

**TAREA ONLINE UNIDAD 3 .-
INTERCONEXIÓN DE EQUIPOS EN REDES
LOCALES (1ª PARTE)**

IES CASTILLO DE LUNA, ROTA (CÁDIZ)
GRADO MEDIO SEMIPRESENCIAL SISTEMA MICROINFORMÁTICOS Y REDES
MODULO: REDES LOCALES
CURSO ACADEMICO: 2021/2022
ALUMNO: ANTONIO NAVAS BERNAL
FEBRERO 2022

INDICE

	PÁGINA
<u>Tarea 3.1 - Introducción e Instalación Packet tracer</u>	<u>3</u>
<u>Tarea 3.2 - Configuración de equipos</u>	<u>10</u>
<u>Tarea 3.3 - Configuración Switch</u>	<u>20</u>
<u>Tarea 3.4 - Vlan</u>	<u>36</u>
<u>WEBGRAFIA</u>	<u>43</u>

Tarea 3.1 - Introducción e Instalación Packet tracer

- Instalar Packet Tracer proporcionado por el profesor.
- Crear capturas de pantalla de cada uno de los pasos de instalación.
- Una vez instalado comprobar y cacharrear con cada una de las opciones y dispositivos que aparecen en el simulador, para ello deberéis seguir el siguiente video explicativo, he ir cacharreando con ciertos dispositivos, para ir viendo cómo sería el manejo del simulador y haz captura de pantalla de los dispositivos más importante del simulador.



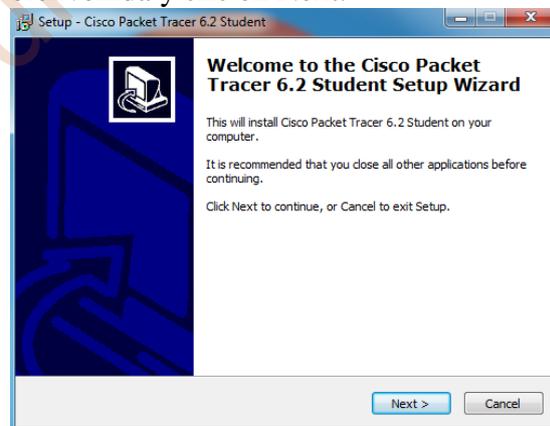
<https://www.youtube.com/watch?v=UXkc7jvF1ZY>

- Instalar Packet Tracer proporcionado por el profesor.

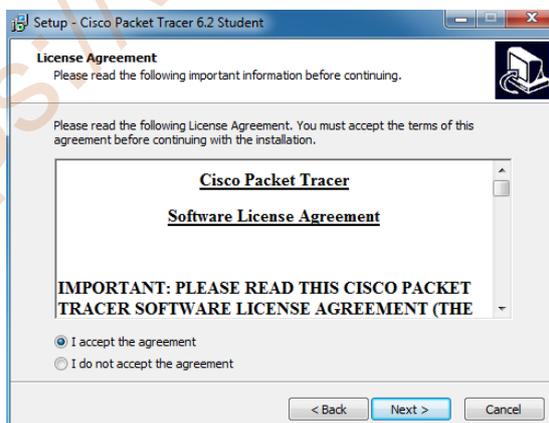
 Cisco Packet Tracer 6.2 for Windows Student Version	11/01/2022 15:48	Aplicación	150.207 KB
 spanish_PT_v2.ptl	11/01/2022 15:48	Archivo PTL	1.096 KB

El profesor facilita el setup de Cisco Packet Tracer de la versión 6.2 de estudiante para Windows y un archivo PTL “spanish_PT_v2.ptl” para pasar el menú a idioma español.

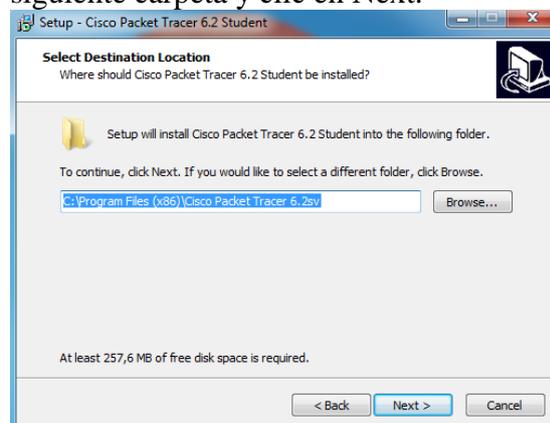
- Crear capturas de pantalla de cada uno de los pasos de instalación.
- 1.- Clic en el archivo setup Cisco Packet
 - 2.- Se abre la siguiente pantalla de bienvenida y clic en Next.



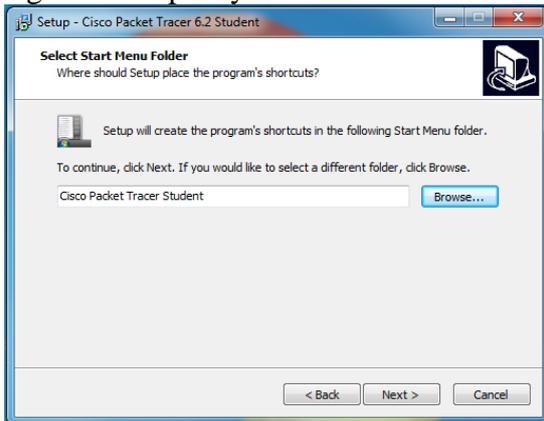
- 3.- Aceptar la licencia y clic en Next.



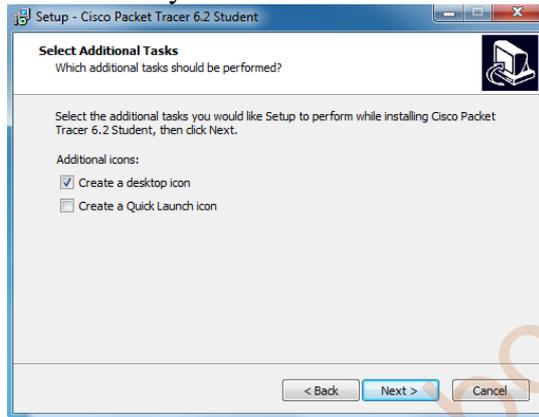
- 4.- Los archivos se almacenaran en la siguiente carpeta y clic en Next.



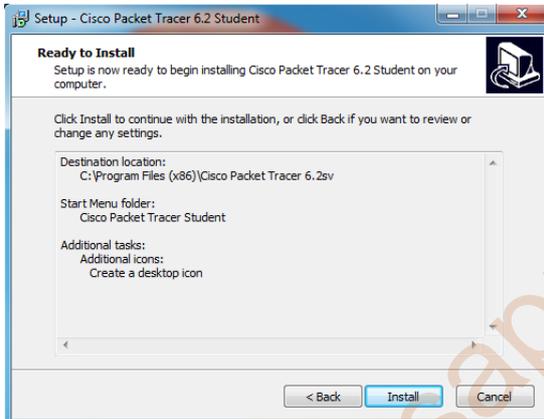
5.- Los archivos se almacenaran en la siguiente carpeta y clic en Next.



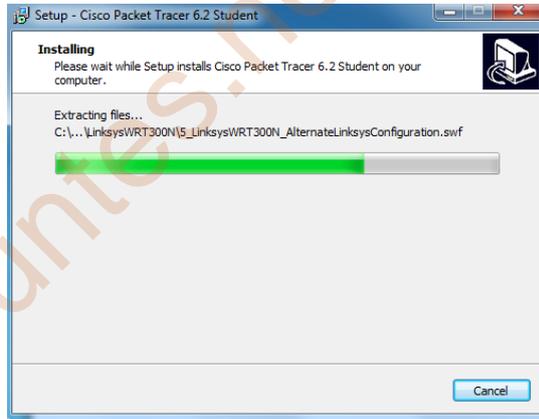
6.- Seleccionar crear icono de arranque en el escritorio y clic en Next.



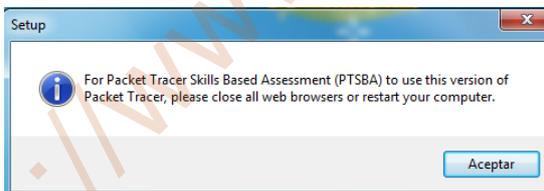
7.- El programa estar localizado en el directorio Programe Files(x86) en la carpeta Cisco Packet Tracer Studen y con un icono de arranque en el escritorio, clic en Install



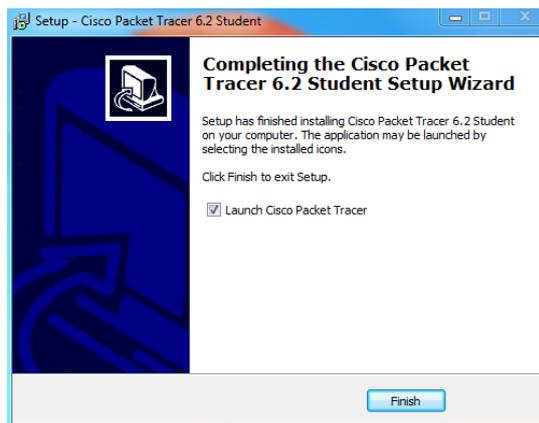
8.- Procediendo automáticamente a la instalación del Cisco Packet Tracer para estudiante.



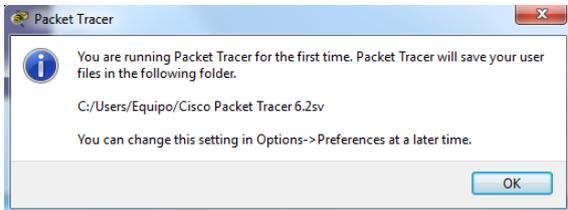
9.- Para usar esta versión de Packet Tracer, cierre todas las direcciones web y enciende el ordenador, clic en Aceptar



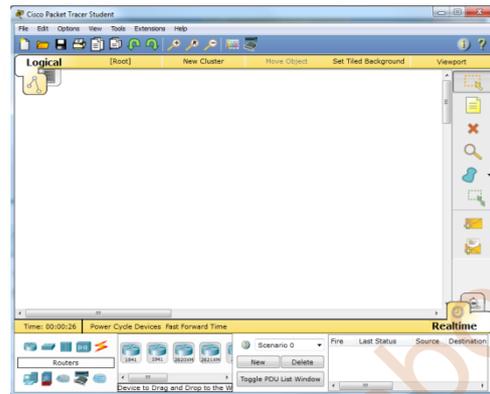
10.- Instalación completada, clic en Finish.



11.- Estas arrancando Packet Tracer por primera vez. Packet Tracer grabará tus ficheros en el siguiente carpeta, clic en Ok



12.- Se abre el programa con la pantalla minimizada.



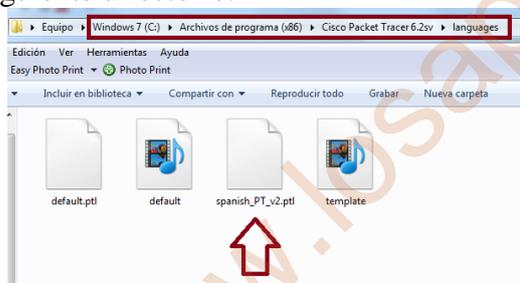
13.- Pantalla con el programa maximizado.



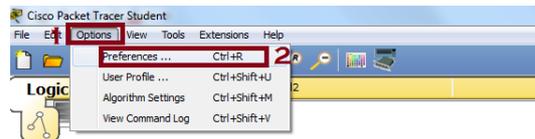
14.- Cierro el programa y el icono de arranque esta en el escritorio con este nombre Cisco Packet Tracer Studen



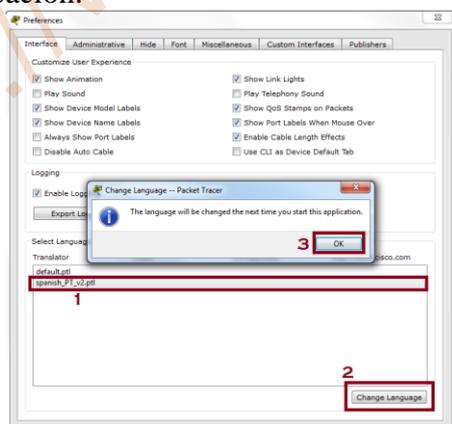
15.- Para instalar el programa con el idioma en español, el archivo spanish_PT_v2.ptl lo incluyo dentro de la carpeta languages del siguiente directorio.



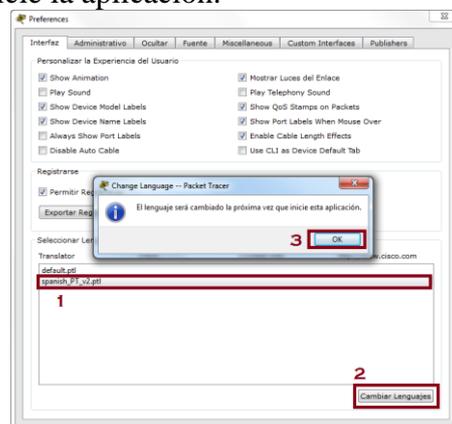
16.- Una vez incluido el archivo spanish_PT_v2.ptl, abro la aplicación y en el menú opción → Preferencias o Ctrl + R acceso a la siguiente pantalla



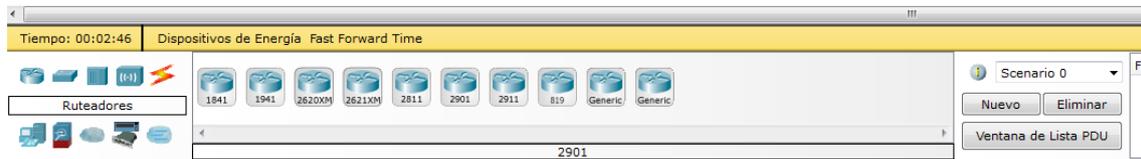
17.- En esta pantalla selecciona 1, 2 y 3 para cambiar al idioma español y el lenguaje se cambiará la primera vez que inicie la aplicación.



17.- En esta pantalla selecciona 1, 2 y 3 para cambiar al idioma español y el lenguaje se cambiará la primera vez que inicie la aplicación.



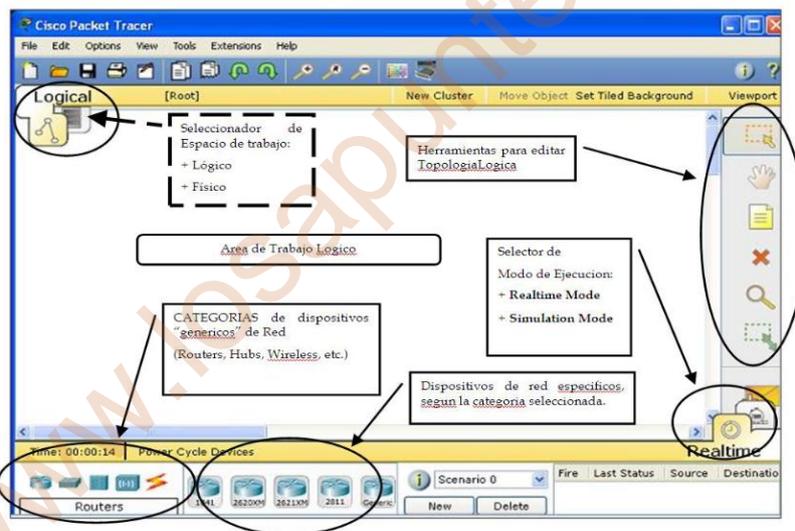
18.- Abriendo la aplicación se observa una parte del programa que ya se encuentra en español.



