

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	1/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada	

Manual de prácticas del laboratorio de Redes de Datos Seguras

Elaborado por:	Revisado por:	Autorizado por:	Vigente desde:
M.C. Cintia Quezada Reyes Ing. Magdalena Reyes Granados	M.C. Ma. Jaquelina López Barrientos Ing. Edgar Martínez Meza M.C. Cintia Quezada Reyes	Dra. Rocío Alejandra Aldeco Pérez	11 de agosto de 2023

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	2/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Índice de prácticas

Práctica 1. Construcción de cables UTP para conexión directa y cruzada	3
Práctica 2. Componentes del cableado estructurado Norma ANSI/EIA/TIA 568	12
Práctica 3. Identificación de un sistema de cableado estructurado	20
Práctica 4. Manejo de Dispositivos de Interconectividad, hub y switch	29
Práctica 5. Instalación de una red básica en las plataformas: Windows de Microsoft y Linux distribución Debian	51
Práctica 6. Encaminamiento y análisis de paquetes	77
Práctica 7. Configuración básica del router	94
Práctica 8. TCP Y UDP	116
Práctica 9. SSH: Secure Shell	139
Práctica 10. Funciones de la capa de presentación	162
Práctica 11. Servidor DHCP	173
Prácticas complementarias y obligatorias para la clase de teoría	198
Anexo. Manual para la creación de una cuenta en Skills for All para descargar y emplear Cisco Packet Tracer	469

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 3/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 1

Construcción de cables UTP para conexión directa y cruzada

Capa 1 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 4/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

1.- Objetivo de Aprendizaje

- El alumno o la alumna aprenderá a construir cables de conexión directa y cruzada empleando las normas ANSI/EIA/TIA T568-A y ANSI/EIA/TIA T568-B

2.- Conceptos teóricos

El cableado es normalmente el medio por el cual la información se mueve de un dispositivo de red a otro. El tipo de cable dependerá de diversos factores como la topología, la tecnología, el tamaño de la red, la velocidad de operación, etcétera.

La construcción del cable de red UTP de conexión directa (en inglés *straight-through*) se usa para conectar la tarjeta de red o NIC (en inglés *Network Interface Card*) de la estación de trabajo al *jack* de datos de la placa de pared o bien para conectar el *patch panel* a un *hub* o *switch Ethernet*. Las salidas de pin serán T568-B y los 8 hilos se deben terminar con conectores modulares RJ-45. Sólo 4 de los 8 hilos se usan para el estándar *Ethernet* 10/100BASE-T. Los 8 hilos se usan para el estándar *Ethernet* 1000BASE-T.

Los cables se encuentran alambrados como cables de conexión directa, ya que el cable desde la estación de trabajo hasta el concentrador se cruza normalmente de forma automática en éste último. Esto significa que los pares de emisión y recepción se cambiarán cuando el cableado llegue al concentrador (Ver Figura No. 1).

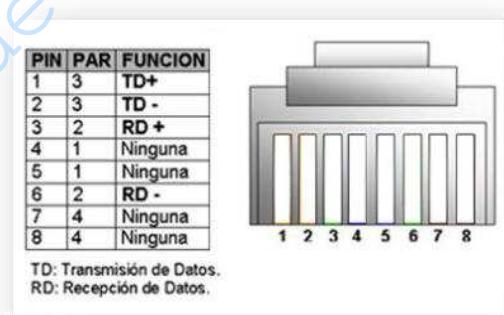


Figura No. 1. Transmisión y Recepción de Datos

Un cable de interconexión cruzada (en inglés *crossover*) se puede utilizar como cable principal para conectar dos hubs o switches en una LAN y para conectar dos estaciones de trabajo aisladas para crear una miniLAN. Esto permite conectar dos estaciones de trabajo entre sí, o una estación de trabajo con un servidor sin que sea necesario que haya un concentrador entre ellos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 5/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

El cable cruzado (*crossover*) cruza las terminales de transmisión de un lado para que llegue a recepción del otro y viceversa.

3.- Equipo y material necesario

Material del alumno o de la alumna:

- 10 conectores RJ-45 categoría 5e o superior
- 4 metros de cable UTP Categoría 5e o superior
- Pinzas de punta
- Flexómetro o cinta métrica

Equipo del Laboratorio (Ver Figura No. 2):

- Pinzas engarzadoras.
- Pinzas de corte.
- Analizador de continuidad de cableado UTP o *tester*

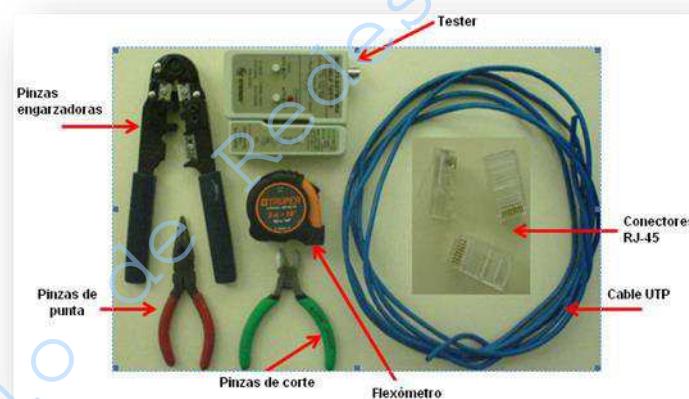


Figura No. 2. Material necesario

4.- Desarrollo:

Modo de trabajar

La construcción de los cables se realizará de manera individual.

NOTA: Las actividades en este apartado serán meramente demostrativas haciendo uso de un video como base y las explicaciones del profesor o profesora cuando la sesión de la clase se realice en modalidad a distancia.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 6/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1 Construcción de cables

El cable categoría UTP está formado de cuatro pares trenzados formando una sola unidad. Estos cuatro pares vienen recubiertos por un tubo de plástico que mantiene el grupo unido mejorando la resistencia ante interferencias externas. Es importante notar que cada uno de los cuatro pares tiene un color diferente, pero a su vez, cada par tiene un cable de un color específico y otro cable blanco con algunas franjas del color de su par.

Esta disposición de los cables permite una adecuada y fácil identificación de los mismos con el objeto de proceder a su instalación. El número de identificación de cada par referente a su color. (Ver Figura No. 3)

A continuación se construirá un cable de conexión directa de acuerdo con la configuración T568-B.

