PROCESO GESTIÓN DEL TALENTO HUMANO

FORMATO INFORME MENSUAL EJECUCIÓN CONTRACTUAL

Barranquilla, Julio de 2023

Señor (a)
JORGE LUIS PEDROZA CABALLERO
SUPERVISOR(A) CONTRATO No. **5209639**
Coordinador Académico Artes Gráficas
Sistemas
Barranquilla

Asunto: Informe mensual de ejecución contractual
Mes Julio del año 2023

Referencia: No 5209639 del año 2023

ROBERTO CARLOS BELTRAN MEDINA, identificado con la cédula de ciudadanía No. 72.216.225 de Barranquilla, en mi calidad de Contratista del SENA, en Sistemas, en cumplimiento del Contrato de Prestación de Servicios de la referencia, a continuación presento el Informe de actividades realizadas en el mes objeto de cobro.

Valor y forma de Pago: a). un pago correspondiente al mes de Julio de 2023 por valor de (1.758.530). Los honorarios serán pagados por el SENA al contratista de acuerdo al cronograma definido por la Dirección Administrativa y Financiera de la Dirección General, en la cuenta de Ahorros No. 77187008495 Bancolombia, cuyo titular es el Contratista.

Plazo: Será hasta el 15 de Diciembre de 2023.

OBJETO:
Desarrollar formación profesional por competencias laborales, mediante la estrategia de aprendizaje por proyectos en los programas de formación de ANALISIS Y DESARROLLO DE SISTEMAS DE INFORMACION, TECNICO EN SISTEMAS, PROGRAMACION DE SOFTWARE, participando en los equipos de diseño y desarrollo curricular y gestionando las actividades y proyectos a través de las tecnologías de la información y la comunicación que brinda la entidad, atendiendo las políticas institucionales y la normatividad vigente

Obligaciones Especificas: *(Trascriba las obligaciones especificas del contrato, dentro del siguiente cuadro)*

No	Obligaciones	Acciones realizadas	Evidencias
1	formular proyecto formativo, planeación pedagógica del proyecto y recursos didácticos (guías de aprendizaje, instrumentos de evaluación y material de apoyo) para el desarrollo de las competencias	Realizar mantenimiento preventivo y predictivo que prolongue el funcionamiento de los equipos de computo.	Ficha No: 2671178

	del programa de formación según lineamientos del procedimiento y guía de desarrollo curricular.		
2	formular proyecto formativo, planeación pedagógica del proyecto y recursos didácticos (guías de aprendizaje, instrumentos de evaluación y material de apoyo) para el desarrollo de las competencias del programa de formación según lineamientos del procedimiento y guía de desarrollo curricular.	Implementar la estructura de la red de acuerdo con un diseño establecido a partir de normas técnicas internacionales.	Ficha No: 2620643
3	formular proyecto formativo, planeación pedagógica del proyecto y recursos didácticos (guías de aprendizaje, instrumentos de evaluación y material de apoyo) para el desarrollo de las competencias del programa de formación según lineamientos del procedimiento y guía de desarrollo curricular.	Configurar dispositivos activos de interconexión según especificaciones del diseño y protocolos técnicos	Ficha No: 2452514
4	formular proyecto formativo, planeación pedagógica del proyecto y recursos didácticos (guías de aprendizaje, instrumentos de evaluación y material de apoyo) para el desarrollo de las competencias del programa de formación según lineamientos del procedimiento y guía de desarrollo curricular.	Configurar dispositivos activos de interconexión según especificaciones del diseño y protocolos técnicos	Ficha No: 2558406
5	formular proyecto formativo, planeación pedagógica del proyecto y recursos didácticos (guías de aprendizaje, instrumentos de evaluación y material de apoyo) para el desarrollo de las competencias del programa de formación según lineamientos del procedimiento y guía de desarrollo curricular.	Configurar dispositivos activos de interconexión según especificaciones del diseño y protocolos técnicos	Ficha No: 2620641

A continuación relaciono los desplazamientos que realicé previo a la presentación de este informe. Una vez finalizado cada desplazamiento presenté al ordenador del gasto el informe en el Formato Informe Legalización Desplazamiento Contratista GTH-F-087, en el que se describieron las actividades desarrolladas y los resultados de cada desplazamiento. Cada informe cuenta con el visto bueno del Supervisor.

Se lista a continuación el soporte de la legalización de los desplazamientos realizados, los cuales forman parte integral del presente informe de ejecución contractual.

ITEM	No DE LA ORDEN DE VIAJE	LUGAR DE DESPLAZAMIENTO	FECHAS DE DESPLAZAMIENTOS	
			INICIO	FINALIZACIÓN

Nota 1: *Por cada desplazamiento que haya realizado el contratista, adjuntará el respectivo informe que la soporte. En caso de haber realizado el desplazamiento en fecha posterior a la presentación del informe de ejecución contractual, deberá reportarlo en el siguiente informe de ejecución contractual.*

Para el trámite de la cuenta me permito adjuntar: Documentos electrónicos enunciados como evidencias del cumplimiento de las obligaciones contractuales y los desplazamientos realizados y el No. 9452598932 de la planilla, operador y periodo. (Decreto Ley 2106 de 2019 – " *Decreto Ley Antitrámites"*)

Declaración bajo la gravedad de juramento.

Me permito declarar **bajo la gravedad de juramento** que durante el periodo objeto de cobro SI____NO_X__ he suscrito otro u otros contratos con entidade(s) del Estado el (los) cual(es) se encuentra(n) en ejecución; la anterior declaración de acuerdo con lo establecido en el numeral 5º de la Directiva Presidencial No. 001 de 2022, a fin de identificar potenciales conflictos de interés y hacer la gestión del riesgos para la toma de decisiones dentro del principio de la debida diligencia frente a la ejecución de los contratos de prestación de servicios profesionales o de apoyo a la gestión.

Nota: En el evento de señalar **SI,** el análisis efectuado por el supervisor y ordenador de pago deberá quedar documentado y publicado en el SECOP II en los documentos relacionados en el archivo Gestión Contractual GC_ del periodo objeto de cobro.

Evidencias en () folios

Cordialmente,



ROBERTO CARLOS BELTRAN MEDINA
Contratista
C.C. No. 72.216.225

Recibí a satisfacción:

JORGE LUIS PEDROZA CABALLERO
Supervisor(a) Contrato 5209639 de 2023
Coordinador Académico Artes Gráficas

redes confiables

Las redes confiables son aquellas que han sido diseñadas y configuradas de manera que sean seguras y confiables para el intercambio de información. La seguridad en las redes es crítica para prevenir el acceso no autorizado a datos sensibles, ataques malintencionados y otros riesgos que pueden comprometer la integridad de los sistemas de información y la privacidad de los usuarios.

Algunas de las características de las redes confiables incluyen:

Seguridad: Las redes confiables deben estar protegidas por medidas de seguridad efectivas, como firewalls, sistemas de detección y prevención de intrusiones, autenticación de usuarios y encriptación de datos.

Fiabilidad: Las redes confiables deben ser confiables y estar disponibles en todo momento, para que los usuarios puedan acceder a la información de manera rápida y eficiente.

Escalabilidad: Las redes confiables deben ser escalables, es decir, capaces de manejar un gran número de usuarios y dispositivos conectados sin comprometer la seguridad o la fiabilidad.

Facilidad de uso: Las redes confiables deben ser fáciles de usar y administrar, para que los usuarios puedan acceder a la información de manera rápida y eficiente.

Monitoreo y gestión: Las redes confiables deben ser monitoreadas y gestionadas constantemente para detectar posibles problemas de seguridad y resolverlos antes de que se conviertan en una amenaza.

Para lograr una red confiable, es importante seguir las mejores prácticas de seguridad de la información, implementar políticas de seguridad efectivas y capacitar a los usuarios en la importancia de mantener una buena seguridad en la red.

Las redes confiables son aquellas que han sido diseñadas y configuradas para ser seguras y confiables en el intercambio de información. Para lograr esto, deben contar con medidas de seguridad efectivas, ser confiables y escalables, fáciles de usar y administrar, y monitoreadas y gestionadas constantemente. Para garantizar la seguridad de las redes, es importante seguir las mejores prácticas de seguridad de la información, implementar políticas de seguridad efectivas y capacitar a los usuarios.

Tolerancia a fallas

La tolerancia a fallas se refiere a la capacidad de un sistema para seguir funcionando en caso de que ocurran fallas o errores. Se logra mediante la implementación de técnicas como redundancia, detección de fallas, aislamiento de fallas y recuperación de fallas. La tolerancia a fallas es importante para garantizar la disponibilidad y confiabilidad de los sistemas informáticos, especialmente en sistemas críticos.

algunas de las características de las redes confiables incluyen:

Seguridad: Las redes confiables deben estar protegidas por medidas de seguridad efectivas, como firewalls, sistemas de detección y prevención de intrusiones, autenticación de usuarios y encriptación de datos.

Fiabilidad: Las redes confiables deben ser confiables y estar disponibles en todo momento, para que los usuarios puedan acceder a la información de manera rápida y eficiente.

Escalabilidad: Las redes confiables deben ser escalables, es decir, capaces de manejar un gran número de usuarios y dispositivos conectados sin comprometer la seguridad o la fiabilidad.

Facilidad de uso: Las redes confiables deben ser fáciles de usar y administrar, para que los usuarios puedan acceder a la información de manera rápida y eficiente.

Monitoreo y gestión: Las redes confiables deben ser monitoreadas y gestionadas constantemente para detectar posibles problemas de seguridad y resolverlos antes de que se conviertan en una amenaza.

Escalabilidad

La escalabilidad en una red se refiere a su capacidad para manejar un aumento en el número de dispositivos, usuarios y tráfico sin comprometer el rendimiento. Se logra a través de técnicas como topología escalable, redundancia, ancho de banda, balanceo de carga y protocolos escalables. La escalabilidad en redes es importante para garantizar la disponibilidad y confiabilidad de los servicios de red, reducir costos y aumentar la eficiencia.

Existen varias técnicas para lograr la escalabilidad en redes, como:

Topología escalable: Utilizar una topología de red escalable que permita agregar nodos o dispositivos adicionales según sea necesario.

Redundancia: Agregar componentes o recursos adicionales, como enlaces de red, para que en caso de que alguno falle, el tráfico de red pueda ser redirigido sin interrupciones.

Ancho de banda: Asegurar que la red tenga suficiente ancho de banda para manejar la carga de trabajo y tráfico de datos.

Balanceo de carga: Distribuir la carga de trabajo en varios dispositivos o nodos de la red, lo que permite aumentar la capacidad de procesamiento y almacenamiento.

Protocolos escalables: Utilizar protocolos de red escalables que permitan una mayor eficiencia en la gestión de la red y una mayor capacidad de escalabilidad.

La escalabilidad en redes es importante para garantizar la disponibilidad y confiabilidad de los servicios de red, y también para reducir los costos y aumentar la eficiencia en la gestión de la red

La calidad de servicio

La calidad de servicio (QoS) se refiere a la capacidad de un sistema de red para garantizar la transmisión fiable y eficiente del tráfico de datos. Se logra mediante la asignación de prioridades y el control de los flujos de tráfico de red, utilizando técnicas como la clasificación de tráfico, la limitación de ancho de banda, el control de congestión y la reserva de ancho de banda. La QoS es importante para asegurar la entrega de servicios de red de alta calidad y mantener un rendimiento óptimo en situaciones de alta demanda.

La QoS se logra mediante la asignación de prioridades y el control de los flujos de tráfico de red. Algunas técnicas utilizadas para implementar la QoS incluyen:

Clasificación de tráfico: Clasificar el tráfico de red en diferentes categorías, como voz, video y datos, y asignar prioridades según la importancia de cada tipo de tráfico.

Limitación de ancho de banda: Limitar la cantidad de ancho de banda que se asigna a cada tipo de tráfico, lo que garantiza que los flujos de tráfico de alta prioridad tengan un mayor ancho de banda disponible.

Control de congestión: Controlar la congestión de la red mediante la reducción de la velocidad de transmisión de los paquetes de datos, lo que evita que la red se sature.

Reserva de ancho de banda: Reservar un ancho de banda específico para flujos de tráfico de alta prioridad, lo que garantiza que se entreguen sin interrupciones o retrasos.

La seguridad de la red

La seguridad de la red se refiere a la protección de los recursos de la red contra posibles amenazas, ataques o vulnerabilidades. Las medidas de seguridad incluyen autenticación, control de acceso, firewall, encriptación, actualizaciones de software, detección de intrusos y gestión de políticas de seguridad. Mantener la seguridad de la red es importante para proteger la información y los datos confidenciales, garantizar la disponibilidad y confiabilidad de los servicios de red y evitar posibles riesgos de seguridad

Autenticación: Verificar la identidad de los usuarios y dispositivos antes de permitir el acceso a la red.

Control de acceso: Limitar el acceso a la red solo a usuarios autorizados y restringir el acceso a recursos de red específicos.

Firewall: Utilizar un firewall para bloquear el tráfico no autorizado y proteger la red contra posibles ataques.

Encriptación: Utilizar técnicas de encriptación para proteger los datos transmitidos en la red y evitar el acceso no autorizado.

Actualizaciones de software: Mantener actualizado el software de red para corregir posibles vulnerabilidades y agujeros de seguridad.

La seguridad en redes es una tarea continua que requiere atención y esfuerzo constante para mantener la red protegida contra posibles amenazas y ataques.

Nombre: *Cristian David Redondo Orozco*

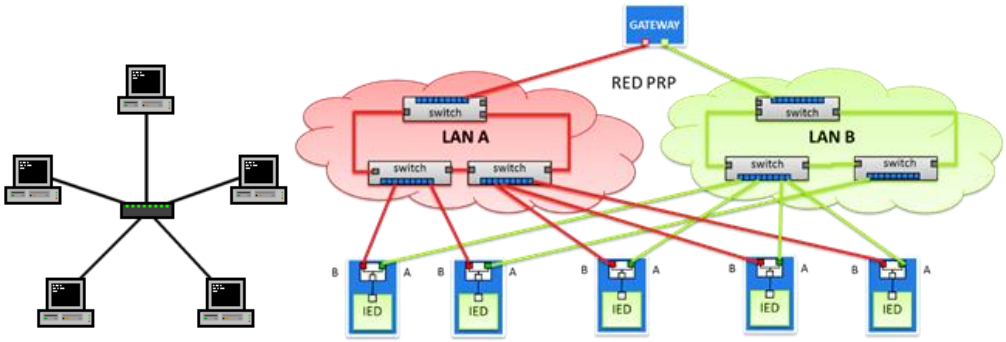
Redes confiables

Este sistema está diseñado para garantizar la seguridad y protección de bases de datos para tener todo en privado por si desean hacer un ataque o un acceso no autorizado se pueda detectar y detener el posible ataque.

Tolerancia a falla

es cuando nos permite reducir las fallas en una red, para tener una red tolerante a falla se puede implementar la redundancia y topologías que eviten la detención de datos a causa de fallas lógicas, de equipos activos/pasivos de red o desconexión de un enlace, haciendo que los mismos busquen una nueva ruta para seguir transmitiendo los datos y de esta manera reducir el impacto negativo en la red.

Una de las topologías que nos podría ayudar para realizar una red tolerante a falla seria, la de estrella.



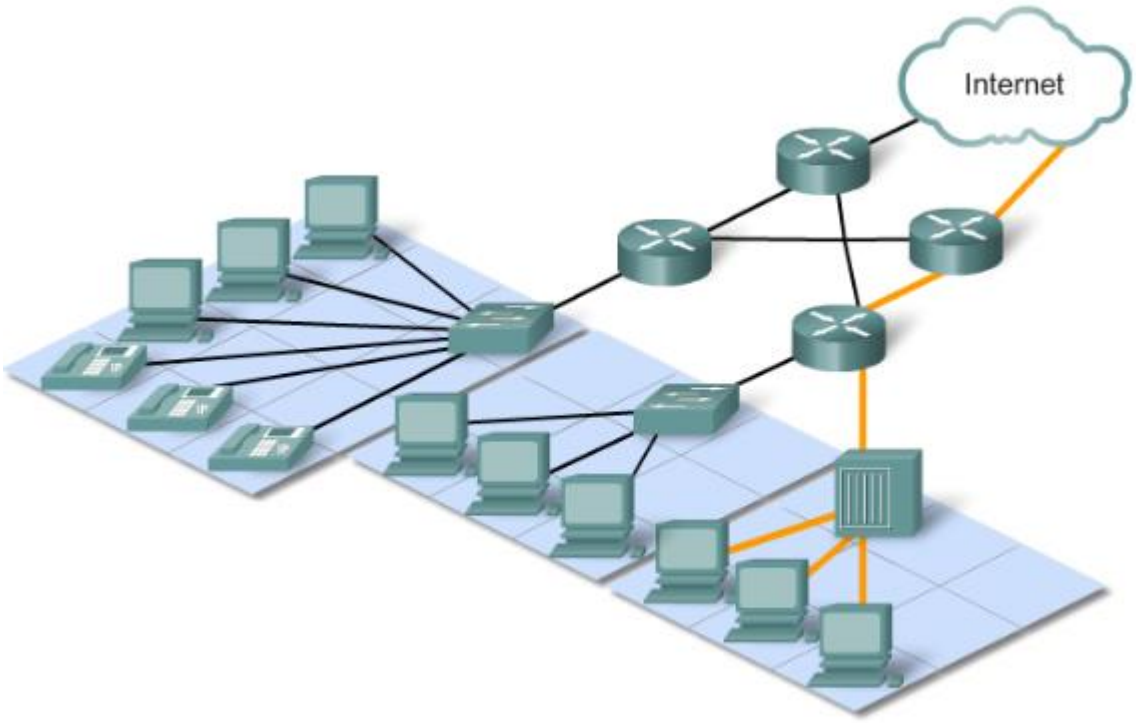
Ya que de esta manera los dispositivos de la red tienen enlaces diferentes y si hay una desconexión de enlace solo se verá afectada una pequeña parte de la red y no su totalidad. Por otra parte, una conexión redundante, es cuando los equipos tienen conectados dos o más enlaces permitiendo que los dispositivos busquen otras alternativas o ruta para enviar la información de esta manera no frenar la transmisión de datos en la red.

Escalabilidad

La escalabilidad permite que una red pueda expandirse rápidamente, de esta manera se puede conectar nuevos equipos, servidores o aplicaciones a una topología y no tendrán interferencia los usuarios existentes en la red. Para las empresas en desarrollo, esto es muy útil ya que ellos al crecer como empresa van a necesitar más equipos más usuarios y al conectar o configurar los nuevos equipos no van a afectar a los equipos o usuarios existentes. Hay dos clases de escalabilidad, escalabilidad vertical y escalabilidad horizontal.

Escalabilidad vertical: cuando hablamos de escalabilidad vertical nos referimos a la parte de sistema o software, lo que serian las aplicaciones o capacidad en el sistema.

Escalabilidad horizontal: cuando hablamos de escalabilidad horizontal nos referimos a la parte de hardware que serian los computadores, servidores, switches entre otros.

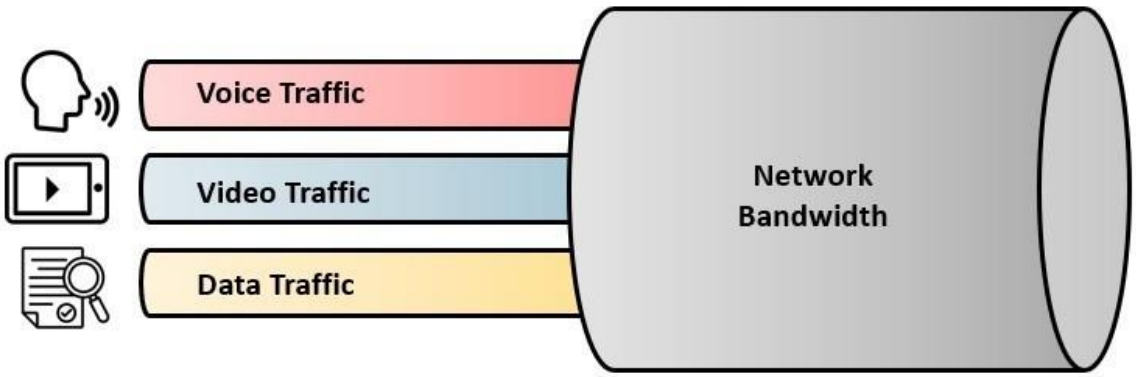


Calidad de servicio

Es la practica realizada para mejor rendimiento a una red se compone de un paquete de regla que sirve para mejorar estabilidad y priorizar el tráfico según su importancia mejorando la experiencia del usuario final a la hora de navegar por internet o sistemas locales.

Actualmente es una sola red que maneja varios tipos de trafico como la Voz, video y Datos. Es necesario dar prioridad al trafico critico del negocio, ya que cuando hay congestión se interrumpe el trafico y esto puede afectar significativamente la red, la transmisión y recopilación de datos. Por ello el Qos se encarga de darle prioridad al tráfico más “valioso” un ejemplo si es un negocio de video juegos el QoS le estará dando máxima importancia al trafico de video y menos prioridad a la voz o datos.

Uno de los aspectos fundamentales de la QoS son la clasificación, como anteriormente se comenta, es necesario identificar el tráfico de la red para poder brindar una buena calidad de servicio. Tres componentes clave de la implementación de la QoS son, crear mapas de clase / políticas y aplicar las políticas creadas.



Seguridad:

Debido a la rápida expansión de los sectores de comunicación que no eran atendidas por las redes de datos tradicionales se aumentó la necesidad de incorporar seguridad en la arquitectura de red. Gracias a esto se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

Una manera de proteger la red es mediante ACL (listas de acceso), firewall, entre otros, son configuraciones, sistemas o equipos que permiten controlar el tráfico a través de la encriptación de datos protegiendo de esta manera la información y la red.



ACTIVIDAD

REDES CONFIABLES

KRHISTEN PINO JIMENEZ

GESTION DE REDES DE DATOS

CODIGO: 2620641

Que es una red confiable: Pues una red confiable se basa en una arquitectura bien diseñada y escalable, que garantiza la tolerancia a fallas y proporciona una calidad de servicio óptima. Además, se implementan medidas de seguridad adecuadas para proteger la red y la información que se transmite a través de ella.

Arquitectura de la Red: Se refiere al diseño y estructura de la red. Una arquitectura bien planificada y diseñada garantiza un flujo eficiente de datos, minimiza los puntos de falla y permite la implementación de medidas de seguridad adecuadas.

Tolerancia a fallas: Una red confiable debe ser capaz de hacer frente a fallas o interrupciones sin afectar significativamente la disponibilidad y la continuidad del servicio

Escalabilidad: Una red confiable debe ser escalable, lo que significa que debe poder crecer y adaptarse a medida que aumentan las necesidades de conectividad y capacidad

Calidad de Servicio (QoS): La calidad de servicio se refiere a la capacidad de la red para garantizar un rendimiento y una experiencia satisfactorios a los usuarios.

Seguridad de la Red: La seguridad es un aspecto esencial de una red confiable. Esto incluye la implementación de medidas de seguridad, como firewalls, sistemas de detección y prevención de intrusiones, encriptación de datos y autenticación de usuarios.

Ejemplos de cada punto

Arquitectura de la Red: Un ejemplo de una buena arquitectura de red es la implementación de una topología en estrella con un conmutador central que conecta todos los dispositivos. Esta estructura permite una fácil administración y resolución de problemas, ya que cada dispositivo se conecta directamente al conmutador central.

Tolerancia a fallas: Supongamos que una empresa tiene dos enlaces de Internet de proveedores diferentes para garantizar la redundancia y la tolerancia a fallas. Si uno de los enlaces falla, el tráfico de la red se desvía automáticamente al enlace de respaldo, asegurando que la conectividad a Internet se mantenga sin interrupciones.

Escalabilidad: Una red confiable debe ser escalable para adaptarse al crecimiento. Por ejemplo, una empresa que experimenta un aumento en el número de empleados puede agregar fácilmente nuevos puntos de acceso Wi-Fi a su red inalámbrica existente sin afectar negativamente el rendimiento o la seguridad.

Calidad de Servicio (QoS): En una red confiable, se puede implementar QoS para priorizar el tráfico en función de su importancia. Por ejemplo, en una red de voz sobre IP (VoIP), se puede asignar una mayor prioridad al tráfico de voz para garantizar una comunicación clara y sin interrupciones, incluso cuando la red está experimentando una alta carga de datos.

Seguridad de la Red: Un ejemplo de seguridad de red es la implementación de un firewall para proteger la red de amenazas externas. El firewall puede configurarse para permitir solo ciertos tipos de tráfico y bloquear los intentos de acceso no autorizados a la red. También puede realizar inspección profunda de paquetes para identificar y bloquear actividades sospechosas o maliciosas.

Práctica de laboratorio: Configuración de EtherChannel

Presentado por: Andres Orozco

Topología

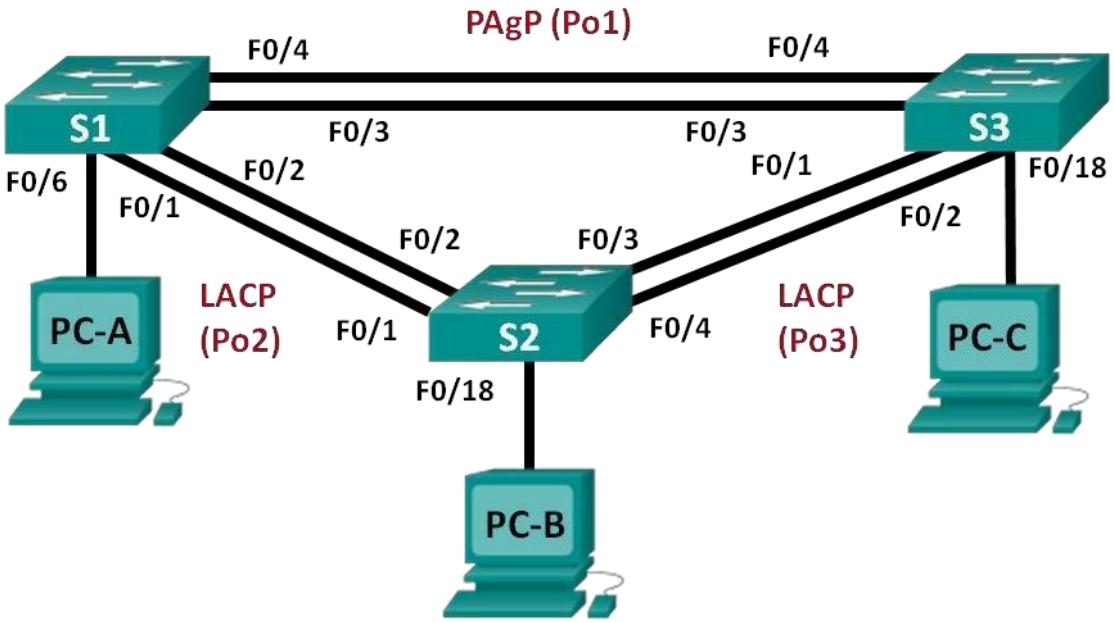
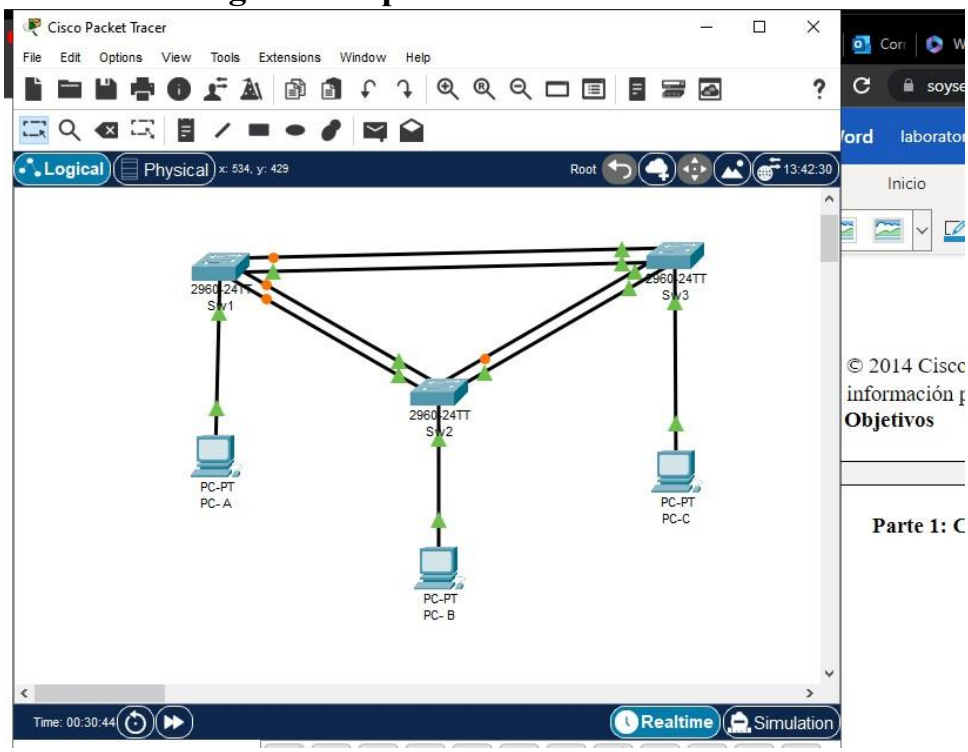


Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco. **Objetivos**

Parte 1: Configurar los parámetros básicos del switch



Parte 2: configurar PAgP

Parte 3: configurar LACP

Información básica/situación

La agregación de enlaces permite la creación de enlaces lógicos que se componen de dos o más enlaces físicos. Esto proporciona un mayor rendimiento más allá del uso de un único enlace físico. Si uno de los enlaces falla, la agregación de enlaces también proporciona redundancia.

