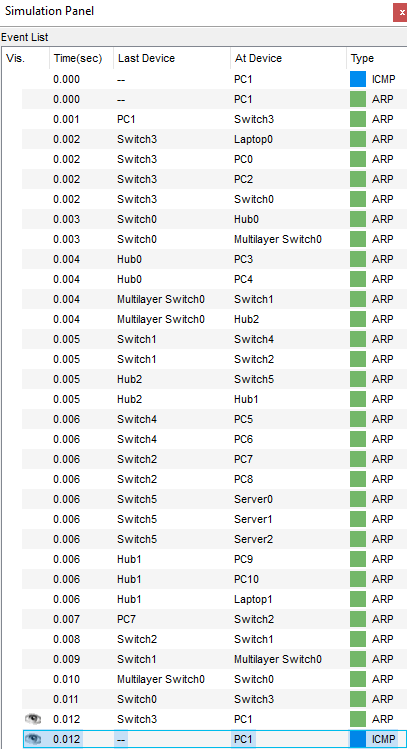


* Usando el modo simulación, revise el comportamiento de la red y el formato de un frame Ethernet al enviar los siguientes frames. Identifique el comportamiento de los switches y las tablas de dispersión.

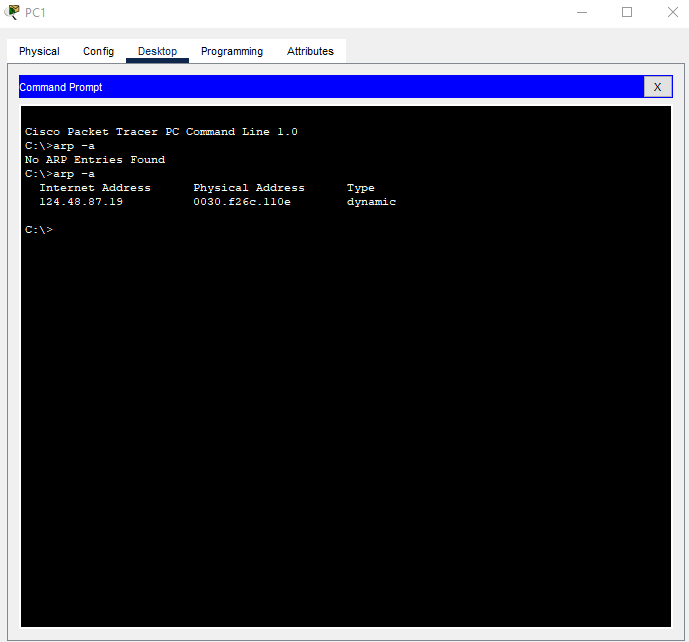
Se ve como está la tabla actual de ARP



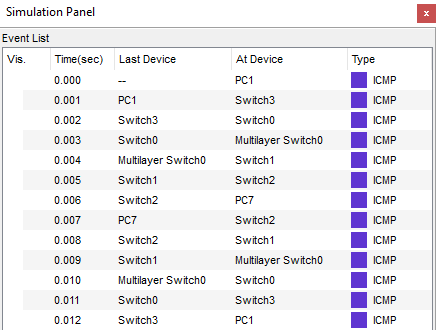
Ahora se envía un paquete desde PC1 hasta PC7 y en el modo simulación se ve el comportamiento de la red.



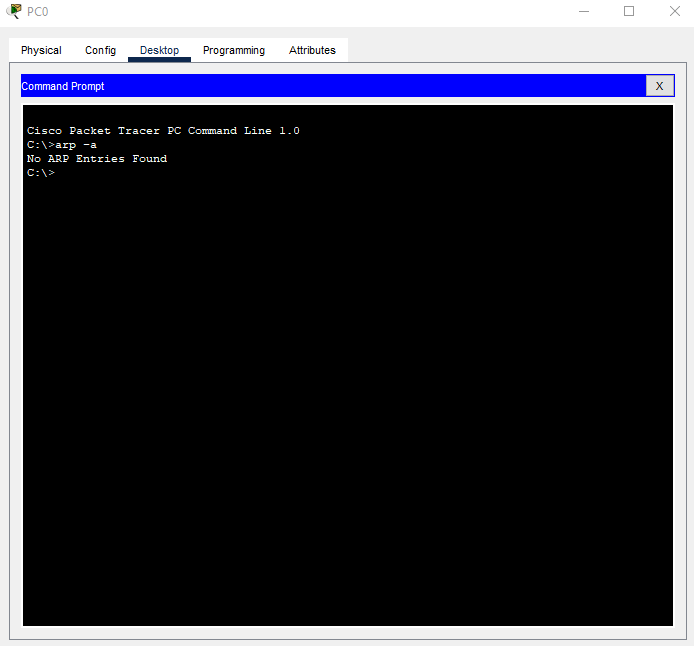
Después de enviar el paquete y con las tablas de ARP limpias, el computador que hace el Echo Request necesita conocer la dirección MAC del host de destino, es acá donde se usa el protocolo ARP que nos permite resolver la dirección IP del host de destino en su dirección MAC, para esto envía un paquete de petición a la dirección broadcast de la red preguntando quien tiene la IP dada en este caso 124.48.87.19, todos los hosts en la red reciben el paquete de solicitud ARP y el host que tenga la dirección IP responden con un paquete de respuesta dando su dirección MAC, en este caso 0030.f26c.110e.