- Una vez instalado comprobar y cacharrear con cada una de las opciones y dispositivos que aparecen en el simulador, para ello deberéis seguir el siguiente video explicativo, he ir cacharreamo con ciertos dispositivos, para ir viendo cómo sería el manejo del simulador y haz captura de pantalla de los dispositivos más importante del simulador.

<https://www.youtube.com/watch?v=UXkc7jvF1ZY>

El programa se divide en el menú en la barra superior, herramienta de diseño en la parte inferior, en la parte lateral derecha tenemos la simulación, tiempo real y lista de eventos al enviar mensajes PDU de un equipo a otro y en la parte inferior derecha la ventana de la lista de eventos o el paquete se ha enviado satisfactoriamente.



Dentro de la herramienta de diseño tenemos los siguientes dispositivos:

Dispositivos Finales



En los dispositivos finales tenemos de izquierda a derecha los siguientes dispositivos: PC-PT, Laptop-PT, Server-PT, Printer-PT, 7960 (IPPhone), Home-VoIP-PT, Analog-Phone-PT, TV-PT, TabletPC-PT, SmartPhone-PT, WirelessEndDevice-PT, WiredEndDevice-PT, Sniffer.

Dispositivos intermedios Routers o enrutadores



En los dispositivos intermedios routers tenemos de izquierda a derecha los siguientes dispositivos: 1841, 1941, 2620XM, 2621XM, 2811, 2901, 2911, 819 (819HGW), Generic (Router-PT), Generic (Router PT-Empty) que cada uno dependerá de la aplicación a utilizar en la instalación.

Dispositivos intermedios Switch o conmutadores

En los dispositivos intermedios switch o conmutadores tenemos de izquierda a derecha los siguientes dispositivos: 2950-24, 2950T (2950T-24), 2960 (2960-24TT), Generic (Switch-PT), Generic (Switch-PT-Empty), 3560-24PS, Generic (Bridge-PT) que cada uno dependerá de la aplicación a utilizar en la instalación.

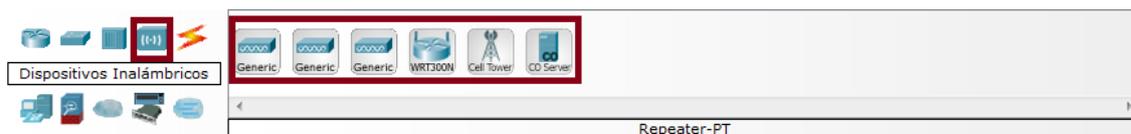


Dispositivos intermedios Hub o concentrador

En los dispositivos intermedios switch o concentrador tenemos de izquierda a derecha los siguientes dispositivos: Generic (Hub-PT), Generic (Repeater-PT), CoaxialSplitter-PT que cada uno dependerá de la aplicación a utilizar en la instalación.



Dispositivos inalámbricos



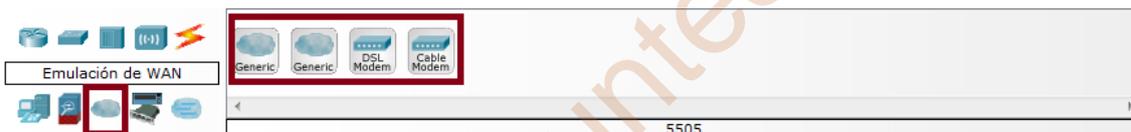
En los dispositivos inalámbricos tenemos de izquierda a derecha los siguientes dispositivos: Generic (AccessPoint-PT), Generic (AccessPoint-PT-A), Generic (AccessPoint-PT-N), WRT300N, Cell-Tower, CD Server (Central-Office-Server) que cada uno dependerá de la aplicación a utilizar en la instalación.

Dispositivos de seguridad



En los dispositivos de seguridad en esta programa solo dispone de 5505 (Repeater-PT)

Dispositivos de emulación de WAN



En los dispositivos de emulación WAN tenemos de izquierda a derecha los siguientes dispositivos: Generic (Cloud-PT), Generic (Cloud-PT-Empty), DSL Modem (DSL-Modem-PT), Cable Modem (Cable-Modem-PT) que cada uno dependerá de la aplicación a utilizar en la instalación.

Dispositivos hechos a la medida (Custom Made Devices)



En los dispositivos hechos a la medida que dispone en este programa son de izquierda a derecha los siguientes dispositivos: 1841 (1841 WIC-2T), 2621XM (2621XM NM-2FE2W (2) WIC-2T), 2811 (2811 NM-ESW-161(2) WIC-2T), Generic (Wireless PC).

Dispositivos conexión multiusuario



En los dispositivos de conexión multiusuario este programa solo dispone del Multiuser (1841 WIC-2T)

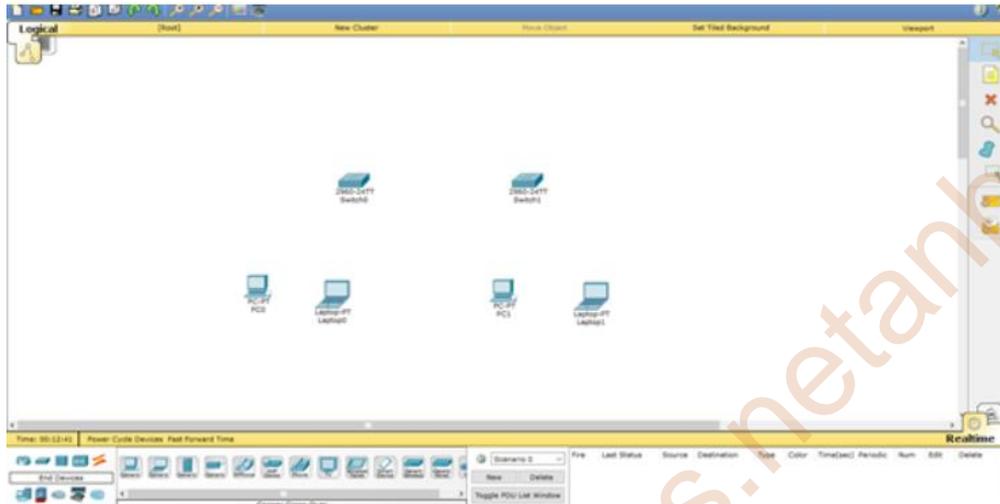
Tipos de conexiones



Los tipos de conexiones a utilizar para la conexión de los distintos dispositivos de izquierda a derecha los siguientes dispositivos: Elegir el tipo de conexión automáticamente (rayo color rojo y amarillo), Consola (color celeste), Cable de cobre directo (color negro), Cable de cobre cruzado (color negro discontinuo), Fibra (color naranja), teléfono (rayo color negro), Coaxial (color azul), Serial DTE (rayo color rojo con tiempo), Serial DTE (rayo color rojo), Octal (color verde) que cada uno dependerá de la aplicación a utilizar en la instalación.

Tarea 3.2 - Configuración de equipos

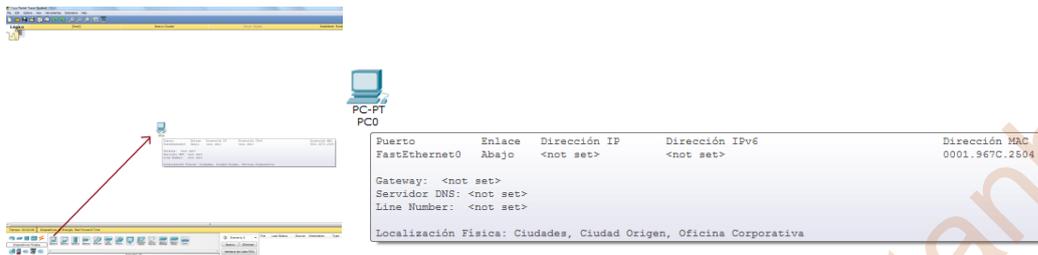
- Investiga en internet cómo se configura un ordenador en packet tracer y haz una breve explicación con sus capturas de pantalla de cómo se configura un ordenador.
- Una vez que sepáis como se configura un PC, deberéis montar la siguiente arquitectura de red:



- El direccionamiento de red que deberéis usar será del rango : **192.168.1.2-5/24**
- Haz una captura de pantalla de cómo sería el conexionado de cables en la arquitectura de red planteada y explica por qué has usado ese cableado en cada uno de los equipos.
- Comprobar la conectividad con los cuatros equipos. ¿Hay conectividad con los cuatros PCs o no?. Haz captura de pantalla de la conectividad de cada una de ellos si la hubiera.
- Si utilizamos un direccionamiento 192.168.1.2-3/24 para los dos PCs del primer Switch y un direccionamiento 192.168.2.2-3/24 para los PCs del otro Switch . ¿Tienen conectividad todos los Pcs?. Haz captura de pantalla de la conectividad de cada uno de ellos y explica el resultado.

- Investiga en internet cómo se configura un ordenador en packet tracer y haz una breve explicación con sus capturas de pantalla de cómo se configura un ordenador.

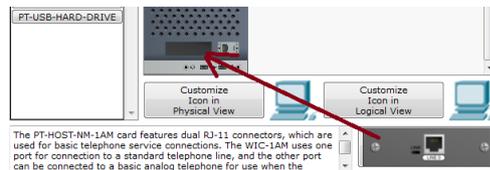
Antes de empezar a configurar un ordenador en packet tracer tenemos que poner en el área de trabajo un PC, seleccionando dispositivos finales y arrastrando hasta el escritorio del Packet Tracer el PC genérico. Con el puntero del ratón encima de PC-PT PC0 nos define la dirección MAC pero no la dirección del Puerto IP al no estar todavía dicho PC configurado ;



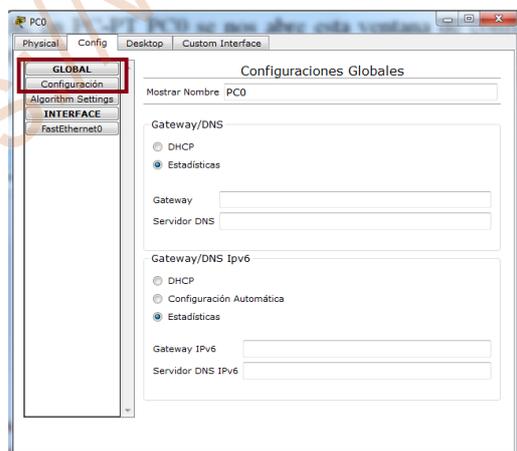
Haciendo clic en PC-PT PC0 se nos abre esta ventana de configuración en donde en la pestaña Physical (física) podemos apagar y encender el ordenador, seleccionar en algunos de los módulos que queremos instalar en el PC. Actualmente tiene instalador el Linksys-WMP300N que tiene una interface inalámbrica de 2.4 GHz.



Para poder instalar un nuevo modelo tenemos que apagar el PC, quitar el modelo del PC y desplazar en la zona inferior, y elegir en nuevo módulo y arrastrando con el ratón el modulo PT-HOST-NM-1AM y encender el PC.

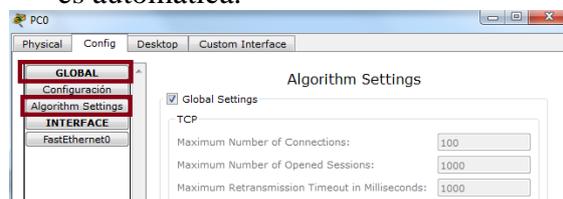


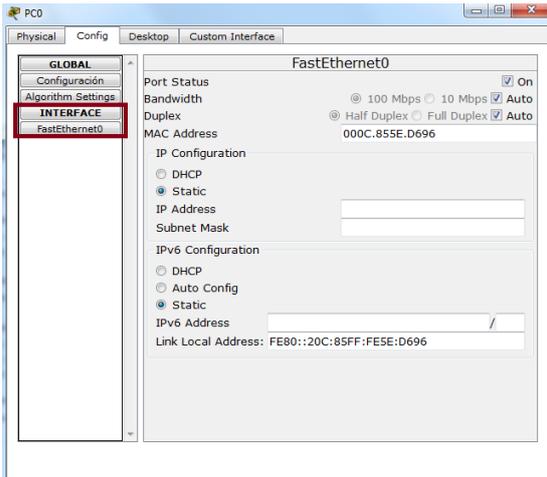
En la misma ventana abierta haciendo clic en config (configuración), nos muestra la configuración global y la configuración de la interface.



En la **configuración global** podemos:

- Cambiar de nombre a la PC.
- En estadísticas introducir la puerta de enlace y servidor DNS asociado al PC. Puede ser con IPv4 o la IPv6.
- Si selecciona DHCP la configuración es automática.



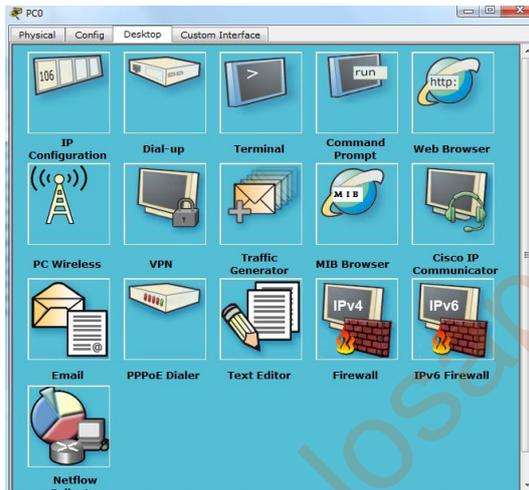


En **configuración INTERFACE** podemos:

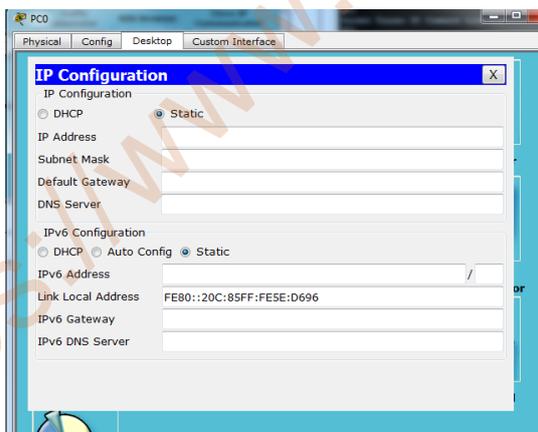
- Apagar o encender la interface.
- Modificar el ancho de banda y dúplex.
- Establecer la dirección IP de forma estático asignando una IP y mascara o de forma automática DHCP
- La configuración IP puede ser IPv4 o IPV6.

La interface tiene establecida su dirección MAC Address.

En la misma ventana abierta haciendo clic en Desktop (escritorio), nos muestra un escritorio con los distintos iconos para acceder a la configuración del PC, al comando prompt, entre otros.



Clic en **Command Prompt** para acceder ping a los equipos y conectarse al internet entre otras;



Clic en **IP Configuración** para acceder a configurar la PC introducimos los siguientes datos de forma estática:

- La dirección IP del PC
- La mascara
- La puerta de enlace
- El servidor DNS (si tiene asociado)

De forma automática sería seleccionando DHCP. La configuración puede ser IPv4 o IPv6.