En esta práctica de laboratorio, configurará EtherChannel, una forma de agregación de enlaces que se utiliza en las redes conmutadas. Configurará EtherChannel mediante el protocolo de agregación de puertos (PAgP) y el protocolo de control de agregación de enlaces (LACP).

Nota: PAgP es un protocolo exclusivo de Cisco que solo se puede ejecutar en switches Cisco y en switches que sean de proveedores con licencia para admitir PAgP. LACP es un protocolo de agregación de enlaces definido en IEEE 802.3ad y no se asocia a ningún proveedor específico.

LACP permite que los switches Cisco administren los canales Ethernet entre los switches que cumplen con el protocolo 802.3ad. Puede configurar hasta 16 puertos para formar un canal. Ocho de los puertos están en modo activo y los otros ocho están en modo de espera. Cuando falla alguno de los puertos activos, se activa un puerto en espera. El modo de espera funciona solo para LACP, no para PAgP.

Nota: los switches que se utilizan en las prácticas de laboratorio de CCNA son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio.

Nota: asegúrese de que los switches se hayan borrado y que no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 3 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: Configurar los parámetros básicos del switch

En la parte 1, configurará la topología de la red y los parámetros básicos, como direcciones IP de la interfaz, el acceso a dispositivos y contraseñas.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos que se muestran en el diagrama de la topología y realice el cableado según sea necesario.

Paso 2: inicializar y volver a cargar los switches.

Paso 3: Configure los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo como se muestra en la topología.

c. Cifre las contraseñas de texto no cifrado.

d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

f. Asigne **cisco** como la contraseña de vty y de la consola, y habilite el inicio de sesión.

g. Configure logging synchronous para evitar que un mensaje de consola interrumpa la entrada de comandos.

h. Desactive todos los puertos del switch, excepto los puertos conectados a computadoras.

i. Configure la VLAN 99 y asígnele el nombre **Management**.

j. Configure la VLAN 10 y asígnele el nombre **Staff**.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

k. Configure los puertos del switch con hosts conectados como puertos de acceso en la VLAN 10.

l. Asigne el direccionamiento IP según la tabla de direccionamiento.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

m. Copie la configuración en ejecución en la configuración de inicio.

Paso 4: Configurar las PC. Asigne direcciones IP a las computadoras según la tabla de direccionamiento.

Parte 2: Configurar PAgP

PAgP es un protocolo exclusivo de Cisco para la agregación de enlaces. En la parte 2, se configurará un enlace entre el S1 y el S3 mediante PAgP.

Paso 1: Configurar PAgP en el S1 y el S3.

Para establecer un enlace entre el S1 y el S3, configure los puertos en el S1 con modo deseado de PAgP y los puertos en el S3 con modo automático de PAgP. Habilite los puertos después de que se configuren los modos PAgP.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown

S3(config)# interface range f0/3-4
S3(config-if-range)# channel-group 1 mode auto
Creating a port-channel interface Port-channel 1

S3(config-if-range)# no shutdown
*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
S3(config-if-range)#
*Mar 1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

*Mar 1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up S3(config-if-range)#

*Mar 1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

*Mar 1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Portchannel1, changed state to up

*Mar 1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Paso 2: Examinar la configuración en los puertos.

Actualmente, las interfaces F0/3, F0/4 y Po1 (canal de puertos 1) en el S1 y el S3 están en modo operativo de acceso con el modo administrativo en dinámico automático. Verifique la configuración mediante los comandos **show run interface** *id-interfaz* y **show interfaces** *id-interfaz* **switchport**, respectivamente. Los resultados de configuración de ejemplo para F0/3 en el S1 son los siguientes: S1# **show run interface f0/3**

Building configuration...

Current configuration : 103

bytes ! interface

FastEthernet0/3 channel-group

1 mode desirable

S1# **show interfaces f0/3 switchport**

Name: Fa0/3

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access (member of bundle Po1)

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Paso 3: Verificar que se hayan agregado los puertos.

S1# **show etherchannel summary**

Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
---- ---------- -------- -----
1 Po1(SU) PAgP Fa0/3(P) Fa0/4(P)

S3# **show etherchannel summary**

Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
---- ---------- -------- -----
1 Po1(SU) PAgP Fa0/3(P) Fa0/4(P)

¿Qué significan los indicadores SU y P en el resumen de Ethernet?

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

R//= El indicador P significa que los puertos están agrupados en un canal de puertos. el indicador S que el canal de puertos es un EtherChannel de capa 2; y el indicador U significa que el EtherChannel está en uso

Paso 4: Configurar los puertos de enlace troncal.

Una vez que se agregaron los puertos, los comandos aplicados a la interfaz de canal de puertos afectan a todos los enlaces que se agruparon. Configure manualmente los puertos Po1 en el S1 y el S3 como puertos de enlace troncal y asígnelos a la VLAN 99 nativa.

S1(config)# **interface port-channel 1** S1(config-if)# **switchport mode trunk** S1(config-if)# **switchport trunk native vlan 99**

S3(config)# **interface port-channel 1** S3(config-if)# **switchport mode trunk**

S3(config-if) # **switchport trunk native vlan 99**

Paso 5: Verificar que los puertos estén configurados como puertos de enlace troncal.

a. Emita los comandos **show run interface** *id-interfaz* en el S1 y el S3. ¿Qué comandos se indican para F0/3 y F0/4 en ambos switches? ¿Compare los resultados con la configuración en ejecución para la interfaz Po1? Registre la observación.

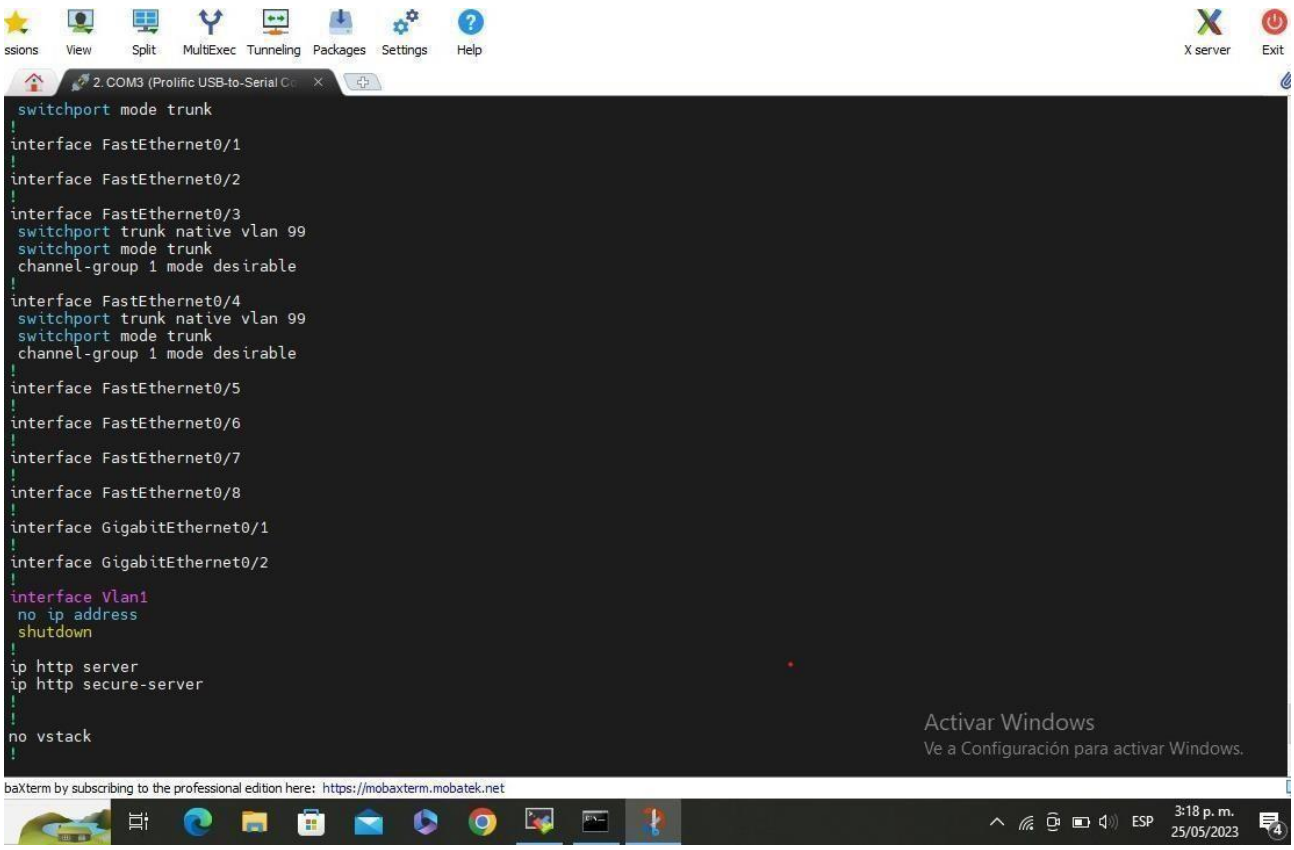
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

```
Switch#show running
Building configuration...

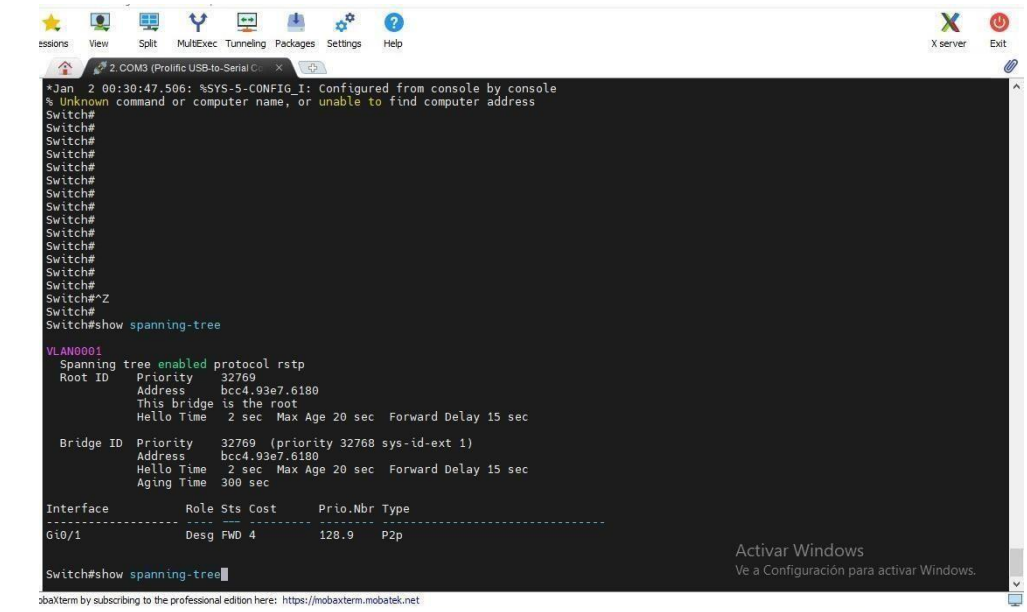
Current configuration : 1131 bytes
!
! Last configuration change at 00:43:10 UTC Mon Jan 2 2006
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
!
```

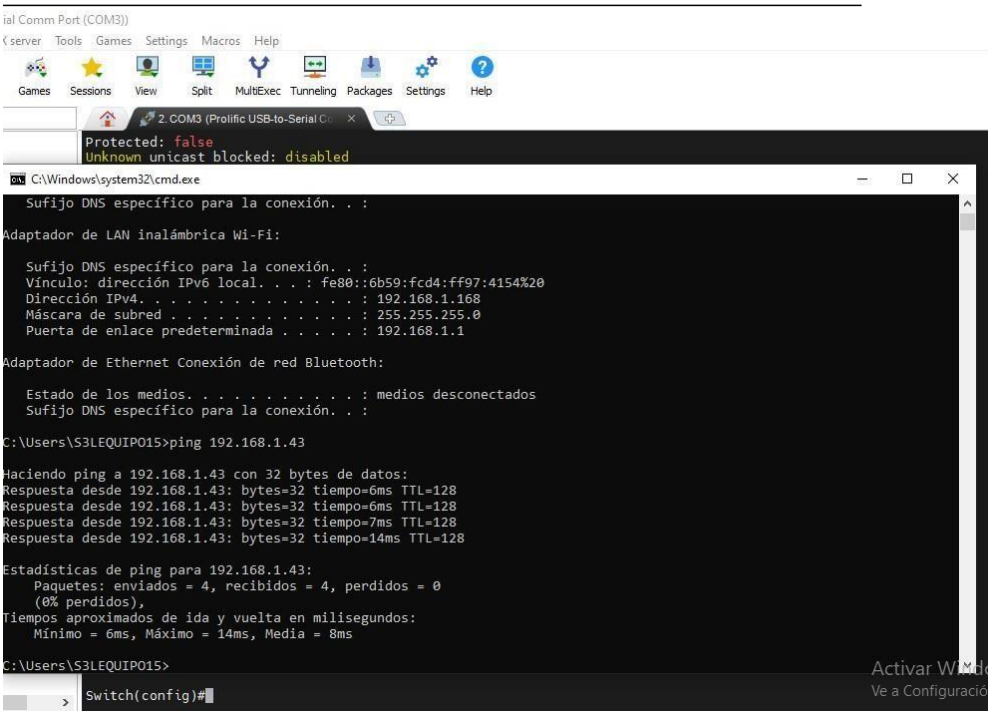
Activar Windows
Ve a Configuración para activar Windows.

b. Emita los comandos **show interfaces trunk** y **show spanning-tree** en el S1 y el S3. ¿Qué puerto de enlace troncal se indica? ¿Cuál es la VLAN nativa? ¿Cuál es la conclusión del resultado?



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

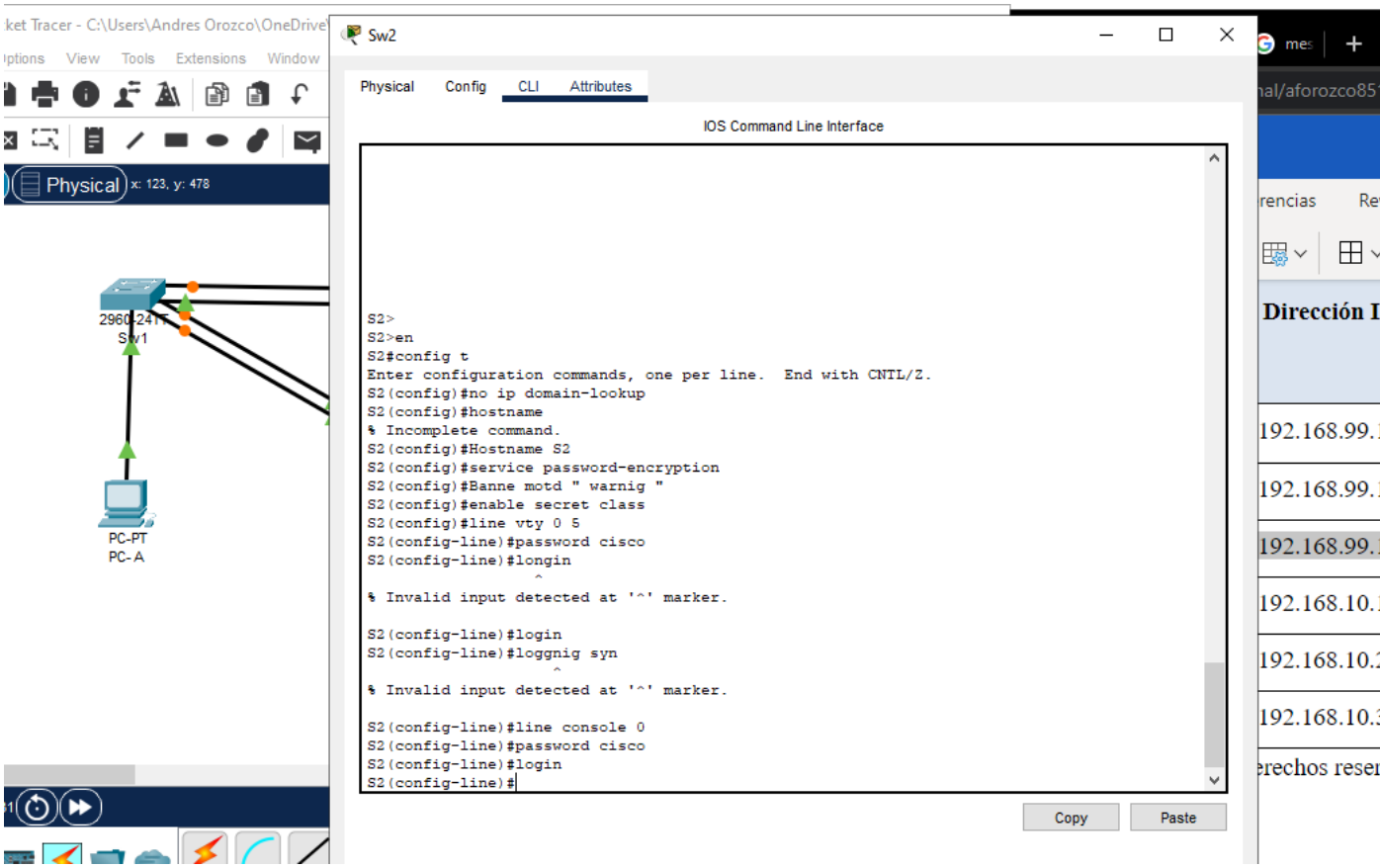




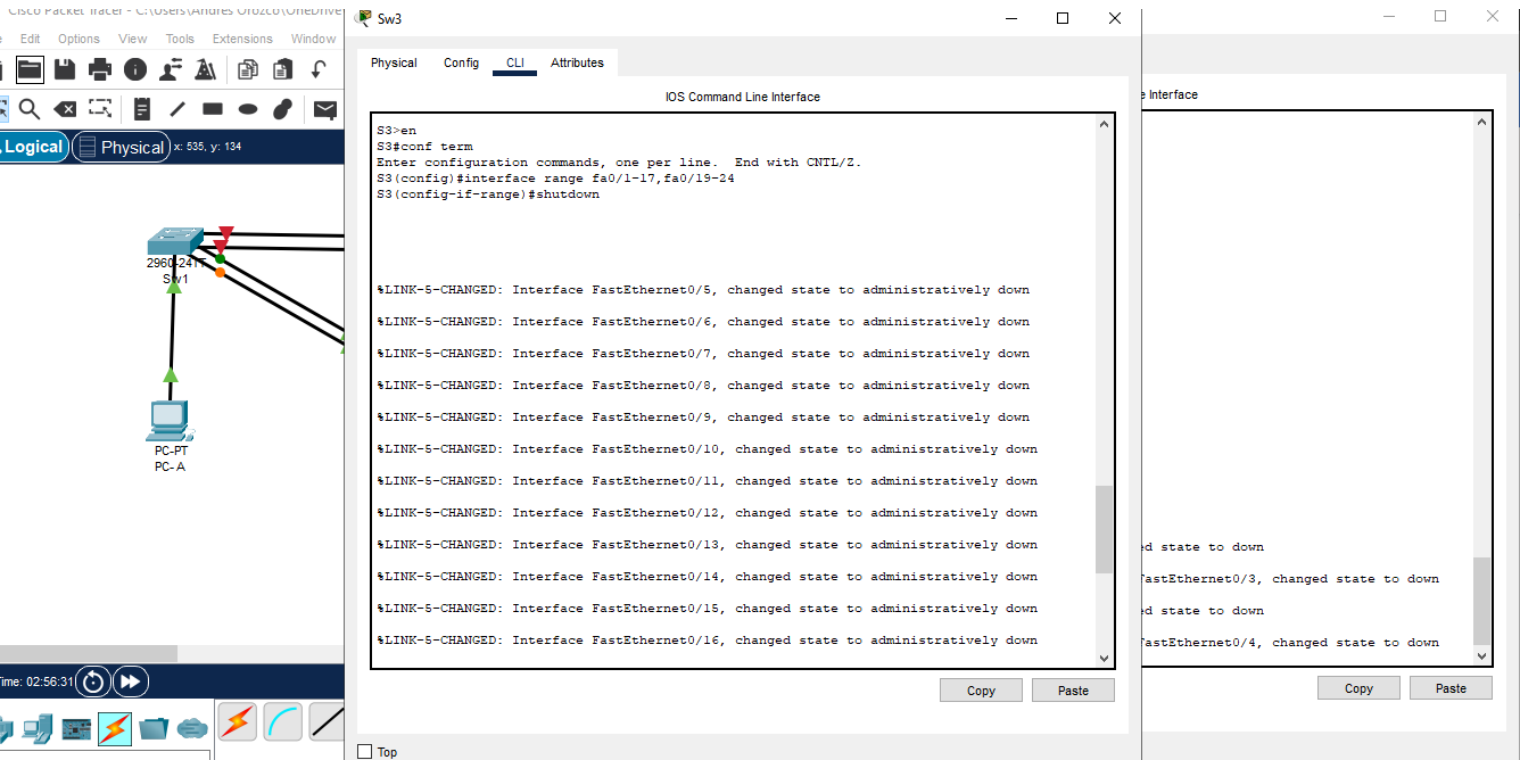
Según el resultado de **show spanning-tree**, ¿cuál es el costo y la prioridad de puerto para el enlace agregado?

Se le procura hacer un ping al PAGP de tu compañero (auto)

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

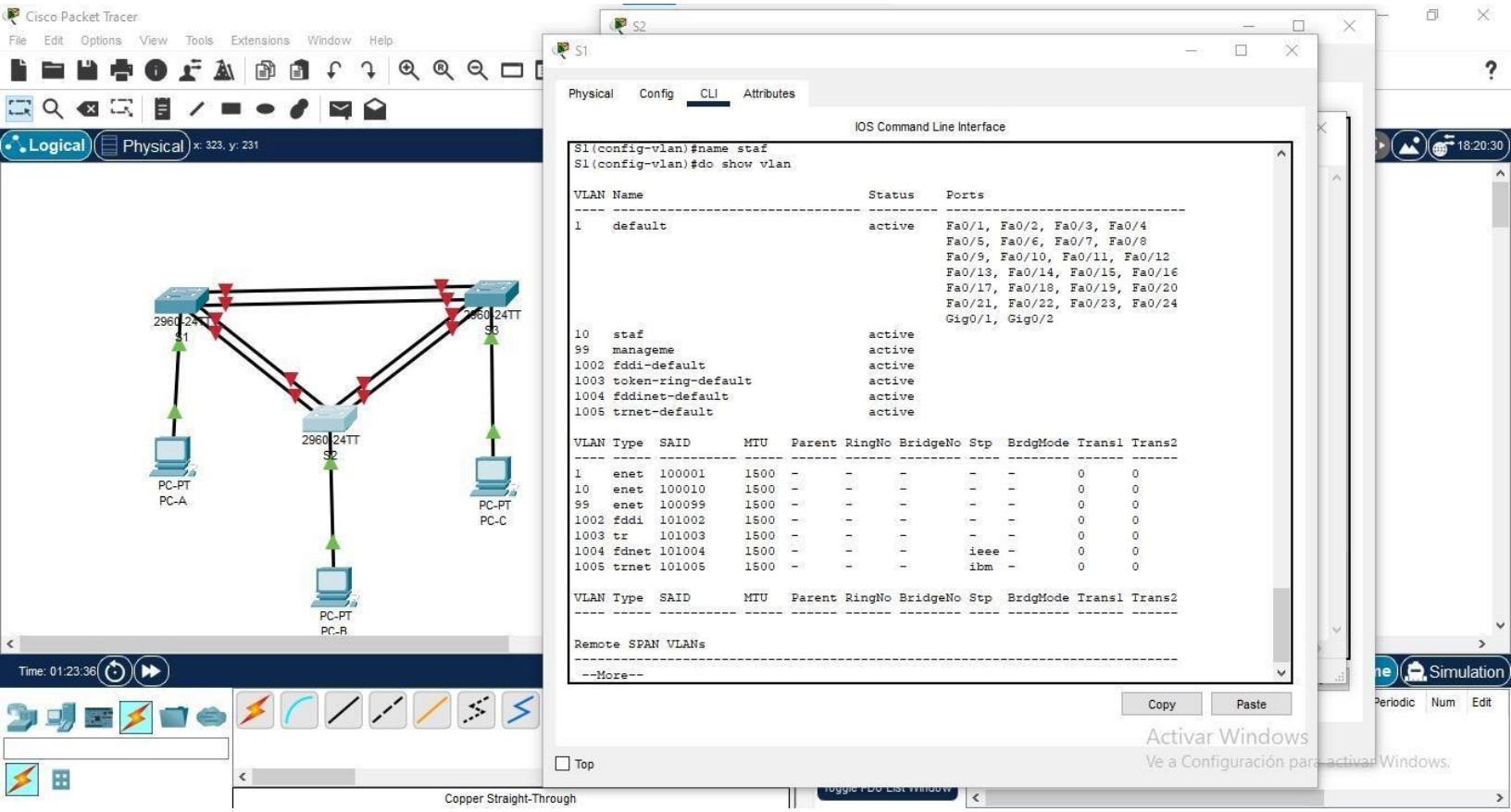


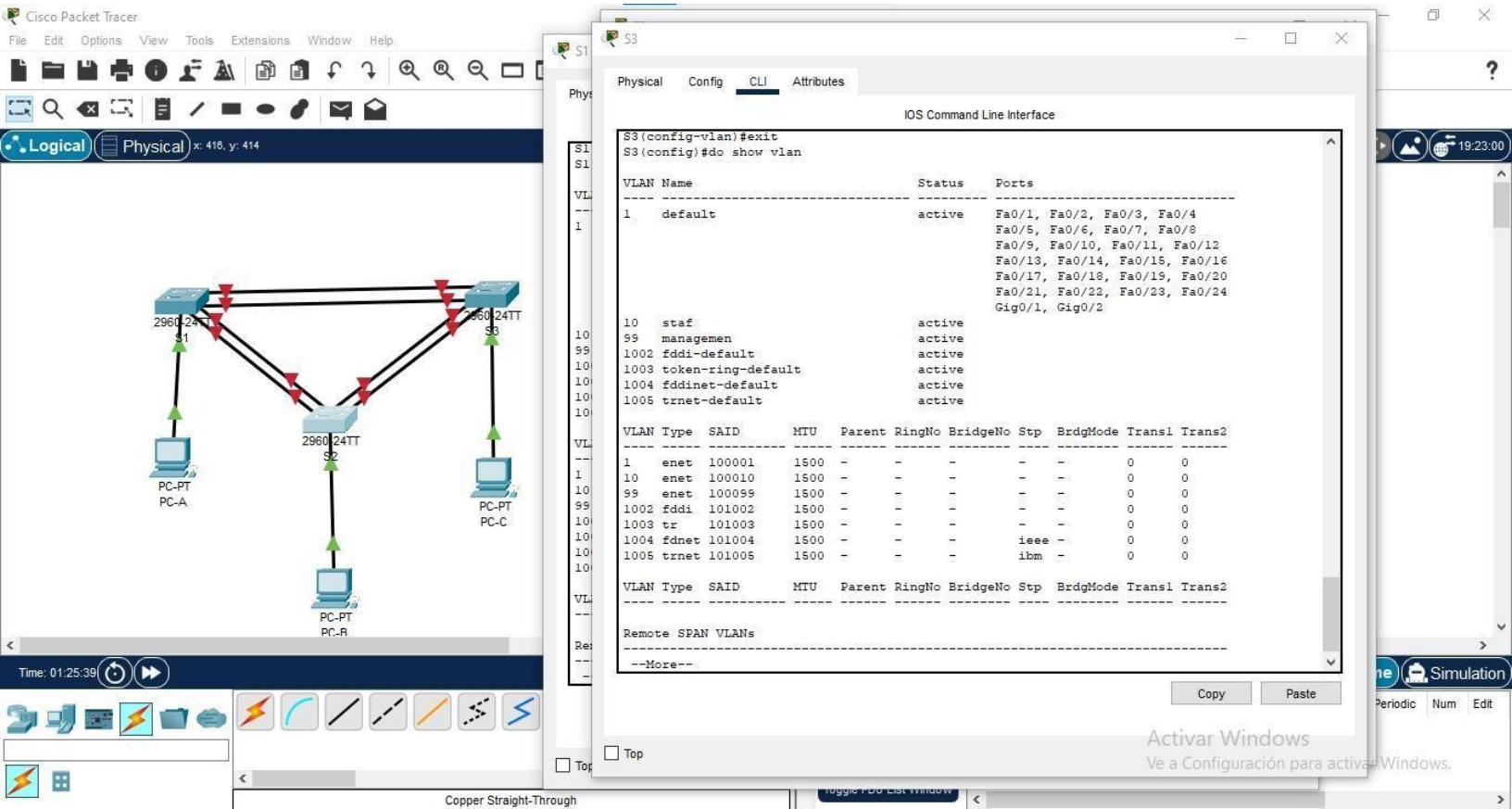
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