4.1.1 Cable de conexión directa T568-A y T568-B

4.1.1.1 Corte un trozo de cable de par trenzado no blindado de una longitud de 2 metros.

4.1.1.2 Retire 3 cm de la envoltura de uno de los extremos del cable.

4.1.1.3 Sostenga la envoltura y el cable, destrelle y ordene los pares de hilos de modo que cumplan con el diagrama de color del cableado T568-B (Ver Figura No. 3).

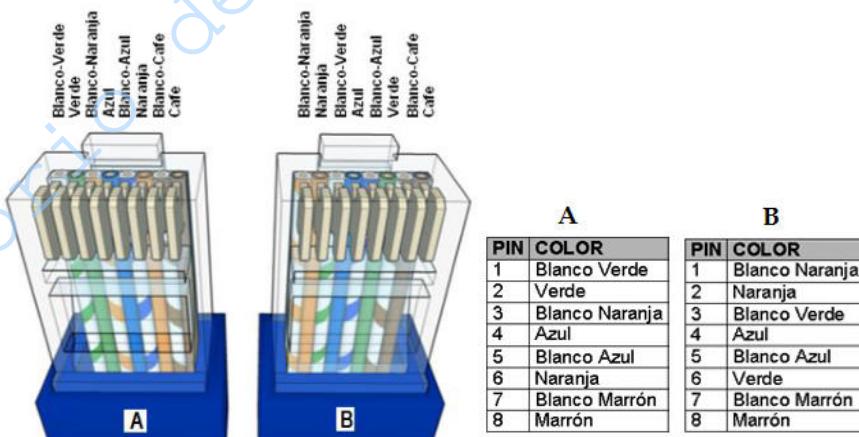


Figura No. 3. Configuración del cableado T568-A y T568-B

4.1.1.4 Aplane, enderece y haga coincidir los hilos, luego recórtelos en línea recta con una distancia de 3mm a partir del borde del forro (Ver Figura No. 4).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	7/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				



Figura No. 4 Distancia de corte de los alambres.

4.1.1.5 Coloque un conector RJ-45 en el extremo del cable, de tal forma que se cumpla la configuración correcta mostrada en la Figura No. 2.

4.1.1.6 Empuje suavemente los hilos dentro del conector hasta que pueda ver los extremos de cobre de éstos a través del extremo del conector (Ver Figura No. 5). Asegúrese de que el extremo de la envoltura del cable también esté dentro y de que todos los hilos estén en el orden correcto (Ver figura No. 5).

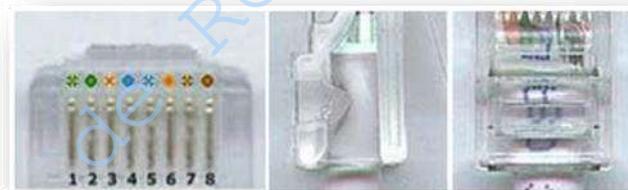


Figura No. 5. Alambres y forro en el lugar adecuado dentro del conector

4.1.1.7 Utilice las pinzas engarzadoras (Ver Figura No. 6) y apriete el conector con suficiente fuerza como para forzar los contactos a través del aislamiento en los hilos, completando así el camino conductor.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 8/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 6 Uso de las pinzas engarzadoras

4.1.1.8 Finalizando así la construcción de un extremo del cable (Ver Figura No.7).



Figura No. 7. Cable de conexión finalizado.

4.1.2 Cable de conexión cruzada (crossover)

4.1.2.1 Repita desde el paso 4.1.1.1 hasta el paso 4.1.1.7, ordenando los pares de hilos de acuerdo con el estándar de cableado T568-A para un extremo y el estándar de cableado T568-B para el otro extremo. Finalizando así el cable de conexión cruzada.

5.- Pruebas

5.1 Finalmente pruebe los cables terminados empleando el analizador de continuidad Ethernet.

5.2 En las pruebas de continuidad del multímetro o tester; si falla una conexión, el cable estará mal construido, por lo que tendrá que rehacerse nuevamente.

6.- Cuestionario

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 9/479 8.3 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1. ¿Cuál es la diferencia que existe al emplear (no al construir) el código de colores T568-A y T568-B dentro del cableado estructurado?

2. Investigue la configuración para un cable cruzado en redes de tipo Gigabit Ethernet.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	10/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

7.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	11/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 1
Construcción de cables UTP para conexión directa y cruzada
Cuestionario Previo

1. Explique la razón por la cual los alambres del cable UTP están trenzados.
2. ¿Qué es un par trenzado: UTP (UnShielded Twisted Pair) cable par trenzado no blindado (no apantallado)? Explique las características así como ventajas y desventajas.
3. ¿Qué es un par trenzado: STP (Shielded Twisted Pair) cable de par trenzado blindado (apantallado)? Explique las características así como ventajas y desventajas.
4. Mencione las categorías de cables UTP que existen. Explique más a detalle las principales aplicaciones de los cables de la categoría UTP 5e (5 enhance - mejorada) y UTP 6.
5. ¿Qué categoría de cable UTP es conveniente utilizar en nuevas instalaciones de cableado y por qué?
6. Mencione las características de otros medios de transmisión: el cable coaxial y la fibra óptica.
7. Si se va a tender un cable que transmita voz a través de cable UTP ¿Qué pines se utilizarían, cómo se armaría?
8. Investigue la configuración para un cable cruzado en redes de tipo Gigabit Ethernet
9. ¿Qué significan las normas ANSI/EIA/TIA T568-A y ANSI/EIA/TIA T568-B
10. ¿Cuál es la importancia de la capa 1 del modelo OSI?
11. Investigue costos del cable UTP categorías 5e, 6 y 6a.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	12/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 2

Componentes del cableado estructurado Norma ANSI/EIA/TIA 568

Capa 1 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	13/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivo de Aprendizaje

- El alumno o la alumna conocerá aspectos generales del cableado estructurado al aprender cómo se realiza el proceso de instalación de un *jack* y un panel de parcheo con cable UTP categoría 5e o superior.

2.- Conceptos teóricos

Un sistema de cableado estructurado es una red de cable única y completa con un tiempo largo de vida útil, flexible, que soporta cambios y crecimiento a futuro, además cumple con ciertas normas locales o internacionales. El diseño de esta infraestructura está planeado para maximizar la velocidad, eficiencia y seguridad de una red.

El diseño del sistema de cableado estructurado es independiente de la información que se transmite a través de él. De este modo es posible disponer de cualquier servicio de datos, voz, video, audio, seguridad, control y monitoreo.