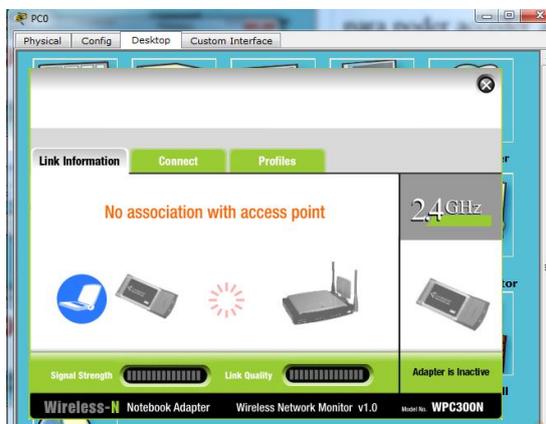


Clic en **Web Browser** que podemos entrar en cualquier dirección que tengamos configurado en cualquier servidor DNS



Clic en **PC Wireless** no podemos acceder al interface porque el seleccionado en el PC no es el WMP300N o WPC300N. Para hacer la prueba modifico el interfaz para poder acceder a PC Wireless;

El Linksys-WMP300N tiene una interfase inalambrica de 2.4 GHz para conectarse a redes inalamblicas. El módulo soporta protocolos que usan ethernet para acceso a LAN.

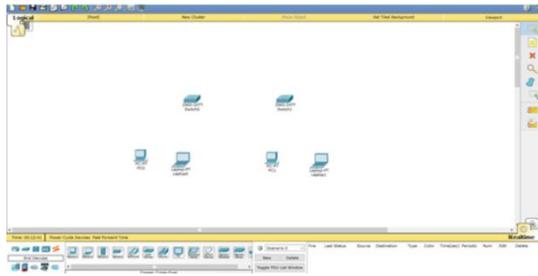


Clic de nuevo en **PC Wireless** con el interface Linksys-WMP300N y en esta caso si puedo acceder a su configuración.

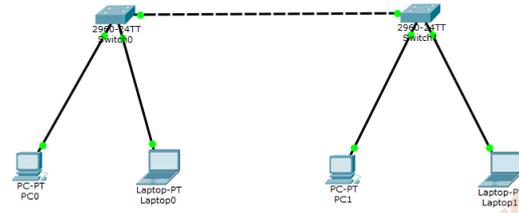
Como vemos en las distintas imaganes podemos configurar el PC de dos formas:

- **Primera forma:** Directamente con **IP Configuración (en desktop)** introduciendo todos los datos, la dirección IP del PC, la mascara, la puerta de enlace, el servidor DNS (si tiene asociado).
- **Segunda forma:** Accediendo a la pestaña config en **configuración global** (puerta de enlace y servidor DNS) y **configuración Interface** (dirección IP del PC y dirección Mascara).

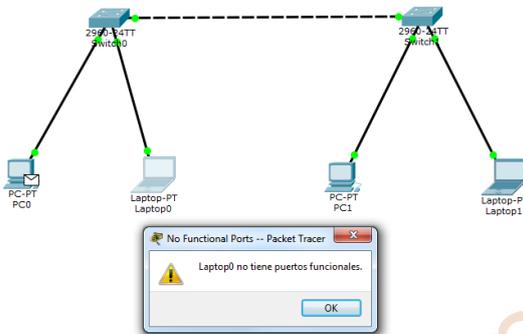
- Una vez que sepáis como se configura un PC, deberéis montar la siguiente arquitectura de red:



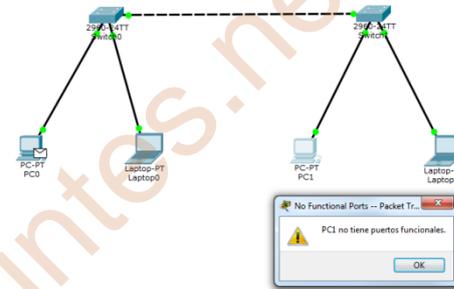
Arquitectura montada en el packet tracer:



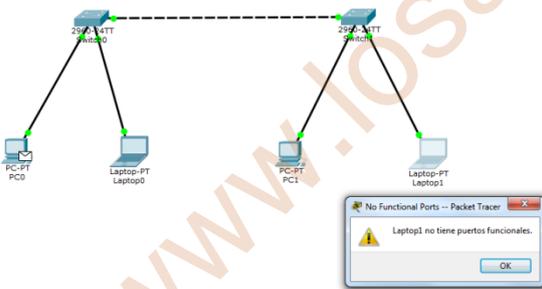
En este caso si comprobará si hay conectividad en los equipos, no lo habría porque aunque los interfaces están conectados y activados en verde, no está configurado ningunos de los equipos con su dirección IP por eso no hay conectividad. Se muestra en las siguientes imágenes:



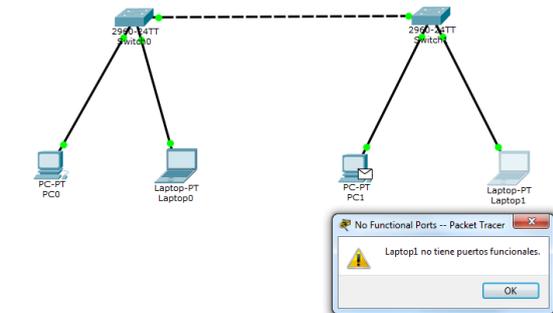
No hay conectividad entre PC0 y Laptop0



No hay conectividad entre PC0 y PC1

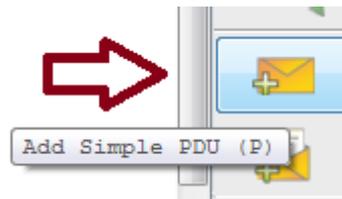


No hay conectividad entre PC0 y Laptop1



No hay conectividad entre PC1 y Laptop1

Esta prueba se ha llevado a cabo con un ping desde un equipo a otro con el mensaje PDU y se observa además que en cada uno de los PC y Laptop no tiene asignado la dirección IP;



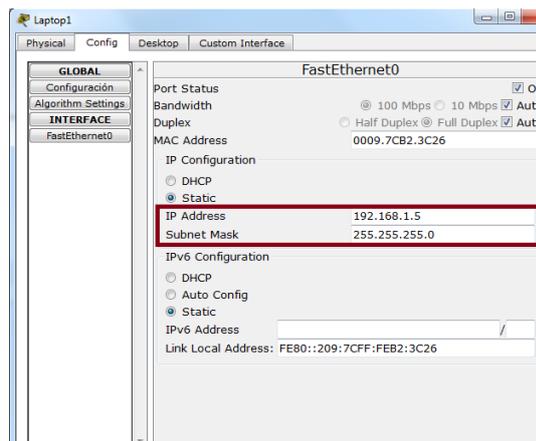
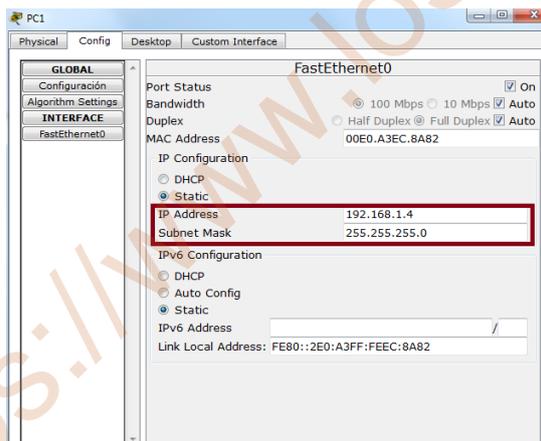
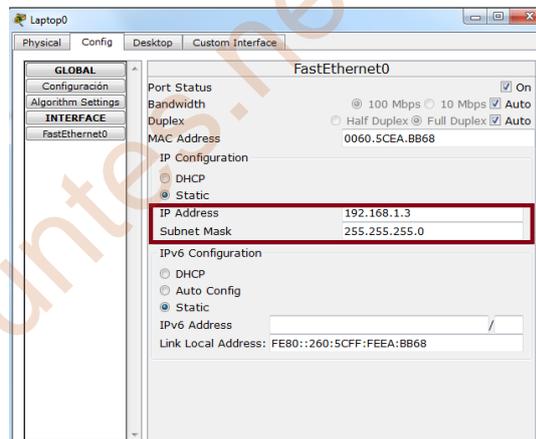
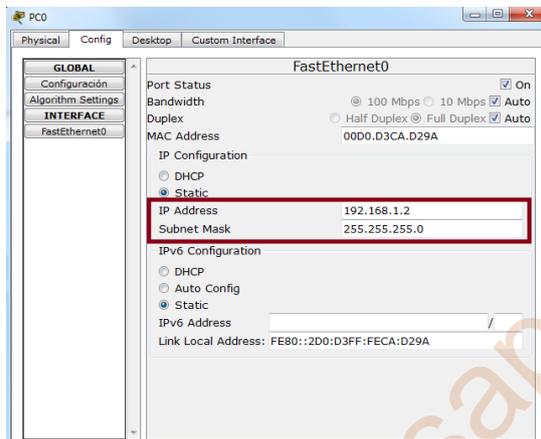
Puerto	Enlace	Dirección IP	Dirección IPv6	Dirección MAC
FastEthernet0	Arriba	<not set>	<not set>	00D0.D3CA.D29A

Gateway: <not set>
 Servidor DNS: <not set>
 Line Number: <not set>

Localización Física: Ciudades, Ciudad Origen, Oficina Corporativa

- El direccionamiento de red que deberéis usar será del rango : **192.168.1.2-5/24**

Entro la configuración de cada uno de los PC y Laptops he introduzco sus rangos de dirección 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5, tal como se muestra en las imágenes;



También con el puntero del ratón sobre el equipo se despliega este cuadro de información donde se observa que cada uno de los equipos tienen asignada su dirección IP tal como se introdujo anteriormente en la configuración de los equipos:



PC0

Puerto	Enlace	Dirección IP	Dirección IPv6	Dirección MAC
FastEthernet0	Arriba	192.168.1.2/24	<not set>	00D0.D3CA.D29A

Gateway: <not set>
 Servidor DNS: <not set>
 Line Number: <not set>

Localización Física: Ciudades, Ciudad Origen, Oficina Corporativa



Laptop0

Puerto	Enlace	Dirección IP	Dirección IPv6	Dirección MAC
FastEthernet0	Arriba	192.168.1.3/24	<not set>	0060.5CEA.BB68

Gateway: <not set>
 Servidor DNS: <not set>
 Line Number: <not set>

Localización Física: Ciudades, Ciudad Origen, Oficina Corporativa



PC1

Puerto	Enlace	Dirección IP	Dirección IPv6	Dirección MAC
FastEthernet0	Arriba	192.168.1.4/24	<not set>	00E0.A3EC.8A82

Gateway: <not set>
 Servidor DNS: <not set>
 Line Number: <not set>

Localización Física: Ciudades, Ciudad Origen, Oficina Corporativa



Laptop1

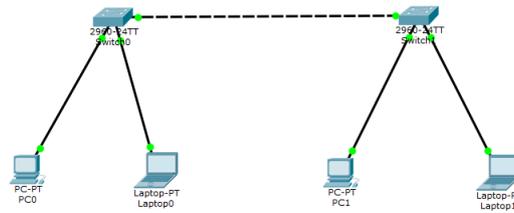
Puerto	Enlace	Dirección IP	Dirección IPv6	Dirección MAC
FastEthernet0	Arriba	192.168.1.5/24	<not set>	0009.7CB2.3C26

Gateway: <not set>
 Servidor DNS: <not set>
 Line Number: <not set>

Localización Física: Ciudades, Ciudad Origen, Oficina Corporativa

- Haz una captura de pantalla de cómo sería el conexionado de cables en la arquitectura de red planteada y explica por qué has usado ese cableado en cada uno de los equipos.

He conectado entre los PC y los Laptop con el Switch con cable de cobre directo y entre los switch con cable de cobre cruzado, salvo que el Switch funcione en modo Auto-MDIX que es un mecanismo introducido para eliminar la necesidad de utilizar cables específicos para cada conexión ("cable directo" o "cable cruzado") detectando automáticamente la señal eléctrica que se recibe para adecuar el puerto del dispositivo a esa señal.



Cable de cobre directo



Cable de cobre cruzado

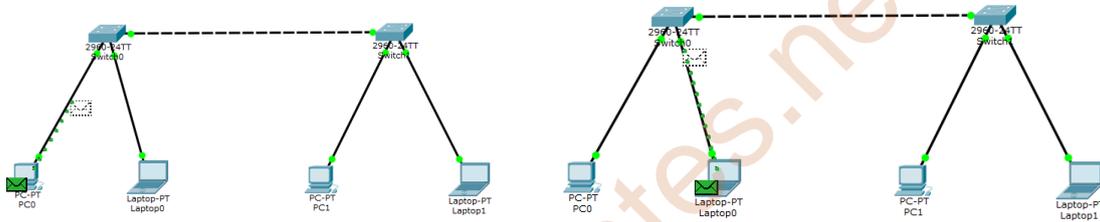


- Comprobar la conectividad con los cuatros equipos. ¿Hay conectividad con los cuatros PCs o no?. Haz captura de pantalla de la conectividad de cada una de ellos si la hubiera.

Si hay conectividad con los cuatros equipos al tener la configuración con la dirección IP con la misma parte de la red se puede conectar entre todos y la parte del host son los sufijo 2, 3, 4 y 5 con la máscara 255.255.255.0 o /24;

<u>Dirección IP</u>	<u>Parte de red (prefijo)</u>	<u>Parte de host (sufijo)</u>	<u>Mascara 255.255.255.0</u>
PC0	192.168.1.	2	/24
Laptop1	192.168.1.	3	/24
PC1	192.168.1.	4	/24
Laptop2	192.168.1.	5	/24

Se muestra en las siguientes imágenes:

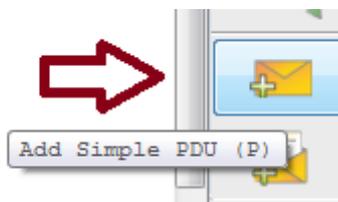


Hay conectividad haciendo un ping desde el PC0 al Laptop0 con la misma conexión de Switch0 con mensaje de vuelta con acuse de recibo.



Hay conectividad haciendo un ping desde el PC0 al PC1 con distinta conexión Switch con mensaje de vuelta con acuse de recibo.

Esta prueba se ha llevado a cabo con un ping desde un equipo a otro con el mensaje PDU y se observa además que en cada uno de los PC y Laptop tiene asignado la dirección IP;



PC-PT PC0	Laptop-PT Laptop0	PC-PT PC1	Laptop-PT Laptop1	
Puerto	Enlace	Dirección IP	Dirección IPv6	Dirección MAC
FastEthernet0	Arriba	192.168.1.2/24	<not set>	00D0.D3CA.D29A
Gateway:	<not set>			
Servidor DNS:	<not set>			
Line Number:	<not set>			
Localización Física: Ciudades, Ciudad Origen, Oficina Corporativa				

- Si utilizamos un direccionamiento 192.168.1.2-3/24 para los dos PCs del primer Switch y un direccionamiento 192.168.2.2-3/24 para los PCs del otro Switch. ¿Tienen conectividad todos los Pcs?. Haz captura de pantalla de la conectividad de cada uno de ellos y explica el resultado.