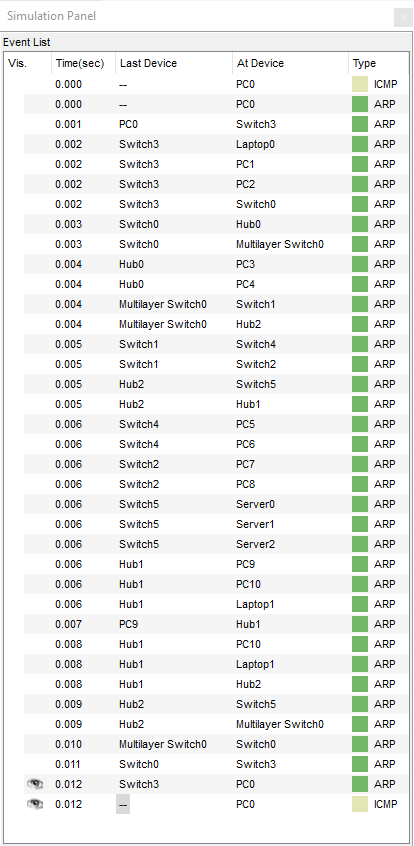
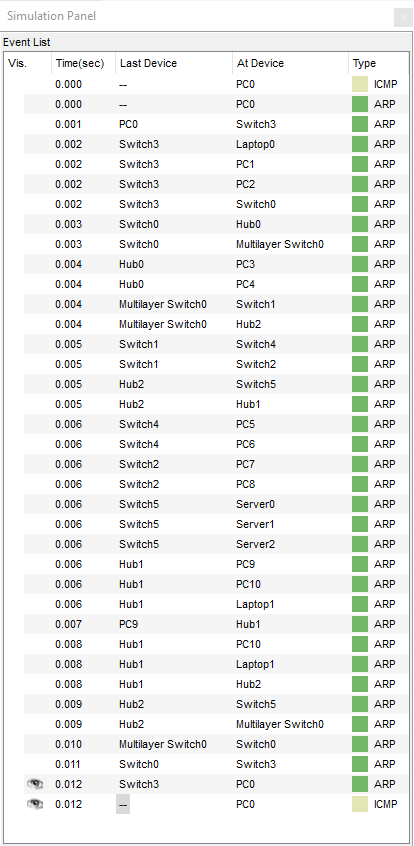
Ahora como el computador ya conoce a que dirección MAC corresponde a la IP 124.48.87.19, puede enviar el paquete directamente a el.



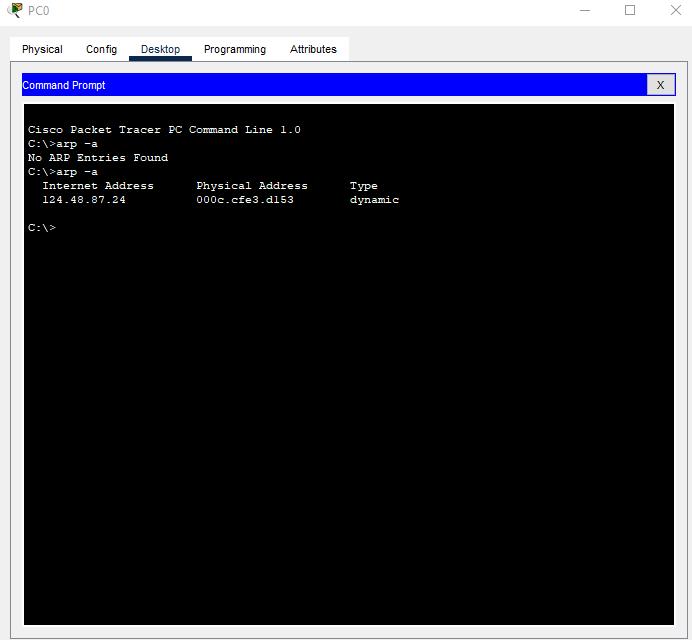
Ahora se hace lo mismo con el PC0, verificamos su table de ARP



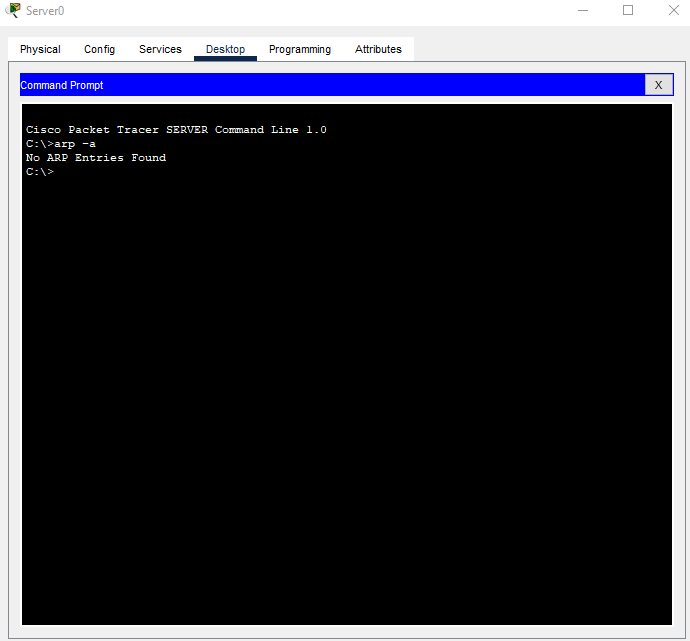
En el modo simulación se revisa el envío de los paquetes.



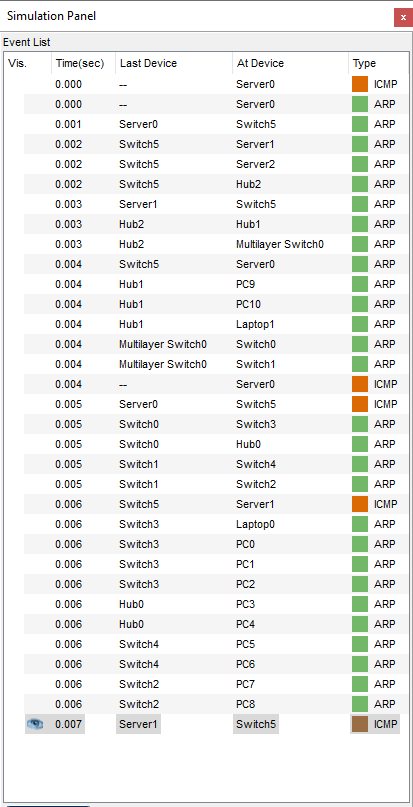
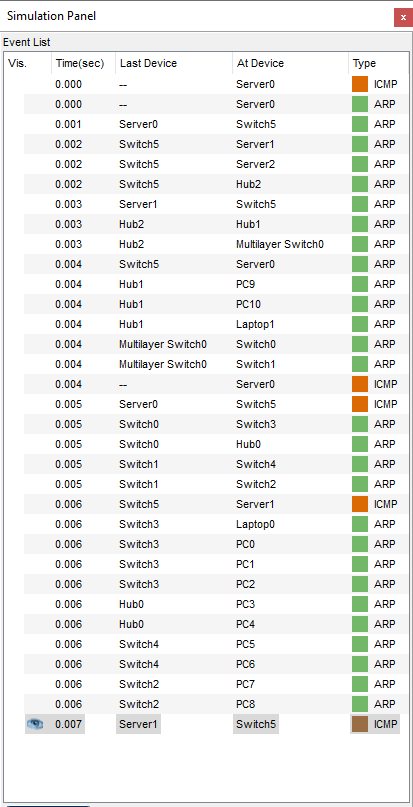
Se agrega a la tabla ARP la nueva resolución para la dirección IP 124.48.87.24, que es 000c.cfe3.d153.