Estandarización

Los organismos: ANSI, EIA y TIA publican de manera conjunta estándares para la manufactura e instalación de equipo electrónico y sistemas de telecomunicaciones. Los principales estándares que se refieren al cableado de telecomunicaciones en edificios son:

- ANSI/EIA/TIA 568-A: Alambrado de Telecomunicaciones para Edificios Comerciales.
- ANSI/EIA/TIA 569: Rutas y Espacios de Telecomunicaciones para Edificios Comerciales.
- ANSI/EIA/TIA 606: Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.
- ANSI/EIA/TIA 607: Requerimientos de Puesta a Tierra y Puenteado de Telecomunicaciones para Edificios Comerciales.

Norma ANSI/EIA/TIA 568-A

Especifica los requerimientos mínimos del cableado de espacios de oficinas, incluyendo las salidas y los conectores para que soporte distintos tipos de edificios así como aplicaciones de usuario, parámetros de medios de comunicación que determinan el rendimiento.

Establece que un sistema de cableado estructurado consta de seis subsistemas funcionales:

1. Subsistema de cableado horizontal.
2. Subsistema de cableado vertical (*backbone*).
3. Subsistema de área de trabajo.
4. Subsistema de cuarto de telecomunicaciones.
5. Subsistema de cuarto de equipos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 14/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

6. Subsistema de entrada de servicios.

3.- Equipo y material necesario (Figuras No. 1a y 1b)

Material del alumno o de la alumna:

- 1 metro de cable UTP categoría 5e o superior.
- 2 conectores hembra (*jacks*) RJ-45 categoría 5e o superior similares a los de la Figura No. 1a.

NOTA: Evite adquirir los conectores hembra (*jacks*) RJ-45 que su vía de conexión sea a presión y por ende no empleen herramientas de impacto.



Figura No. 1a. Jacks

- 1 cable de conexión directa (construido en la práctica 1)
- 1 cable de conexión cruzada (construido en la práctica 1)
- Flexómetro o cinta métrica

Equipo del Laboratorio:

- 1 panel de parcheo
- 1 pinza de impacto
- Pinzas de corte
- Pinzas de punta
- Analizador de continuidad de cableado UTP o tester

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 15/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

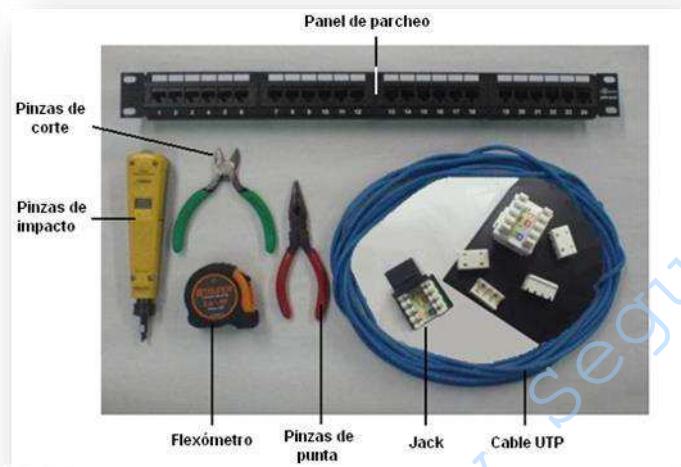


Figura No. 1b. Material necesario

4.- Desarrollo:

Modo de trabajar

La construcción del *jack* RJ-45 y del panel de parcheo se realizará de manera individual.

NOTA: Las actividades en este apartado serán meramente demostrativas haciendo uso de un video como base y las explicaciones del profesor o profesora cuando la sesión de la clase se realice en modalidad a distancia.

4.1 Instalación del *jack* RJ-45

A continuación se explicará la instalación del *jack* RJ-45 utilizando la configuración según la norma T568-B.

- 4.1.1** Retire 3 cm del forro de ambos extremos del cable.
- 4.1.2** Sin destrenzar completamente los hilos insértelos en cada uno de los canales del *jack* RJ45 siguiendo la configuración T568-B indicada en el *jack* (Ver Figura No. 2).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	16/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

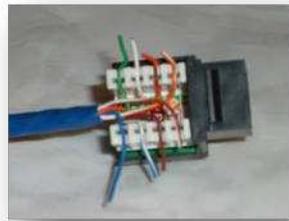


Figura No. 2. Construcción del jack

- 4.1.3** Utilice la pinza de impacto para introducir los hilos del cable hasta el fondo de cada canal y para cortar el excedente de cable (Ver Figura No. 3).



Figura No. 3. Uso de las pinzas de impacto

4.2 Instalación del panel de parcheo

La instalación se llevará a cabo según lo indique la profesora o el profesor.

5.- Pruebas

- 5.1** Realice las conexiones necesarias para comprobar la continuidad con el tester.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 17/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Cuestionario

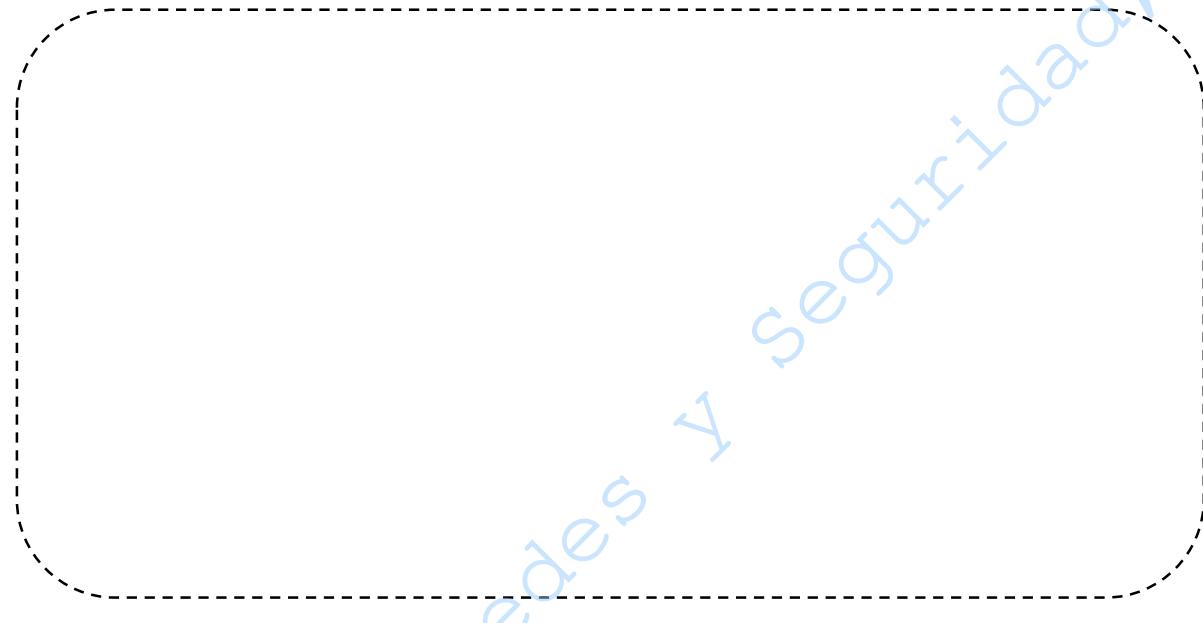
1. ¿Cuál es el estándar que regula a nivel internacional el sistema de cableado estructurado?