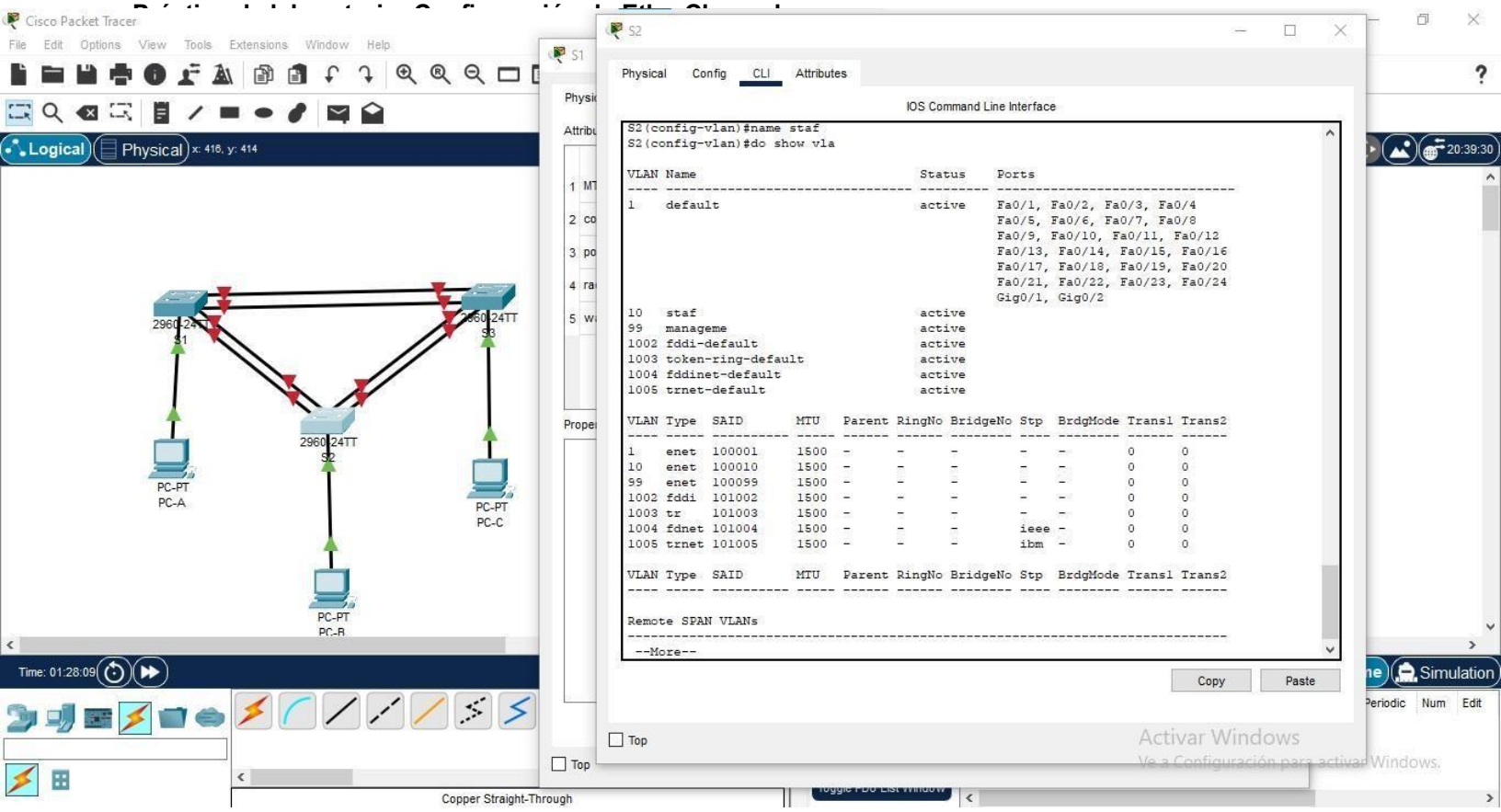


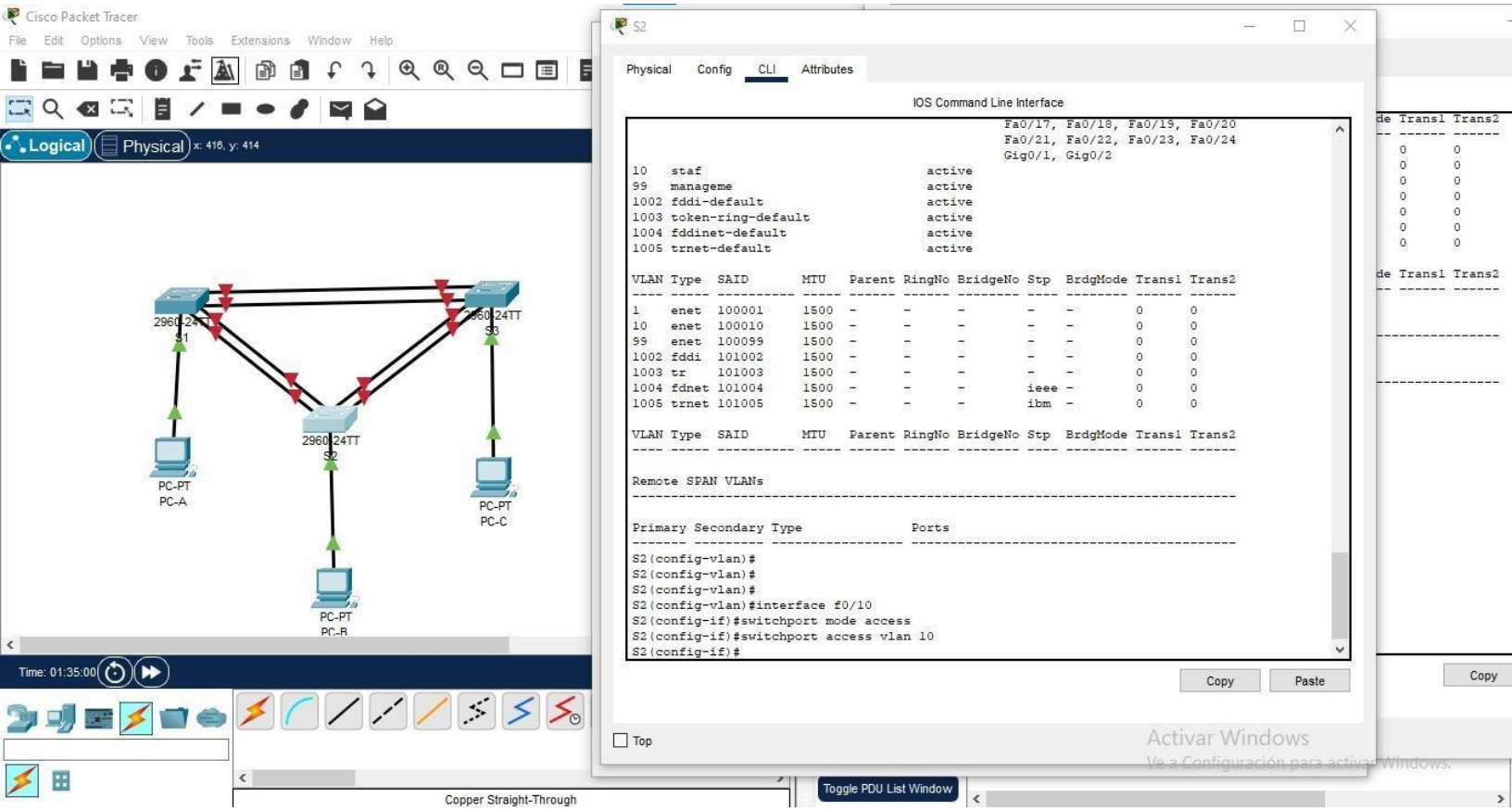
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

Práctica de laboratorio: Configuración de EtherChannel

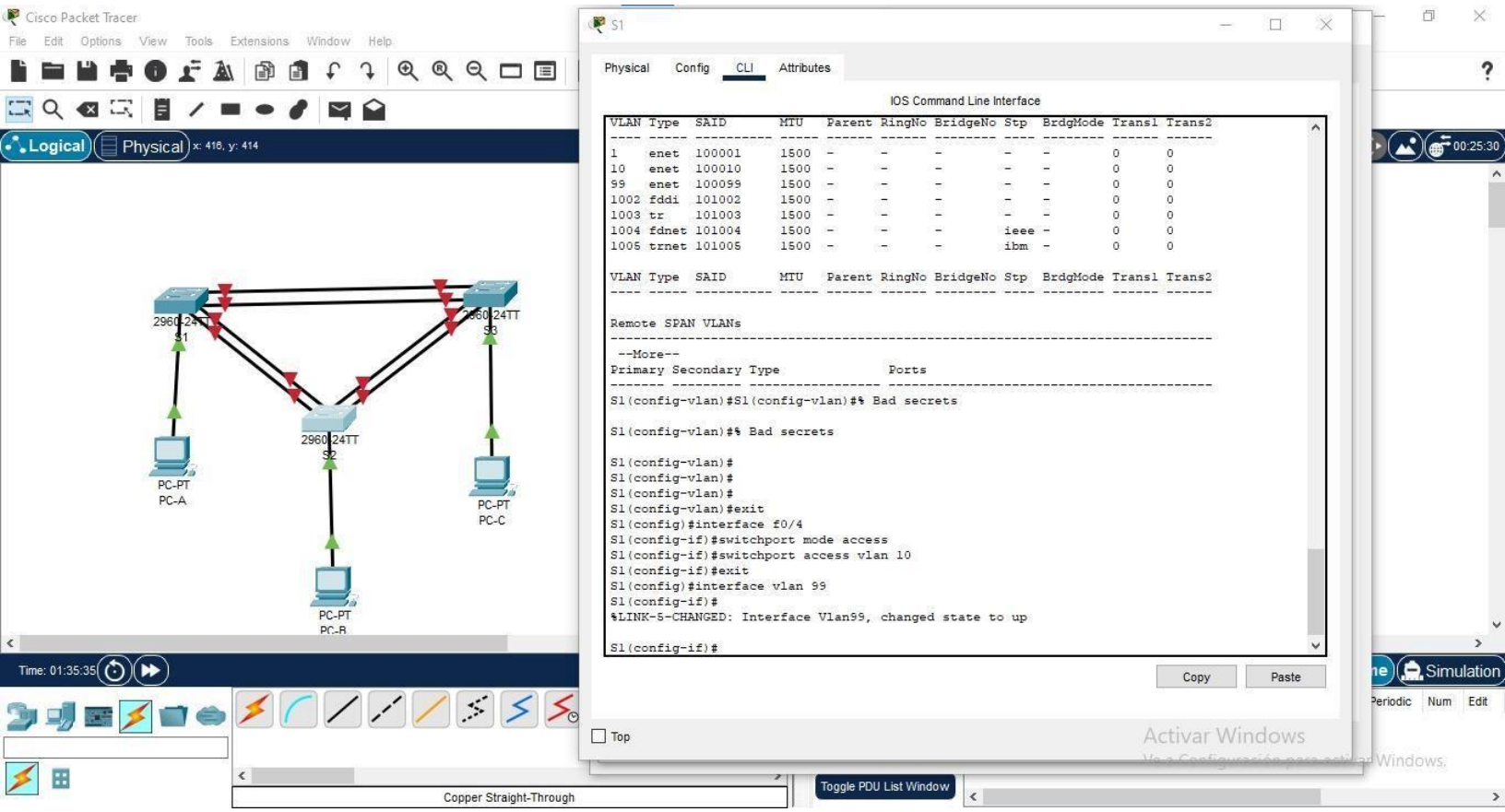


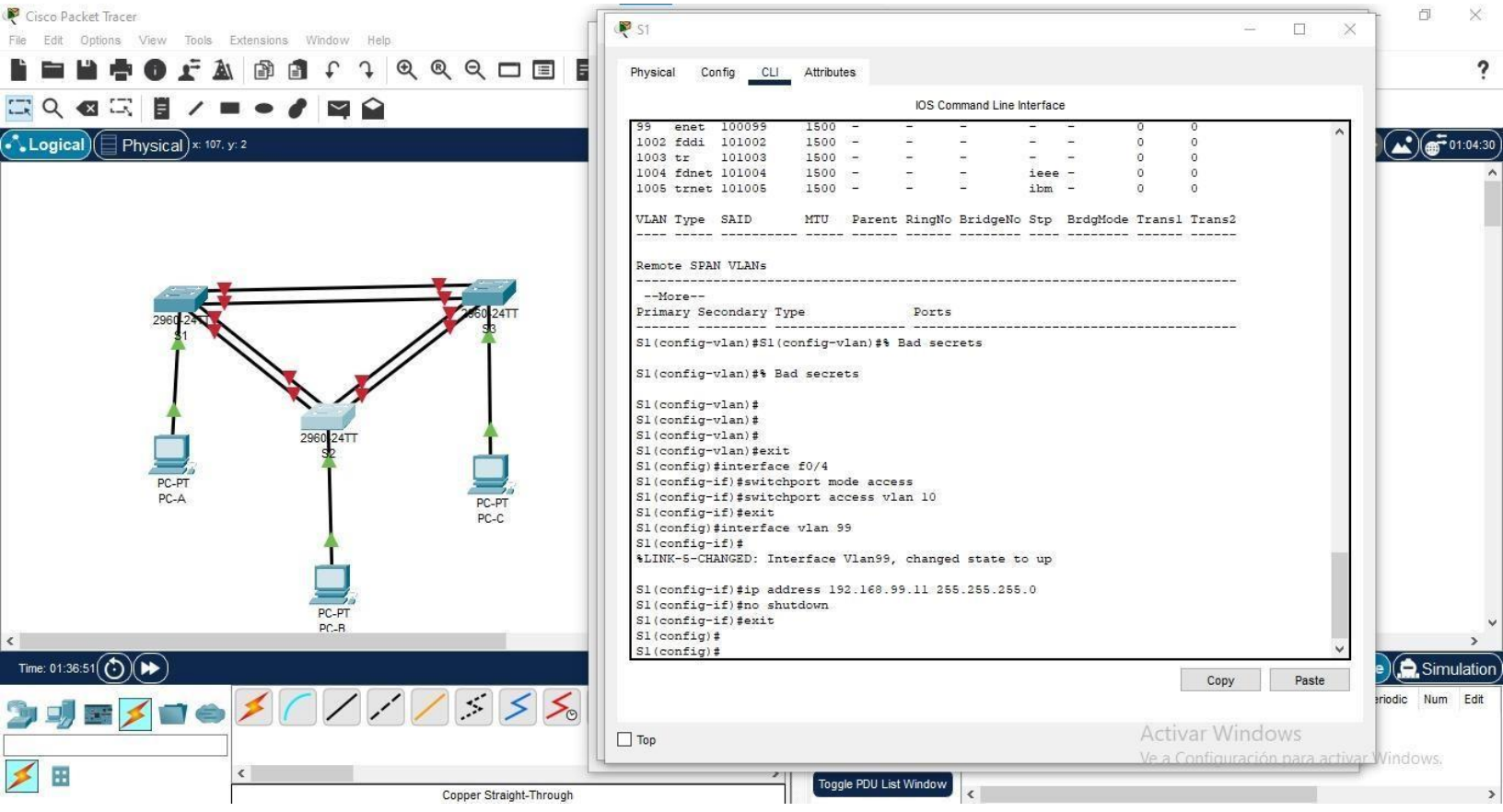




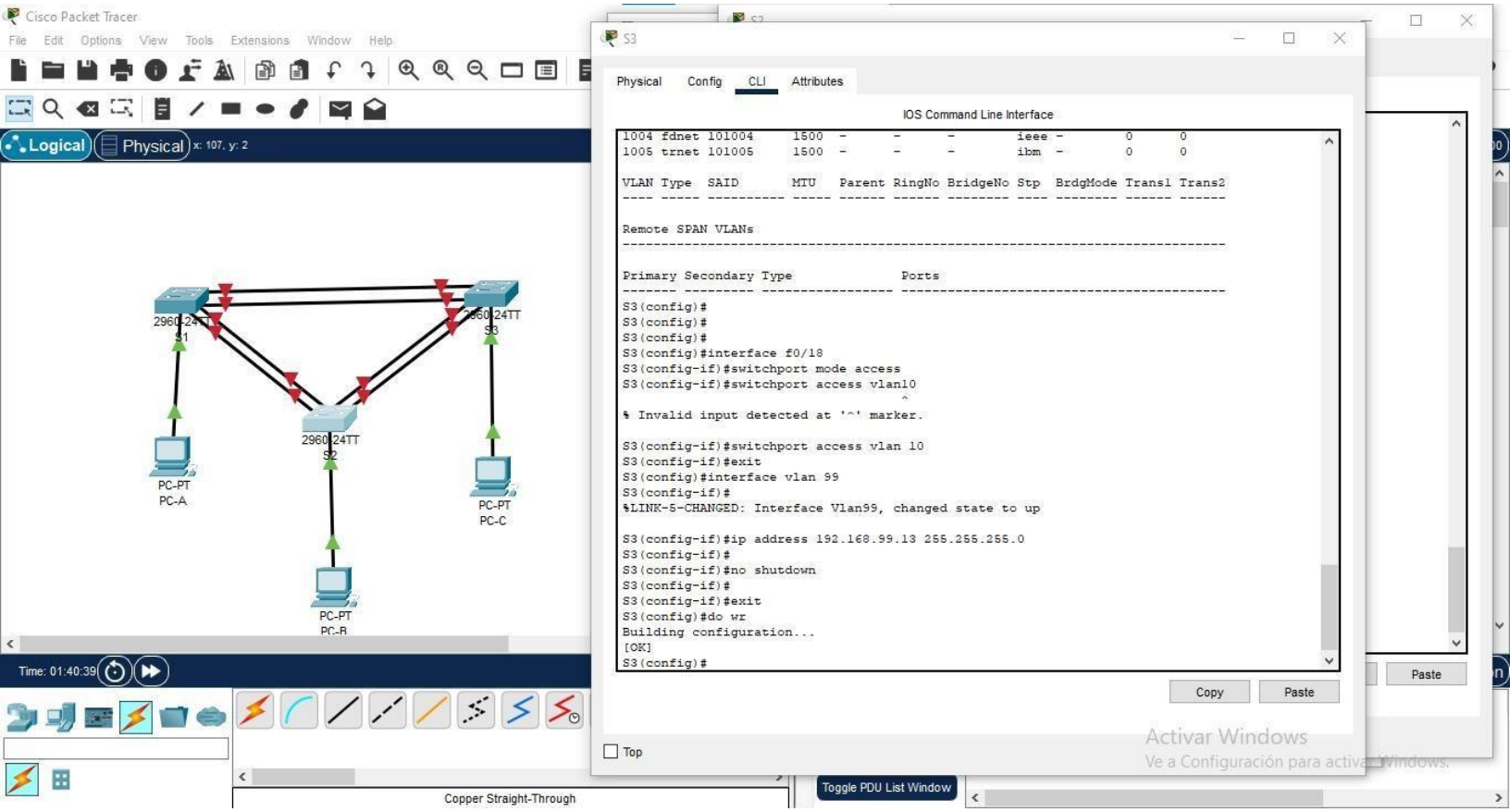


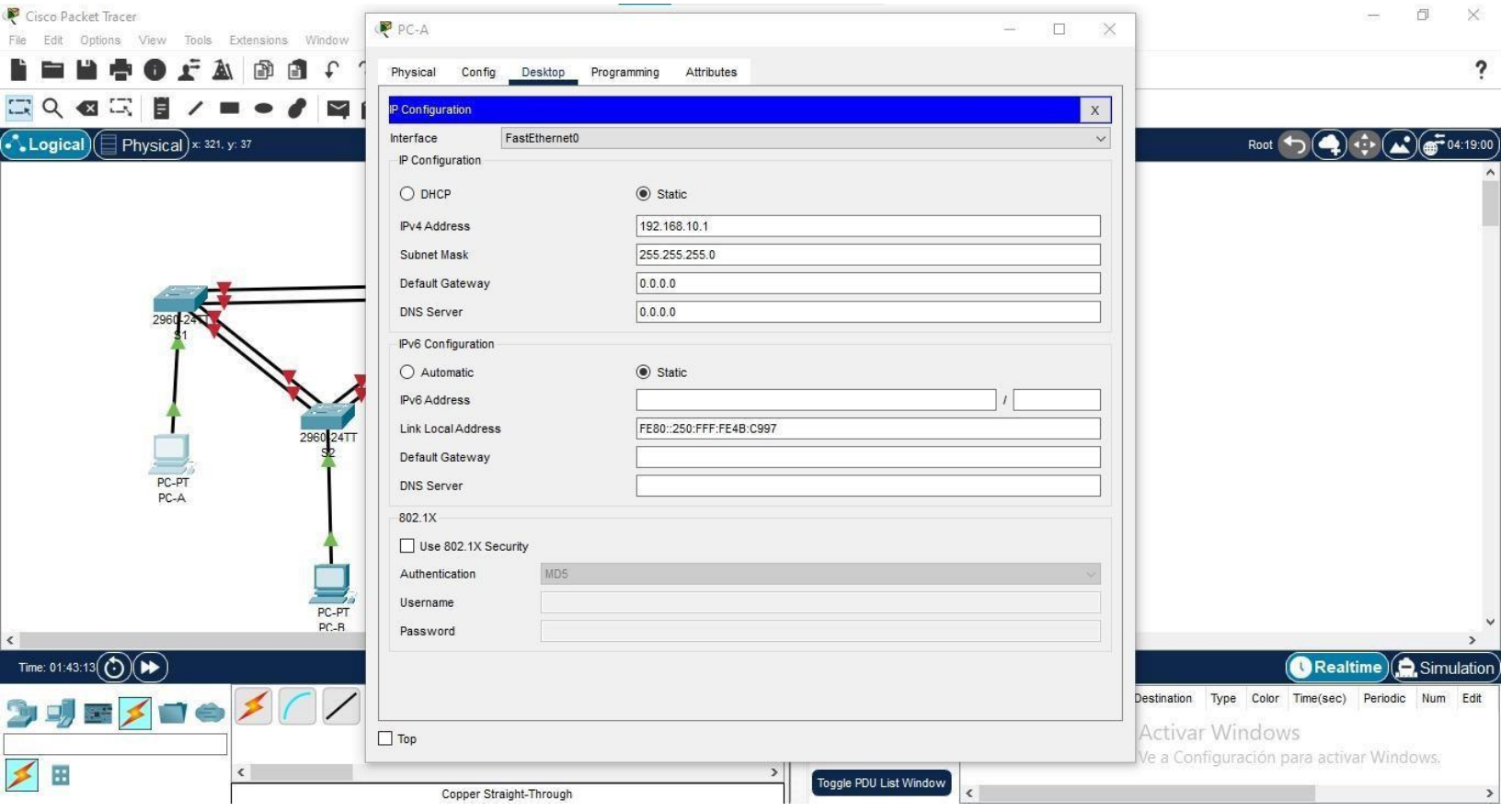
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.



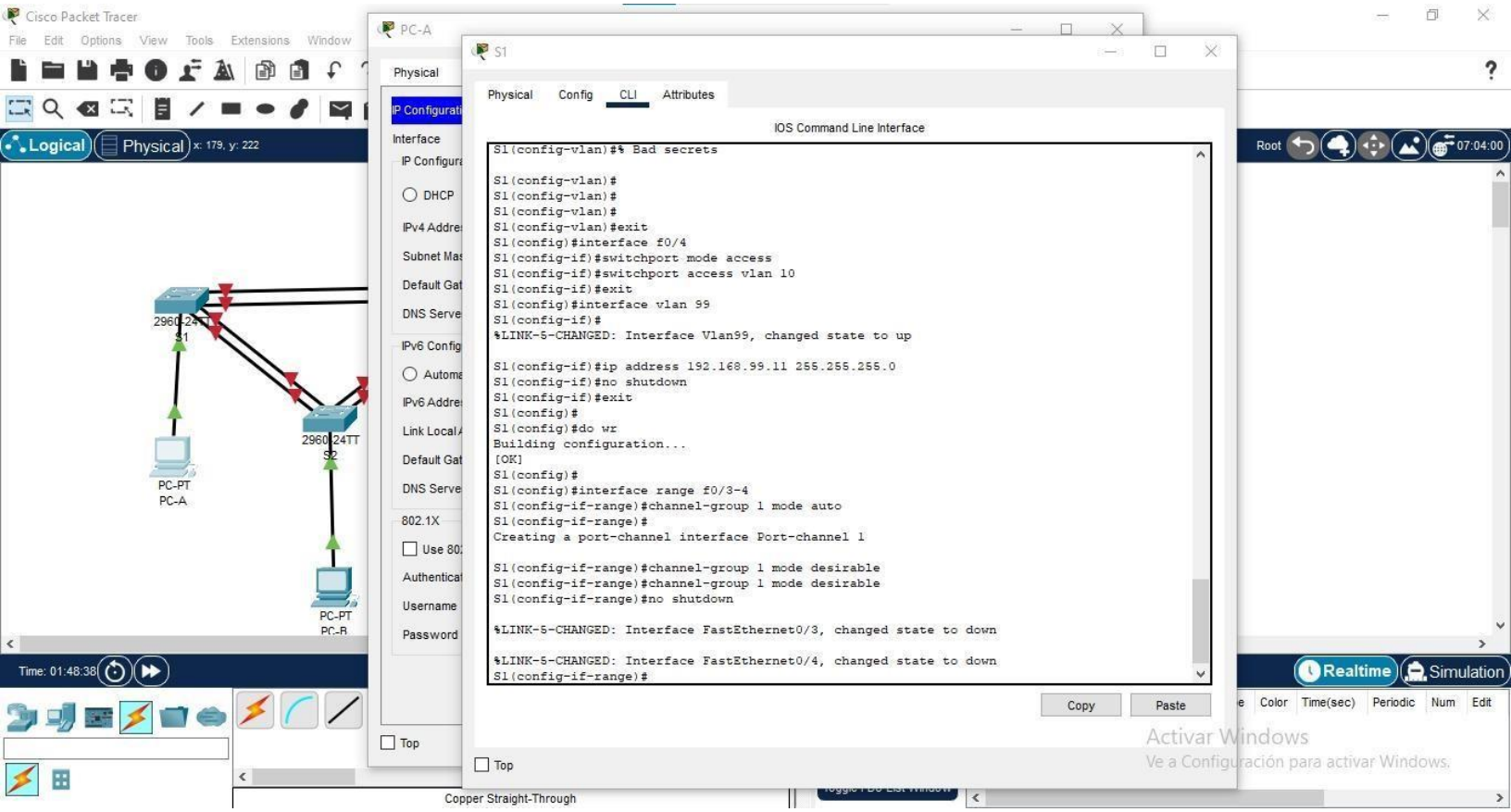


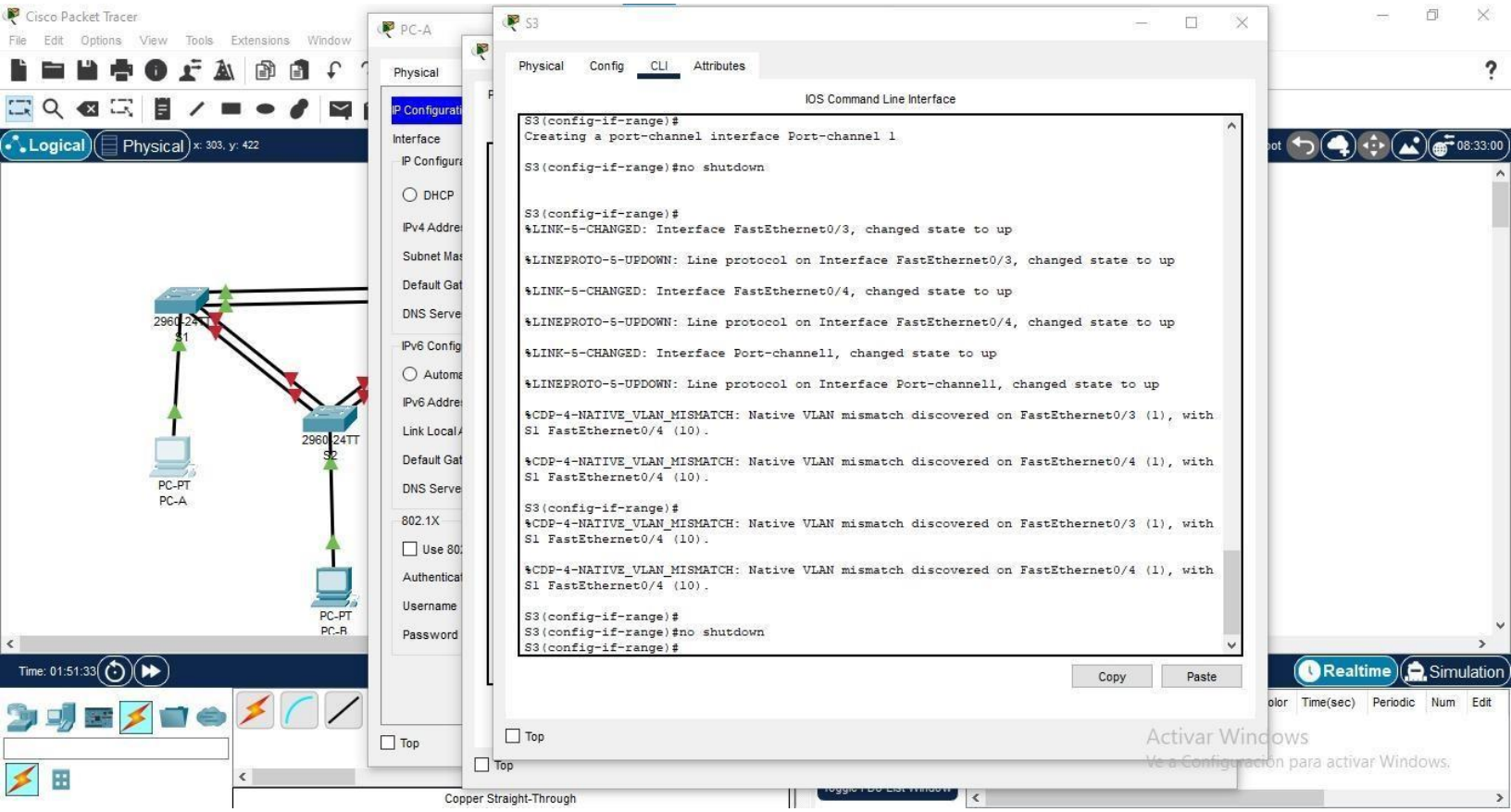
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.