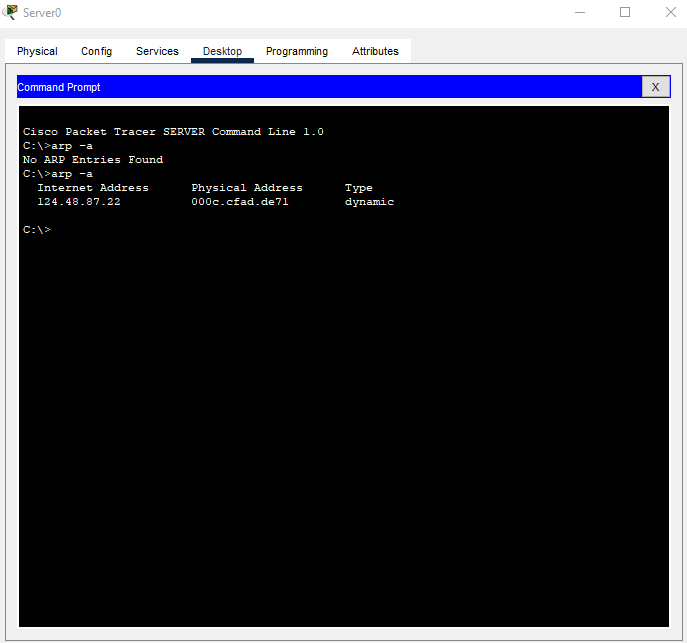
Verificamos la table ARP del Server 0, esta debe estar vacía.



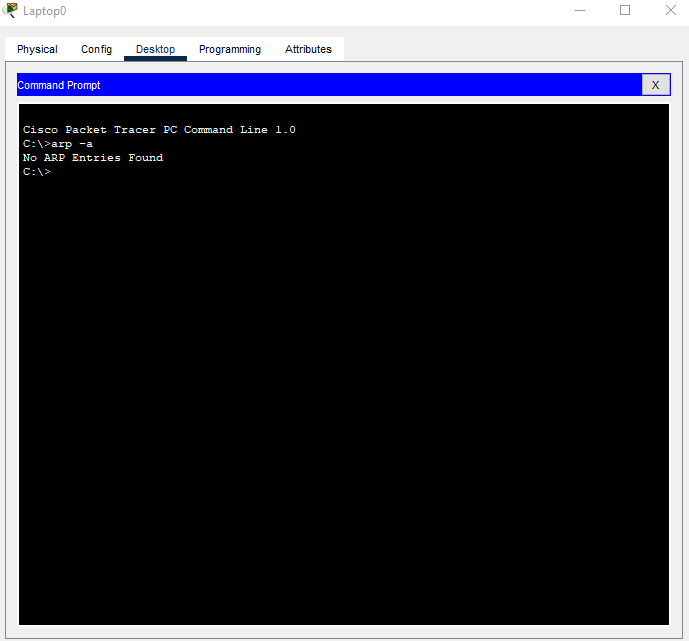
Después de enviar el mensaje comienza enviando un broadcast para ver a que host le corresponde la dirección IP, por cada switch que pasa este hace broadcast, como se puede ver aunque ya se haya encontrado al que le corresponde la IP, los switches siguen enviando mensajes broadcast.



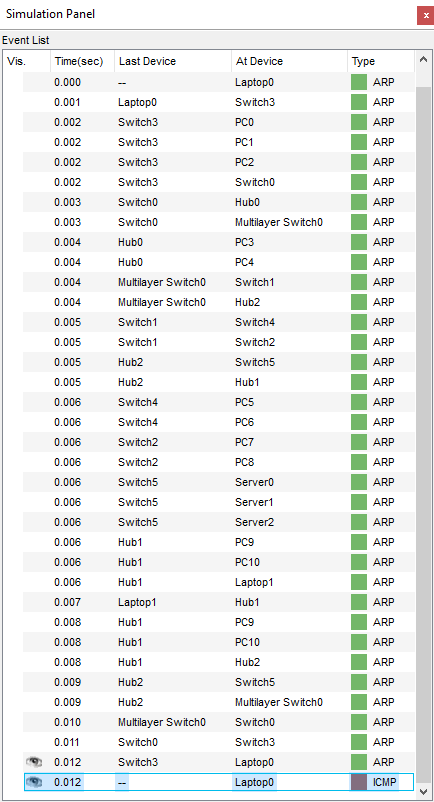
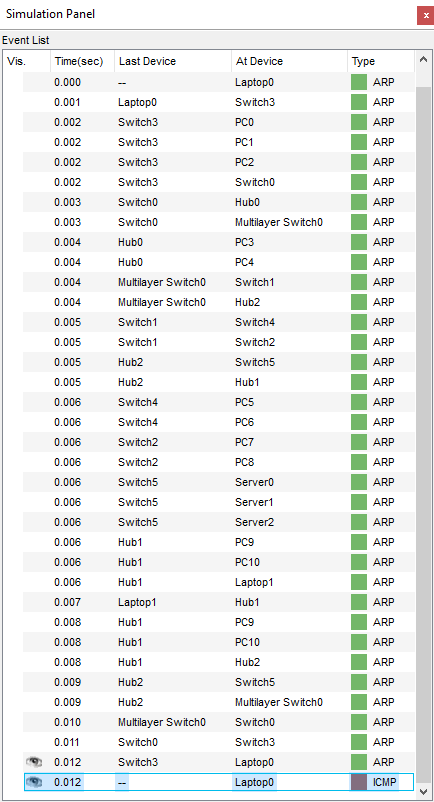
Se verifica que ahora se tenga la equivalencia MAC de la dirección IP a la cual habíamos enviado el mensaje.