2. Explique con sus propias palabras el concepto de **cableado estructurado**.

3. ¿Cuál es la distancia máxima que puede tener el cableado horizontal?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	18/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4. Dibuje la conexión realizada en el laboratorio para probar tanto la construcción del *jack RJ-45* como la del panel de parcheo.



7.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	19/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 2

Componentes del cableado estructurado Norma ANSI/EIA/TIA 568

Cuestionario Previo

1. ¿Cuál es la función de las siguientes organizaciones: ANSI, EIA y TIA?
2. Mencione las características de los seis subsistemas funcionales que conforman el cableado estructurado.
3. ¿Qué es un panel de parcheo?
4. ¿Qué es un rack?
5. ¿Qué es un jack?
6. ¿Qué es una roseta?
7. ¿Qué es una placa de pared y cuál es su utilidad?
8. ¿Qué es un patch cord y cuál es su objetivo principal?
9. Investigue costos de patch panels, placas de pared y pinzas de impacto
10. Realice un diagrama mostrando la trayectoria de conexiones desde el equipo de cómputo en el área de trabajo hasta el equipo activo ubicado en el cuarto de telecomunicaciones. Haga uso de los elementos que indica el cableado estructurado (rosetas, canaletas, rack, panel de parcheo, etcétera.)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 20/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 3

Identificación de un sistema de cableado estructurado

Capa 1 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	21/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

-
- El alumno o la alumna aplicará los estándares ANSI/EIA/TIA 568 y ANSI/EIA/TIA 569 para el diseño de una red de datos con cableado estructurado.
- El alumno o la alumna identificará los subsistemas del cableado estructurado.

2.- Conceptos teóricos

Un sistema de cableado estructurado puede proporcionar soluciones a las necesidades de comunicación de una organización. Estos sistemas de cableado pueden soportar múltiples ambientes de cómputo y aplicaciones, simplificar las tareas de administración, ahorrar costos y permitir la migración transparente a nuevas tecnologías y topologías sin necesidad de realizar costosas actualizaciones en la infraestructura de comunicaciones.

El cableado estructurado permite la implementación planeada y ordenada de la infraestructura de cable que conecta equipo de cómputo, teléfonos, comutadores, equipo de procesamiento y sistemas de control de calefacción, ventilación, iluminación, etcétera.

Una red de computadoras es un sistema de interconexión entre equipos que permite compartir recursos e información; para ello, es necesario contar no sólo con las computadoras, también con tarjetas de red, cables de conexión, dispositivos periféricos y el software conveniente.

Inicialmente, la instalación de una red se realiza con el objetivo de compartir dispositivos e información, pero a medida que crece, permite el enlace entre personas mediante diversas aplicaciones, como el correo electrónico, mensajes instantáneos, etcétera.

Las redes se clasifican de acuerdo con su alcance geográfico en PAN, LAN, MAN y WAN. Una red de área local está formada por computadoras, periféricos y los elementos de conexión de los mismos.

Las computadoras pueden desarrollar dos funciones: como servidores o estaciones de trabajo. Los elementos de conexión son los cables, tarjetas de red y los dispositivos de interconectividad como los hubs.

Dentro de los cables de conexión se tienen: el cable UTP, que consiste en dos hilos trenzados en forma independiente y recubiertos de una capa aislante, y que es considerado de fácil instalación; el cable STP, consistente en dos hilos trenzados en forma independiente y recubiertos de una malla metálica que ofrece una protección contra las interferencias externas; el cable coaxial, hilo de cobre envuelto en una malla trenzada, separado por un material aislante; y, finalmente, la fibra óptica, formada por un núcleo de material transparente fino cuyo funcionamiento se basa en la transmisión de las refracciones de luz.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	22/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

En la actualidad, en el mundo de los sistemas de cableado estructurado existen diferentes tipos de servicios, por ejemplo, voz, datos, video, monitoreo, control de dispositivos, etcétera; éstos pueden transmitirse sobre un mismo tipo de cable. El estándar más conocido de cableado estructurado está definido por la EIA/TIA, y específicamente sobre el cable de par trenzado UTP de categoría 5e, 6 y 6a, estos estándares son: EIA/TIA 568A y EIA/TIA 568B.

Los dispositivos de interconexión proporcionan la capacidad de extender la distancia de cobertura de una LAN, interconectar redes distantes o distintas y acceder a recursos centralizados; de la misma manera, reducen los dominios de colisión y mejoran el rendimiento de las redes.

3.- Equipo y material necesario

Material del alumno o de la alumna:

- Flexómetro
- Plumones de punto fino , lápices o plumas de colores
- Regla
- Hojas blancas

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en equipos.

NOTA: Las actividades en este apartado serán realizadas haciendo uso de un video como base y las explicaciones del profesor o profesora cuando la sesión de la clase se realice en modalidad a distancia.

4.1 Identificación del cableado estructurado en el laboratorio

En este ejercicio el alumno o la alumna pondrá en práctica los conocimientos adquiridos en la clase teórica sobre los distintos subsistemas que componen un sistema de cableado estructurado, aplicando las normas y utilizando los componentes que requiere cada subsistema para identificar su implementación en un espacio real.