No tiene conectividad todos los PC, solo tiene conectividad los host que están en su propio Switch. Esto es debido a que la dirección IP de la parte de red no coinciden con cada uno de los PCs y Laptops, es por eso la imposibilidad de su conexión de los cuatros equipos y solo en tiene conectividad los equipos que están su switch.

<u>Dirección IP</u>	<u>Parte de red (prefijo)</u>	<u>Parte de host (sufijo)</u>	<u>Mascara 255.255.255.0</u>
PC0	192.168.1.	2	/24
Laptop1	192.168.1.	3	/24
PC1	192.168.2.	2	/24
Laptop2	192.168.2.	3	/24

Se muestra en las siguientes imágenes con conectividad en su propio switch:

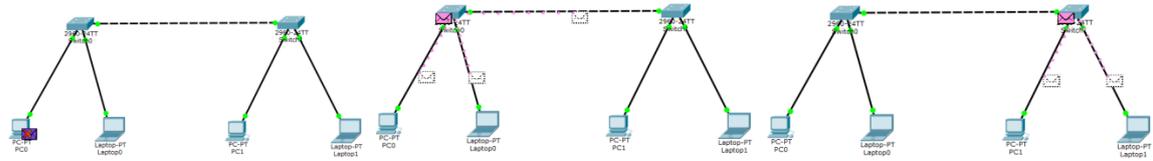
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Exitoso	PC0	Laptop0	ICMP		0.000	N	0	(edit)	(delete)

Hay conectividad haciendo un ping desde el PC0 al Laptop0 con la misma conexión de Switch0 con mensaje de vuelta con acuse de recibo.

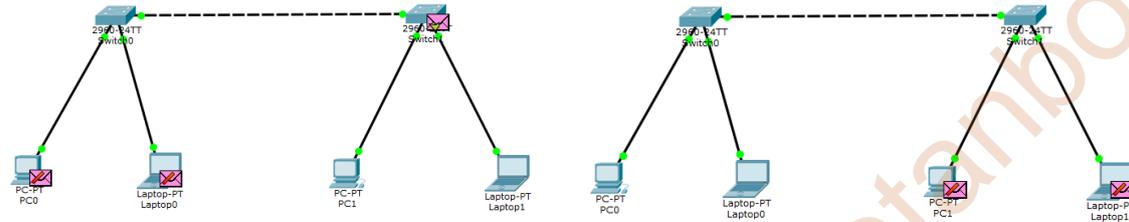
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Exitoso	PC1	Laptop1	ICMP		0.000	N	0	(edit)	(delete)

Hay conectividad haciendo un ping desde el PC1 al Laptop1 con la misma conexión de Switch1 con mensaje de vuelta con acuse de recibo.

Se muestra en las siguientes imágenes sin conectividad con distintos switches:

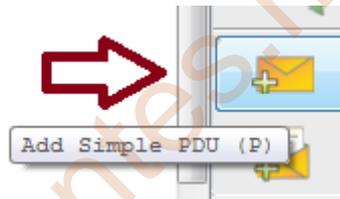


No hay conectividad haciendo un ping desde el PC0 al PC1 con distinta conexión Switch. Al no estar en su misma área de red local y no identificar la dirección IP se envía a la red mediante broadcast, todos a la vez, no recibiendo en este caso el mensaje el destinatario.



El mensaje estaría en la red continuamente buscando el destinatario pero sin éxito.

Esta prueba se ha llevado a cabo con un ping desde un equipo a otro con el mensaje PDU.



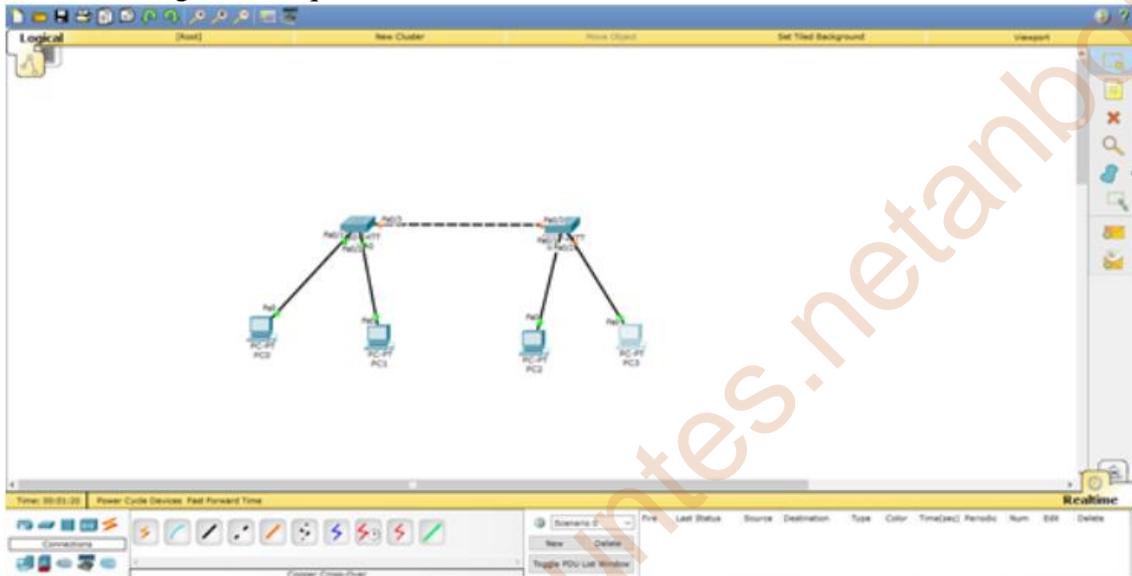
Vis.	Time(sec)	Last Device	All Device	Type	Info
	0.992	Switch0	Switch1	STP	
	0.993	Switch1	PC1	STP	
	0.993	Switch1	Laptop1	STP	
	2.996	--	Switch0	STP	
	2.998	Switch1	PC1	STP	
	2.998	Switch1	Laptop1	STP	
	4.998	--	Switch0	STP	
	5.000	Switch1	PC1	STP	
	5.000	Switch1	Laptop1	STP	

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Falló	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)

Tarea 3.3 - Configuración Switch

En la siguiente práctica vamos a ver que hay dos formas de configurar los switches:

- Usando el entorno gráfico GUI.
- Modo consola (Aconsejado).
- Muestra cómo se configuraría un switch con el entorno gráfico GUI y haz las capturas de pantallas correspondientes, poniendo un ejemplo explicativo.
- Muestra cómo se configuraría un switch en modo consola haciendo las capturas de pantallas correspondientes, poniendo un ejemplo explicativo.
- Crea la siguiente arquitectura de red :



- Cambiales los nombres a los switches mediante consola por los nombres SW1 y SW2 y haz captura de pantalla una vez cambiados y explica los comandos utilizados para el cambio de nombres.
- Asigna una dirección IP de administración a cada uno de los Switches , por ejemplo la 192.168.1.50 y 192.168.1.51 y comprueba si desde cualquier PC tiene conectividad con esa IP, suponiendo que todos los PCs están en la misma Red y haz captura de pantalla de las ips administrativas de cada switch y de la conectividad de cada uno de ellos y explica los comando utilizados para asignar las ips administrativas.

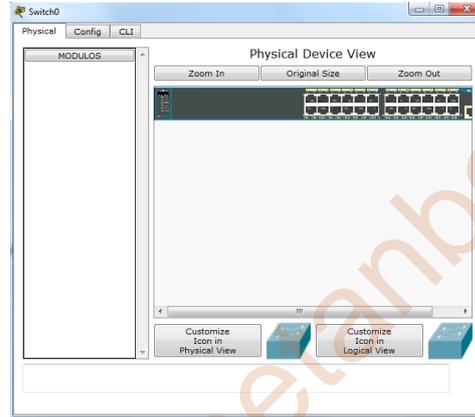
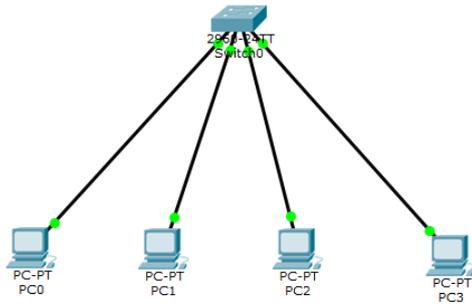
En la siguiente práctica vamos a ver que hay dos formas de configurar los switches:

- Usando el entorno gráfico GUI.
- Modo consola (Aconsejado).

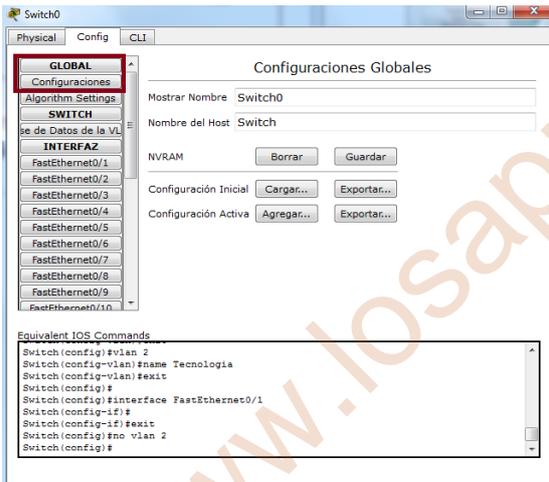
Cisco IOS es el sistema operativo entre redes de los conmutadores y enrutadores de Cisco. Tiene dos interfaces, interfaz de línea de comandos (CLI) e interfaz gráfica de usuario (GUI). La interfaz de línea de comandos (CLI) IOS de Cisco es una interfaz basada en texto integrada con el IOS. Cuando se inicia un conmutador o enrutador, **el IOS carga la configuración de inicio desde la NVRAM** y muestra el indicador del IOS en espera de los comandos. Podemos ingresar los comandos de IOS en el indicador de IOS.

- Muestra cómo se configuraría un switch con el entorno gráfico GUI y haz las capturas de pantallas correspondientes, poniendo un ejemplo explicativo.

Haciendo clic en el switch accedo a la configuración del dispositivo en donde aparece de forma gráfica GUI el panel trasero del switch con 24 puertos de 100 Mbps y 2 puertos de 1 Gbps;

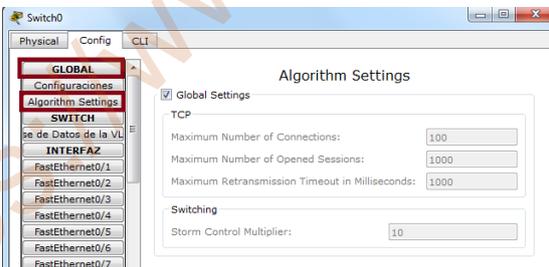


En la misma ventana abierta haciendo clic en config (configuración), nos muestra la configuración global y la configuración de la interface.



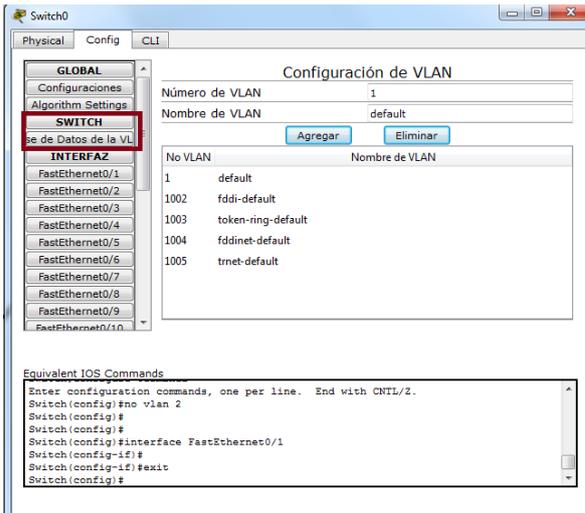
En la **configuración global** podemos:

- Cambiar de nombre de la Switch.
- Borrar y guardar en la memoria NVRAM los datos introducidos.
- Cargar o agregar la configuración inicial o activa.
- En la parte inferior una ventana de línea de comandos que se refleja los cambios que se van realizando en modo gráfico.



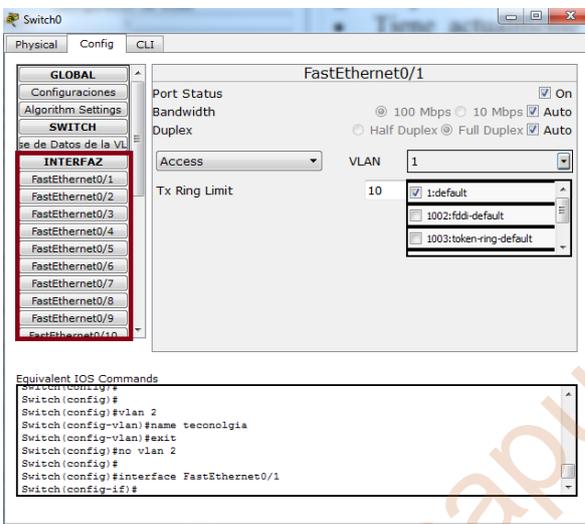
En la **configuración global en algorithm Settings** podemos modificar:

- El número máximo de conexiones.
- El número máximo de sesiones abiertas.
- El tiempo máximo de la transmisión.



En **SWITCH** en la **configuración de global** podemos:

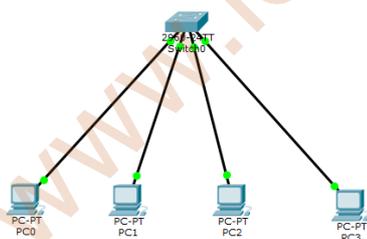
- Tiene actualmente la VLAN1 por defectos y las VLAN 1002, 1003, 1004, 1005
- Agregar nuevos VLAN con el número y nombre de la VLAN y eliminar.
- Al agregar se refleja también en la línea de comandos.