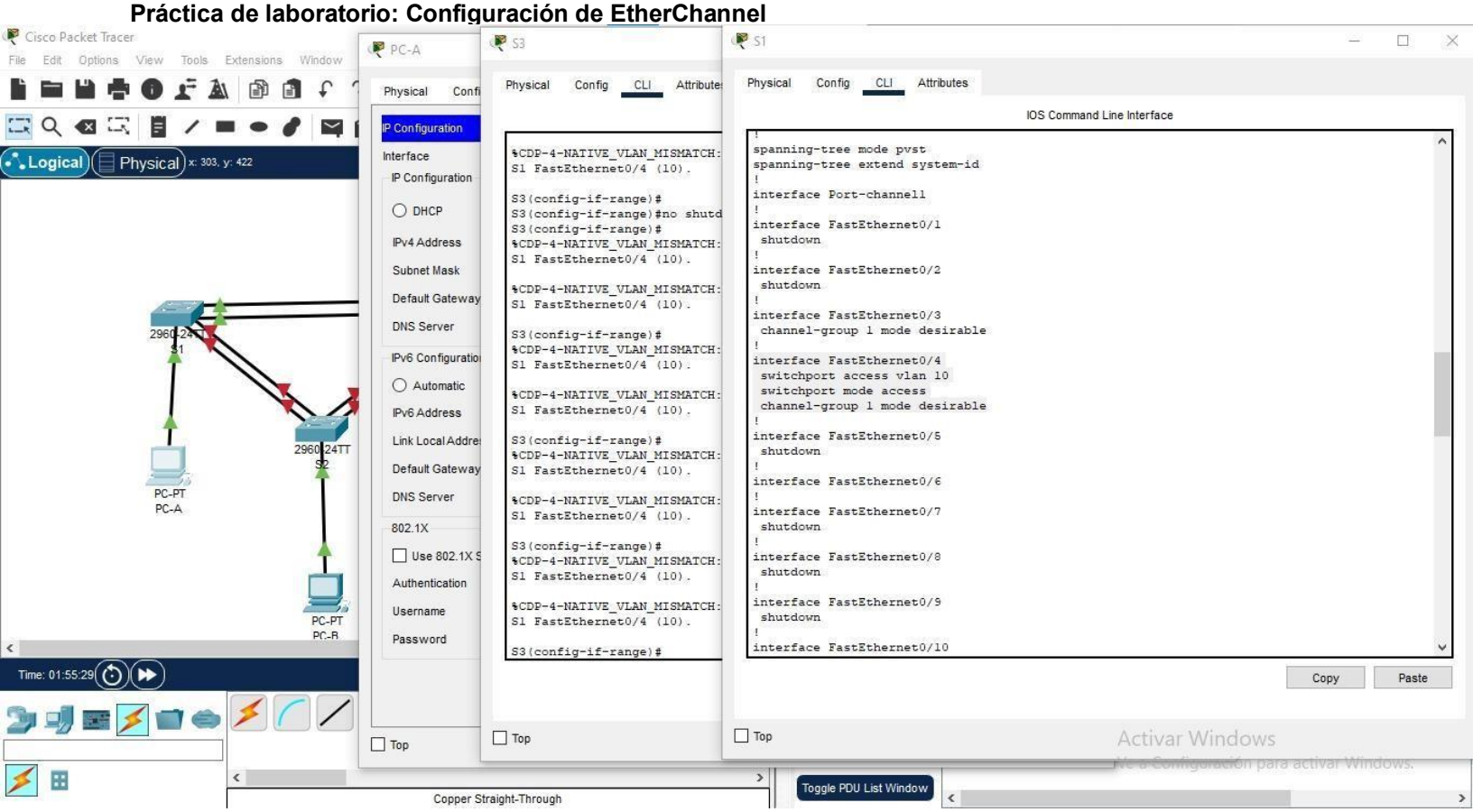
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

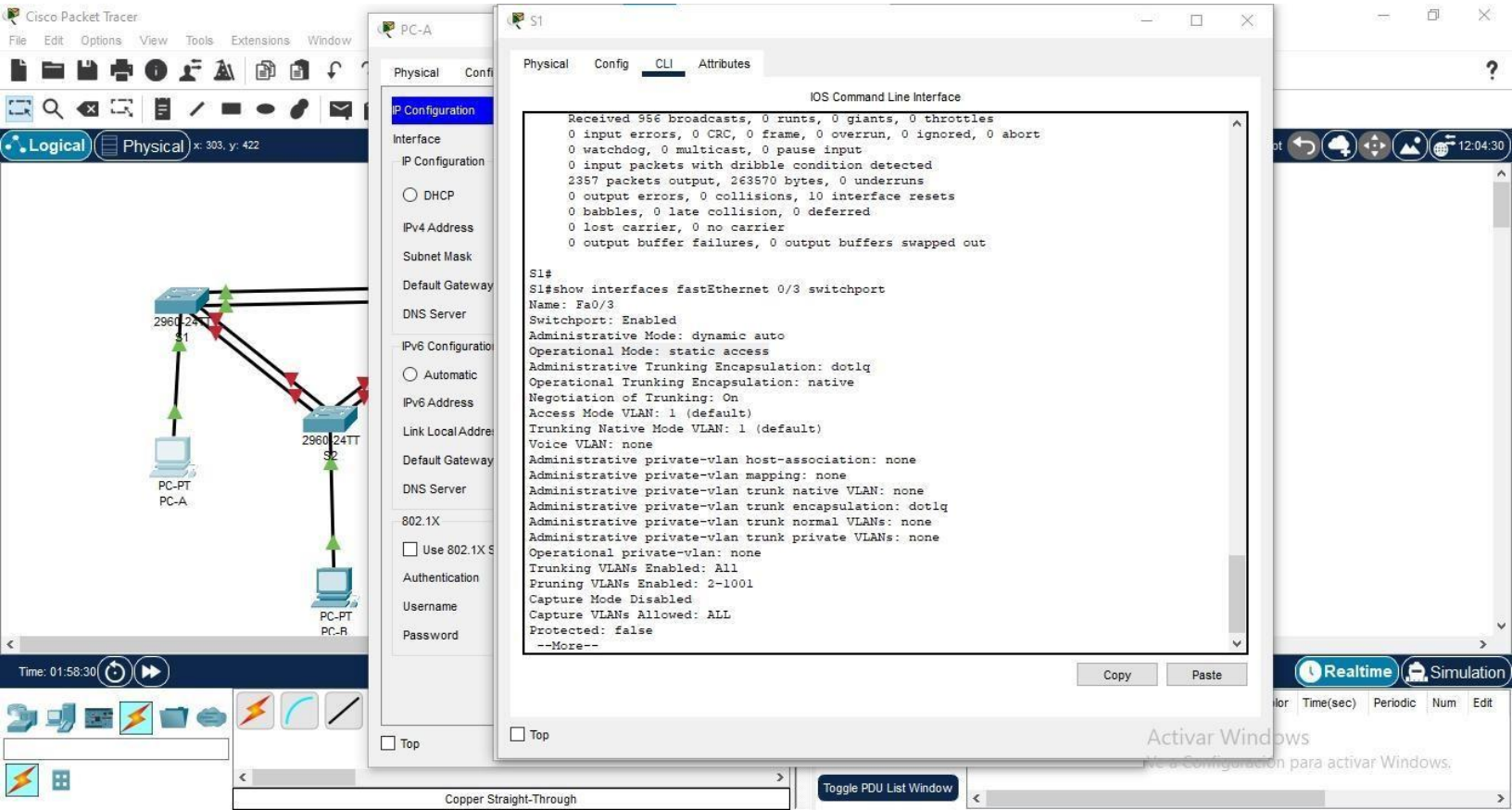




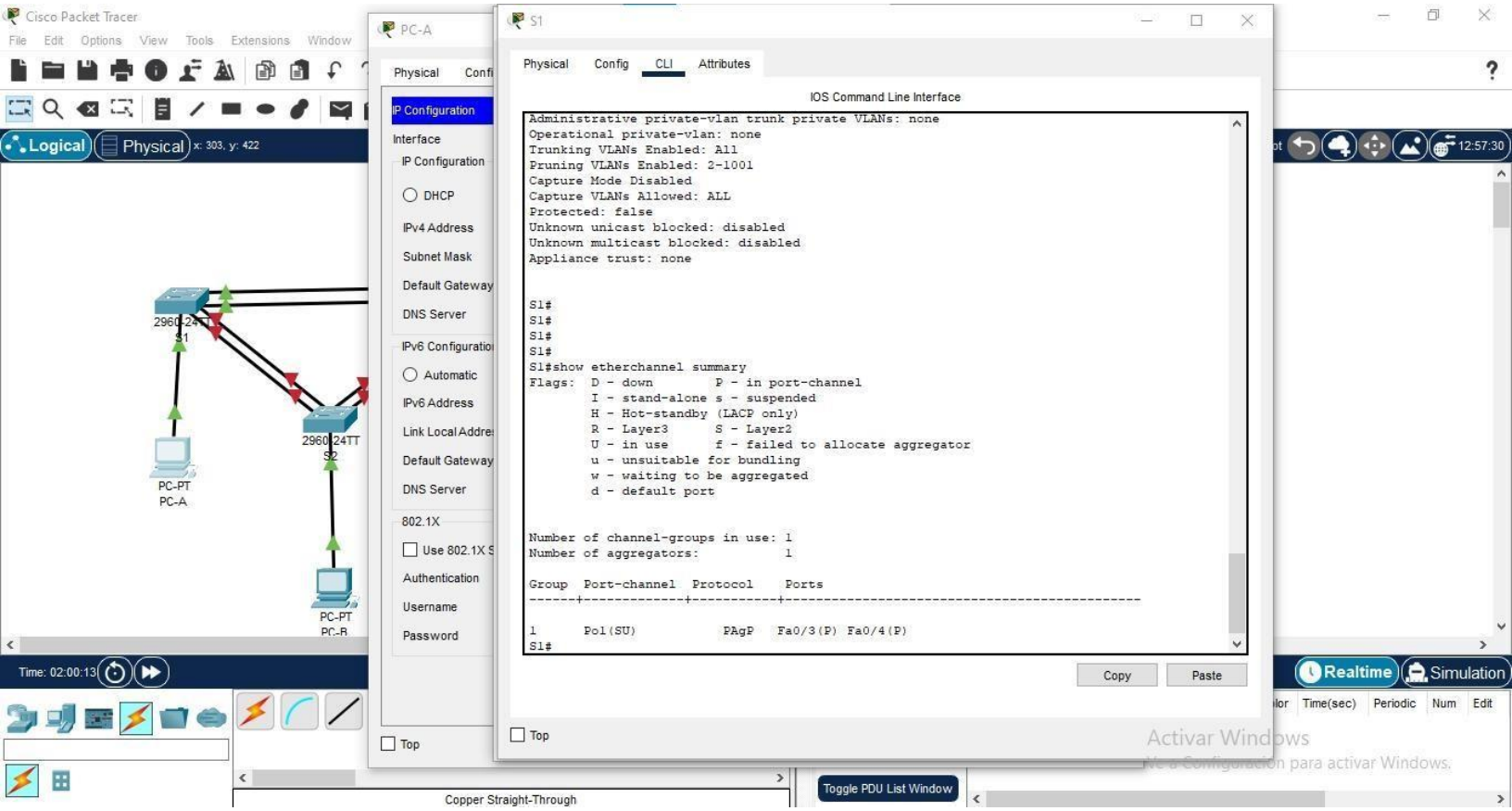
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

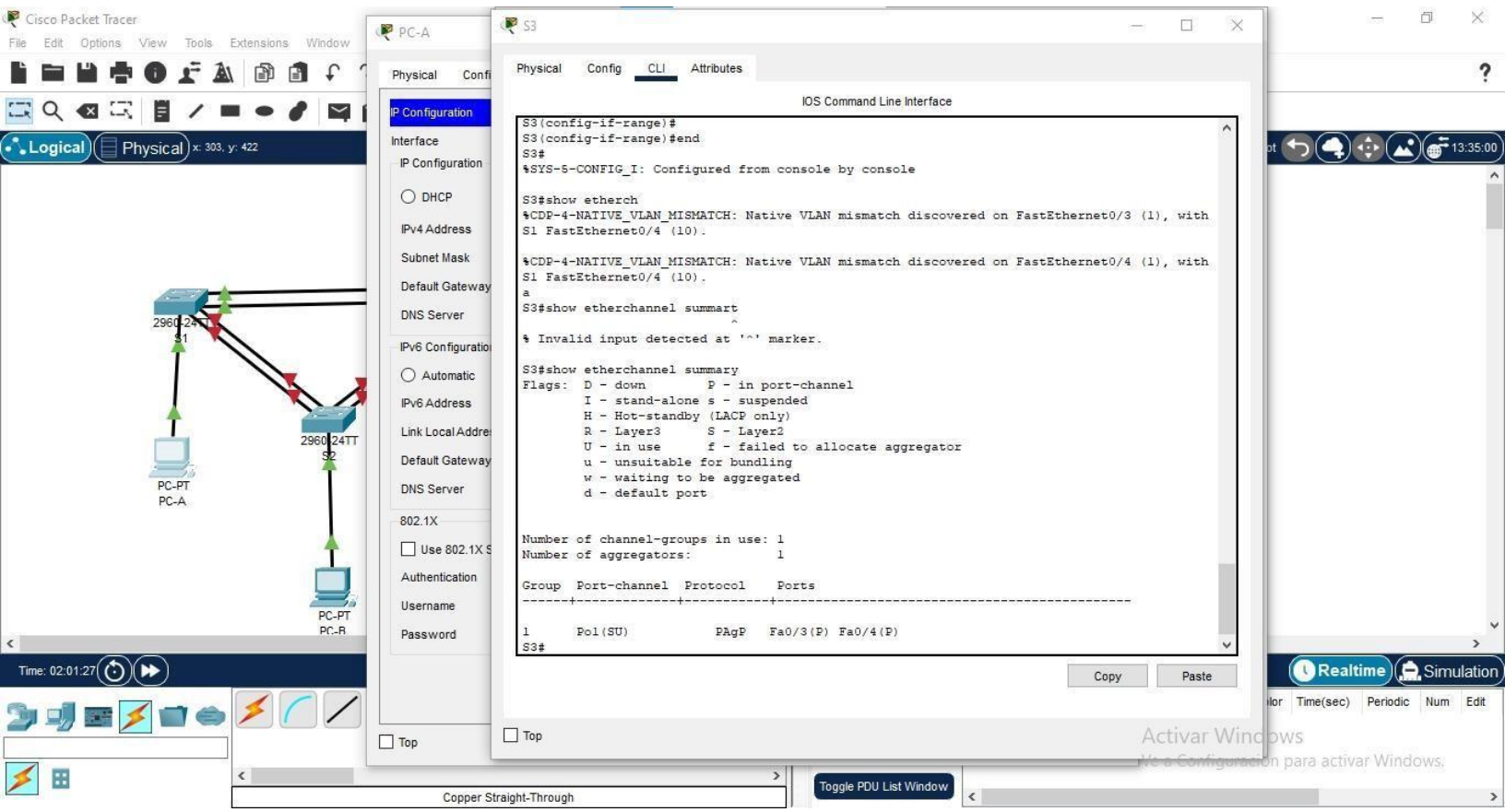
Práctica de laboratorio: Configuración de EtherChannel



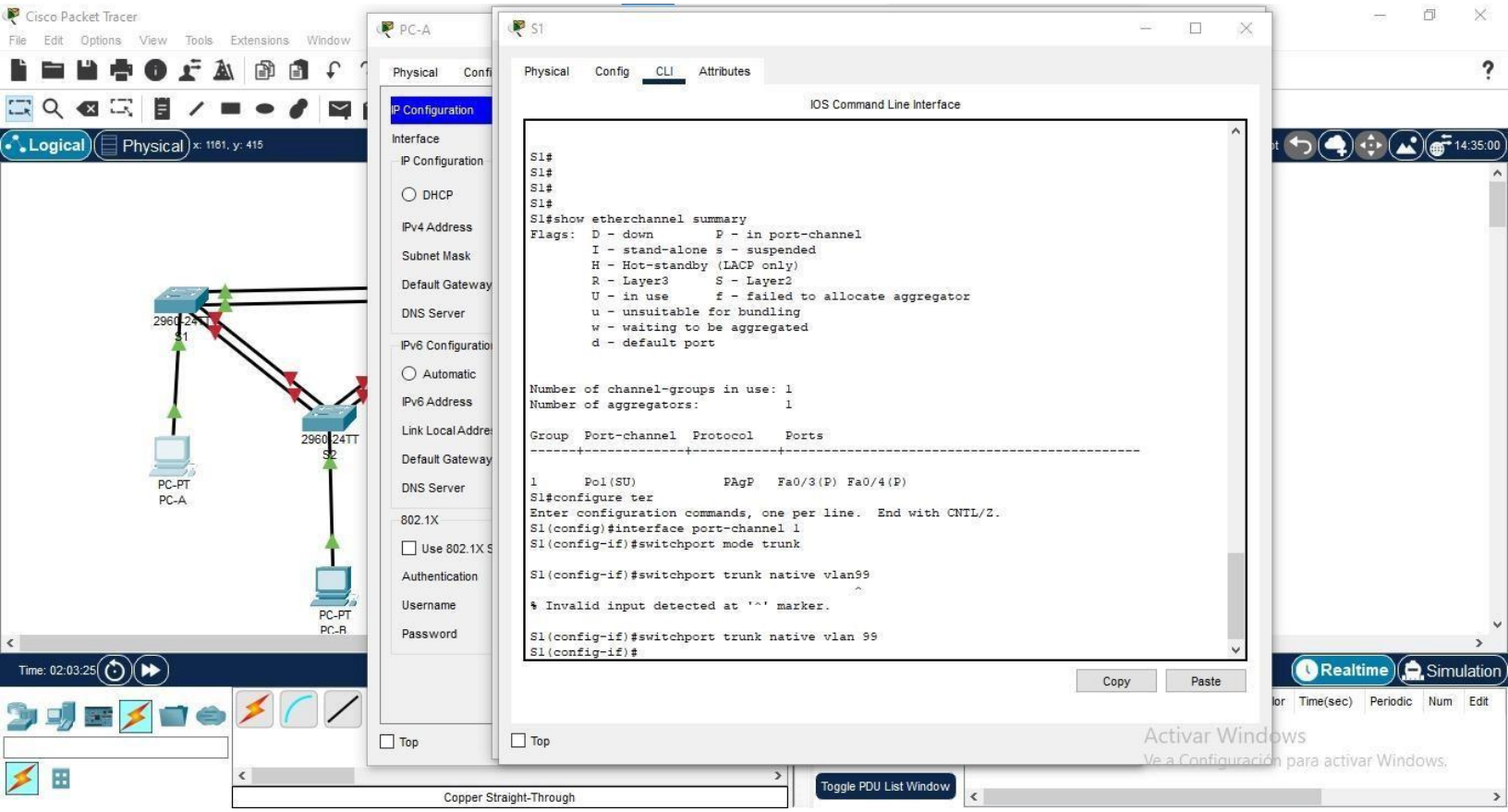


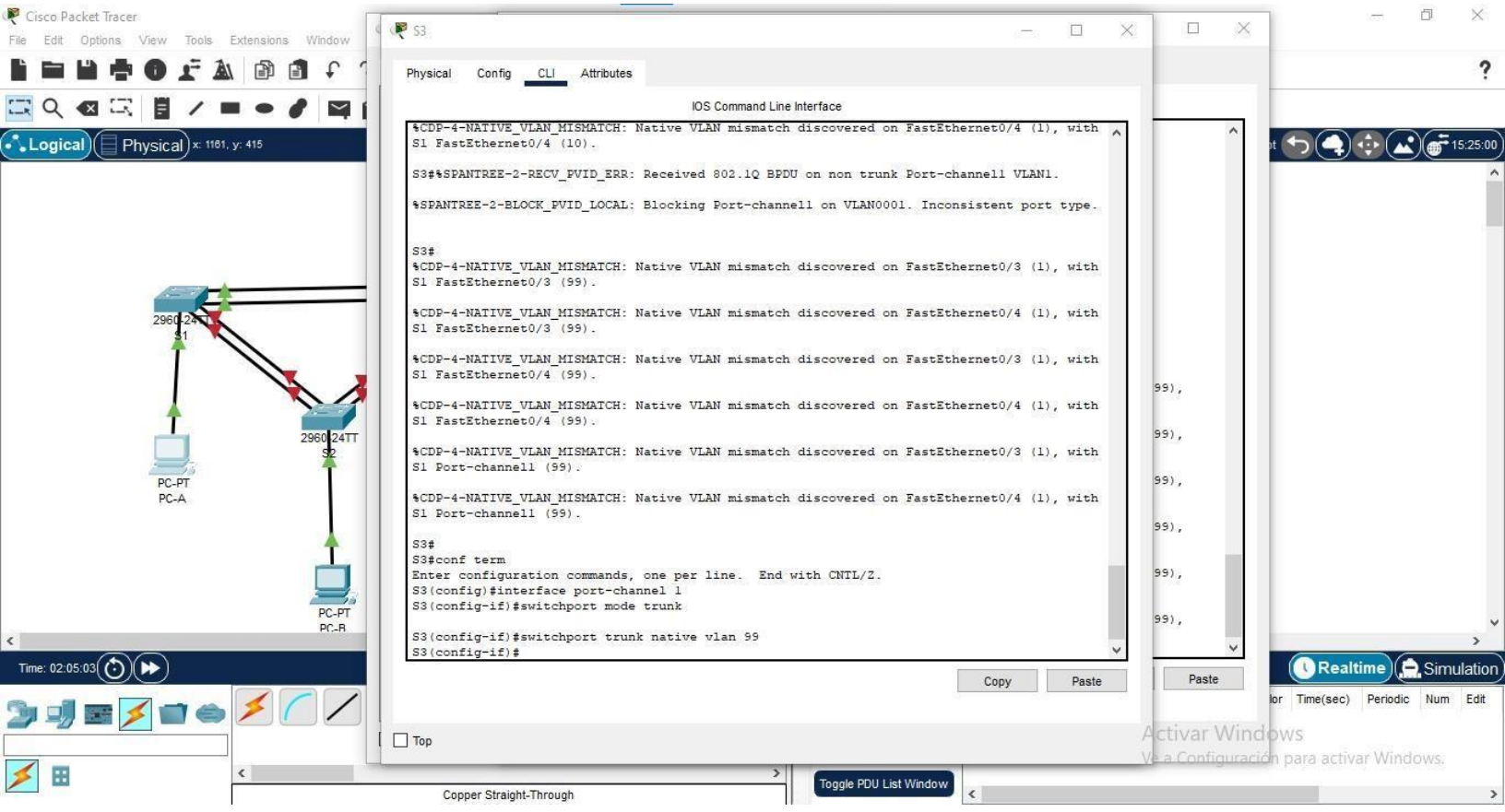
Práctica de laboratorio: Configuración de EtherChannel