Esta primera parte consiste en analizar las características del cableado estructurado implementado en la red LAN Ethernet del Laboratorio de Redes y Seguridad. Se analizará la trayectoria que sigue el cable desde un nodo a través de la canaleta, hasta llegar al rack, donde es distribuido por el panel de parcheo y enlazado con cables patch cord al switch. También se identificarán, de ser posible, los 6 diferentes subsistemas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	23/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Actividades:

4.1.1 Emplee el flexómetro para medir el laboratorio, utilice la regla y los colores para realizar un diagrama físico de la red del Laboratorio indicando los subsistemas del cableado estructurado a detalle y mostrando la ubicación de los equipos dentro del espacio geográfico, remarcando las conexiones con los jacks, número de nodos y cómo el cable UTP viaja a través de las canaletas hasta llegar al rack. El diagrama debe presentar las longitudes, así como el nombre específico y direcciones IP de los hosts que integran a la red.

EJERCICIO OPCIONAL: Anexe una hoja con el diagrama de red detallado del laboratorio, se debe presentar y entregar al profesor o a la profesora de manera clara, limpia, con conexiones legibles, líneas de colores que representen los distintos subsistemas del cableado.

4.1.2 Empleando la fórmula que permite calcular la cantidad de cables que puede albergar una canaleta, indique qué canaletas son las adecuadas para mantener el cableado estructurado dentro del laboratorio y cuál sería el costo respectivo si se deseara cambiarlas para que la instalación contara con nuevas canaletas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	24/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.1.3 Realice las mediciones correspondientes para saber la longitud del cable que se requiere para realizar la conexión de cada nodo (considere medir desde el jack hasta el patch panel).

¿A qué subsistema del cableado estructurado se hace referencia con esta actividad? ¿Por qué?

Realice una tabla donde indique el número de nodo y la longitud del cable (Tabla 1)

Tabla 1. Nodos y longitud del cable

Número de nodo	Longitud del cable
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	25/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

¿Es conveniente colocar canaletas en el laboratorio? Justifique su respuesta.

4.1.4 Identifique en el rack del laboratorio los diversos dispositivos que se utilizan para que la red funcione

¿A qué subsistema del cableado estructurado se hace referencia con esta actividad? ¿Por qué?

¿Qué dispositivos identificados son activos y cuáles pasivos? Justifique su respuesta

¿Qué tipo de cable se emplea para realizar un patch cord? ¿Cuál es la razón principal?

¿Cuál es la longitud de los patch cords? ¿Por qué?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	26/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Cuestionario

1. ¿Qué requisitos debe cumplir el cuarto de telecomunicaciones?

2. ¿Cuál es la máxima capacidad de llenado (en porcentaje) para las canalizaciones por superficie?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 27/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

3. ¿Qué características debe tener la entrada al edificio?

4. ¿Cuál es la distancia mínima que debe existir entre una canaleta y el piso?

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	28/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA 3
Diseño de un sistema de cableado estructurado
Cuestionario Previo

1. ¿Cuáles son los medios para canalizaciones admitidos por el estándar ANSI/EIA/TIA 569?
2. ¿Qué es una escalera por techo? Indique sus características y objetivos
3. ¿Qué componentes se encuentran en un cuarto de telecomunicaciones?
4. ¿Qué topología usa un sistema de cableado estructurado?
5. ¿Cuáles son las características principales de los 6 subsistemas del cableado estructurado? Indíquelas
6. Realice un dibujo donde identifique claramente los 6 subsistemas del cableado estructurado en un edificio
7. ¿Qué es un equipo activo? Liste ejemplos
8. ¿Qué es un equipo pasivo? Liste ejemplos
9. ¿Qué tipos de canaletas existen? Realice una tabla indicando tipo, características y costos
10. Investigue cuál es la fórmula que permite calcular la cantidad de cables que puede albergar una canaleta
11. ¿A qué se hace referencia cuando se menciona la regla 5-4-3?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 29/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

Práctica 4

Manejo de Dispositivos de Interconectividad, hub y switch

Capas 1 y 2 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	30/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno o la alumna manipulará equipos de interconexión como lo son los hubs y switches.
- El alumno o la alumna analizará el comportamiento del hub y del switch al momento de transmitir información mediante la herramienta de simulación de redes Cisco Packet Tracer.

2.- Conceptos teóricos

Para un administrador de red, es necesario e indispensable conocer los equipos, mecanismos y técnicas para extender las capacidades de las redes que están bajo su cargo. En algunas ocasiones es necesario extender físicamente una red para añadir nuevas estaciones así como para interconectarlas a una LAN con localización geográfica distinta. De igual forma, es conveniente planear el crecimiento de una LAN en términos de ancho de banda para hacer frente a necesidades de comunicación actuales.

La extensión de las capacidades de una red, se logra mediante dispositivos hardware definidos para cada uno de los tipos de redes, en el caso de las LAN encontramos los *hubs*, *switches*, repetidores, puentes, *access point*; para las redes *MAN*, tenemos repetidores, canalizadores, módems analógicos, modéms cable; en el caso de las redes *WAN*, encontramos routers, multicanalizadores, módems satelitales, etc.

Hub

Dispositivo que opera en la capa 1 del modelo OSI que tiene la finalidad de interconectar a los dispositivos finales en una red de datos mediante la transmisión de paquetes a todos y cada uno de los hosts conectados no importándole cuál sea el destinatario.

El *hub* es un dispositivo activo que actúa como elemento central. Cada estación se conecta al *hub* mediante dos enlaces: transmisión y recepción. El *hub* actúa como un repetidor: cuando transmite una única estación, el *hub* replica la señal en la línea de salida hacia cada host conectado. Regularmente el enlace consiste en dos pares trenzados no apantallados. Dada la alta velocidad y baja calidad de transmisión del par trenzado no apantallado, la longitud de un enlace está limitada a un entorno de 100m. Como alternativa se puede usar un enlace de fibra óptica en cuyo caso la longitud máxima es del orden de 500m.

Varios niveles de hub se pueden colocar en cascada formando una configuración jerárquica, teniendo un hub raíz denominado HHUB, Encabezado Hub (Header Hub) y uno o más hubs intermedios denominados IHUB, Hub Intermedios (Intermediate Hub). Esta estructura se adapta bien a edificios cableados donde regularmente existe un armario de interconexiones en cada planta del edificio.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	31/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Existen hubs pasivos y activos, los primeros sólo interconectan dispositivos mientras que los segundos además regeneran la señal recibida, como si fuera un repetidor, de ahí la denominación de repetidor multipuerto.

Switch

Dispositivo que opera en la capa 2 del modelo OSI que tiene el fin de integrar a los equipos finales en una red de datos, empleando la transmisión de paquetes únicamente al destinatario seleccionado para transmitir.