En **INTERFAZ** configuramos cada uno de los puertos en:

- Por access o trunk.
- Seleccionar para cada puerto al la VLAN que se desea que se conecta. En este caso el puerto 0/1 está por defecto en la VLAN 1

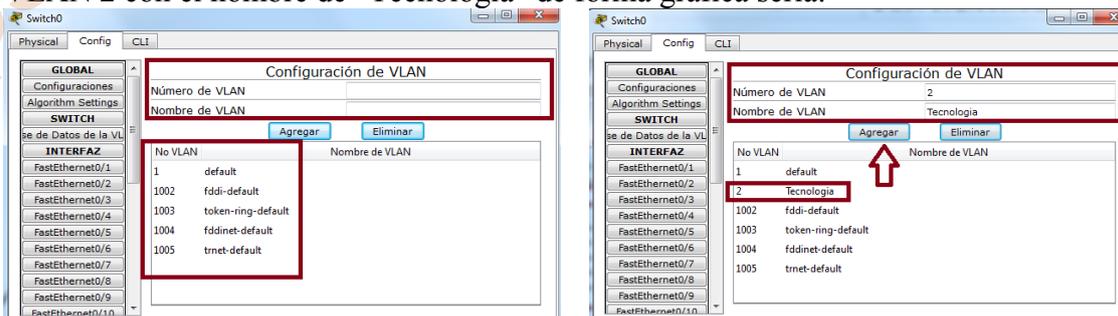
Ejemplo:



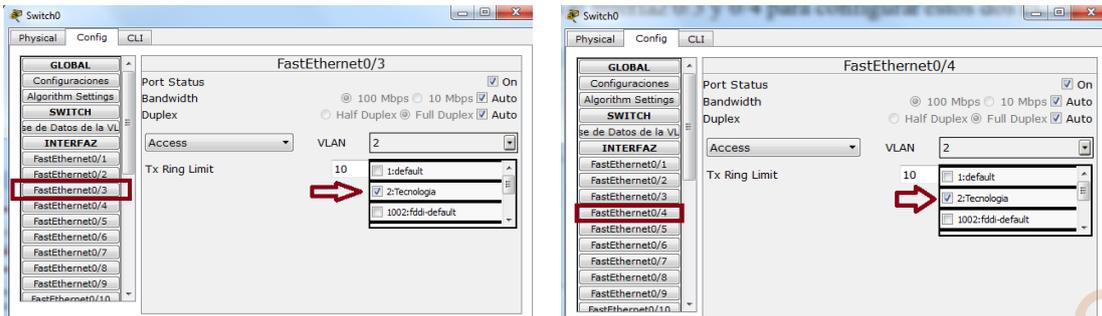
Configuramos con esta arquitectura los PC con estas dirección IP y con VLAN;

- PC0: 192.168.1.20/24 – VLAN 1
- PC1: 192.168.1.21/24 – VLAN 1
- PC2: 192.168.1.22/24 – VLAN 2
- PC3: 192.168.1.23/24 – VLAN 2

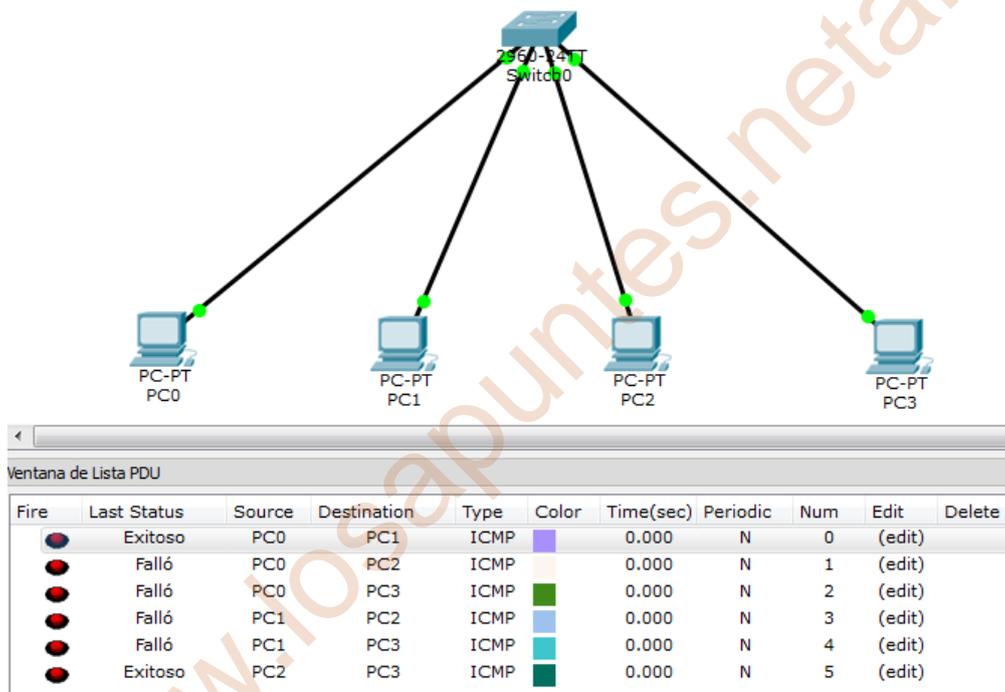
Los PC0 y PC1 por defecto está en la VLAN 1. Para configurar los PC2 y PC3 en el VLAN 2 con el nombre de “Tecnología” de forma gráfica sería:



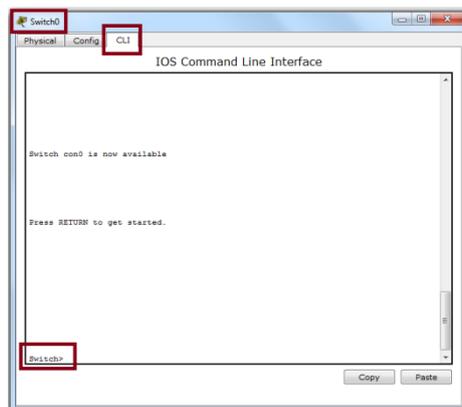
Ahora accedemos al interfaz 0/3 y 0/4 para configurar estos dos PC2 y PC3 en la VLAN 2;



Realizo un ping entre ordenadores con el mismo VLAN se conectan entre ellos, pero ordenadores con distintos VLAN no se comunican;

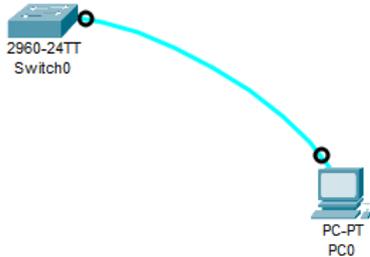


También, en la misma ventana abierta haciendo clic en la pestaña CLI (línea de comandos), nos muestra la línea de comandos de interface para acceder al Switch de forma manual para introducir los comandos;

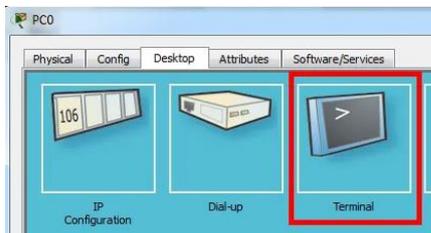


- Muestra cómo se configuraría un switch en modo consola haciendo las capturas de pantallas correspondientes, poniendo un ejemplo explicativo.

Hay varios modos de línea de comando en los conmutadores de Cisco que utilizan Packet Tracer. Abro Packet Tracer y selecciono un conmutador **Cisco 2960** como se muestra a continuación.

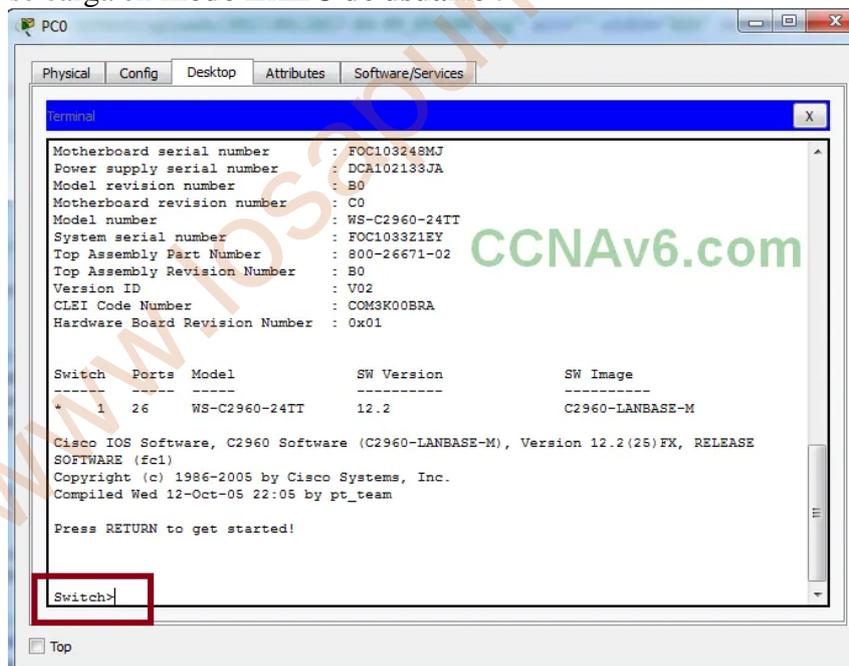


Seleccione un ordenador de los dispositivos finales y conecto el **puerto de consola del ordenador al puerto RS 232 del ordenador** con un cable de consola. Lo que estamos simulando aquí es la conexión al conmutador desde una PC a través de una consola.



Hago clic en el dispositivo host (ordenador). En la ventana que se abre, hago clic en la **pestaña Escritorio** y haga clic en **Terminal**.

La consola se abre con el interruptor de arranque. Switch finaliza su operación de arranque y se carga en **modo EXEC de usuario**.



Al llegar a los modos de Cisco IOS, Cisco IOS tiene cinco modos de línea de comando:

- Modo de configuración
- Modo EXEC de usuario
- Modo EXEC privilegiado
- Modo de configuración global
- Modo de configuración específico

Modo de configuración

El modo de configuración es el modo de configuración inicial de los conmutadores y enrutadores de Cisco. Comienzan en el modo de configuración cuando no existe ninguna configuración de inicio en la NVRAM. Después de completar el modo de configuración, Cisco IOS pasa al modo EXEC de usuario.

Modo EXEC de usuario

El modo **EXEC del usuario** es el modo de funcionamiento normal en los conmutadores y enrutadores Cisco. El indicador EXEC del usuario de Cisco IOS es el nombre del conmutador o enrutador seguido del carácter 'mayor que'. Podemos ver todos los comandos disponibles en el indicador EXEC del usuario escribiendo '?'

Modo EXEC privilegiado

El modo EXEC privilegiado es el modo de funcionamiento avanzado de Cisco IOS. Ha sido diseñado para restringir el acceso a los comandos IOS que pueden tener efectos adversos en el dispositivo Cisco y su configuración. Para ingresar al modo EXEC privilegiado, escriba "enable" o "en". El indicador de **EXEC privilegiado** se compone del nombre del conmutador o enrutador seguido del carácter #. Para salir del indicador EXEC privilegiado, escriba "disable".

```
Switch>?
Exec commands:
connect      Open a terminal connection
disable      Turn off privileged commands
disconnect   Disconnect an existing network connection
enable       Turn on privileged commands
exit         Exit from the EXEC
logout       Exit from the EXEC
ping         Send echo messages
resume       Resume an active network connection
show         Show running system information
telnet       Open a telnet connection
terminal     Set terminal line parameters
traceroute   Trace route to destination
```

```
Switch>
Switch>|
Switch>
Switch>enable
Switch#
Switch#disable
Switch>
Switch>en
Switch#
Switch#disable
Switch>
Switch>|
```

Para ver los comandos disponibles en el indicador EXEC privilegiado, escriba ?.

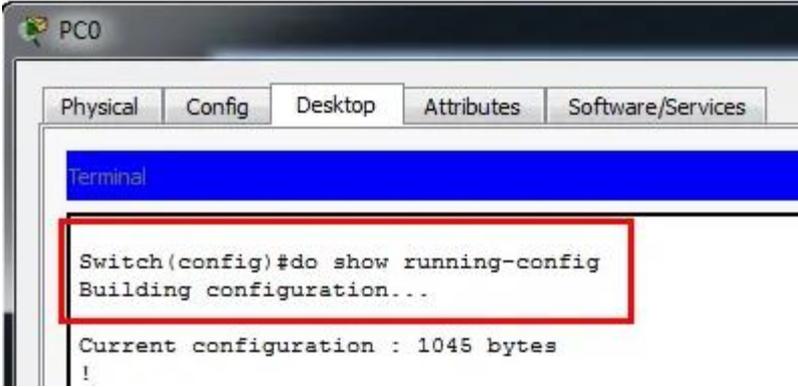
```
Switch>
Switch>enable
Switch#?
Exec commands:
clear        Reset functions
clock        Manage the system clock
configure    Enter configuration mode
connect      Open a terminal connection
```

Modo de configuración global

El modo de configuración global se compone de comandos pertenecientes a todo el dispositivo Cisco. En otras palabras, si necesitamos ejecutar comandos para modificar el comportamiento de todo el conmutador o de todo el enrutador, debemos configurar el IOS en modo de configuración global. El modo de configuración global solo se puede habilitar desde el modo EXEC privilegiado escribiendo los comandos "config t" o "conf t". El mensaje en este modo se compone del nombre del dispositivo seguido de "(config) #".

```
Switch>
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#|
```

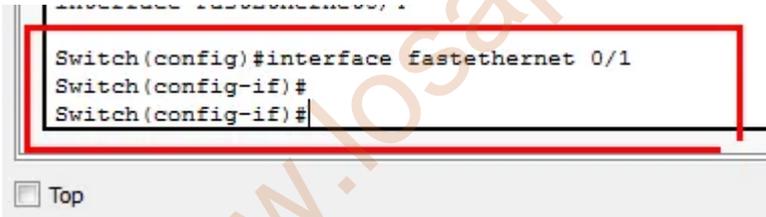
Escribiendo '?' vemos los comandos disponibles en ese modo. Si necesitamos ejecutar un comando que no está disponible en el modo de configuración global, debemos anteponer el comando con "do" .



```
PCO
Physical Config Desktop Attributes Software/Services
Terminal
Switch(config)#do show running-config
Building configuration...
Current configuration : 1045 bytes
!
```

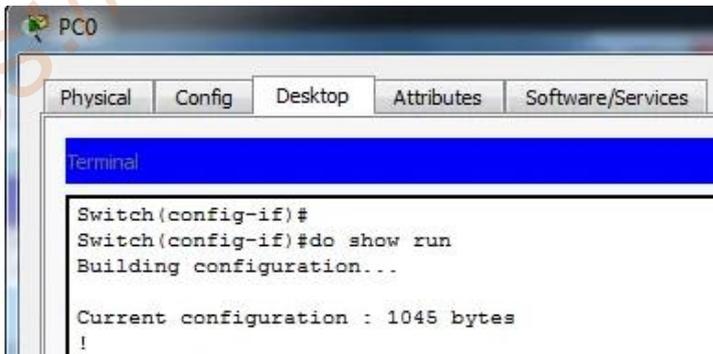
Modo de configuración específico

El modo de configuración específico se utiliza para los comandos que afectan la configuración de solo una parte o rango de componentes del dispositivo Cisco. Supongamos que queremos trabajar en algunas interfaces (o puertos) en nuestro conmutador o enrutador, necesitamos habilitar el modo de configuración específico. Podemos habilitar el modo de configuración específico solo desde el modo de configuración global seleccionando los componentes con los que queremos trabajar. El indicador en este modo está compuesto por el enrutador o el nombre de host del conmutador seguido de "(config-< component >)#". Seleccionemos la interfaz fastethernet 0/1 escribiendo "interface fastethernet 0/1" o "int f 0/1" .



```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#
Switch(config-if)#
```

Si queremos ejecutar un comando que no está disponible en el modo de configuración específico, prefija el comando con "do" . Por ejemplo, ejecute el comando "do show running-config" o "do show runn" en el modo de configuración específico



```
PCO
Physical Config Desktop Attributes Software/Services
Terminal
Switch(config-if)#
Switch(config-if)#do show run
Building configuration...
Current configuration : 1045 bytes
!
```

Configuración básica de un switch Cisco

Pasos de configuración

1. Cambiar el nombre del Switch Cisco

```
Switch(config)#hostname eclassvirtual
```

2. Contraseña secret

```
switch(config)#enable secret cisco
```

3. Usuario de acceso local

```
switch(config)#username cisco privilege 15 secret cisco
```

4. Acceso remoto Telnet usando cuenta de usuario local

```
switch(config)#line vty 0 4  
switch(config-line)#transport input telnet  
switch(config-line)#login local
```

5. Acceso por consola usando cuenta de usuario local

```
switch(config)#line console 0  
switch(config-line)#login local
```

6. Mensaje o banner para acceso de usuarios

```
switch(config)#banner motd #Prohibido el ingreso#
```

7. Configuración de una IP de administración

```
switch(config-if)#int vlan 1  
switch(config-if)#ip address 192.168.1.1 255.255.255.0  
switch(config-if)#no shutdown
```