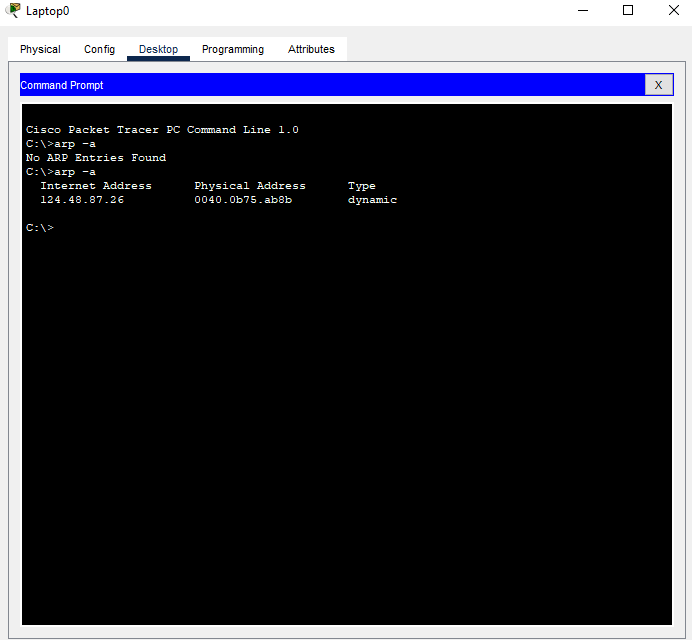
Por ultimo se envía un mensaje desde la Laptop 0 hasta la Laptop 1, inicialmente la Laptop 0 no tiene ningún registro en la table ARP.



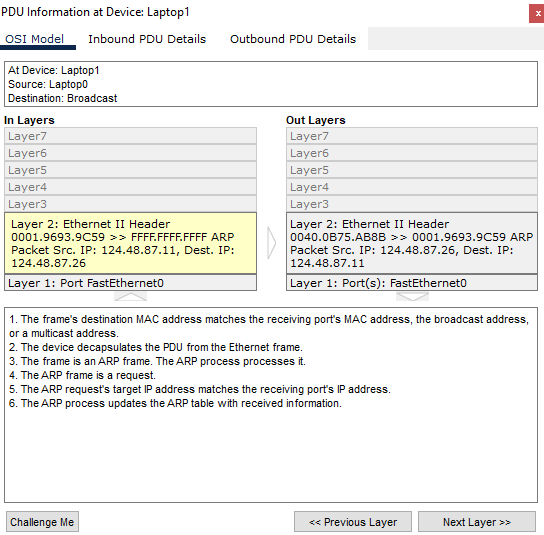
Al igual que en los anteriores casos, para que pueda enviar el paquete, primero debe conocer la dirección MAC correspondiente al host que se le quiere hacer llevar, para esto actúa el protocolo ARP enviando mensajes de broadcast con el fin de saber a quién le corresponde.



Después de que le llegue la respuesta a la Laptop 0 con la dirección MAC correspondiente a la IP que dio, se llena la table ARP con esta equivalencia.

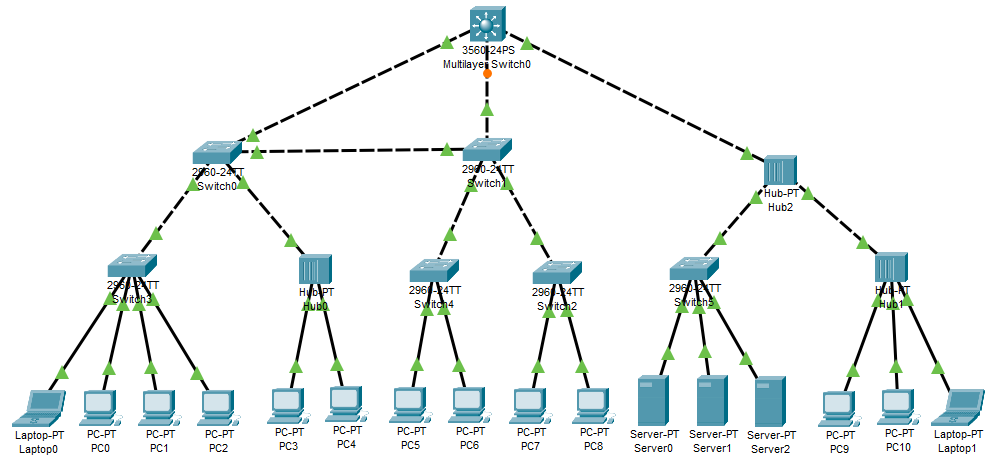


En el frame Ethernet se puede ver la dirección de origen desde donde se quiere enviar el mensaje y la dirección de destino que al conocer la dirección MAC de destino se envía el mensaje broadcast el cual, después de que le llega al correspondiente host, ya se pueden ver las direcciones MAC tanto de origen como de destino, en ambas partes también se incluyen las dirección IP de destino y origen.

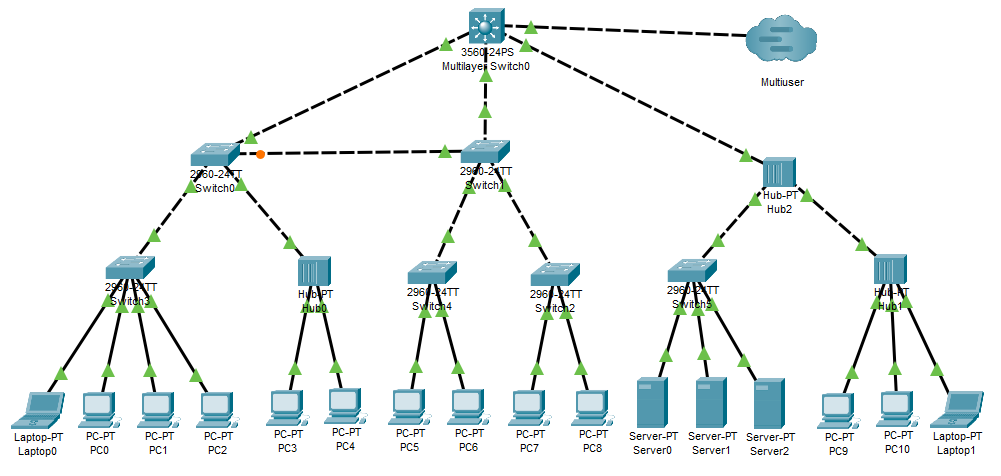


* Revise la operación del algoritmo spanning tree, para ello interconecte los switches 0 y 1 y vea el comportamiento de los enlaces.