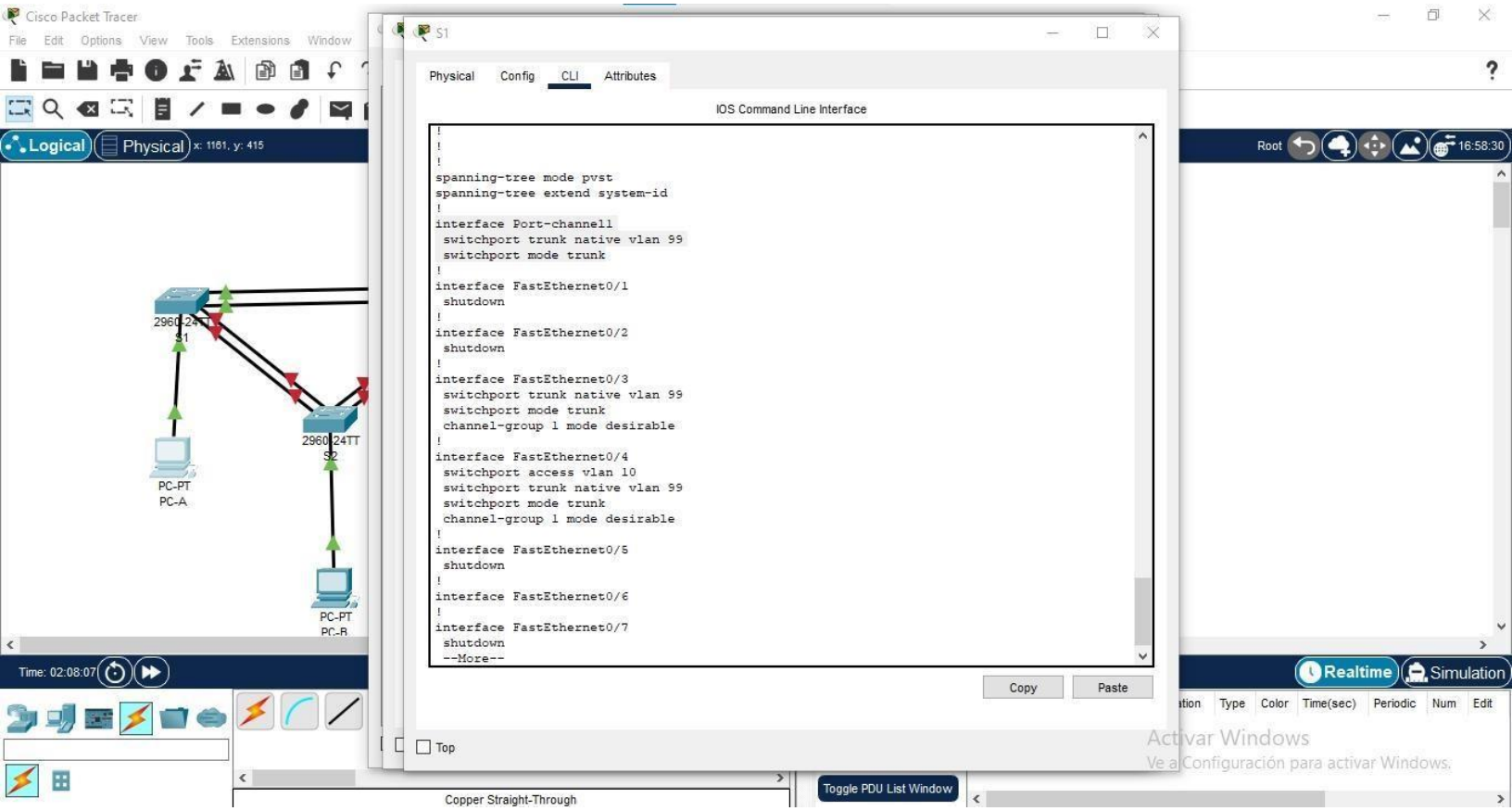


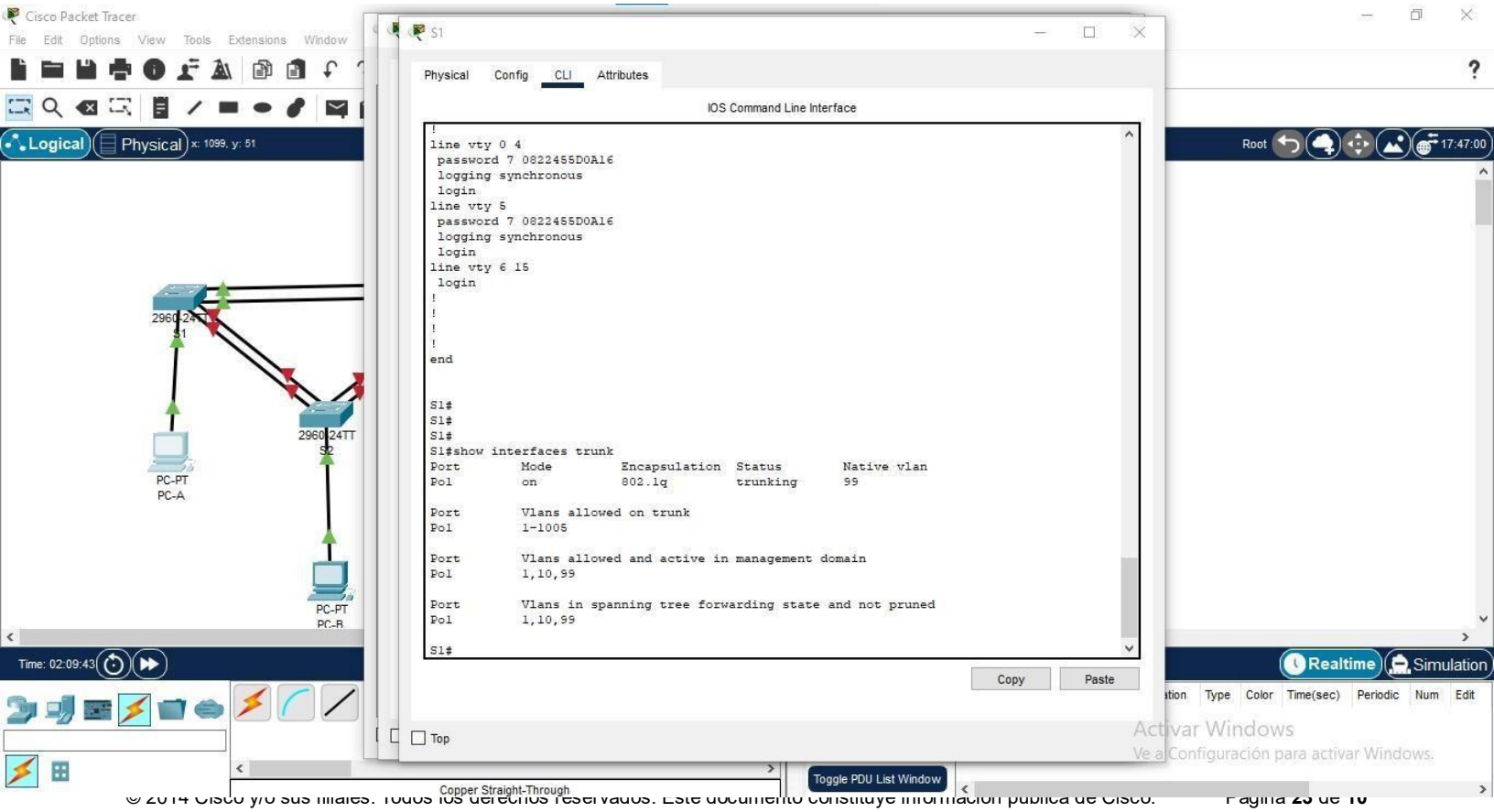
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.





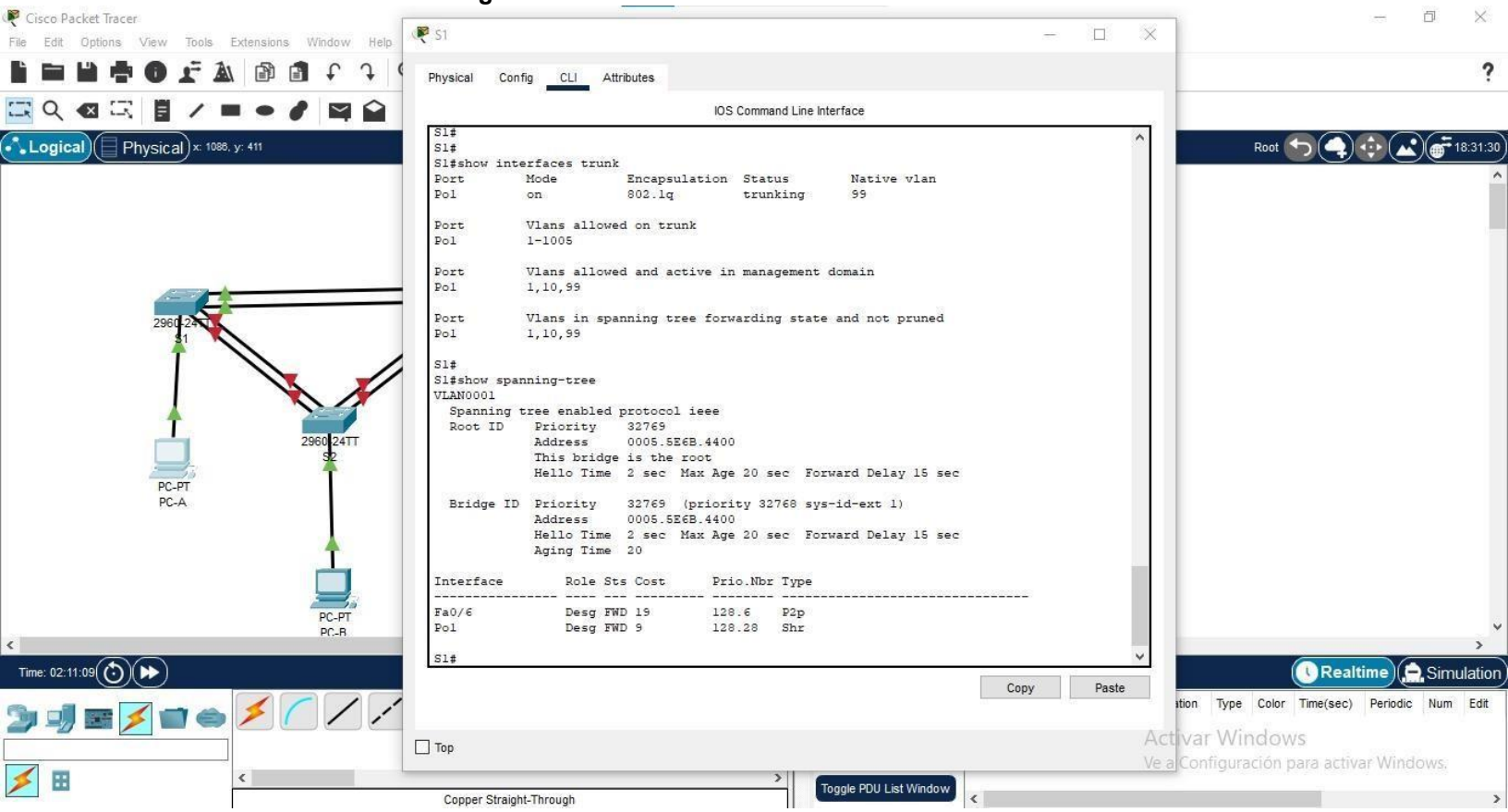
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

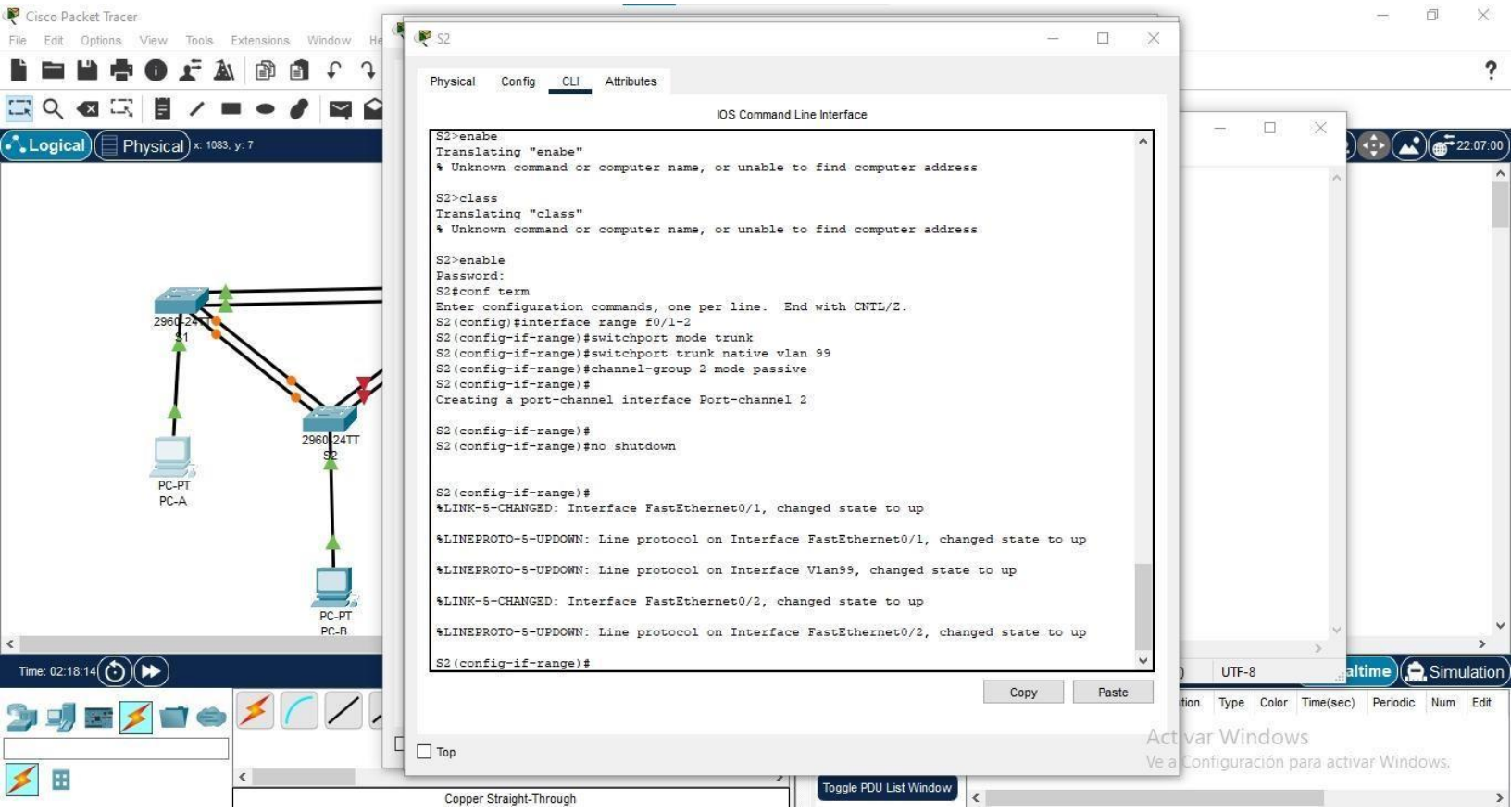




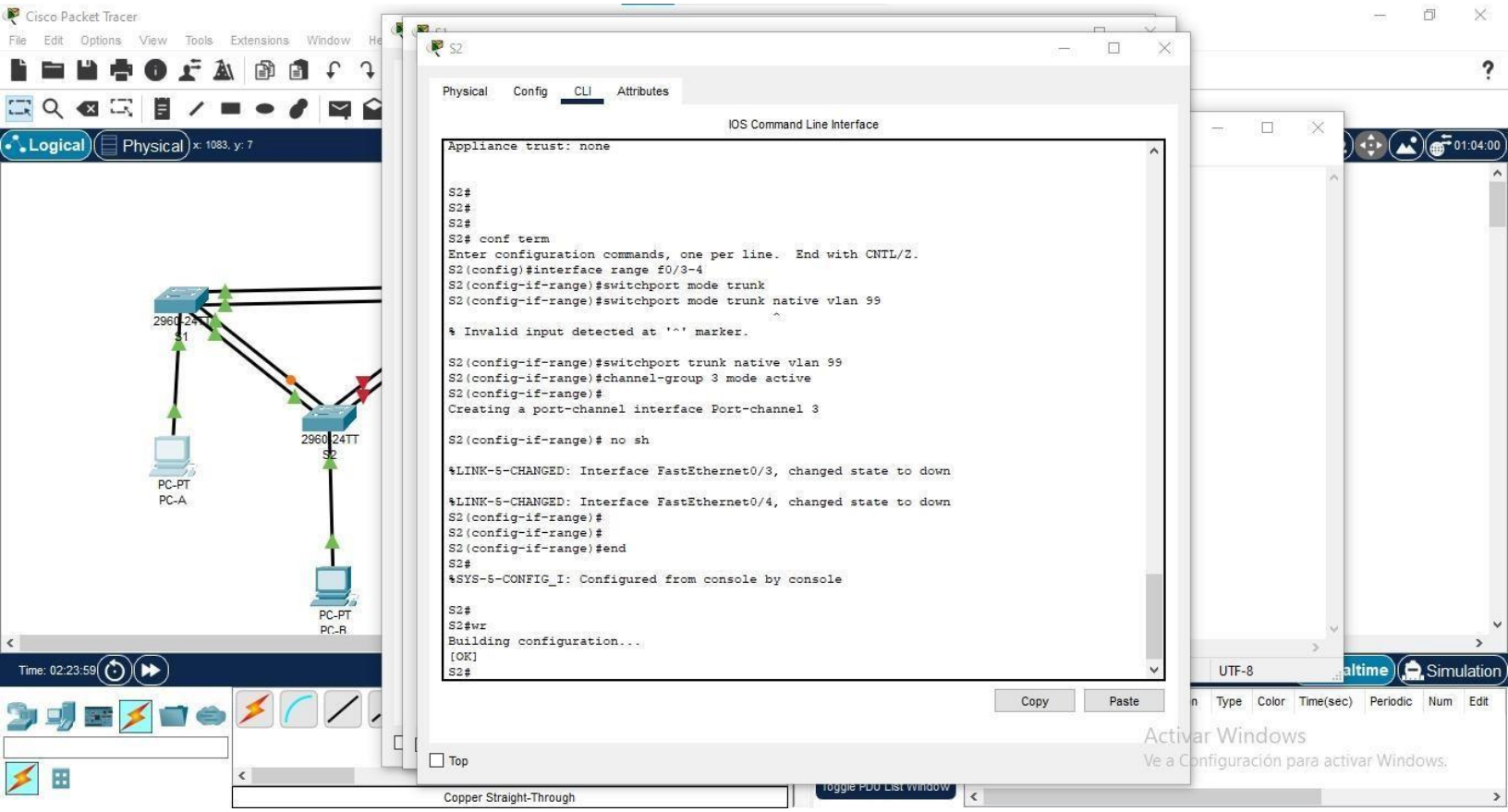
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento constituye información pública de Cisco.

Práctica de laboratorio: Configuración de EtherChannel

Presentado por:

Janir Yuni
C.C. 1.129.506.072

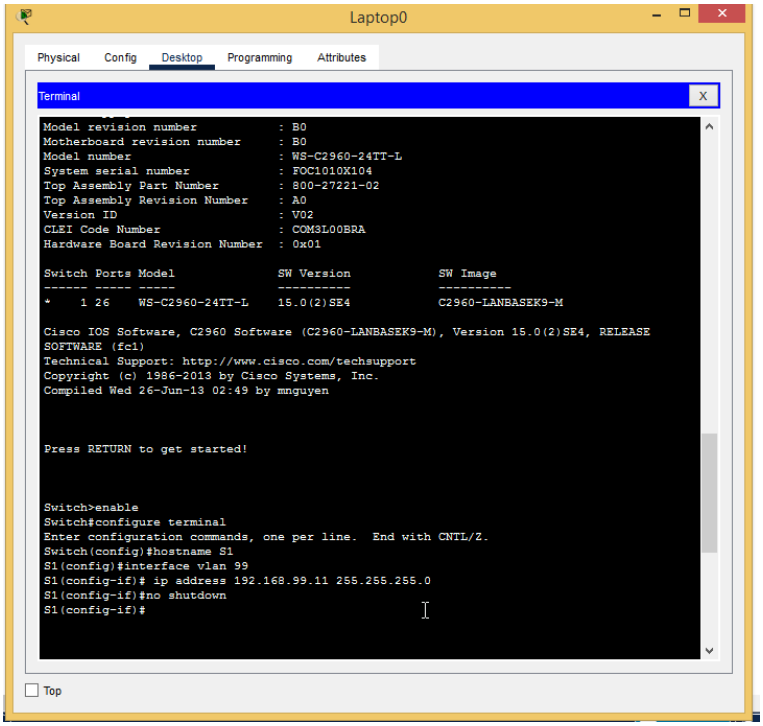
GESTIÓN DE REDES DE DATOS
FICHA 2558406

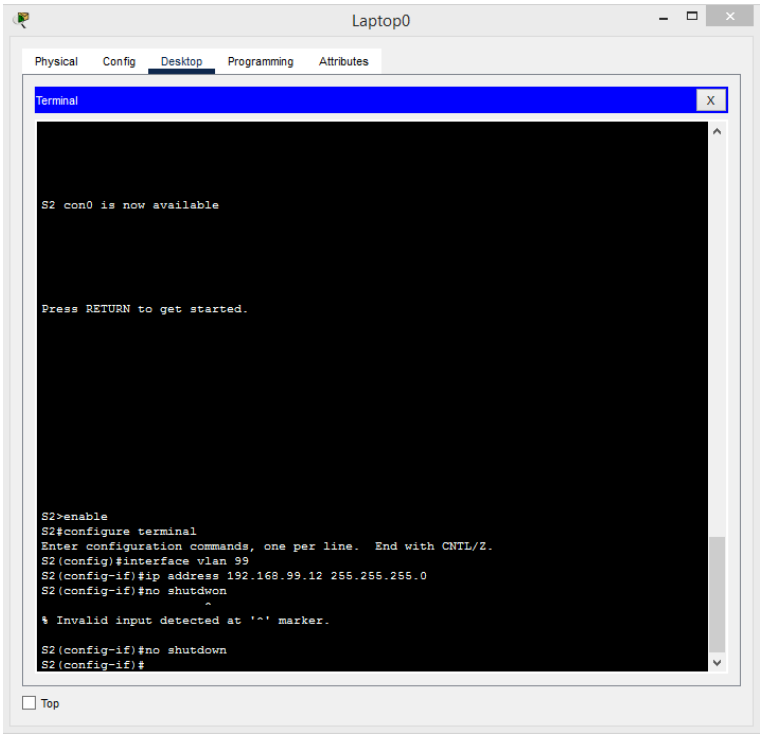
Instructor

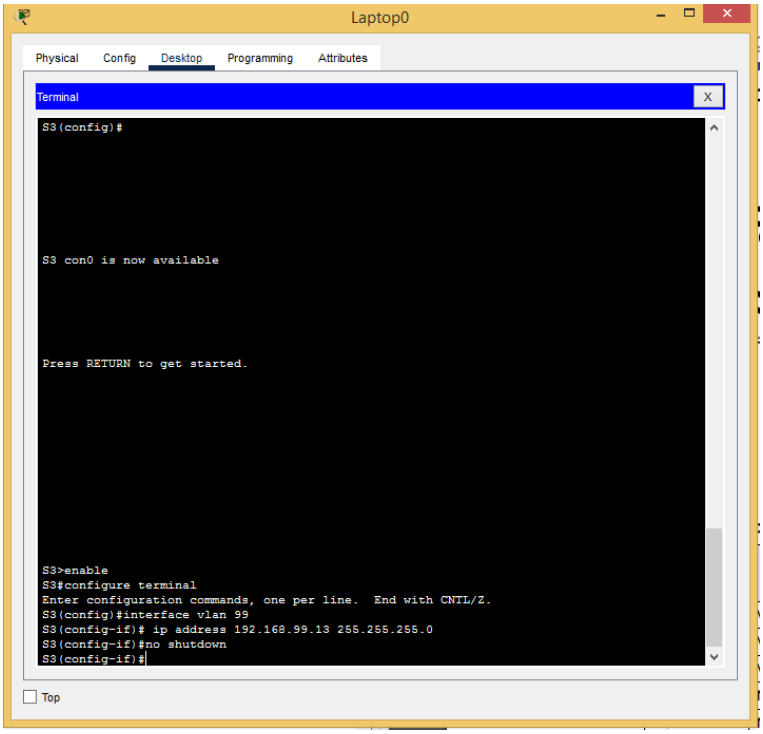
ROBERTO CARLOS BELTRAN MEDINA

SERVICIO NACIONAL DE APRENDIZAJE - SENA
Junio - 2023

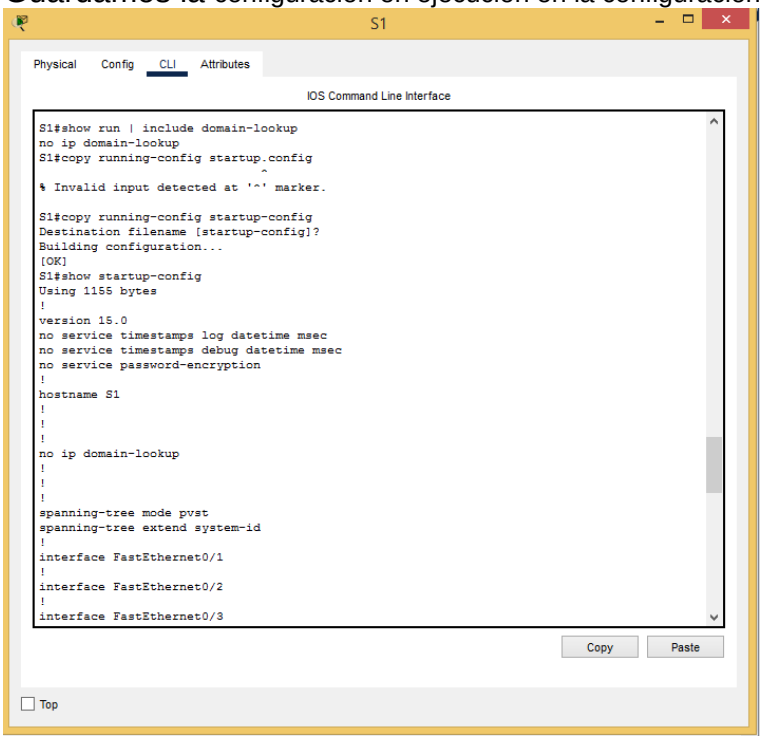
Le cambiamos el nombre al switch y le colocamos la ip a la vlan



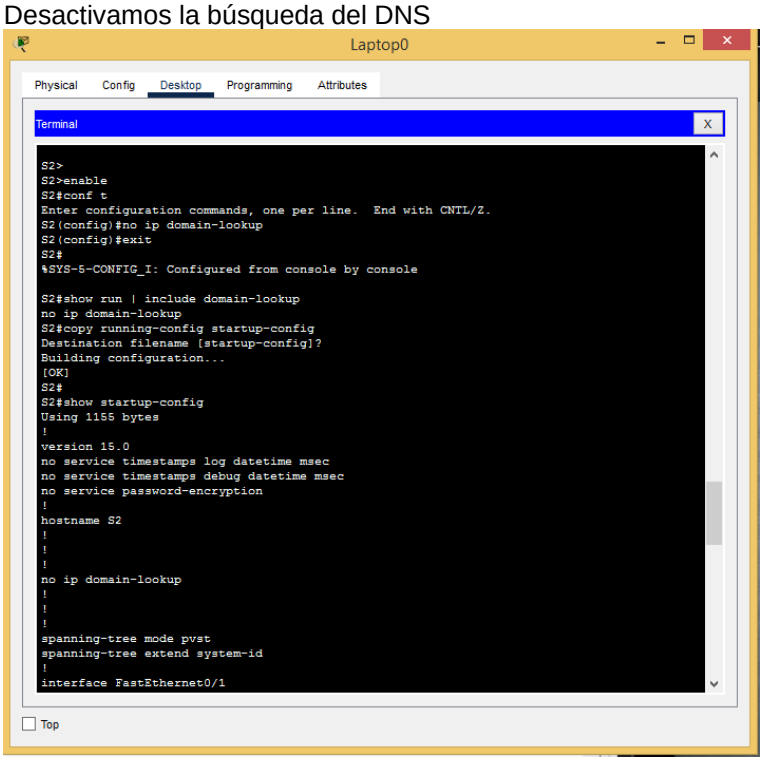


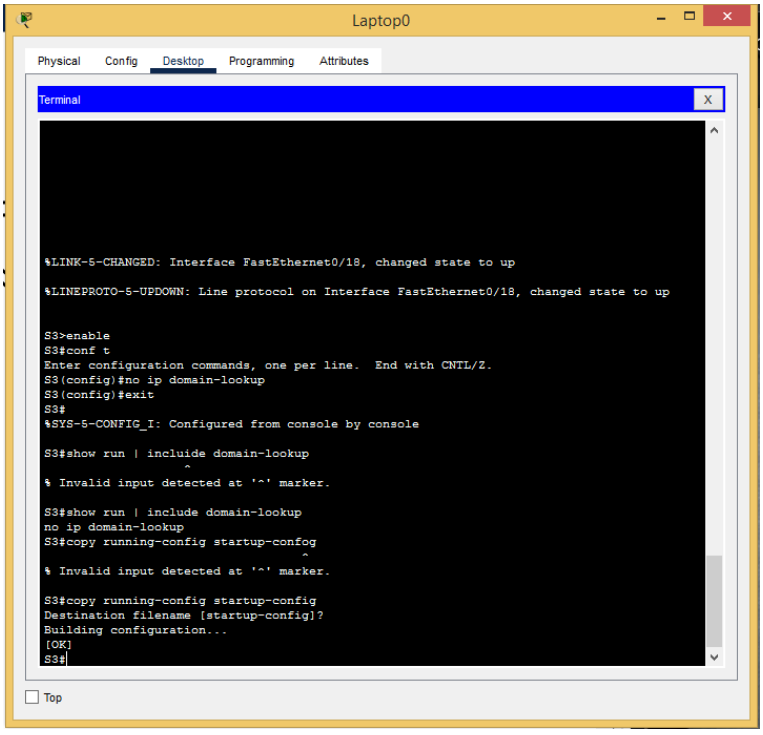


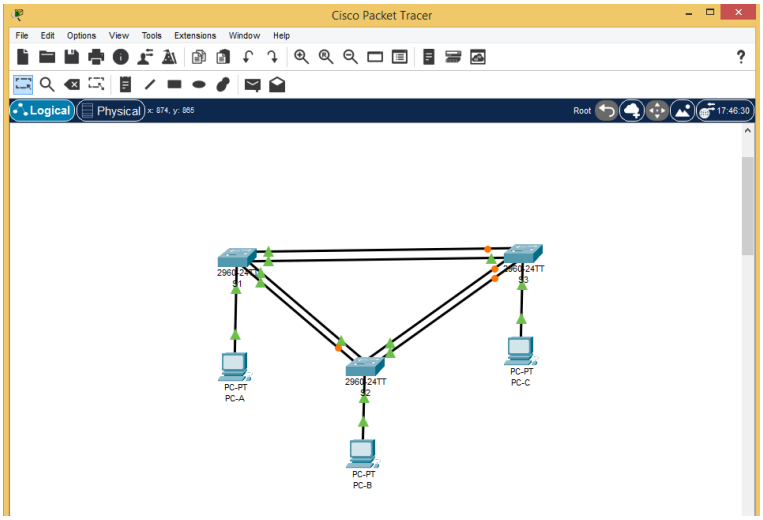
Guardamos la configuración en ejecución en la configuración de inicio