8. Configuración de la puerta de enlace

```
switch(config)#ip default-gateway 192.168.1.254
```

9. Creación de una VLAN

```
switch(config)#vlan 10  
switch(config-vlan)#name Ingenieria
```

10. Asignar una VLAN a un puerto de switch

```
switch(config)#interface g1/0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 10
```

11 Asignar una VLAN a un rango de puertos

```
switch(config)#interface range g1/0/1 - 10
switch(config-if-range)#switchport mode access
switch(config-if-range)#switchport access vlan 10
```

12. Configuración de puerto de Trunk (Transporte de varias VLANs)

```
switch(config)#int g1/0/24
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
```

13. Delimitación de transporte de VLANs por enlace Trunk

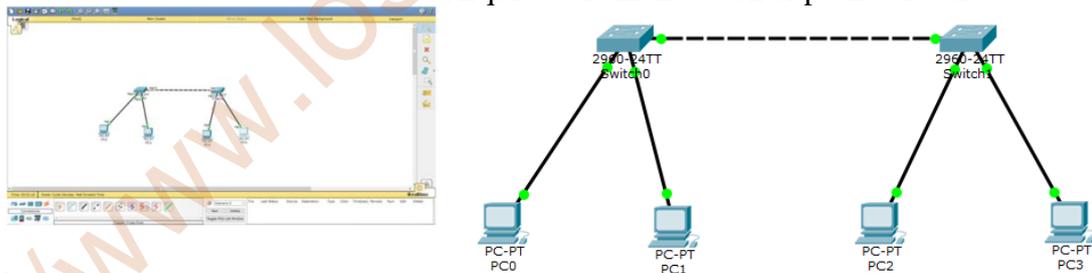
```
switch(config)#int g1/0/24
switch(config-if)#switchport trunk allowed vlan 10,11
```

14. Grabar la configuración

```
switch#copy running-config startup-config
```

- Crea la siguiente arquitectura de red :

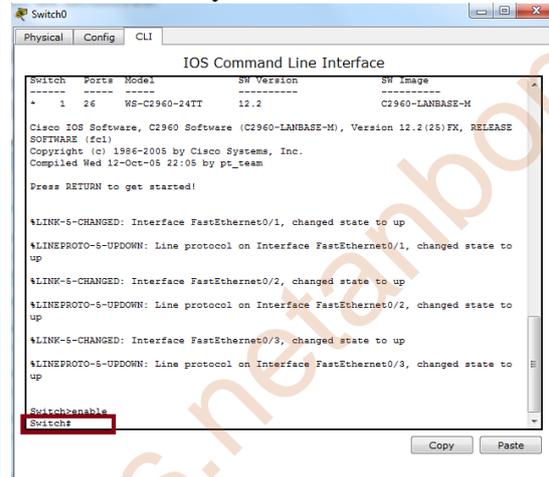
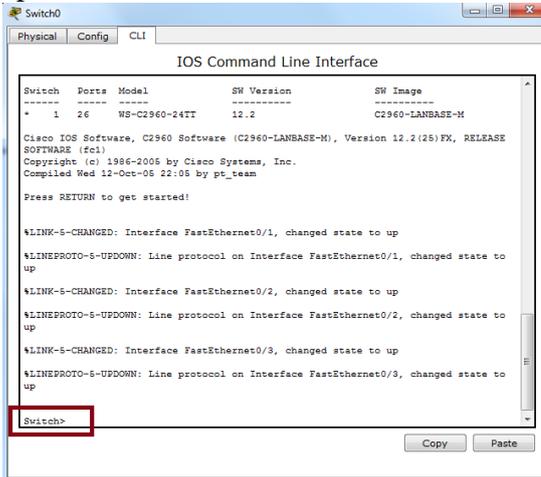
Arquitectura montada en el packet tracer:



- Cambiales los nombres a los switches mediante consola por los nombres SW1 y SW2 y haz captura de pantalla una vez cambiados y explica los comandos utilizados para el cambio de nombres.

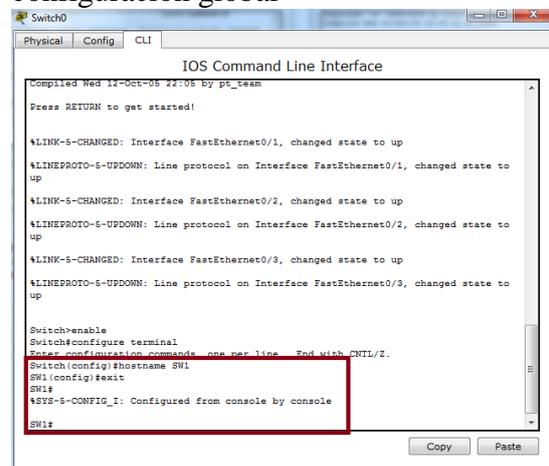
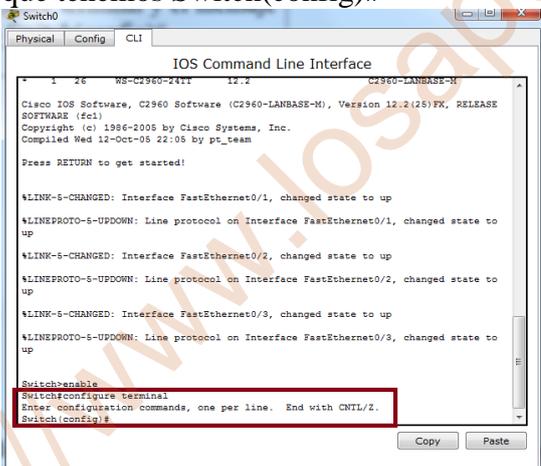
1.- Clic con el ratón en Switch0 y accedo a la pestaña de comando de línea interface IOS (CLI) y la pantalla aparecerá Switch> en modo de usuario.

2.- Para pasar de modo EXEC usuario a modo EXEC privilegio con funcionamiento avanzado escribo Switch>enable y tenemos Switch#

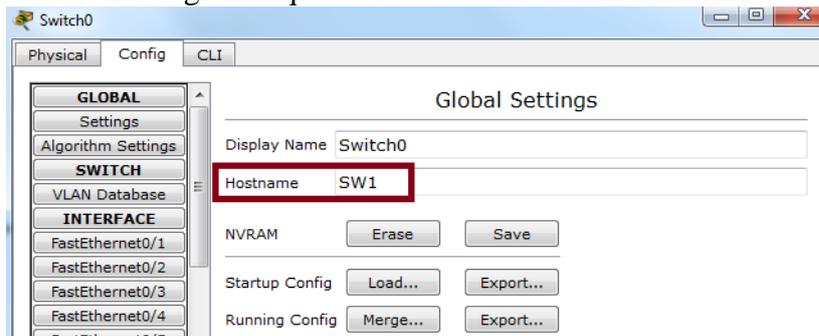


3.- Para pasar en modo configuración global para modificar el comportamiento del conmutador, escribimos Switch#configure terminal y el mensaje que tenemos Switch(config)#

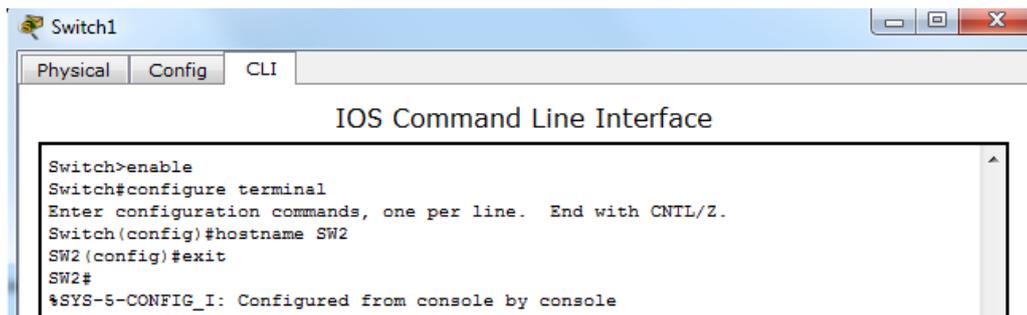
4.- Ahora procedemos a cambiar el nombre del switch a SW1 con el comando Switch(config)#hostname SW1 y salimos con exit de la configuración global



Se comprueba en modo gráfica que se ha cambiado automáticamente.

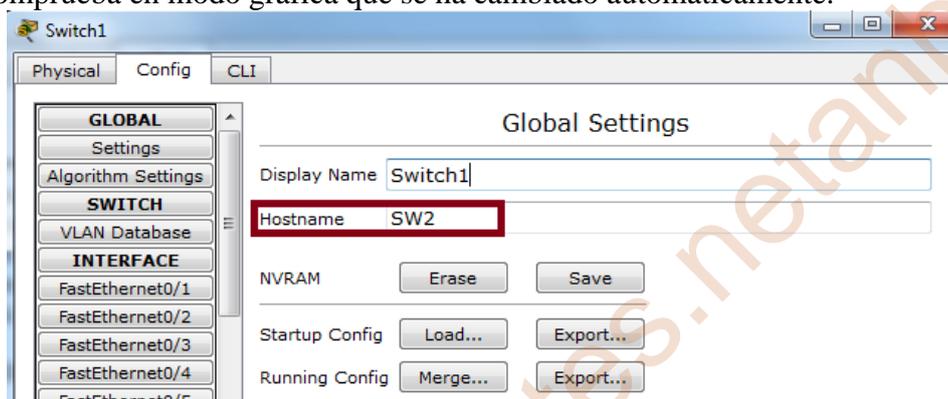


Repetimos el mismo proceso para el conmutador Switch1 y tenemos;



```
Switch1
Physical Config CLI
IOS Command Line Interface
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#exit
SW2#
%SYS-5-CONFIG_I: Configured from console by console
```

Se comprueba en modo gráfico que se ha cambiado automáticamente.



- Asigna una dirección IP de administración a cada uno de los Switches , por ejemplo la 192.168.1.50 y 192.168.1.51 y comprueba si desde cualquier PC tiene conectividad con esa IP, suponiendo que todos los PCs están en la misma Red y haz captura de pantalla de las ips administrativas de cada switch y de la conectividad de cada uno de ellos y explica los comando utilizados para asignar las ips administrativas.

Accedo al interface de línea de comandos de la IOS de Packet Tracer del Switch0 (SW1) utilizando los siguientes comandos para asignar la IP administrativa a SW1;

```
SW1>enable
SW1#configure terminal
SW1(config-if)#interface vlan 1 (accede a la vlan 1 para introducir la IP administrativa)
SW1(config-if)#ip address 192.168.1.50 255.255.255.0
SW1(config-if)#no shutdown (subir la dirección arriba en el SW1)
SW1(config-if)#exit
SW1(config)#
```

```
Switch0
Physical Config CLI
IOS Command Line Interface
SW1>enable
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.50 255.255.255.0
SW1(config-if)#no shutdown

SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW1(config-if)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console
```

Para comprobar la IP administrativa del SW1 es accediendo al comando;

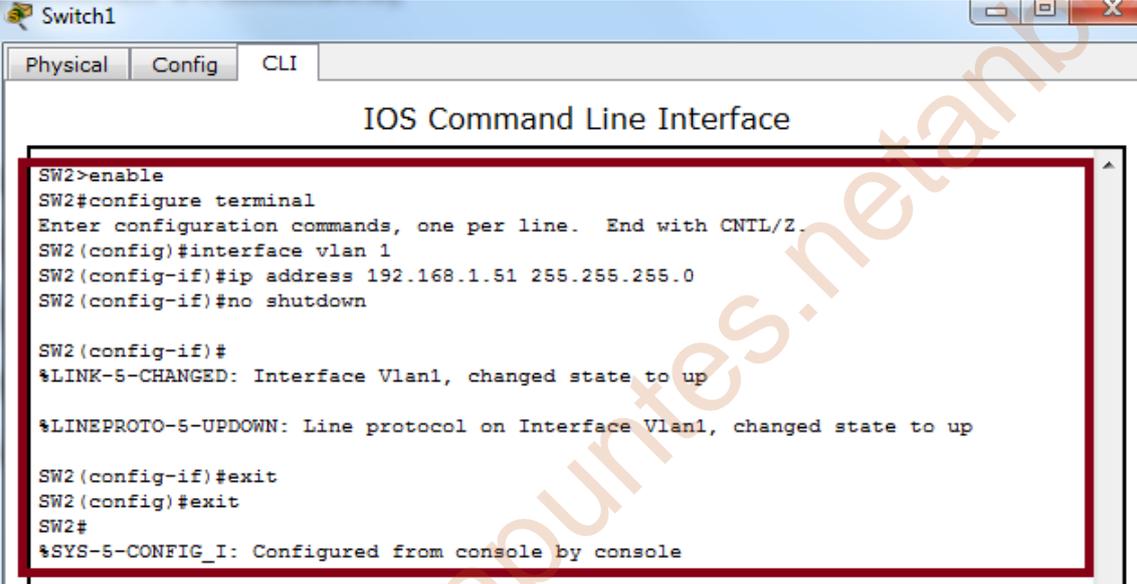
SW1#show ip interface brief

Se observa en la siguiente pantalla que tiene conectado las tres interface F0/1 y F0/2 que corresponde con la conexión de los PC0, PC1 y la interace F0/3 que es la conexión con el switch SW2. También tiene activada la vlan 1 con la IP 192.168.1.50

```
Switch0
Physical Config CLI
IOS Command Line Interface
SW1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual up up
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual down down
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual down down
FastEthernet0/11 unassigned YES manual down down
FastEthernet0/12 unassigned YES manual down down
FastEthernet0/13 unassigned YES manual down down
FastEthernet0/23 unassigned YES manual down down
FastEthernet0/24 unassigned YES manual down down
GigabitEthernet0/1 unassigned YES manual down down
GigabitEthernet0/2 unassigned YES manual down down
Vlan1 192.168.1.50 YES manual up up
SW1#
```

Accedo al interface de línea de comandos de la IOS de Packet Tracer del Switch1(SW2) utilizando los siguientes comandos para asignar la IP administrativa a SW2;

```
SW2>enable
SW2#configure terminal
SW2(config-if)#interface vlan 1 (accede a la vlan 1 para introducir la IP administrativa)
SW2(config-if)#ip address 192.168.1.51 255.255.255.0
SW2(config-if)#no shutdown (subir la dirección arriba en el SW2)
SW2(config-if)#exit
SW2(config)#
```



```
Switch1
Physical Config CLI
IOS Command Line Interface
SW2>enable
SW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2 (config)#interface vlan 1
SW2 (config-if)#ip address 192.168.1.51 255.255.255.0
SW2 (config-if)#no shutdown

SW2 (config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

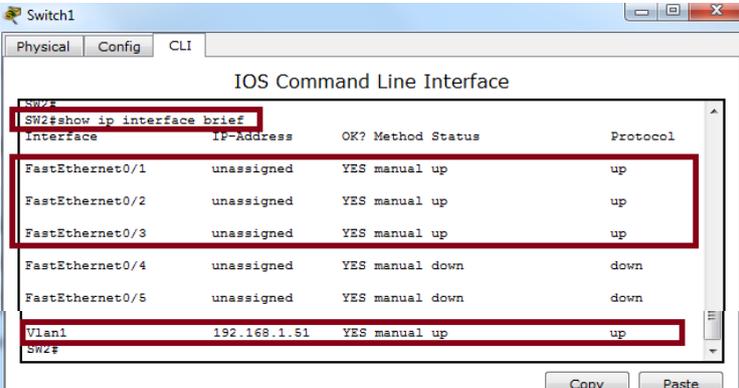
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW2 (config-if)#exit
SW2 (config)#exit
SW2#
%SYS-5-CONFIG_I: Configured from console by console
```