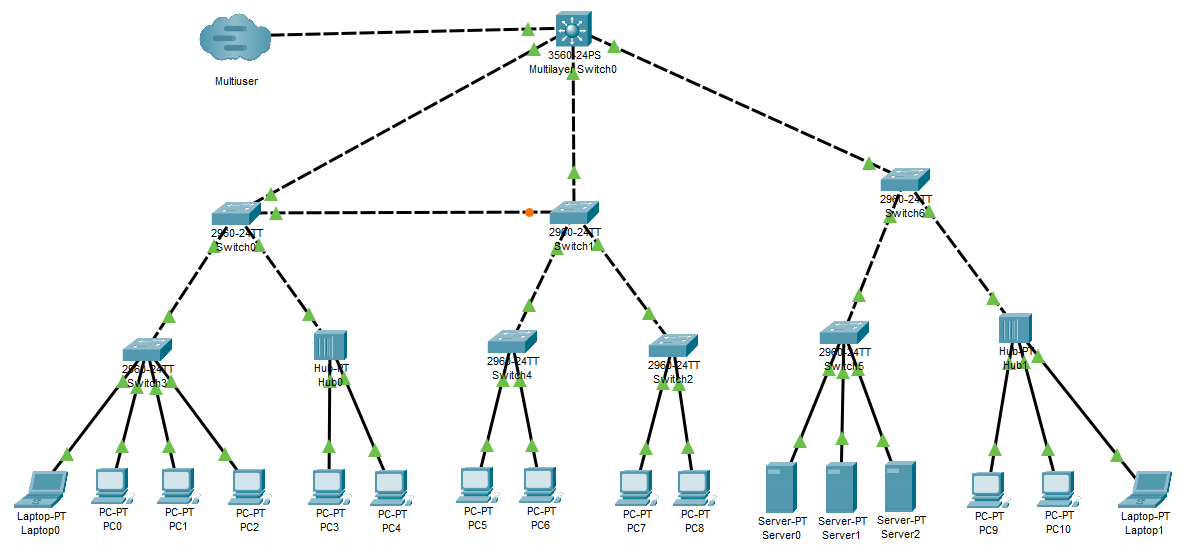
El objetivo de Spanning Tree es controlar los enlaces redundantes, para asegurar el rendimiento de una red. Como se ve para llegar del switch 1 al Multilayer Switch0 lo hace a través del Switch 0, deshabilitando el camino que tiene directo con este (Punto Naranja)



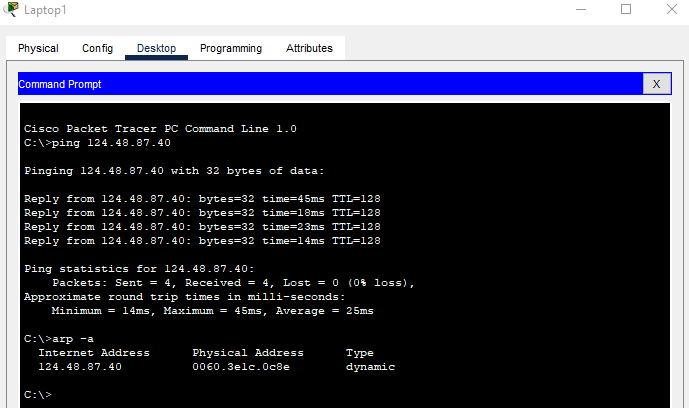
* Interconecte los archivos de los miembros del equipo.



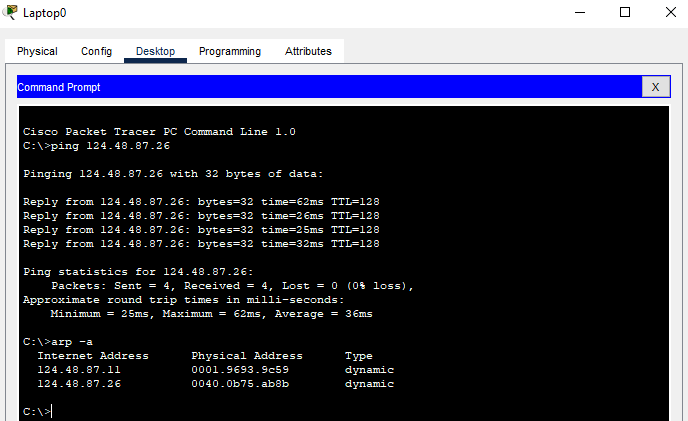
El archivo con el montaje fue facilitado por Ricardo Pulido



Comprobamos la conexión con el comando ping hacienda la petición desde Laptop 0 del estudiante 2 (Ricardo) que tiene IP 124.48.87.40 hasta la Laptop 1 del estudiante 1 (Alexis) con dirección IP 124.48.87.26 y verificamos la table de ARP.