Un switch es un dispositivo hardware que incluye componentes similares a una computadora personal: CPU, RAM y un IOS, Sistema Operativo de Red (Internetworking Operating System). Puede ser administrado de la misma forma que un router o bien mediante una consola conectada a un puerto ya sea por Telnet o bien vía FTP.

Estos dispositivos de interconexión corresponden con la capa de enlace de datos, regularmente son implementados para preservar el ancho de banda de la red al utilizar la segmentación, ya que reenvían paquetes a un segmento en particular, utilizando el direccionamiento de hardware MAC.

Los *switches* pueden ser clasificados de acuerdo con la técnica que emplean, para el reenvío de los paquetes al segmento apropiado en:

- *Store-and-forward*, en esta técnica los switches procesan completamente el paquete incluyendo el campo del algoritmo CRC y la determinación del direccionamiento del paquete. Esto requiere el almacenamiento temporal del paquete antes de ser enviado al segmento apropiado. Su principal ventaja es la eliminación del número de paquetes dañados que son enviados a la red.
- *Cut-through*, esta técnica implementada por los switches hace que sean más rápidos, debido a que envían los paquetes tan pronto la dirección MAC es leída.

El switch implementado en el Laboratorio utiliza la primera técnica: store and forward.

3.- Equipo y material necesario

Material del alumno o de la alumna:

- Un cable directo, norma B construido en la práctica 1.

Equipo del Laboratorio:

- Software de simulación de redes Cisco Packet Tracer.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	32/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada	

- Software Analizador de paquetes Wireshark
- Switches Ethernet, FastEthernet o Gigabit Ethernet
- Hub

4.- Desarrollo:

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Análisis del rendimiento de un hub

- 4.1.1** Encienda el sistema y elija la opción de cargar *Windows*.
- 4.1.2** Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3** El hub extiende la funcionalidad de la red para que el cableado pueda ser extendido a mayor distancia, por eso su nombre de repetidor. El problema es que el hub transmite los broadcasts a todos los puertos que contenga, esto es, si contiene 8 puertos todos los nodos que estén conectados recibirán la misma información, siendo innecesario y excesivo.
- 4.1.4** Ejecute la aplicación Cisco Packet Tracer. (Ver Figura No. 1)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 33/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

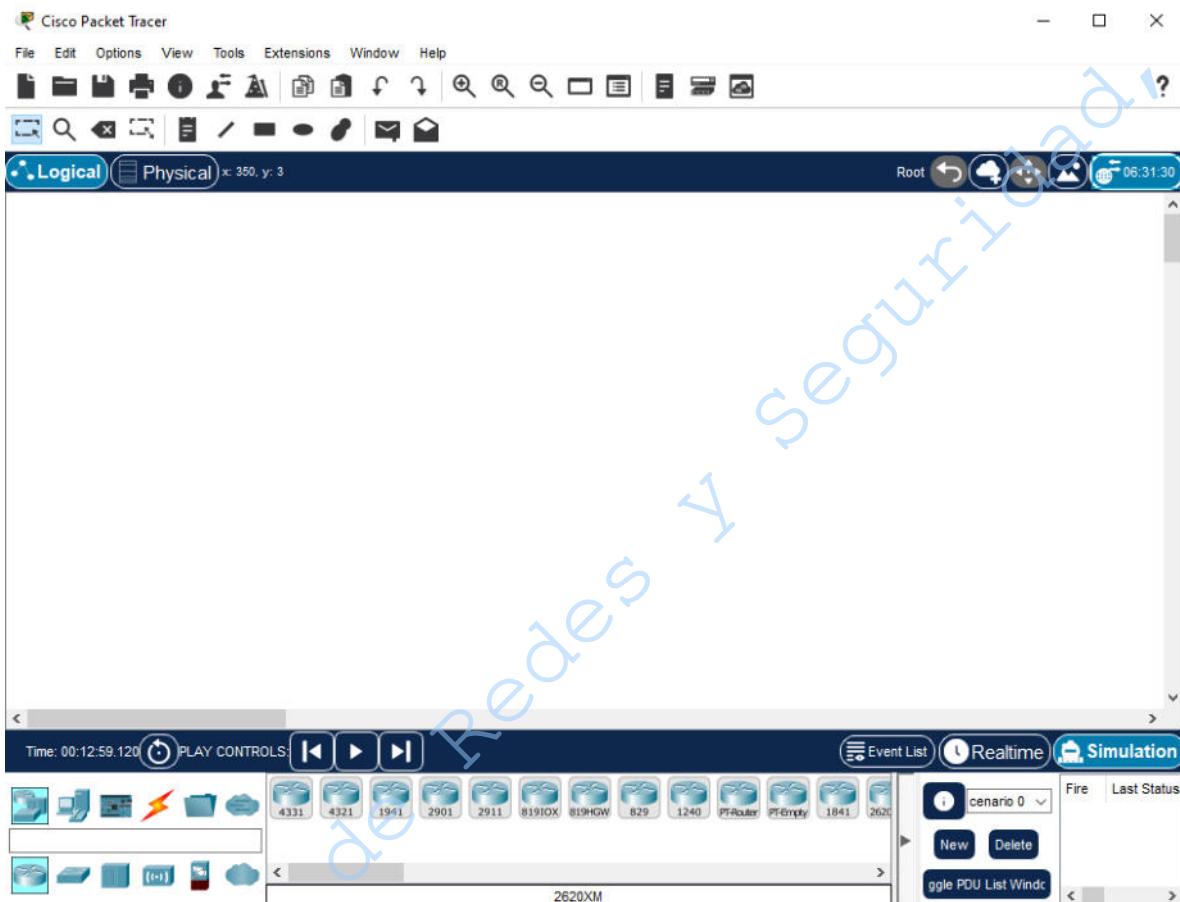


Figura No. 1. Simulador de CISCO Packet Tracer

El objetivo de la Figura No. 2 será conocer la aplicación y los elementos importantes:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 34/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