Para comprobar la IP administrativa del SW2 es accediendo al comando;

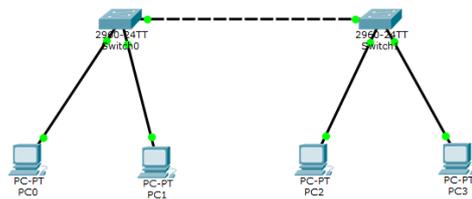
```
SW2#show ip interface brief
```

Se observa en la siguiente pantalla que tiene conectado las tres interface F0/1 y F0/2 que corresponde con la conexión de los PC2, PC3 y la interace F0/3 que es la conexión con el switch SW1. También tiene activada la vlan 1 con la IP 192.168.1.51



```
Switch1
Physical Config CLI
IOS Command Line Interface
SW2#
SW2#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual up up
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
Vlan1 192.168.1.51 YES manual up up
SW2#
```

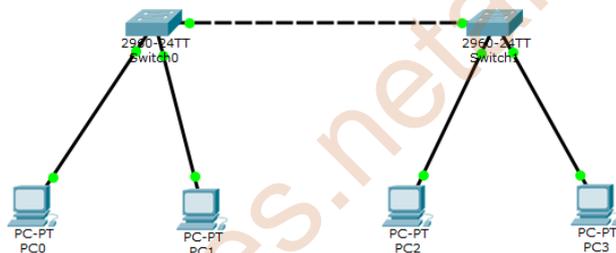
Una vez que cada switch tiene su IP administrativa compruebo si desde cualquier PC tiene conectividad con esa IP administrativa con los Switchs, suponiendo que todos los PCs están en la misma Red;



Configuramos con esta arquitectura los PC con estas dirección IP y con VLAN para que esten en la misma res:

- PC0: 192.168.1.10/24 – VLAN 1
- PC1: 192.168.1.11/24 – VLAN 1
- PC2: 192.168.1.12/24 – VLAN 1
- PC3: 192.168.1.13/24 – VLAN 1

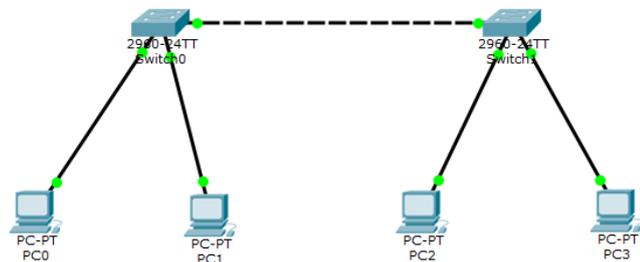
Se realiza el ping entre cada uno de los PC y es satisfactorio.



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC1	ICMP	Green	0.000	N	0	(edit)	
●	Successful	PC0	PC2	ICMP	Purple	0.000	N	1	(edit)	
●	Successful	PC0	PC3	ICMP	Pink	0.000	N	2	(edit)	
●	Successful	PC1	PC0	ICMP	Light Blue	0.000	N	3	(edit)	
●	Successful	PC1	PC2	ICMP	Light Green	0.000	N	4	(edit)	
●	Successful	PC1	PC3	ICMP	Light Green	0.000	N	5	(edit)	
●	Successful	PC2	PC3	ICMP	Light Blue	0.000	N	6	(edit)	
●	Successful	PC2	PC1	ICMP	Light Green	0.000	N	7	(edit)	
●	Successful	PC2	PC0	ICMP	Light Green	0.000	N	8	(edit)	

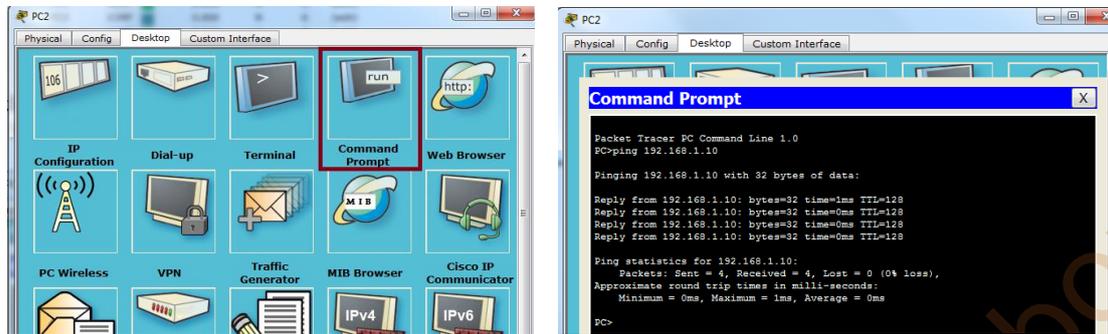
Se realiza el ping entre cada uno de los PC a cada uno de los Switch y es satisfactorio.



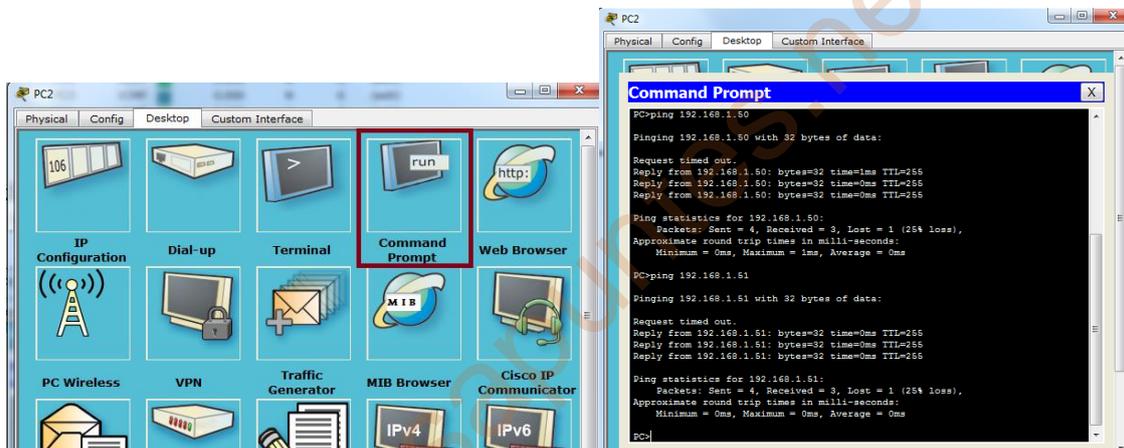
PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	Switch0	ICMP	Light Green	0.000	N	0	(edit)	
●	Successful	PC0	Switch1	ICMP	Light Green	0.000	N	1	(edit)	
●	Successful	PC1	Switch0	ICMP	Light Green	0.000	N	2	(edit)	
●	Successful	PC1	Switch1	ICMP	Light Green	0.000	N	3	(edit)	
●	Successful	PC2	Switch1	ICMP	Light Green	0.000	N	4	(edit)	
●	Successful	PC2	Switch0	ICMP	Light Green	0.000	N	5	(edit)	
●	Successful	PC3	Switch1	ICMP	Light Green	0.000	N	6	(edit)	
●	Failed	PC3	Switch0	ICMP	Light Green	0.000	N	7	(edit)	
●	Successful	PC3	Switch0	ICMP	Light Green	0.000	N	8	(edit)	

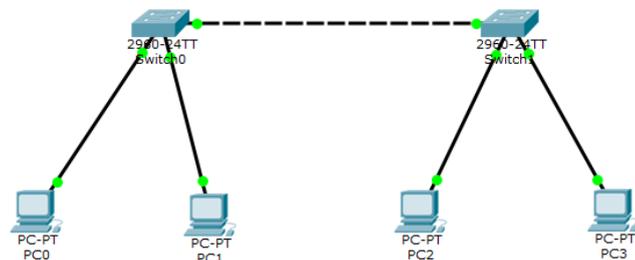
También se puede hacer la comprobación por el comando prompt, por ejemplo, desde el PC2 al PC0 con ping 192.168.1.10 y los paquetes enviados y recibidos son satisfactorios;



También se puede hacer la comprobación por el comando prompt, por ejemplo, desde el PC2 a los dos Switch con ping 192.168.1.50 y ping 192.168.1.51 y los paquetes enviados y recibidos son satisfactorios;



Se realiza el ping entre cada uno de los Switch y es satisfactorio.



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Switch0	Switch1	ICMP		0.000	N	0	(edit)	
	Successful	Switch1	Switch0	ICMP		0.000	N	1	(edit)	

También se puede hacer la comprobación por el interface de línea de comandos IOS del Packet Tracer;

The diagram shows two 2950-24TT switches connected via their console ports. The left switch is labeled 192.168.1.50 and is connected to PC-PT PC0 and PC-PT PC1. The right switch is labeled 192.168.1.51 and is connected to PC-PT PC2 and PC-PT PC3.

The top screenshot shows the CLI of Switch0. The command `SW1>ping 192.168.1.51` has been executed, resulting in a successful ping with a 100% success rate. The output is as follows:

```
SW1 con0 is now available
Press RETURN to get started.

SW1>ping 192.168.1.51
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.51, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
SW1#
```

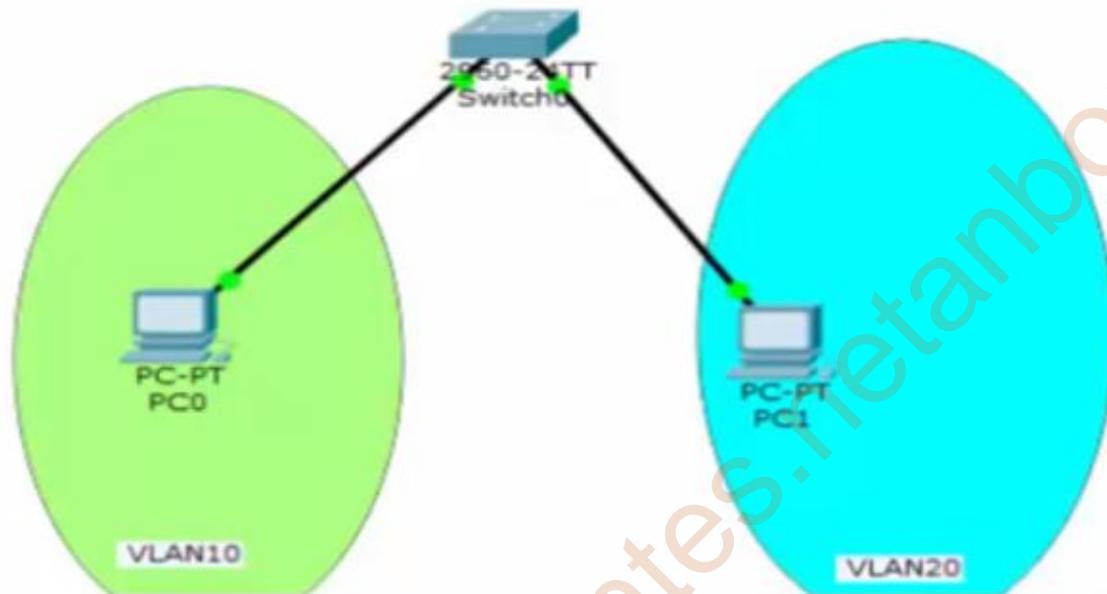
The bottom screenshot shows the CLI of Switch1. The command `SW2>ping 192.168.1.50` has been executed, resulting in a successful ping with a 100% success rate. The output is as follows:

```
SW2 con0 is now available
Press RETURN to get started.

SW2>ping 192.168.1.50
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.50, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
SW2#
```

Tarea 3.4 - Vlan

- ¿Busca por Internet que es una VLAN y explícalo con tus palabras?
- Utilizando el packet tracer monta la arquitectura de red que se muestra a continuación:

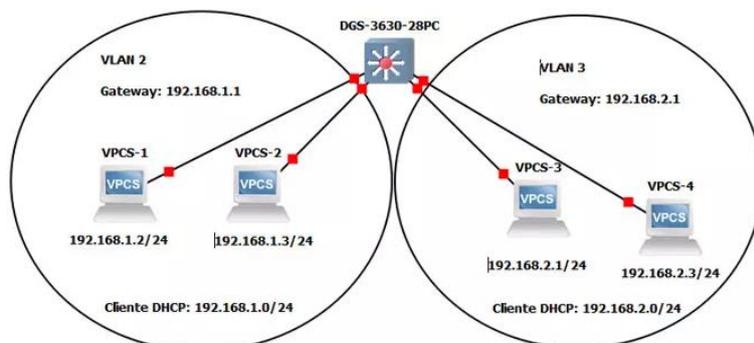


- Configura los diferentes dispositivos de red, utilizando el siguiente direccionamiento 192.168.1.2-3/24, haciendo que cada uno de ellos esté en una vlan distinta.
 - Copia y explica cada una de las configuraciones de cada uno de los dispositivos utilizados.
 - Comprueba si hay conectividad entre las distintas Vlan, ¿Hay conectividad? ¿Si, No y por qué? ¿Qué necesitaríamos para que haya conectividad en el caso de que no hubiera?
-
- ¿Busca por Internet que es una VLAN y explícalo con tus palabras?

Las **VLAN (Virtual LAN)**, o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo L3 (capa 3) como un router o un switch multicapa L3(capa 3).

Las VLAN «**Virtual LAN**» nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soporten VLANs para segmentar adecuadamente la red. También es muy importante que los routers que utilicemos soporten VLAN, de lo contrario, no podremos gestionarlas todas ni permitir o denegar la comunicación entre ellas. Actualmente la mayoría de routers profesionales e incluso sistemas operativos orientados a firewall/router como pfSense o OPNsense soportan VLAN porque es un estándar hoy en día. El uso de VLANs nos proporciona lo siguiente:

- **Seguridad:** las VLAN nos permite **crear redes lógicamente independientes**, por tanto, podremos aislarlas para que solamente tengan conexión a Internet, y denegar el tráfico de una VLAN a otra. Por defecto no se permite a las VLANs intercambiar tráfico con otra VLAN, es totalmente necesario ascender a nivel de red (L3) con un router o un switch multicapa, con el objetivo de activar el inter-vlan routing, es decir, el enrutamiento entre VLANs para sí permitir la comunicación entre ellas siempre que lo necesitemos.
- **Segmentación:** las VLAN nos permite **segmentar todos los equipos en diferentes subredes**, a cada subred le asignaremos una VLAN diferente. Por ejemplo, podremos crear una subred de gestión interna de todos los routers, switches y puntos de acceso, podremos crear una subred principal para los administradores, otra subred para dispositivos IoT y otra subred diferente para invitados. Es decir, podremos segmentar la red principal en subred con el objetivo de que cada subred haga uso de las comunicaciones como deseen. Gracias a la segmentación, podremos agrupar una gran cantidad de equipos dentro del mismo dominio de broadcast, aunque estén muy lejos físicamente.
- **Flexibilidad:** gracias a las VLAN podremos colocar a los diferentes equipos en una subred o en otra, de manera fácil y rápida, y tener unas políticas de comunicación donde permitiremos o denegaremos el tráfico hacia otras VLANs o hacia Internet. Por ejemplo, si creamos una VLAN de invitados, podríamos prohibirles el uso de servicios de streaming de vídeo.
- **Optimización de la red.** Al tener subredes más pequeñas, en entornos donde tengamos cientos o miles de equipos conectados, contendremos el broadcast en dominios más pequeños, por tanto, el rendimiento de la red será óptimo, sin tener que transmitir los mensajes de broadcast a todos los equipos conectados, lo que haría que el rendimiento de la red baje radicalmente e incluso podría llegar a colapsarse. Al usar VLAN, tendremos varios dominios de difusión en el mismo switch.