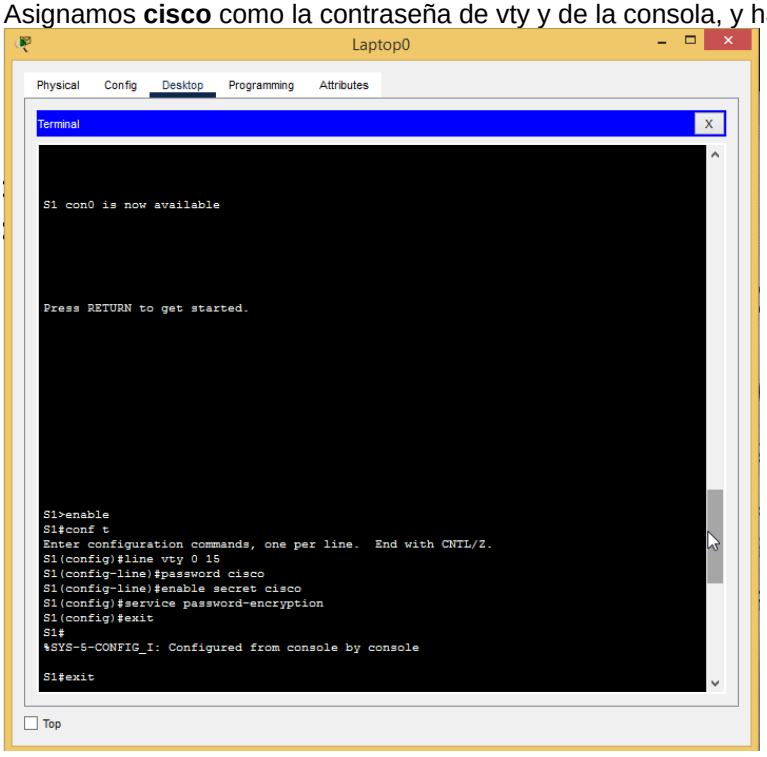
Desactivamos la búsqueda del DNS

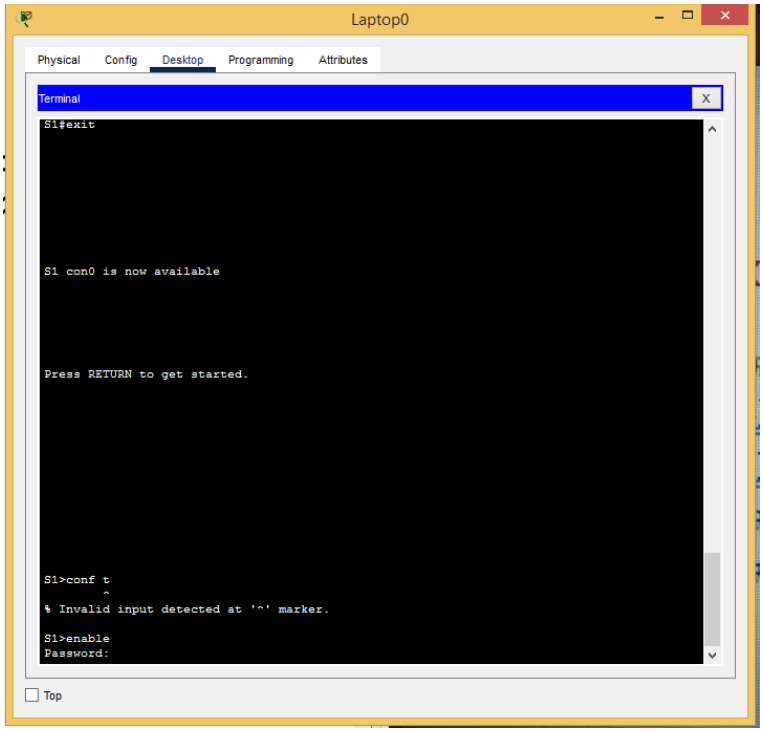


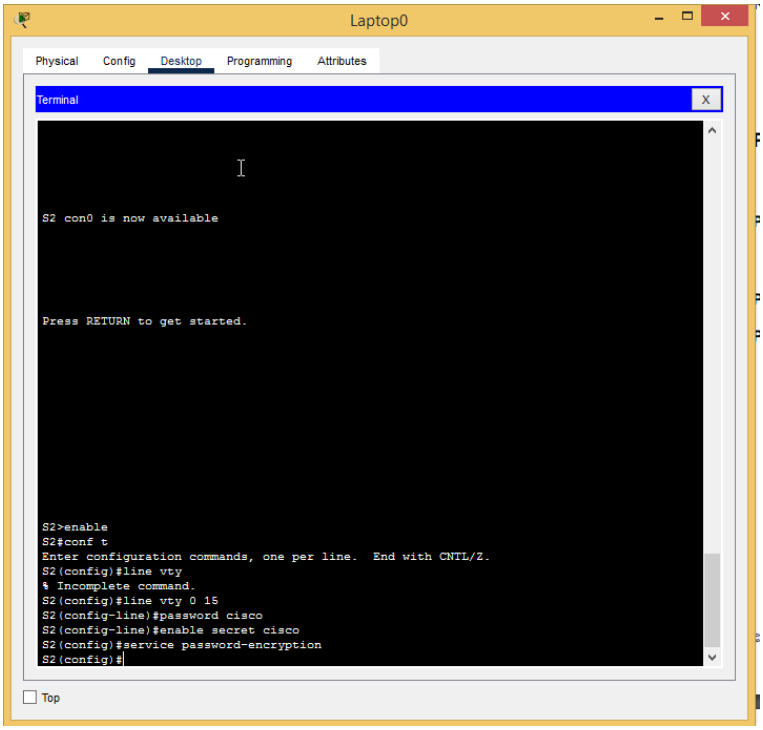


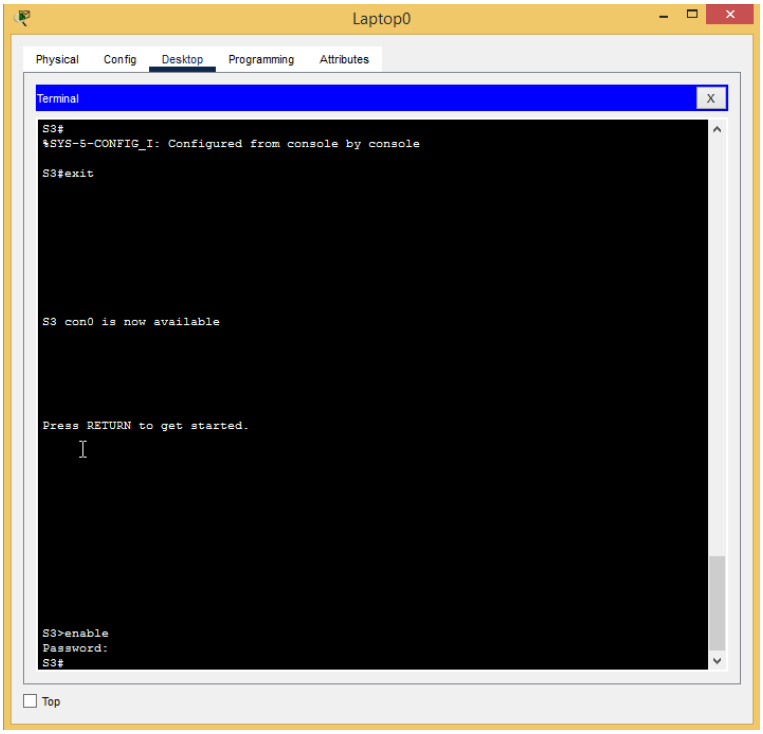


Asignamos **cisco** como la contraseña de vty y de la consola, y habilite el inicio de sesión.

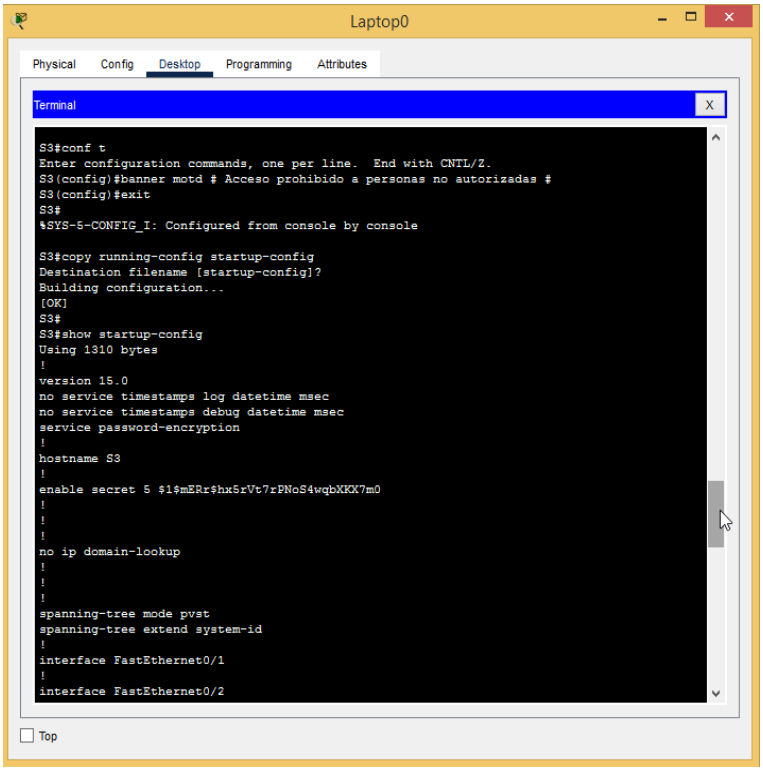


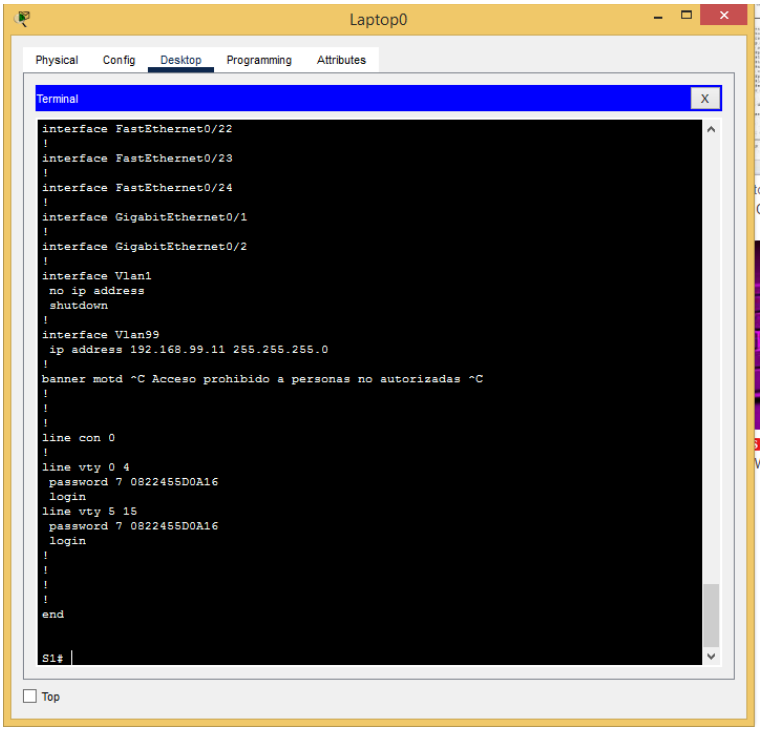

Laptop0
Physical
Config
Desktop
Programming
Attributes
Terminal
S1#exit
S1 con0 is now available
Press RETURN to get started.
S1>conf t
% Invalid input detected at '^' marker.
S1>enable
Password:
Top


Laptop0
Physical
Config
Desktop
Programming
Attributes
Terminal
S2 con0 is now available
Press RETURN to get started.
S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#line vty
% Incomplete command.
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#enable secret cisco
S2(config)#service password-encryption
S2(config)#
Top

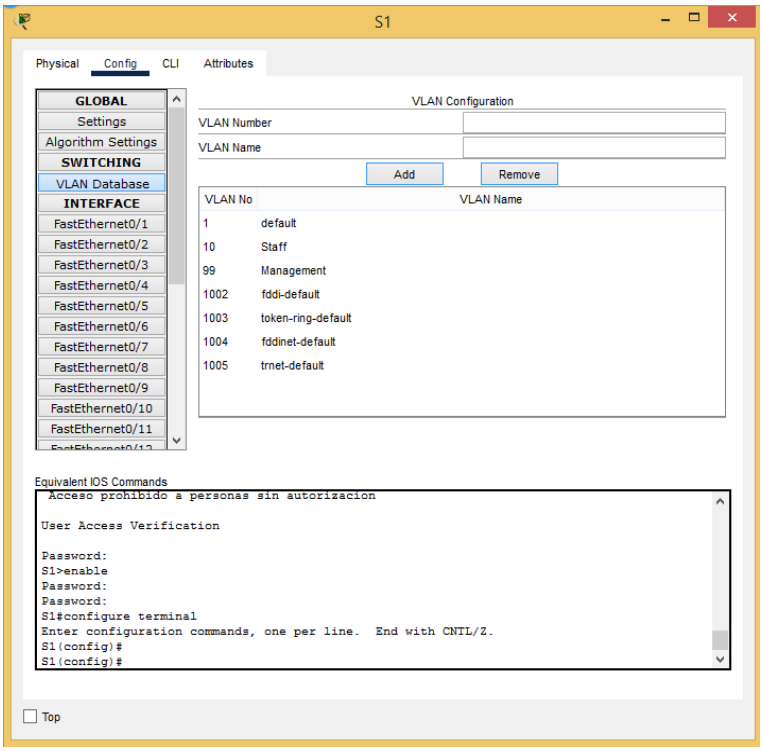


Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.

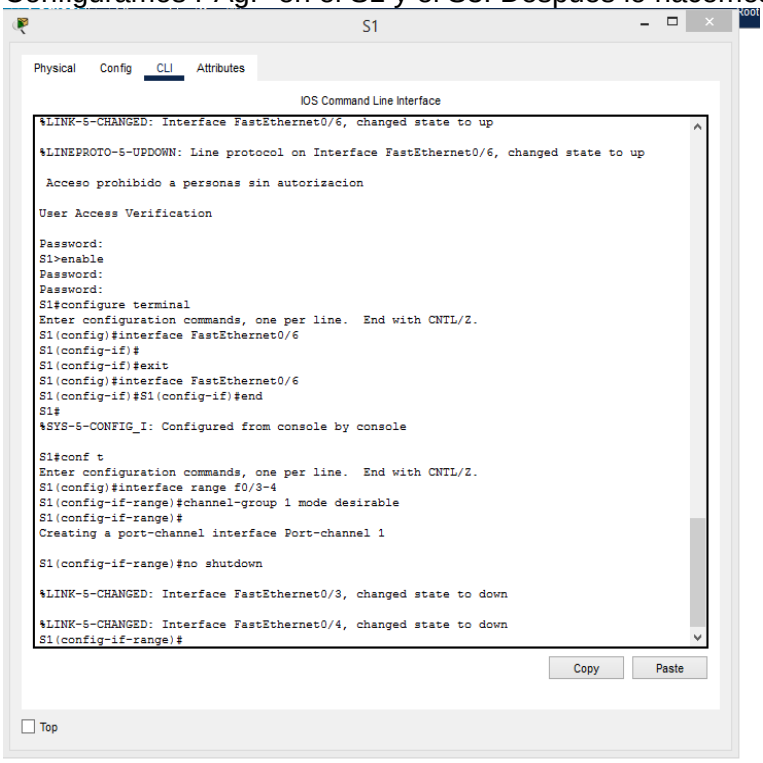


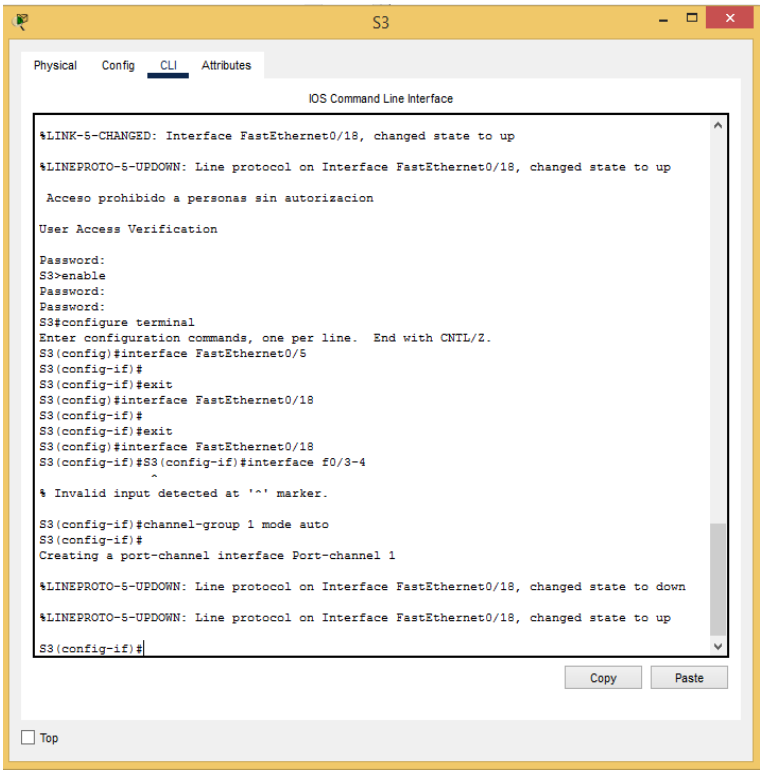


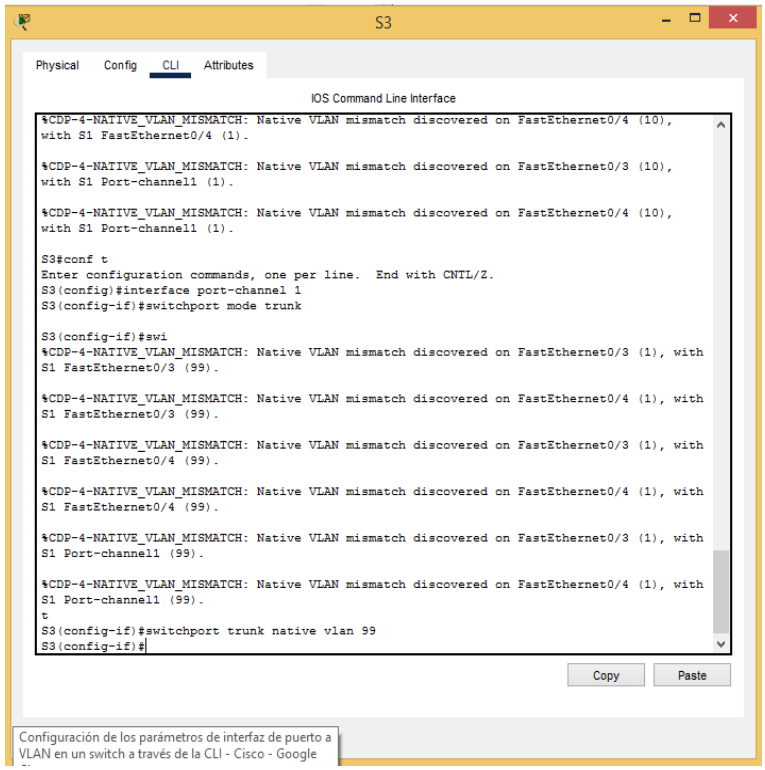
Configure la VLAN 99 y asígnele el nombre **Management** y a la VLAN 10 y asígnele el nombre **Staff**.

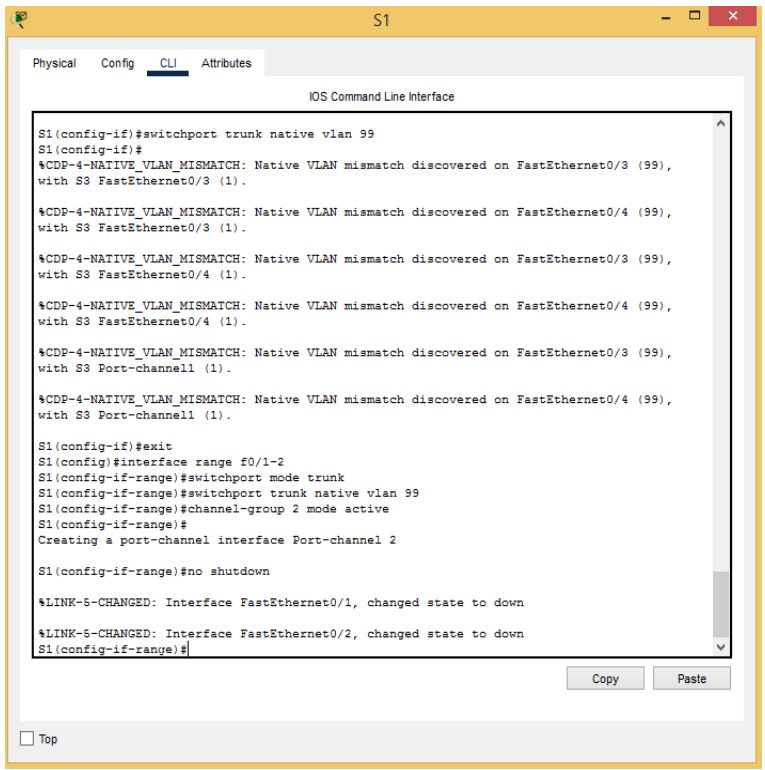


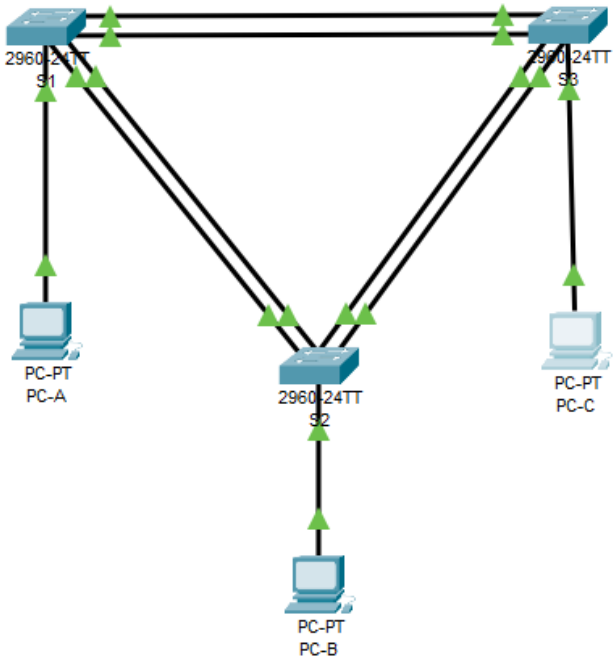
Configuramos PAgP en el S1 y el S3. Despues lo hacemos entre el S1-S2 y el S2-S3



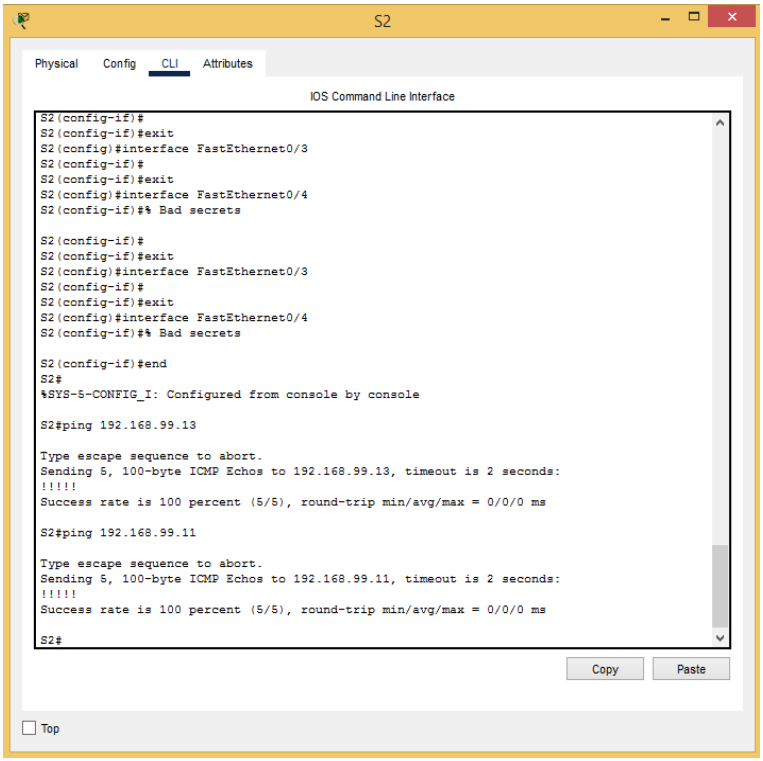



S3
Physical
Config
CLI
Attributes
IOS Command Line Interface
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (10), with S1 FastEthernet0/4 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (10), with S1 Port-channel1 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (10), with S1 Port-channel1 (1).
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface port-channel 1
S3(config-if)#switchport mode trunk
S3(config-if)#swi
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 FastEthernet0/3 (99).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 FastEthernet0/3 (99).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 FastEthernet0/4 (99).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 FastEthernet0/4 (99).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (1), with S1 Port-channel1 (99).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (1), with S1 Port-channel1 (99).
t
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#
Copy
Paste
Configuración de los parámetros de interfaz de puerto a VLAN en un switch a través de la CLI - Cisco - Google

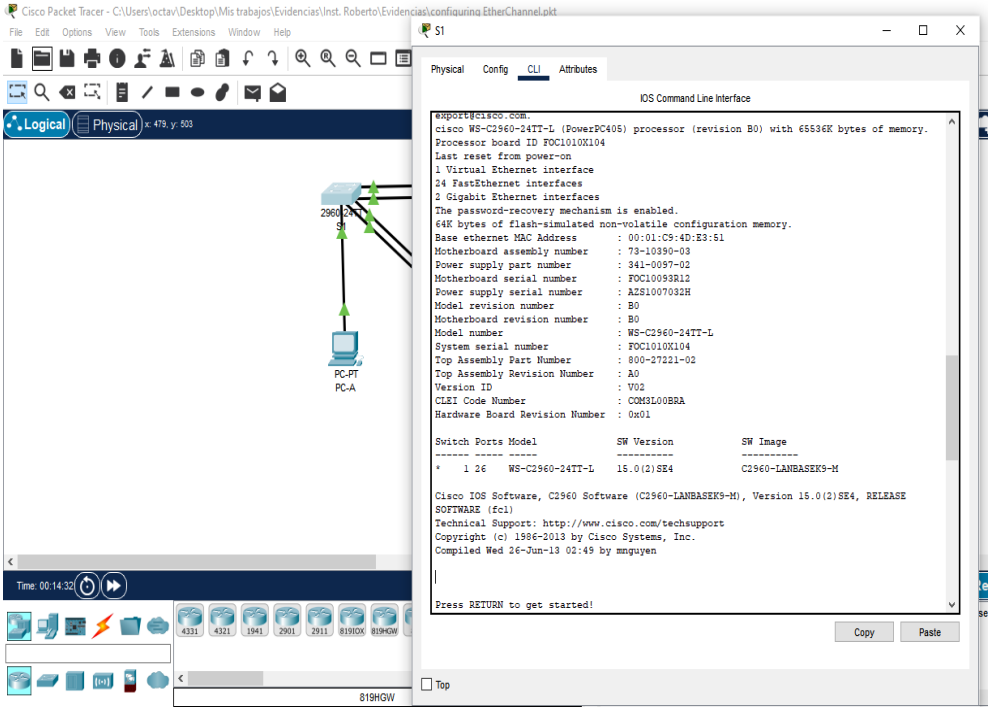

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (99), with S3 FastEthernet0/3 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (99), with S3 FastEthernet0/3 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (99), with S3 FastEthernet0/4 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (99), with S3 FastEthernet0/4 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (99), with S3 Port-channel1 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (99), with S3 Port-channel1 (1).
S1(config-if)#exit
S1(config)#interface range f0/1-2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#channel-group 2 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 2
S1(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down
S1(config-if-range)#
Copy
Paste
Top