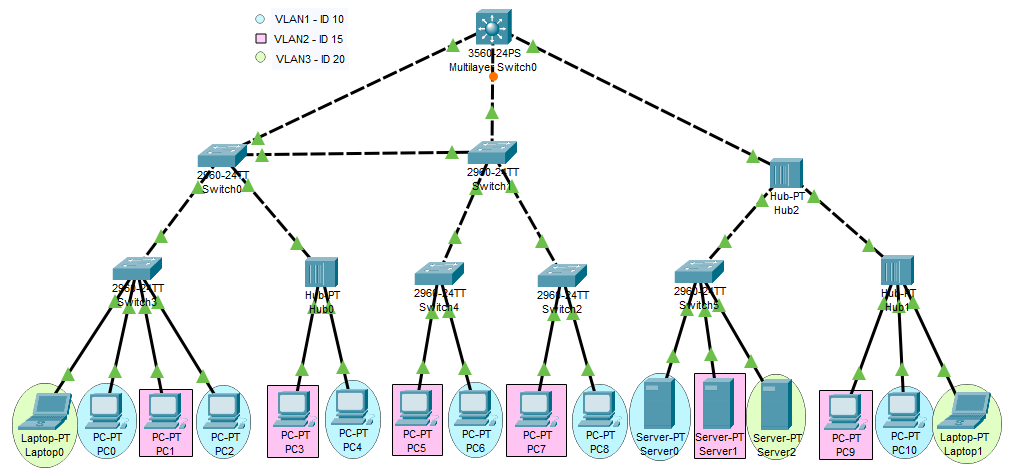


Hacemos lo mismo, pero ahora al contrario, desde Laptop 1 hasta Laptop 2



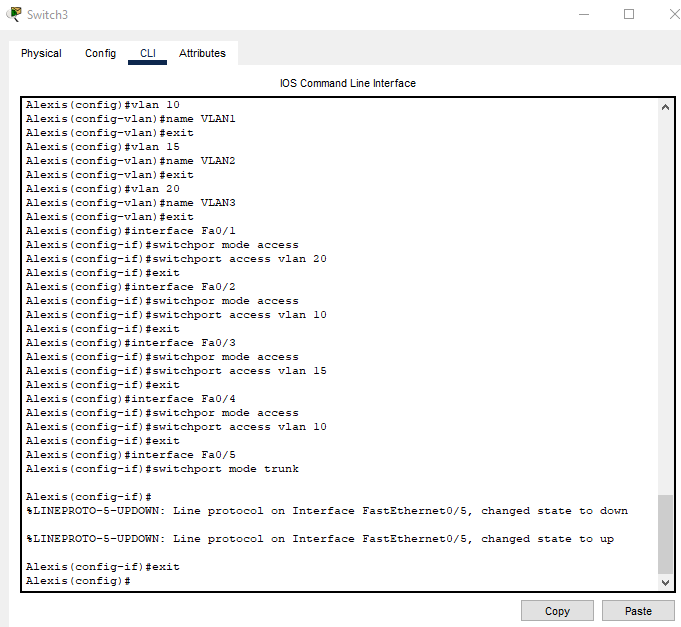
1. **Redes de switches más grandes con VLANs**

* Cree tres VLANs (ID 10, 15 y 20) y nombre VLAN1, VLAN2 y VLAN3 respectivamente.

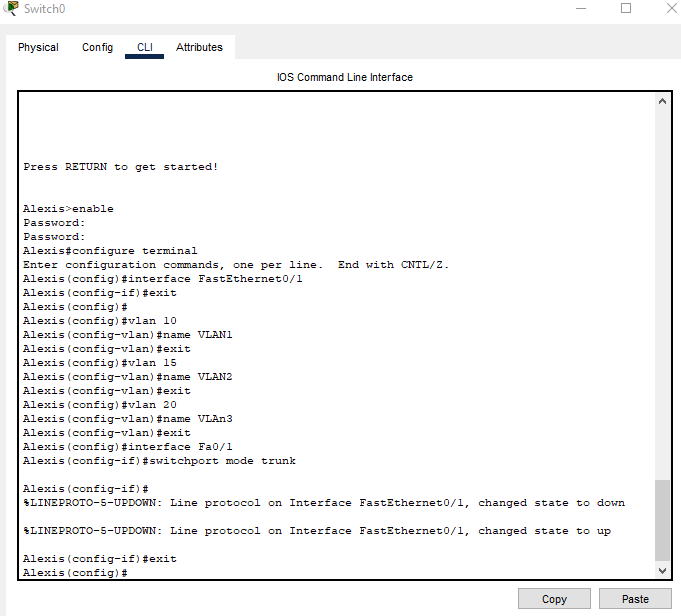


En cada switch se configuran la VLAN indicando su nombre y el ID, también las VLAN correspondiente a cada interfaz y los enlaces troncales correspondientes para intercambiar la información de todas las VLAN entre los switches.