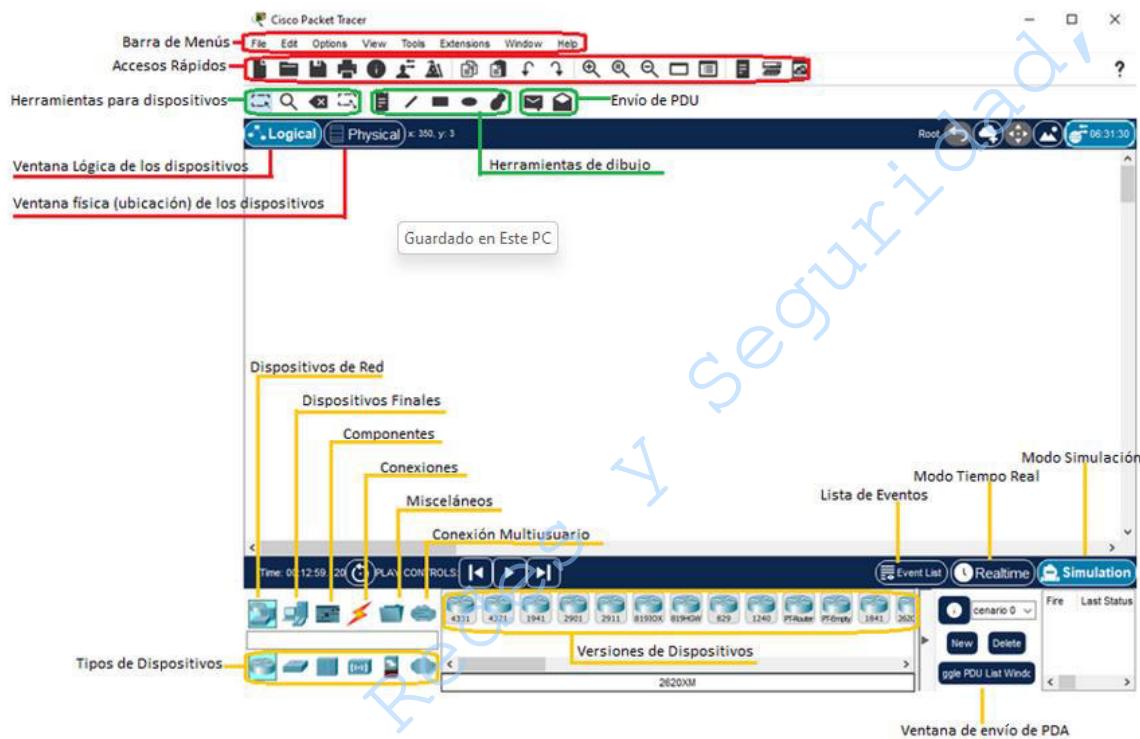


Figura No. 2. Área de trabajo del Simulador de CISCO Packet Tracer

El objetivo de este segundo punto es crear una topología en el área de trabajo

- 4.1.5** Arrastre un switch 2950-24, un hub-PT y 6 PC (la PC puede encontrarse en la opción End Devices en la sección marcada como Dispositivos y medios de transmisión) al área de trabajo de Packet Tracer y construya la topología de la figura No. 3, atendiendo las indicaciones de su profesora o profesor.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 35/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

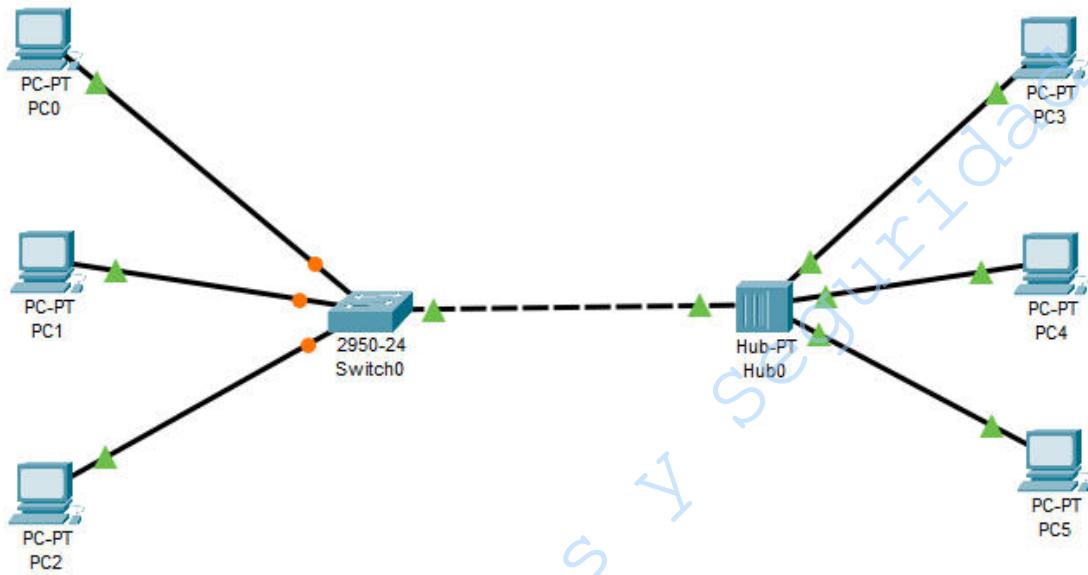


Figura No. 3 Creando la topología en Cisco Packet Tracer.

4.1.6 Dé clic sobre una PC y vaya a la pestaña de Desktop (ver Figura No. 4).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 36/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