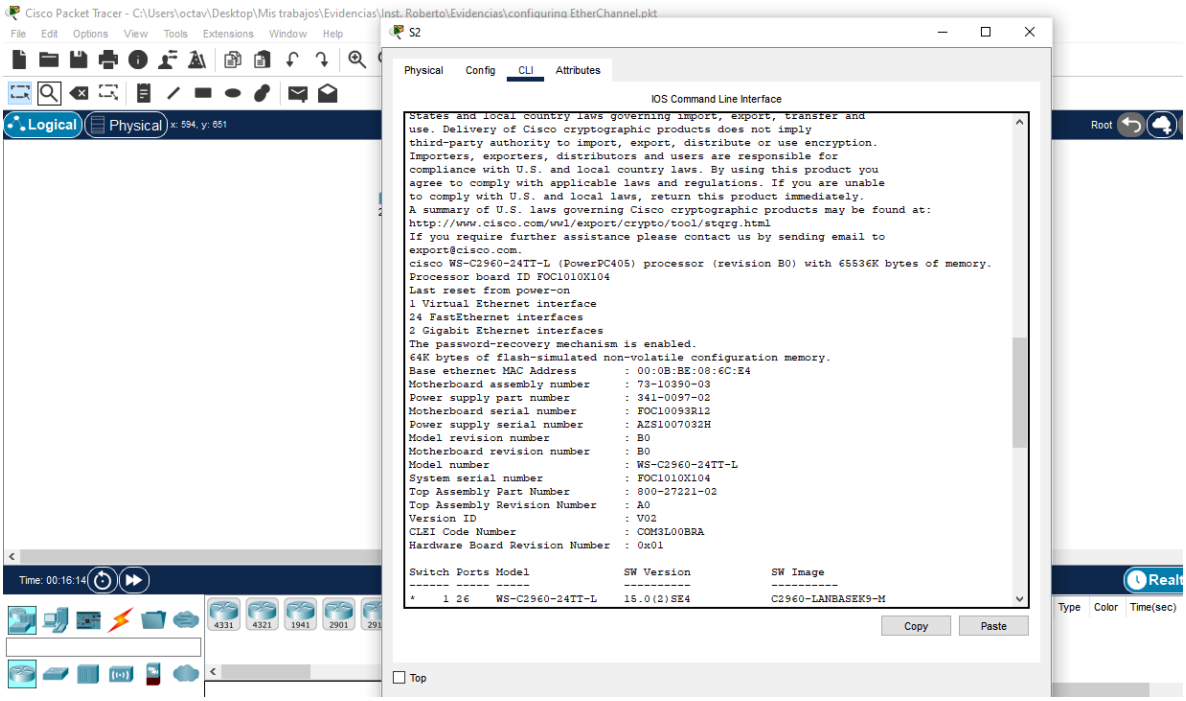
Hacemos ping entre los swicthes



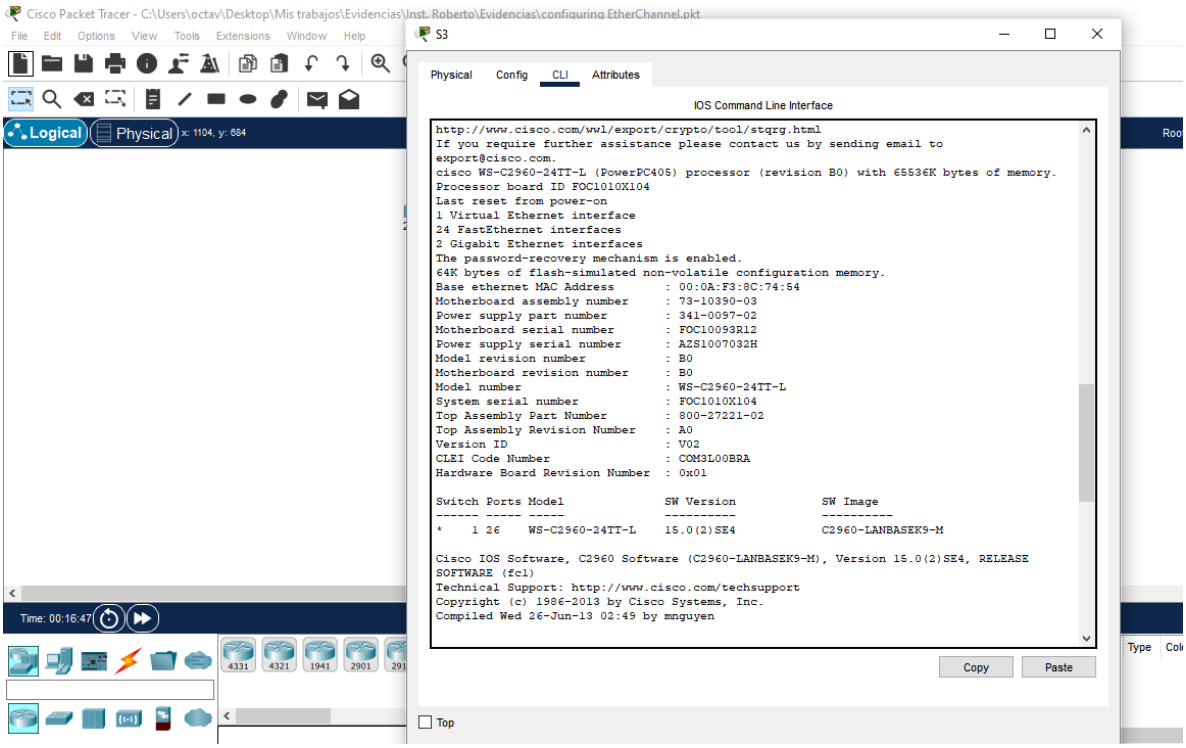
Switch1



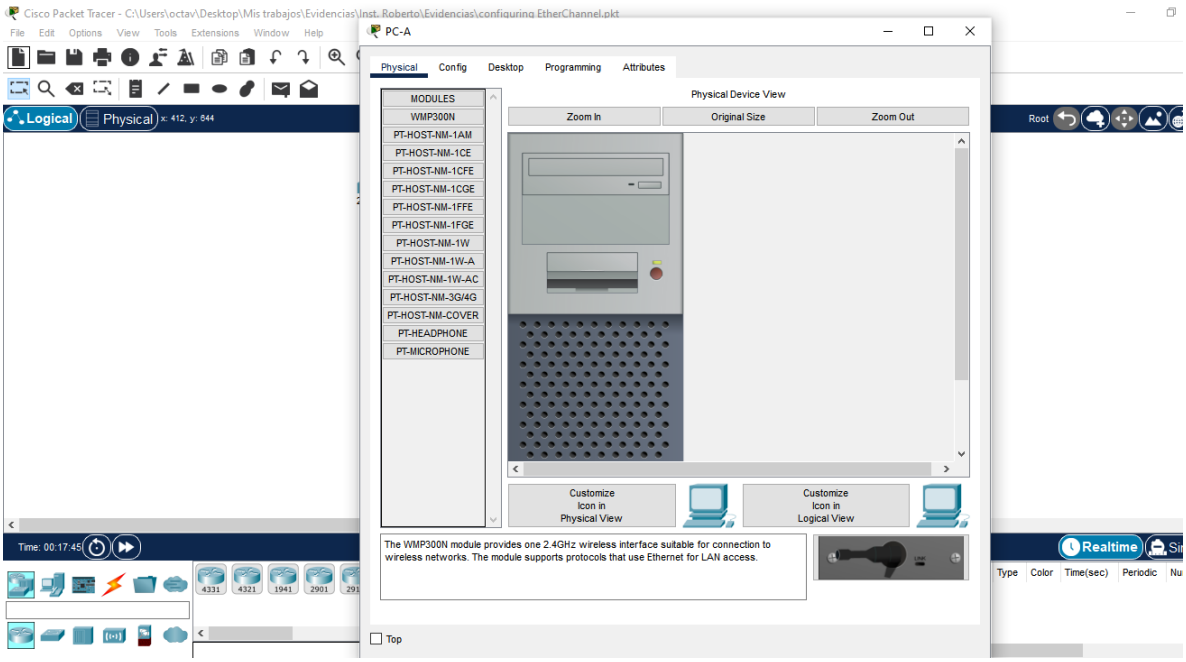
Switch2

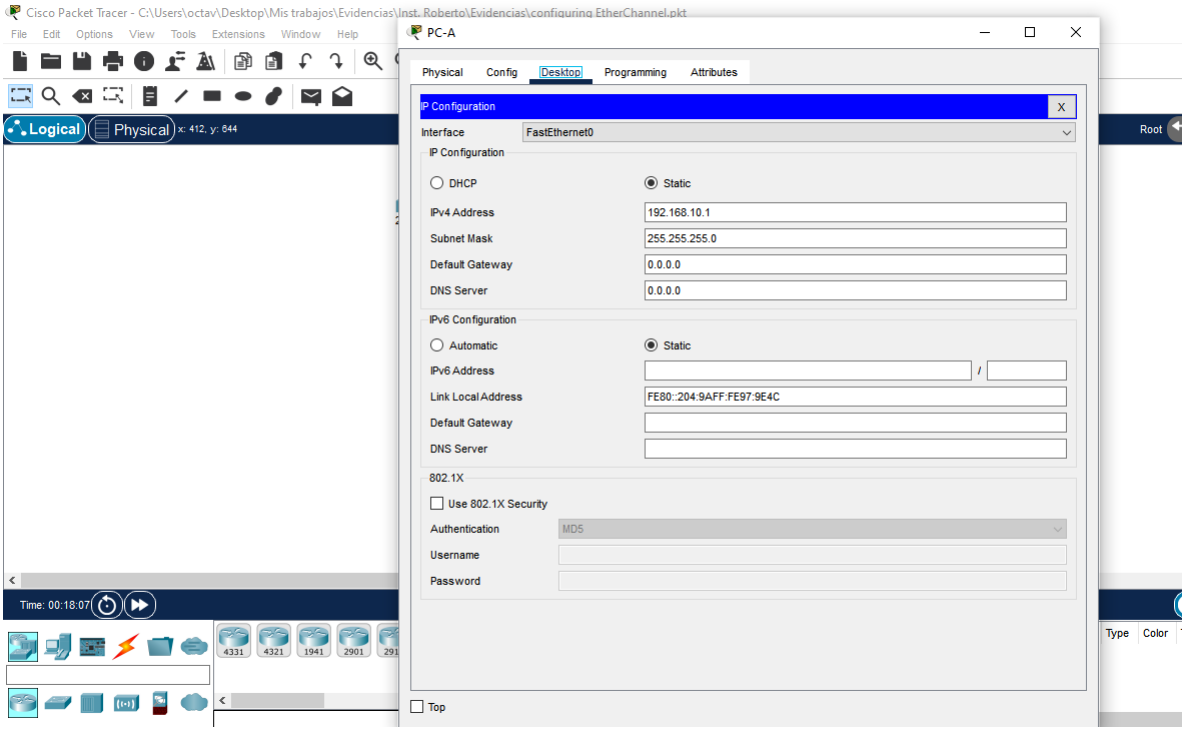


Switch 3

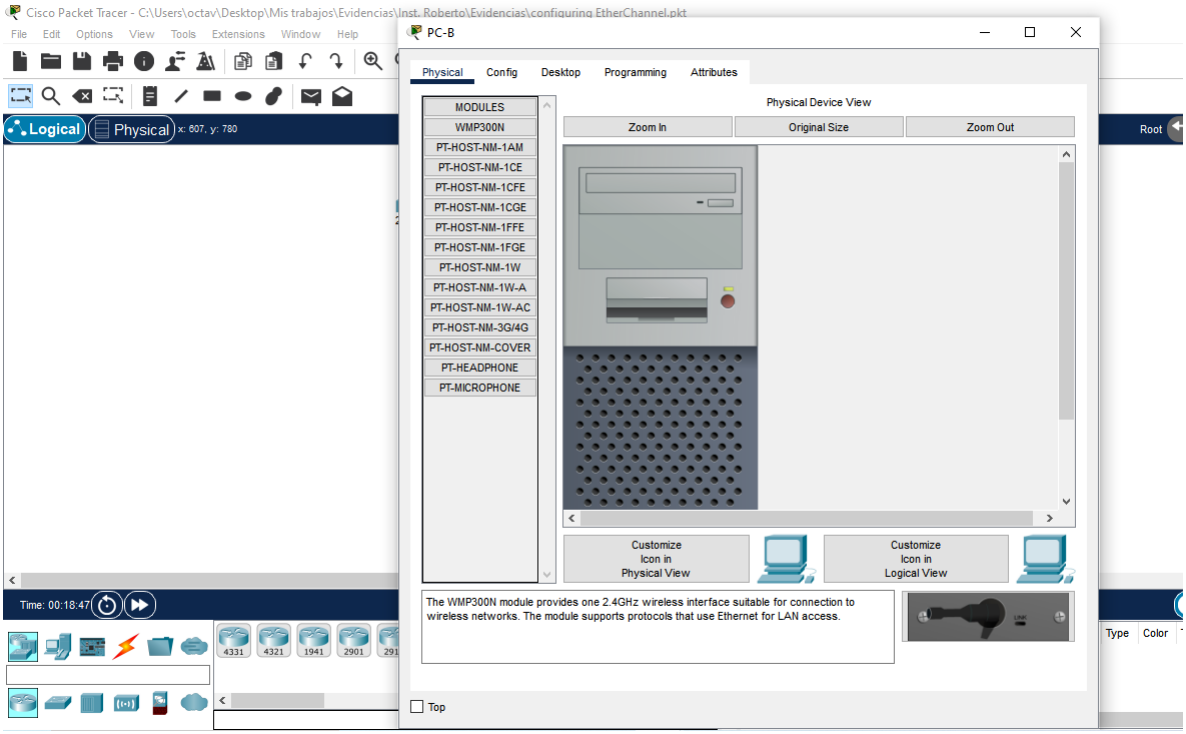

Cisco Packet Tracer - C:\Users\octav\Desktop\Mis trabajos\Evidencias\Inst. Roberto\Evidencias\configuring EtherChannel.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1104, y: 684
Time: 00:16:47
S3
Physical Config CLI Attributes
IOS Command Line Interface
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 65536K bytes of memory.
Processor board ID FOC1010X104
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address : 00:0A:F3:8C:74:54
Motherboard assembly number : 73-10390-03
Power supply part number : 341-0097-02
Motherboard serial number : FOC10093R12
Power supply serial number : AZS1007032H
Model revision number : B0
Motherboard revision number : B0
Model number : WS-C2960-24TT-L
System serial number : FOC1010X104
Top Assembly Part Number : 800-27221-02
Top Assembly Revision Number : A0
Version ID : V02
CLEI Code Number : COM3L00BRA
Hardware Board Revision Number : 0x01
Switch Ports Model SW Version SW Image
* 1 26 WS-C2960-24TT-L 15.0(2)SE4 C2960-LANBASEK9-M
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen
Copy
Paste
Top

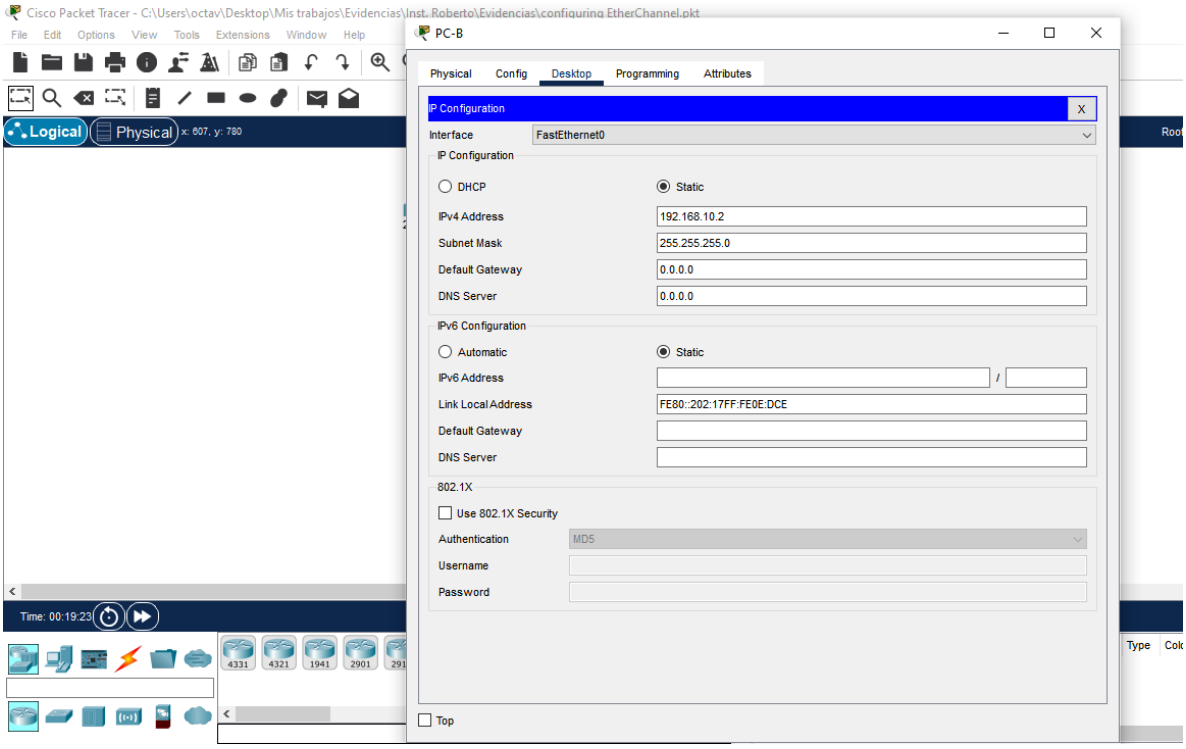
PC1


Cisco Packet Tracer - C:\Users\octav\Desktop\Mis trabajos\Evidencias\Inst. Roberto\Evidencias\configuring EtherChannel.pkt
Logical Physical x: 412, y: 644
Time: 00:17:45
PC-A
Physical Config Desktop Programming Attributes
MODULES
WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
PT-HOST-NM-1W-AC
PT-HOST-NM-3G/4G
PT-HOST-NM-COVER
PT-HEADPHONE
PT-MICROPHONE
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.
Top
Realtime

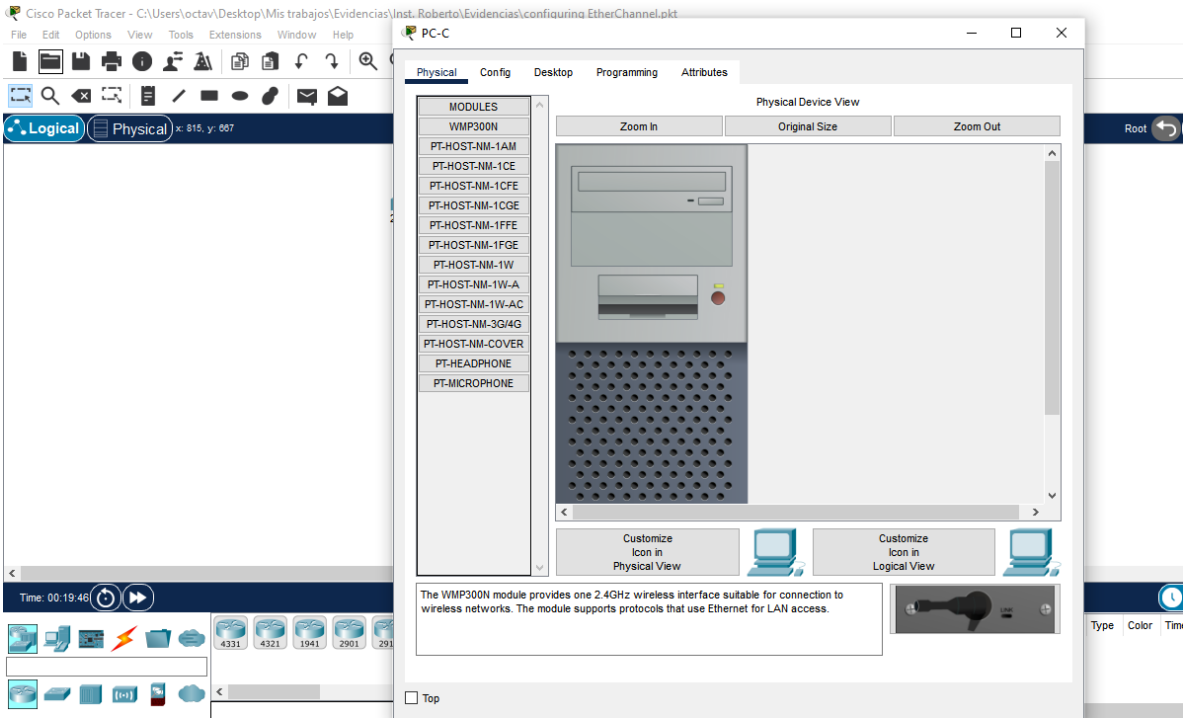

Cisco Packet Tracer - C:\Users\octav\Desktop\Mis trabajos\Evidencias\Inst. Roberto\Evidencias\configuring EtherChannel.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 412, y: 644
Root
PC-A
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP Static
IPv4 Address 192.168.10.1
Subnet Mask 255.255.255.0
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
IPv6 Configuration
Automatic Static
IPv6 Address
Link Local Address FE80::204:9AFF:FE97:9E4C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
Time: 00:18:07
Type Color

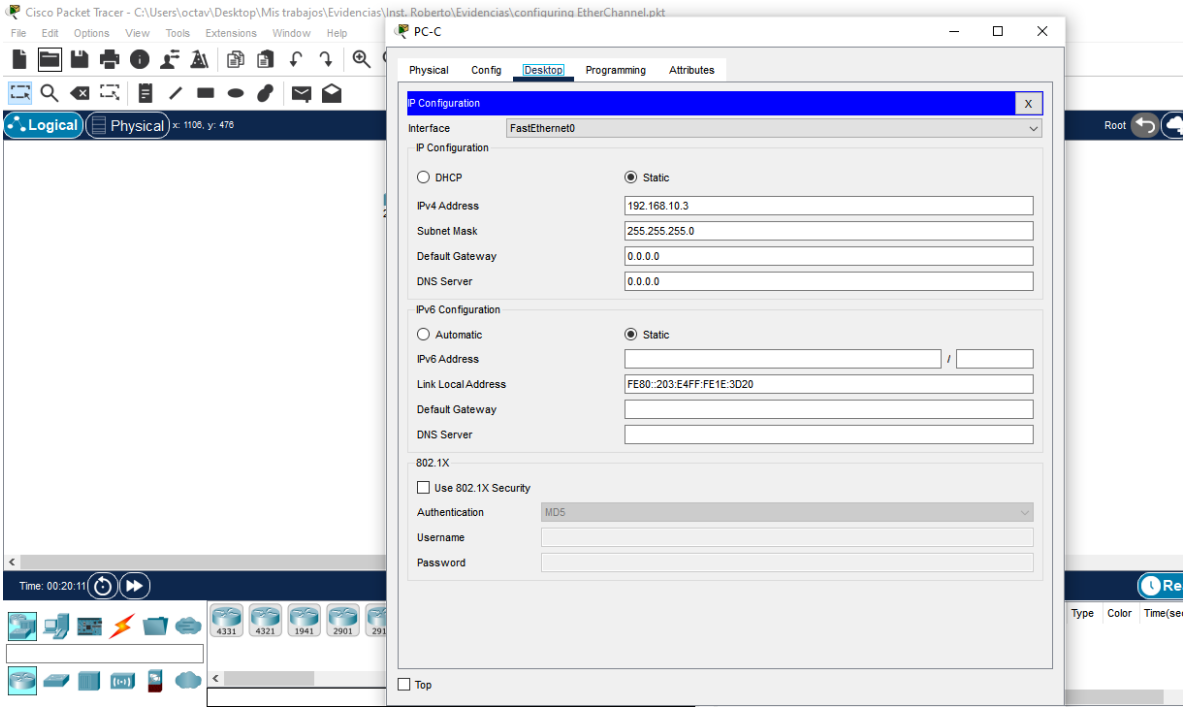
PC2

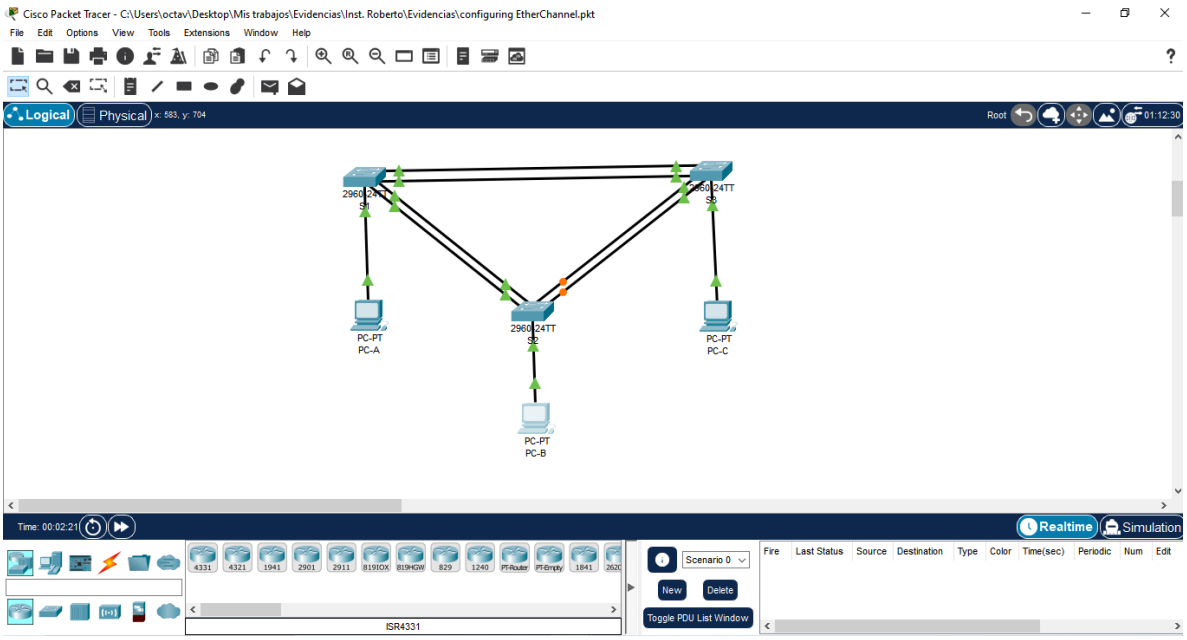

Cisco Packet Tracer - C:\Users\octav\Desktop\Mis trabajos\Evidencias\Inst. Roberto\Evidencias\configuring EtherChannel.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 607, y: 780
Root
PC-B
Physical Config Desktop Programming Attributes
MODULES
WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
PT-HOST-NM-1W-AC
PT-HOST-NM-3G/4G
PT-HOST-NM-COVER
PT-HEADPHONE
PT-MICROPHONE
Physical Device View
Zoom In Original Size Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.
Top
Time: 00:18:47
Type Color


PC-B
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.2
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::202:17FF:FE0E:DCE
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PC3


PC-C
Physical
Config
Desktop
Programming
Attributes
MODULES
WMP300N
PT-HOST-NM-1AM
PT-HOST-NM-1CE
PT-HOST-NM-1CFE
PT-HOST-NM-1CGE
PT-HOST-NM-1FFE
PT-HOST-NM-1FGE
PT-HOST-NM-1W
PT-HOST-NM-1W-A
PT-HOST-NM-1W-AC
PT-HOST-NM-3G/4G
PT-HOST-NM-COVER
PT-HEADPHONE
PT-MICROPHONE
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.
Top





Nombre: Octavio José Monrroy Charris

Ficha: 2558406

Instructor: Roberto Beltrán

SENA Centro Industrial de Aviación
(Regional Atlántico)

Curso

Mantenimiento de Equipos de Computo

Ficha (2671178)