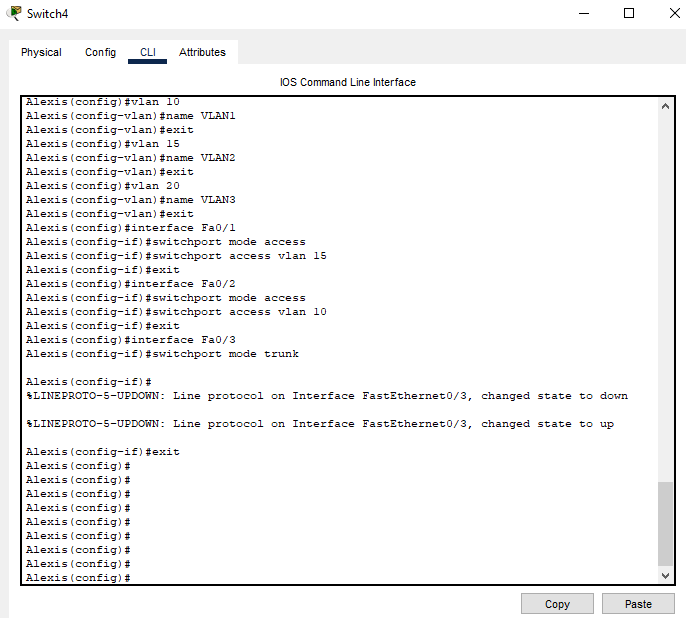
Switch 3



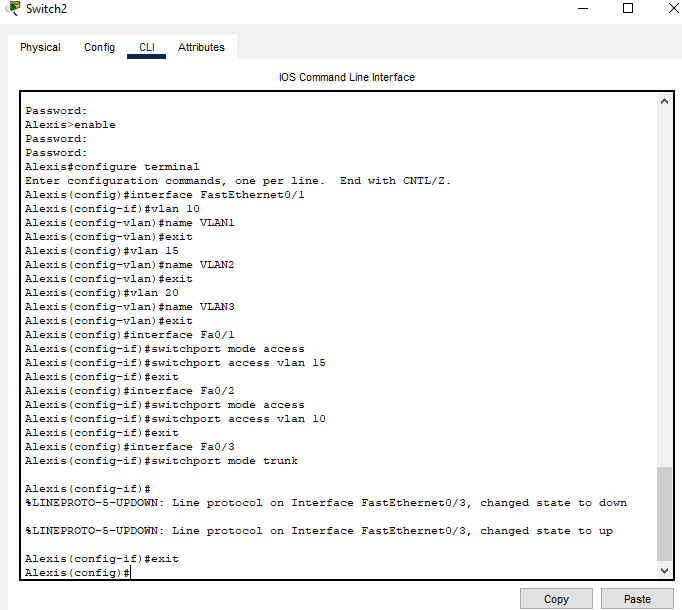
Switch 0



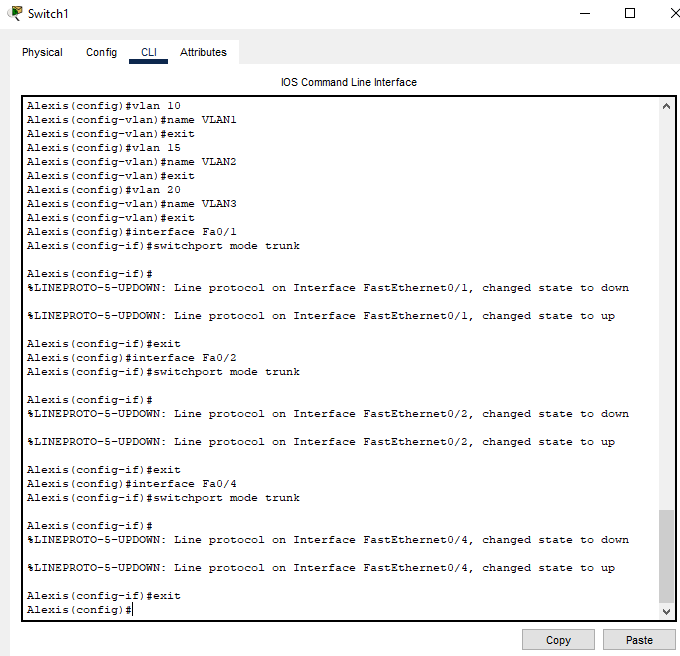
Switch 4



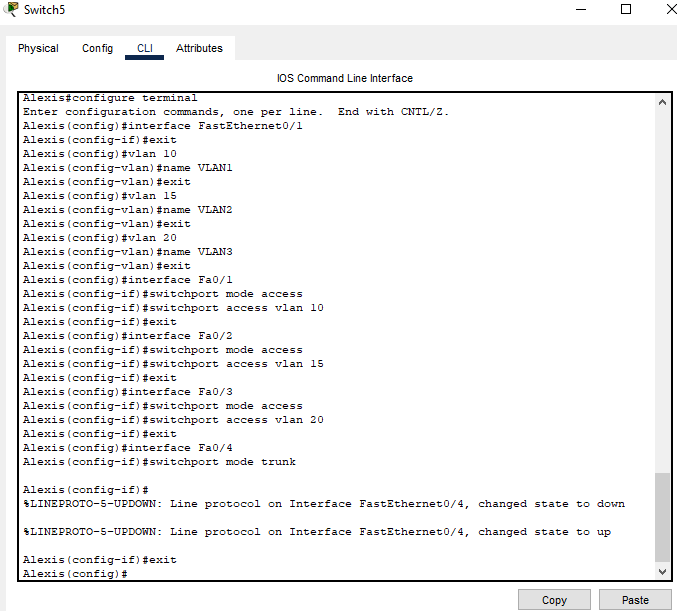
Switch 2



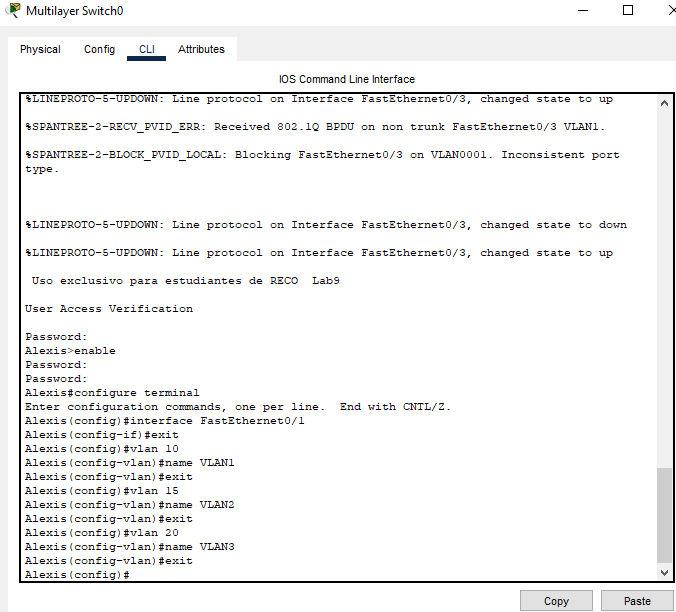
Switch 1



Switch 5

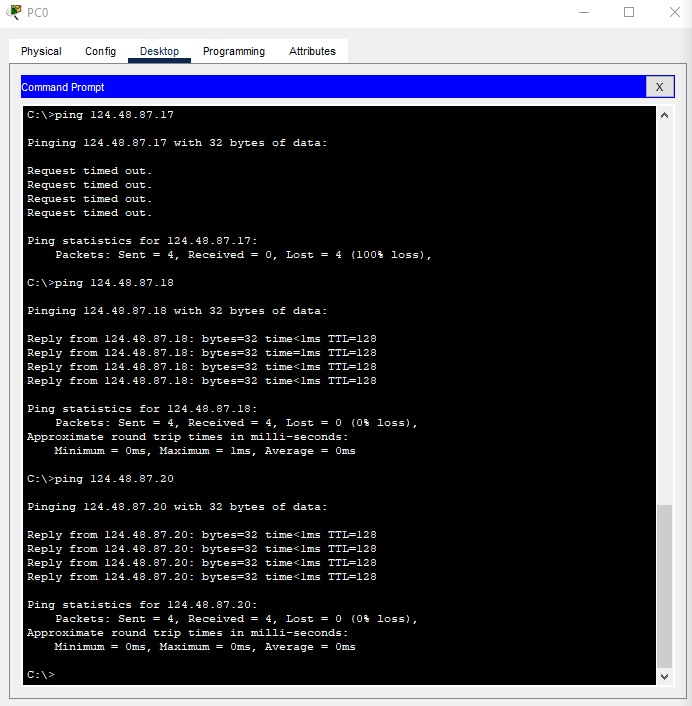


Multilayer Switch 0



* Ahora revise la conectividad entre los equipos de la misma VLAN y aislamiento hacia las otras VLAN.