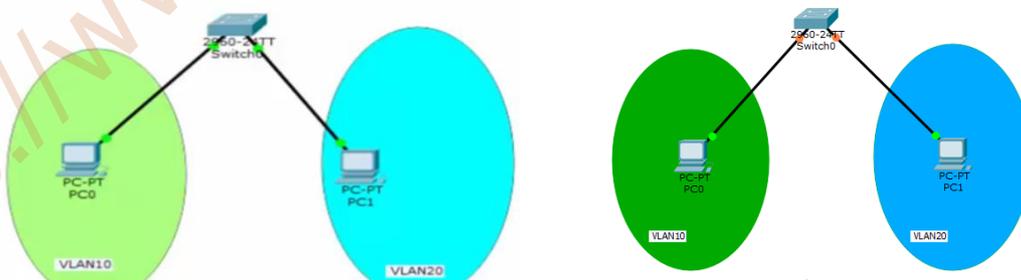
Las VLAN nos permiten **asociar lógicamente a los diferentes usuarios**, en base a etiquetas, puertos del switch, a su dirección MAC e incluso dependiendo de la autenticación que hayan realizado en el sistema. Las VLAN pueden existir en un solo switch gestionable, para asignar después a cada puerto el acceso a una determinada VLAN, pero también pueden existir en varios switches que están interconectados entre ellos, por tanto, las VLAN pueden extenderse por diferentes switches a través de los enlaces troncales. Esto nos permite tener las VLAN en diferentes switches y asignar una determinada VLAN en cualquiera de estos switches o en varios simultáneamente.

Cuando creamos y configuramos las VLAN en un router no se pueden comunicar entre ellas, la única forma de que se puedan comunicar las VLAN es ascendiendo a nivel de red (L3), esto lo podemos hacer de diferentes formas:

- Usar un **router/firewall con soporte para el estándar de VLANs**. El switch le pasará un troncal con todas las VLANs y el router/firewall dará de alta en su firmware o sistema operativo las diferentes VLANs, y permitirán el enrutamiento inter-vlan. Es posible que, por defecto, este enrutamiento esté activado, pero por reglas en el firewall se deniegue la comunicación entre las VLAN, hasta que permitamos el acceso.
- Usar un **switch gestionable L3**. Los switches gestionables L3 nos permiten crear interfaces IPv4 y IPv6, por lo que podremos crear una interfaz por cada VLAN que tengamos configurada en el switch y activar el enrutamiento inter-vlan. Esto es una opción muy buena para intercomunicar las VLANs sin necesidad de que el router se encargue de todo, generalmente estos switches L3 están en el Core de la red.

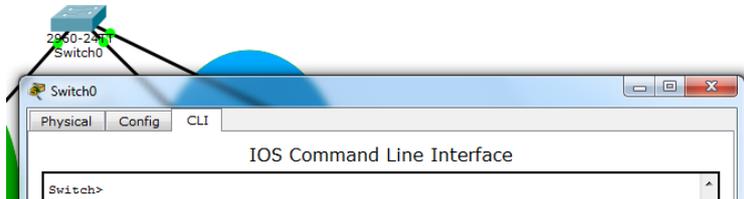
Para permitir la comunicación o la no comunicación de las VLAN se deben hacer uso de **ACL (Listas de Control de Acceso)**, o configurar el firewall correspondiente para permitir o denegar el tráfico. Por ejemplo, se podría permitir la comunicación de una VLAN 2 a una VLAN 3, pero no al revés, por tanto, configurando correctamente el firewall y los estados de conexión, se podría ajustar la comunicación a los requisitos de la empresa.

- Utilizando el packet tracer monta la arquitectura de red que se muestra a continuación:



- Configura los diferentes dispositivos de red, utilizando el siguiente direccionamiento 192.168.1.2-3/24, haciendo que cada uno de ellos esté en una vlan distinta.

Creo en el Switch dos redes de áreas locales virtuales VLAN 10 y VLAN 20;



```
Switch>enable
Switch#vlan database
Switch(config-vlan)#vlan 10 name oficina
Switch(config-vlan)#vlan 20 name taller
Switch(config-vlan)#exit
Switch(config)#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode vlan 10
Switch(config-if)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.1.3 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
Switch#show ip interface brief
```

Accediendo al Switch en modo de línea de comando ejecutamos las siguientes comandos para crear la VLAN 10 y VLAN 20

A la VLAN 10 la denominamos con el nombre de Oficina y la VLAN la denominados con el nombre de Taller. A la interface 0/1 le asignamos el puerto de acceso VLAN 10 y a la interface 0/2 le asignamos el puerto de acceso VLAN 20.

Ahora creamos una IP para la VLAN 10 y otra para la VLAN 20.

Compruebo si se ha creado estas dos IP en el Switch.

<u>Interface</u>	<u>IP-Address</u>	<u>Ok?</u>	<u>Method</u>	<u>Status</u>	<u>Protocol</u>
Vlan10	192.168.1.2	YES	manual	up	up
Vlan20	192.168.1.3	YES	manual	up	up

Switch#show vlan

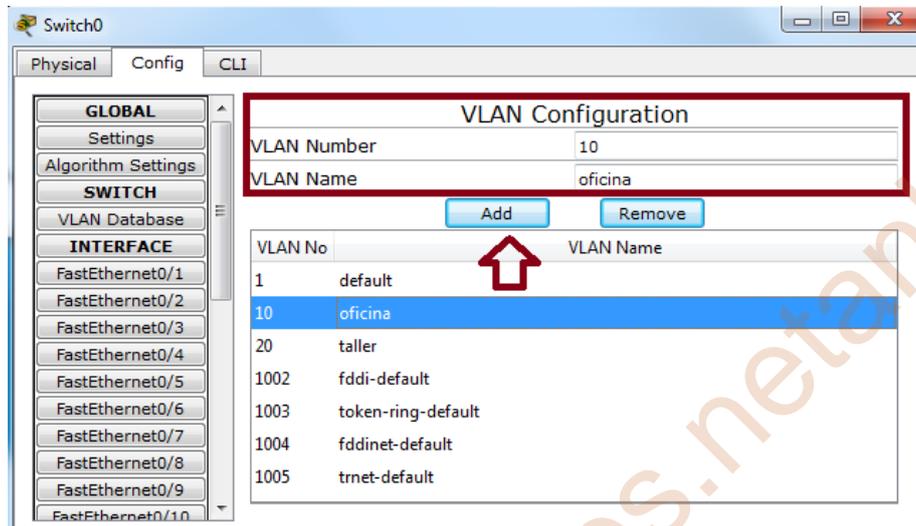
```
Switch#show vlan
VLAN Name      Status Ports
----
1  default      active Fa0/8, Fa0/4, Fa0/5, Fa0/6
   Fa0/7, Fa0/8, Fa0/9, Fa0/10
   Fa0/11, Fa0/12, Fa0/13, Fa0/14
   Fa0/15, Fa0/16, Fa0/17, Fa0/18
   Fa0/19, Fa0/20, Fa0/21, Fa0/22
   Fa0/23, Fa0/24, Gig0/1, Gig0/2
10  Oficina     active Fa0/1
20  Taller      active Fa0/2
1002 fdd-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
```

Switch#show ip interface brief

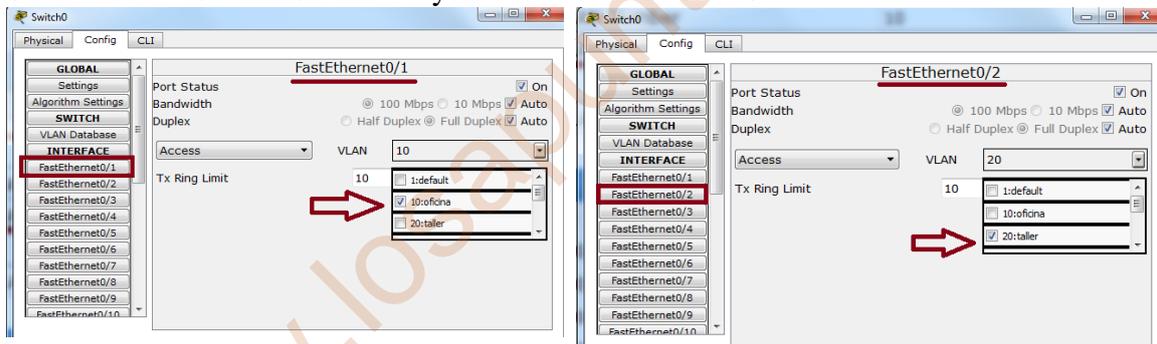
```
Vlan1 unassigned YES manual administratively down
Vlan10 192.168.1.2 YES manual up
Vlan20 192.168.1.3 YES manual up
Switch#
```

- Copia y explica cada una de las configuraciones de cada uno de los dispositivos utilizados.

La configuración de los Switch lo he llevado a cabo mediante la línea de comandos en el apartado anterior, pero también se puede hacer mediante modo gráfico, tanto como la VLAN 10 y VLAN 20;

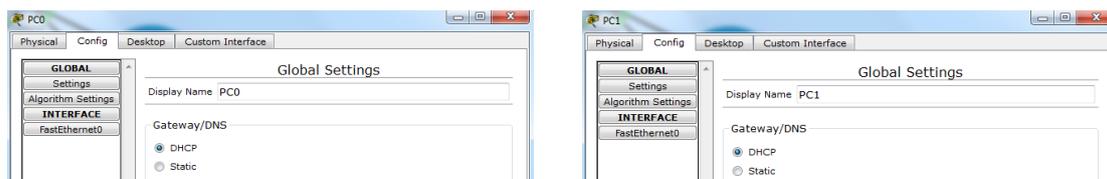


En la interface 0/1 en donde está el PC0 lo incluyo dentro de la VLAN 10 y el interface 0/2 en donde está el PC1 lo incluyo dentro de la VLAN 20.



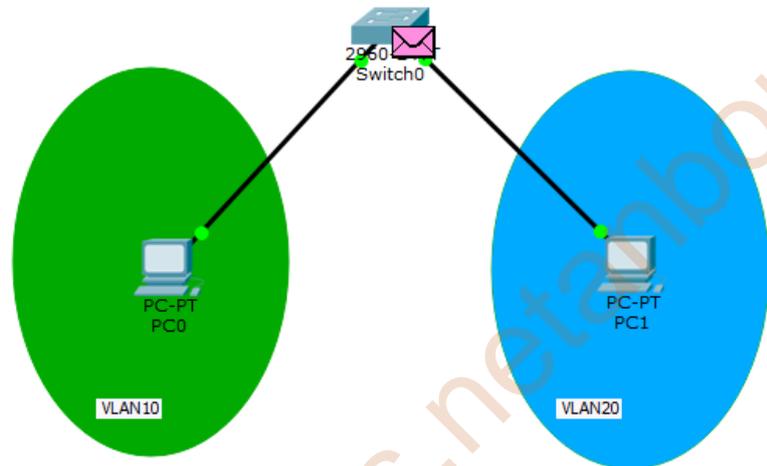
Sin embargo en la Switch para el direccionamiento de su IP en cada una de las VLAN es a través de línea de comandos y no en modo gráfico.

En la configuración de los PC0 y PC1 lo he llevado a cabo mediante IP dinámica ya que en el ejercicio solo tenía dos direccionamiento a utilizar el 192.168.1.2-3/24 y estas direcciones lo he utilizado para las VLAN 10 y VLAN 20.



Comprueba si hay conectividad entre las distintas Vlan, ¿Hay conectividad? ¿Si, No y por qué? ¿Qué necesitaríamos para que haya conectividad en el caso de que no hubiera?

No hay conectividad. Porque aunque cada uno tenga la misma red de IP 192.168.1.2-3/24 la separación de los dos PC, PC0 y PC1 en redes áreas locales virtuales VLAN hacen que dichos ordenadores sean independiente unas de otras.



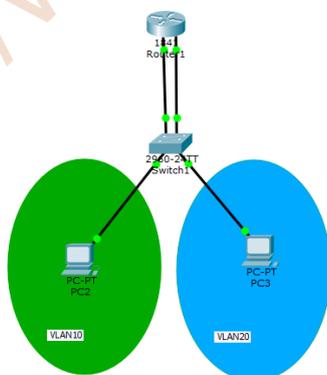
PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC1	ICMP		0.000	N	0	(edit)	
	Failed	PC1	PC0	ICMP		4.160	N	1	(edit)	

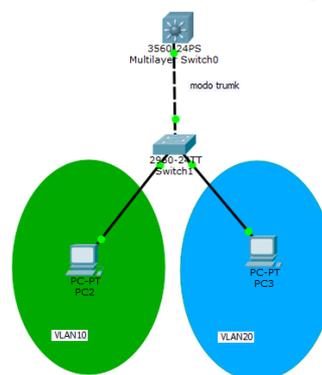
¿Qué necesitaríamos para que haya conectividad en el caso de que no hubiera?

Necesitaríamos de otros dispositivos como router (capa 3) o switch multicapa (también de capa 3) con una configuración de cada uno de los elementos para interconectarse entre ellos cuando fuese necesario, es decir, todos los ordenadores de la VLAN 10 se comunicarían entre ellos sin enviar paquetes al VLAN 20 y viceversa, salvo que algún ordenador enviará algún paquete entre VLANs debidamente programado en el router o Switch multicapa. Por ejemplo:

Ejemplo con un router:



Ejemplo con un Switch Multicapa:



WEBGRAFIA

Tarea 3.1 - Introducción e Instalación Packet tracer

Cacharrear el Packet Tracer.

Tarea 3.2 - Configuración de equipos

Tutorial Packet Tracer - 2 - Configuración de una PC:

<https://www.youtube.com/watch?v=xcKWfX6tSBo>

Tarea 3.3 - Configuración Switch

crear VLANs por interfaz gráfica:

<https://www.youtube.com/watch?v=4ayv0bqhNqE>

02 - Introducción a CLI y Configuración Básica de Switch/Router [Packet Tracer 7.0 - Español]:

<https://www.youtube.com/watch?v=L6404zez4xo>

Configuración básica de un switch [packet tracer]:

<https://www.youtube.com/watch?v=ifwt3Mr6Js8>

Tarea 3.4 - Vlan

VLAN (Red de Área Local Virtual) en Packet Tracer (CYERD):

<https://www.youtube.com/watch?v=cbN4iksKo2A>

VLANs: Qué son, tipos y para qué sirven:

<https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>

Simulación de dos Subredes:

<https://www.youtube.com/watch?v=eRp4UelSO5Y>

Simulación de dos Subredes conexión de las mismas con un Router:

<https://www.youtube.com/watch?v=1HC3KTXwcdA>

Redes 113 Enrutamiento Inter Vlan Switch Multicapa:

<https://www.youtube.com/watch?v=l3MmvBssCzk>