Instructor

ROBERTO CARLOS BELTRAN MEDINA

Estudiante

Jorge Enrique Núñez Rivera

Trabajo

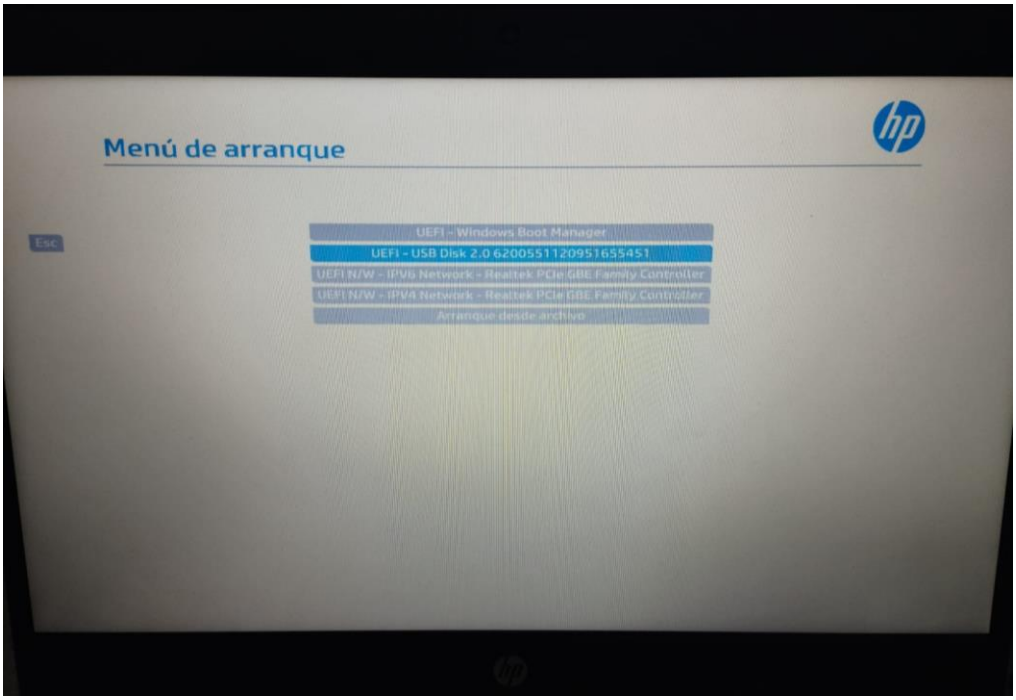
DLC Boot

29 de junio de 2023

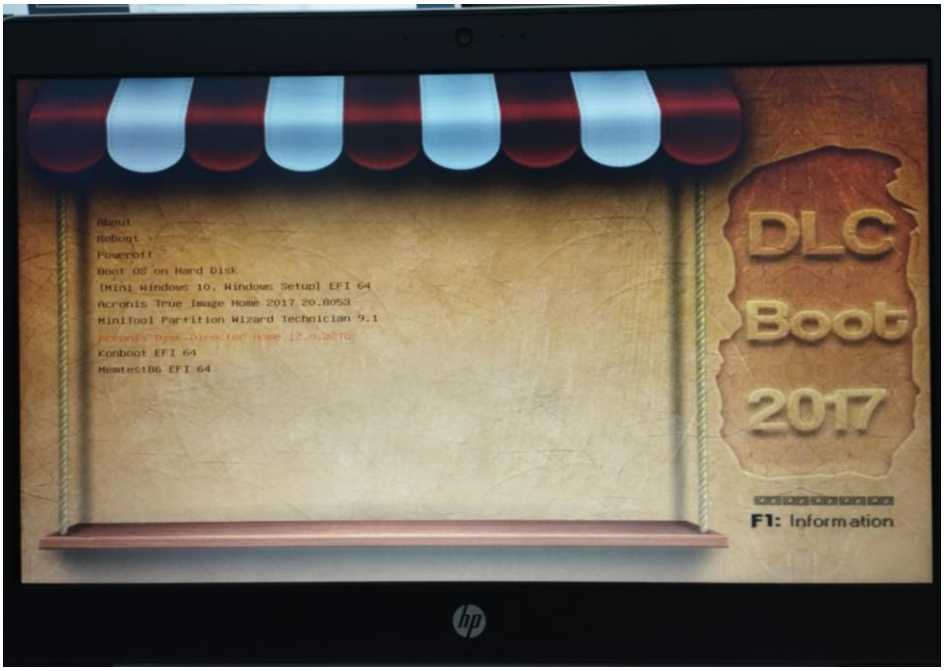
DLC Boot

Mini Windows

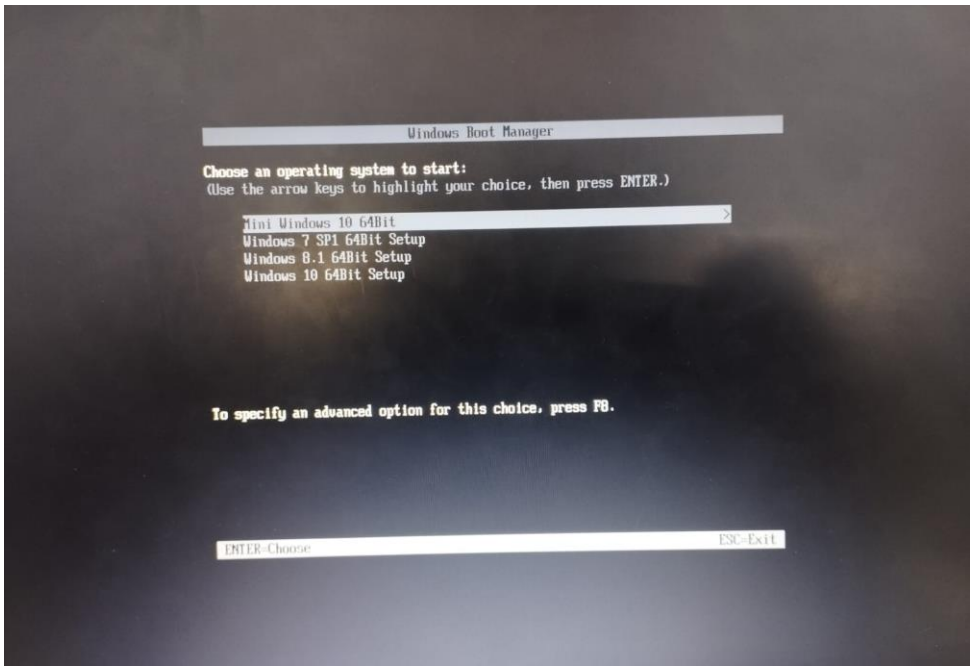
Encendemos la PC y entramos a la BIOS y después a la opción de arranque y elegimos la memoria donde tengamos el DLC Boot



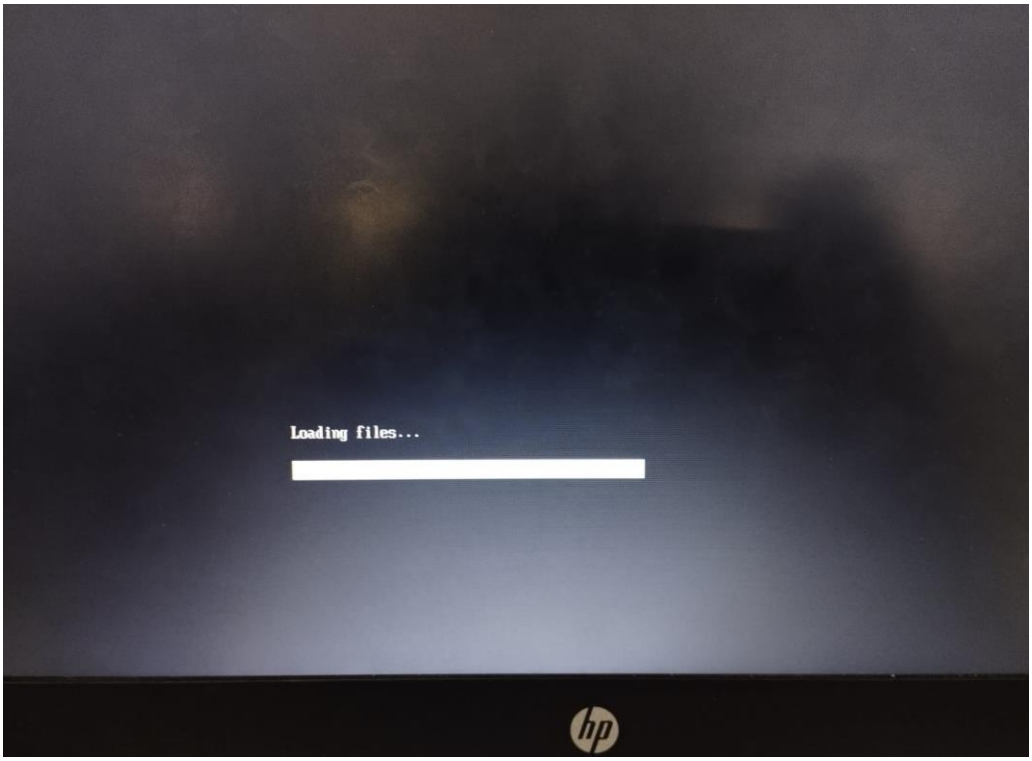
De inmediato se nos muestra la interfaz del DLC Boot, elegimos mini Windows



Nos sale la siguiente pantalla y elegimos mini Windows 10



Se nos muestra la siguiente pantalla de carga



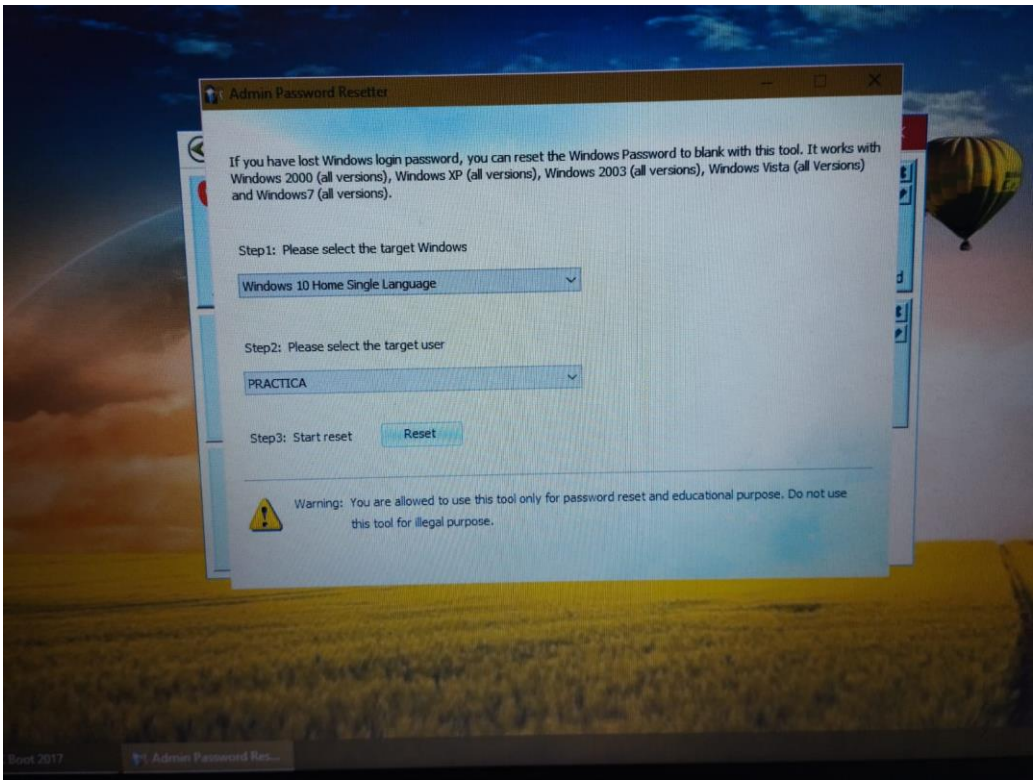
Después se nos muestra lo siguiente, el escritorio del mini Windows y elegimos Password Remove



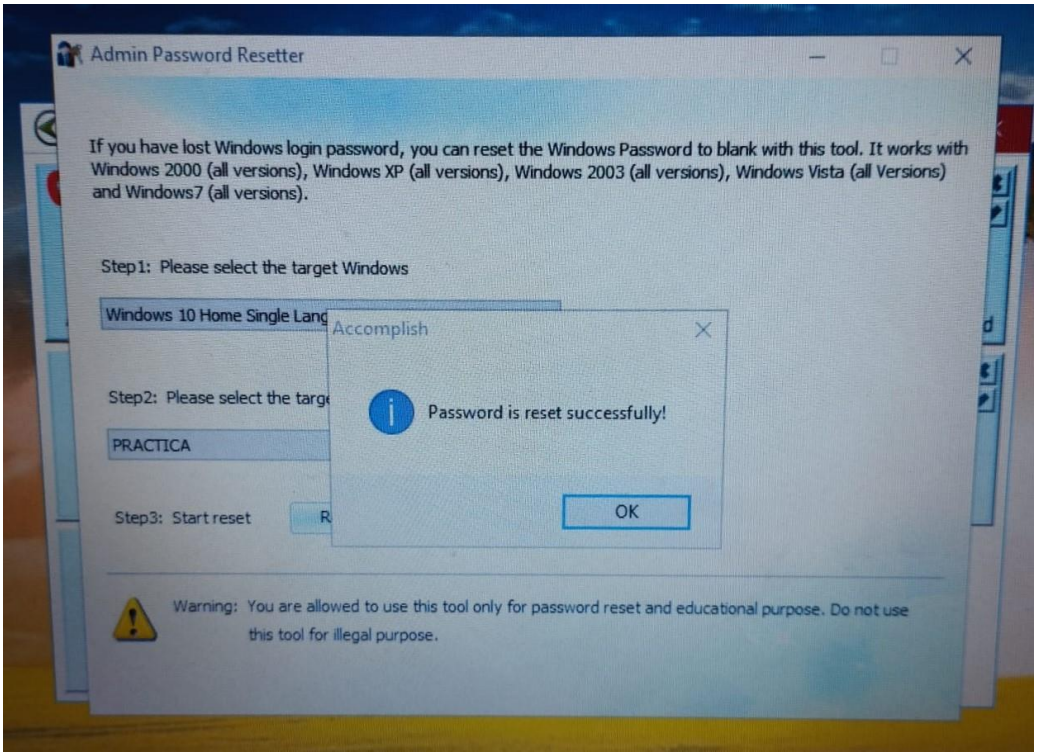
Elegimos Password Remove



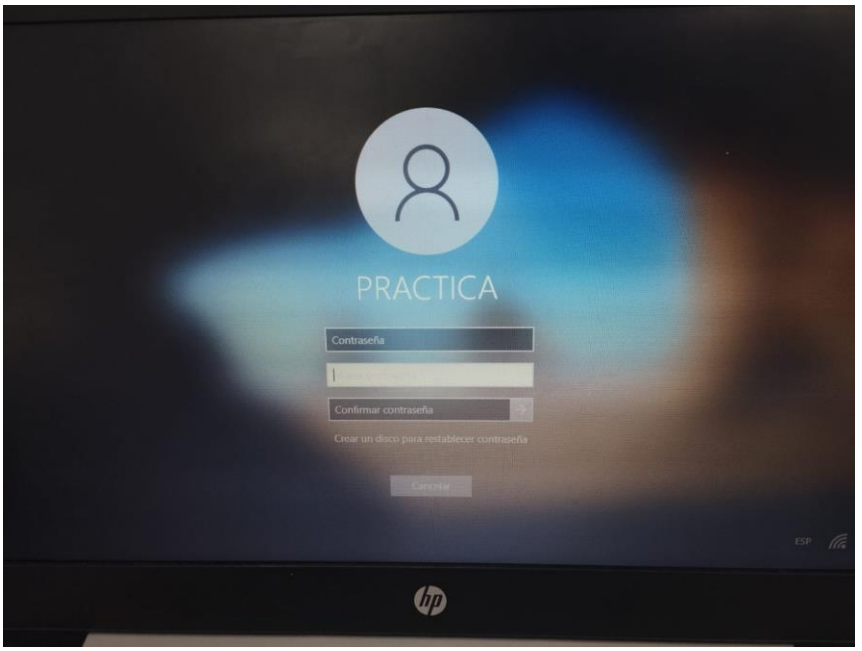
Elegimos el sistema operativo y la cuenta a la cual se le va a resetear la contraseña en este caso se llama PRACTICA



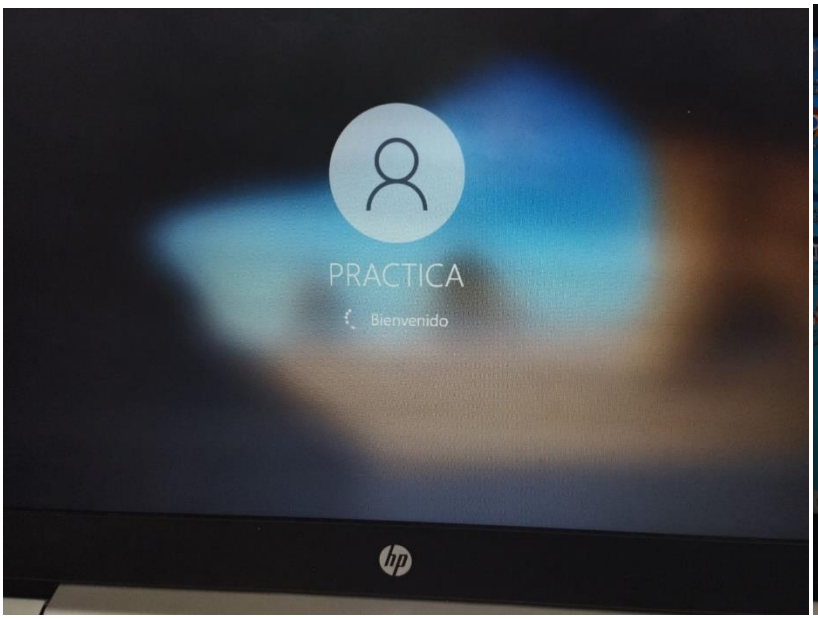
Le damos clic donde dice Reset y nos saldrá este mensaje

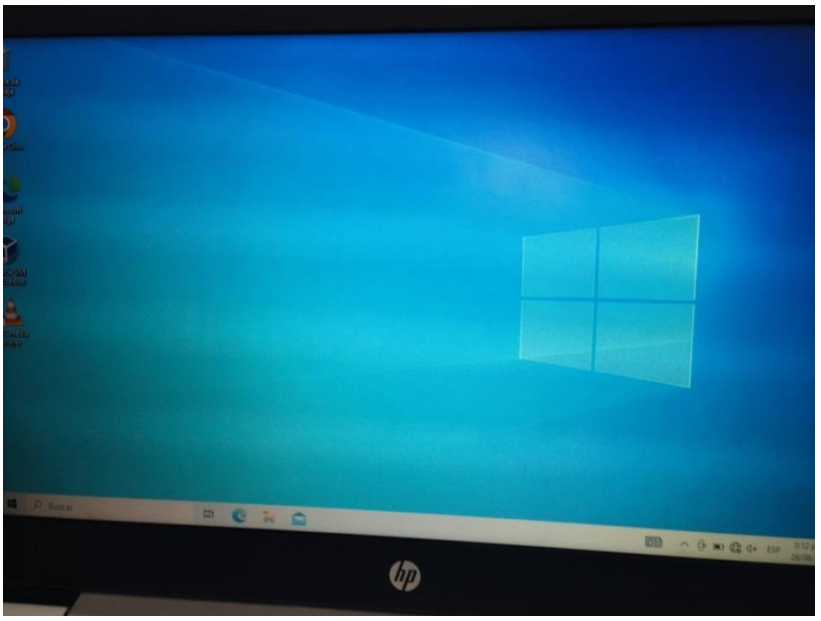


Como podemos ver la cuenta ya no tiene contraseña y está pidiendo que se le ingrese una contraseña nueva



Después podemos ver que esta iniciando sesión y ya se puede usar nuevamente la cuenta o perfil PRACTICA





DLC Boot VS Sergei Strelec

Características	DLC Boot	Sergei Strelec
Plataforma	Windows	Windows
Funciones	Diagnóstico, reparación y mantenimiento de PC	Diagnóstico, reparación y mantenimiento de PC
Base de arranque	Interfaz de Windows, DVD o unidad USB	DVD o unidad USB
Herramientas incluidas	Amplia gama de utilidades y programas	Amplia gama de utilidades y programas
Diagnóstico del sistema	Sí	Sí
Gestión de particiones	Sí	Sí
Copia de seguridad	Sí	Sí
Recuperación de datos	Sí	Sí
Recuperación de contraseñas	Sí	Sí
Análisis de hardware	Sí	Sí
Eliminación de malware	Sí	Sí
Facilidad de uso	Interfaz sencilla	Interfaz sencilla
Actualizaciones	No se actualiza regularmente	Actualizaciones regulares
Comunidad de usuarios	Menos activa	Activa

Ambas herramientas, DLC Boot y Sergei Strelec, tienen características similares, ya que son discos de arranque basados en Windows Preinstallation Environment (WinPE) y ofrecen una amplia gama de utilidades para el diagnóstico y la reparación de sistemas informáticos.

Sin embargo, hay algunas diferencias. Por ejemplo, Sergei Strelec tiene una comunidad de usuarios más activa y ofrece actualizaciones regulares, lo que puede ser beneficioso para mantener las herramientas actualizadas y abordar problemas emergentes. Por otro lado, DLC Boot puede tener una interfaz más sencilla de usar para aquellos que prefieren una experiencia más simple.

En última instancia, la elección entre DLC Boot y Sergei Strelec dependerá de tus necesidades específicas y preferencias personales. Se recomienda evaluar las características y herramientas incluidas en cada uno y seleccionar la que mejor se ajuste a tus requerimientos.



MANTENIMIENTO DE EQUIPOS DE COMPUTO

(2671178)

INSTRUCTOR: ROBERTO CARLOS BELTRAN

APRENDIZ: JESÚS ESTRADA PELUFFO

TRABAJO: DESCRIPCION DLC BOOT, HIRENS BOOT Y CUADRO COMPARATIVO

JUNIO 2023

DLC BOOT



Es un programa de utilidad que permite a los usuarios encontrar y rectificar incidentes que se incluyen en el PC. La aplicación incluye una variedad de herramientas que determinan el estado de software y hardware que se ha instalado en un PC de escritorio o portátil.

Las características de DLC Boot:

-Disktools/Partition tools: función de partición del disco duro.

-Backup/RestoreTool: función de copia de seguridad o restauración o equipo fantasma.

-Driver: herramientas para descargar y actualizar controladores.

-Hardware Tools: función para comprobar la información de configuración del hardware.

-Office: resumen de las herramientas de Office.

-Antivirus: resumen del software antivirus.

-System: software del sistema.

-Ultilities: extensiones.

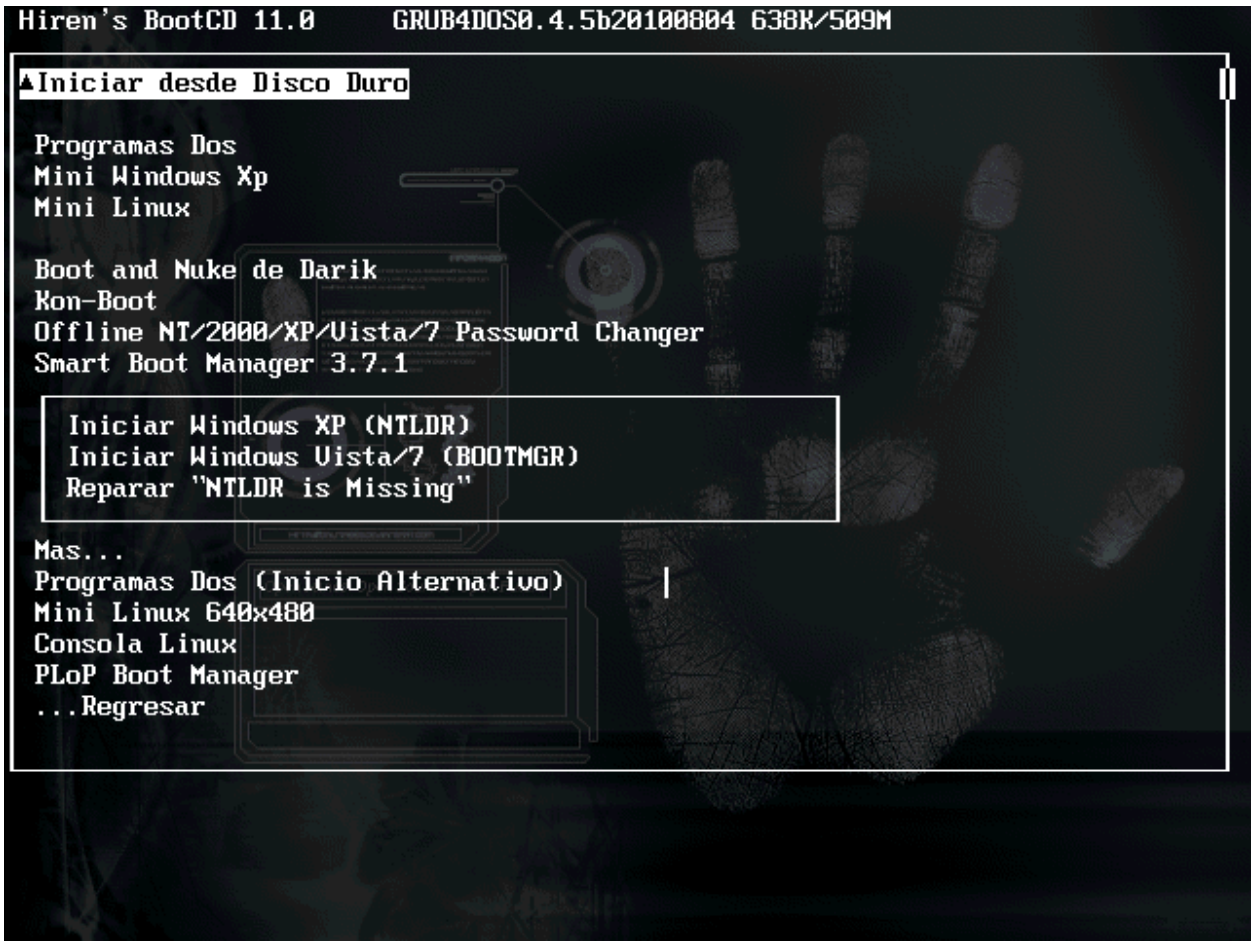
-USB tools: herramientas USB.

-Password: la capacidad de romper o eliminar contraseñas en su computadora.

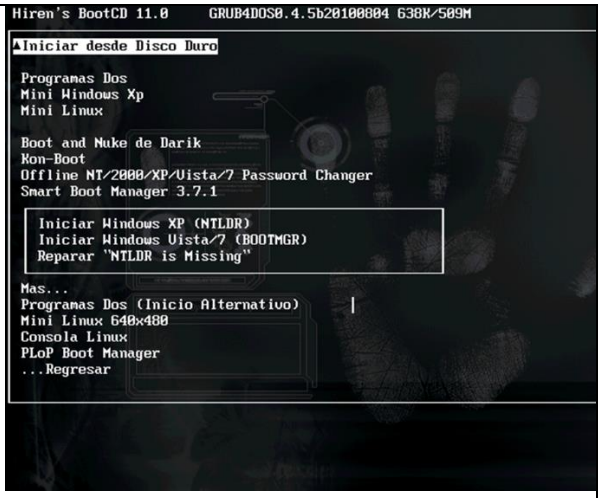
-Microsoft: herramientas de Windows activas.

-Other tools: otras herramientas.

HIRENS BOOT



Hirens Boot es una herramienta para diagnóstico de equipos que todo técnico debe utilizar o por lo menos conocer, esta herramienta es un live cd (Funciona independiente del sistema operativo que tengamos) y podamos montarlo en una memoria USB o un disco DVD.

	
Programa de arranque y recuperación de datos que se ejecuta desde una USB.	es una colección de herramientas de arranque y recuperación utilizadas para diagnosticar y solucionar problemas en sistemas informáticos.
Proporciona una amplia gama de herramientas, como particionadores de disco, antivirus, herramientas de clonación de discos, herramientas de recuperación de archivos y más.	Incluye una variedad de utilidades como antivirus, gestores de particiones, herramientas de copia de seguridad, herramientas de recuperación de datos, programas de diagnóstico del sistema, entre otros.
La interfaz de DLC Boot es intuitiva y fácil de usar. Proporciona acceso rápido a todas las herramientas a través de un menú.	Hiren's Boot presenta una interfaz basada en texto y un menú en forma de lista que permite navegar por las herramientas y seleccionar las que se deseen ejecutar.
DLC Boot es compatible con una amplia gama de sistemas operativos, incluyendo Windows XP, Windows 7, Windows 8 y Windows 10.	Hiren's Boot es compatible con sistemas operativos antiguos y nuevos, incluyendo versiones de Windows y otras plataformas.
DLC Boot es un software de pago y requiere adquirir una licencia para su uso completo.	Hiren's Boot es un software gratuito y de código abierto que puede ser utilizado sin restricciones.