Desde el PC 0 (VLAN1) se intenta hacer conectar con el PC5 (VLAN2 – 124.48.87.17), ya que están en diferentes VLAN no se pueden conectar, después se intenta con una que si este en la misma VLAN (PC 6 – 124.48.87.18 / PC 8 – 124.48.87.20) y se logra la conexión con estos.



* Interconecte los archivos de los miembros del equipo.

Diagrama

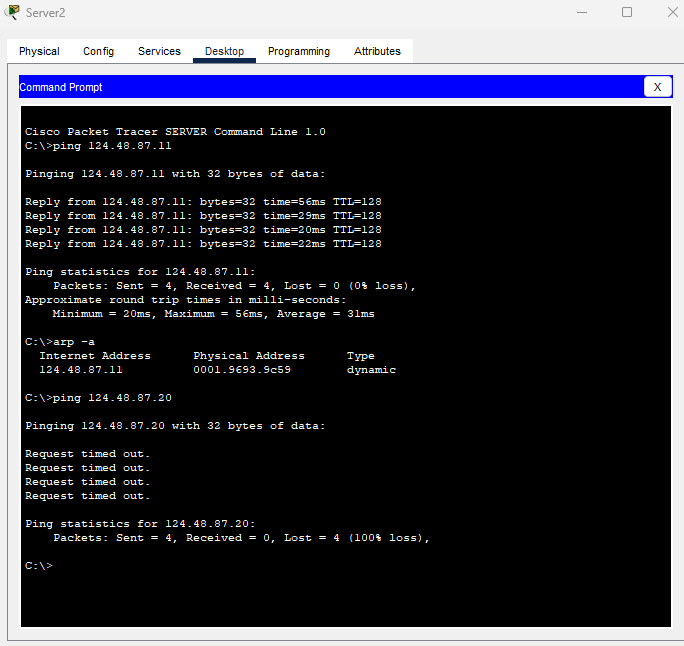
Descripción generada automáticamente

El archivo con el montaje fue facilitado por Juan Vivas.

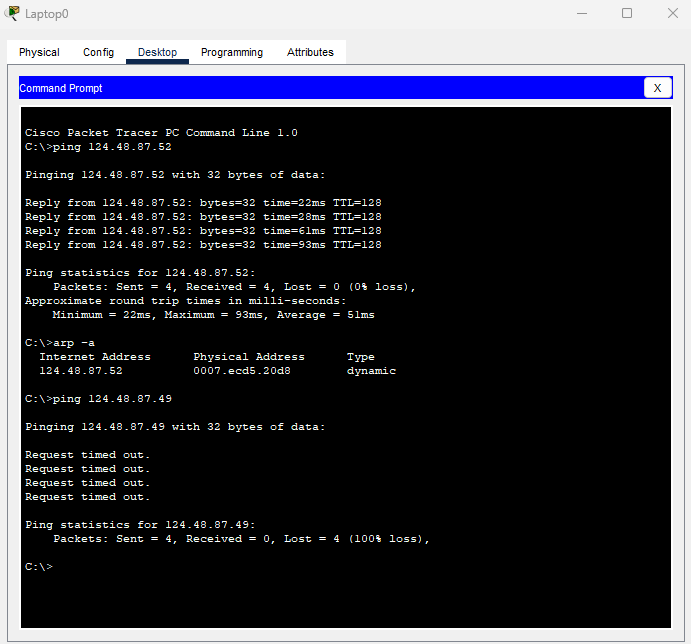
Imagen que contiene báscula, barco, grupo, colgando

Descripción generada automáticamente

Comprobamos la conexión con el comando ping haciendo la petición desde el Server 2 del estudiante 2 (Juan) que tiene IP 124.48.87.52 hasta la Laptop 0 del estudiante 1 (Alexis) con dirección IP 124.48.87.11, verificamos la table de ARP y verificamos el aislamiento haciendo ping a un dispositivo de otra VLAN que se hace al PC 8 que tiene como dirección IP 124.48.87.20.



Hacemos lo mismo, pero ahora al contrario, desde Laptop 0 hasta Server 2 y desde PC 8 hasta Server 2.



**Conclusiones**

En resumen, el laboratorio nos permitió profundizar en el conocimiento de

la configuración básica de switches, enfocándose en la creación de una red de área local (LAN) y en el estudio de su infraestructura. Se repasaron conceptos como la asignación de nombres, mensajes del día, sincronización de la pantalla y bloqueo de la búsqueda de comandos en un servidor externo.

Además, se utilizó un sniffer para capturar paquetes y examinar los frames Ethernet, lo que permitió obtener un mayor conocimiento sobre la estructura de los mismos y su funcionamiento en la red.

Durante la configuración de las redes LAN, se puso énfasis en la configuración de las redes de área local virtual (VLAN). Se prestaron atención a aspectos como el ID y nombre de las VLAN, el modo de asociación de VLAN para los puertos y la forma en que se asigna una VLAN a cada uno.

Adicionalmente, se realizó un montaje utilizando Cisco Packet Tracer para analizar el comportamiento de la red. Se reforzó el protocolo ARP y se estudió el formato de los frames Ethernet. Se llevaron a cabo envíos de paquetes entre hosts, partiendo de una tabla de ARP vacía y culminando con la configuración de tres VLAN.

# **Referencias**

*Cisco Networking Academy*. (s.f.). Obtenido de https://www.netacad.com/courses/packet-tracer?dtid=osscdc000283

*Clodflare*. (s.f.). Obtenido de https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-lan/

*Geyma*. (28 de Mayo de 2021). Obtenido de https://www.geyma.com/blog/trama-ethernet/

*IBM*. (03 de 03 de 2021). Obtenido de https://www.ibm.com/docs/es/aix/7.1?topic=protocols-address-resolution-protocol

*Keepcoding*. (13 de Octubre de 2022). Obtenido de https://keepcoding.io/blog/que-es-wireshark/#Que\_es\_Wireshark

*Redes Telemáticas*. (08 de Noviembre de 2013). Obtenido de https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/