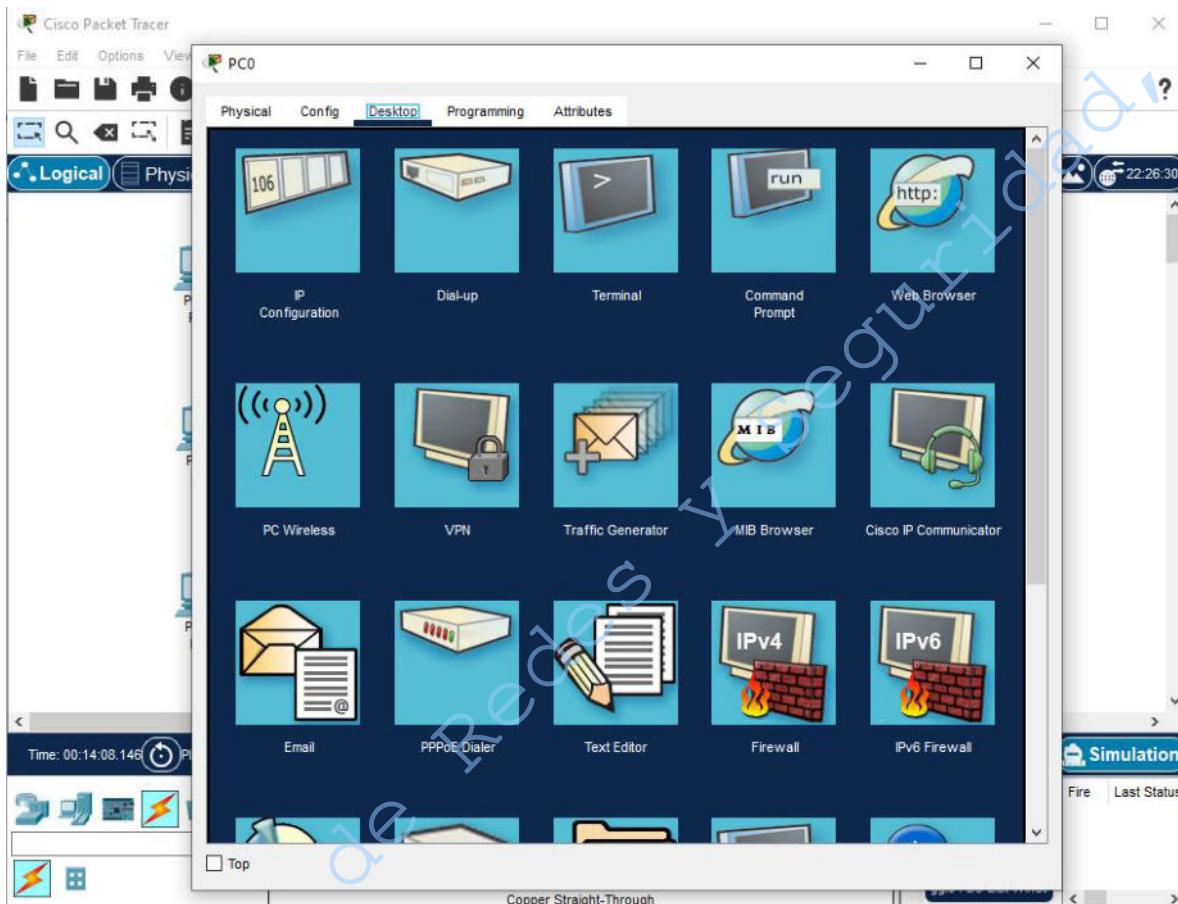


Figura No. 4 Pestaña de configuración de dispositivo.

- 4.1.7** Dé clic sobre la opción IP configuration y coloque la dirección IP y máscara de subred designadas por su profesora o profesor (ver Figura No. 5).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 37/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

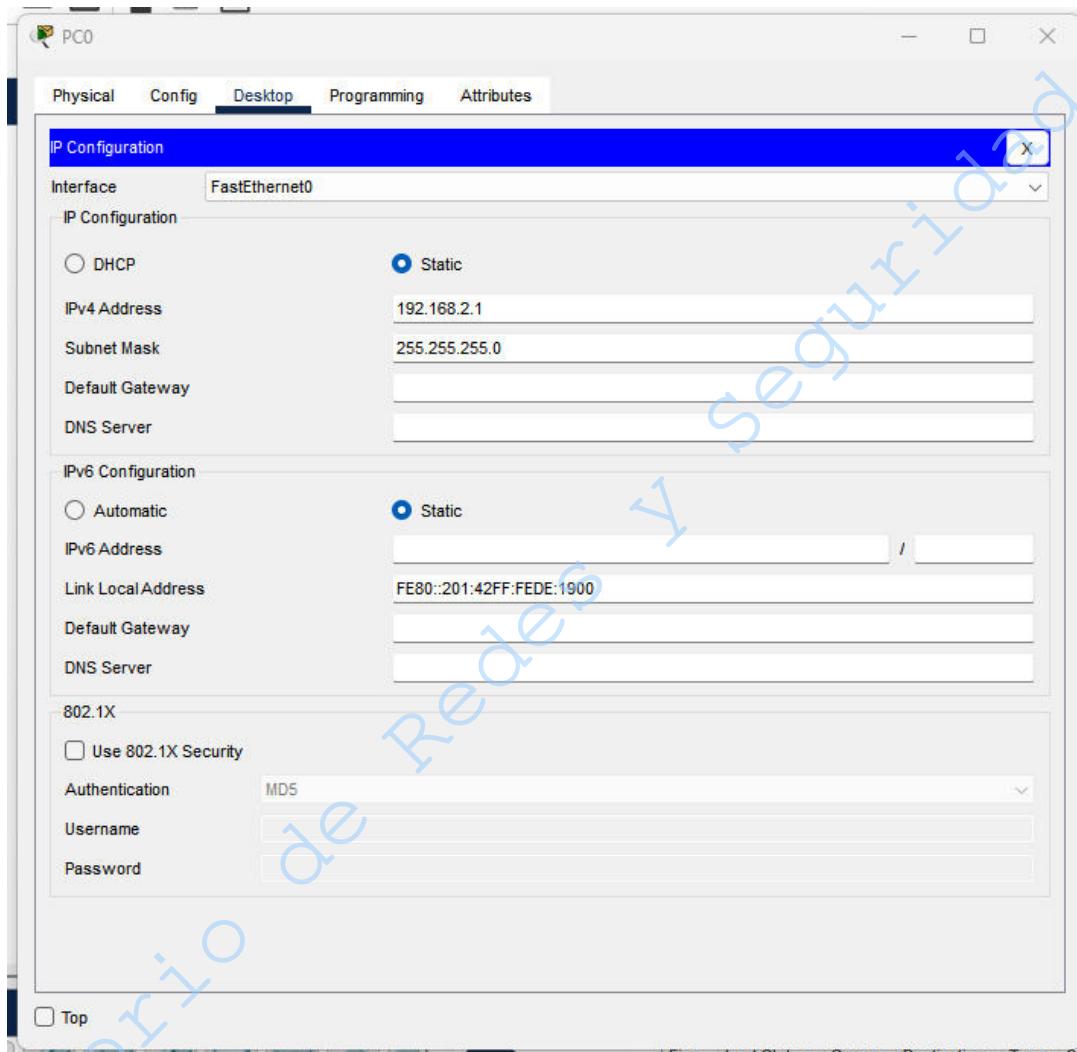


Figura No. 5 Configuración de direcciones.

4.1.8 Repita los pasos 4.1.6 y 4.1.7 para las cinco PC restantes.

4.1.9 Vaya a la pestaña Simulation en el ángulo inferior derecho del área de trabajo de Packet Tracer (ver figura No. 6a), y edite el filtrado de protocolos al dar clic en el botón Show All/None para limpiar los protocolos visibles durante la simulación. A continuación dé clic en el botón Edit Filters y seleccione únicamente el protocolo ICMP (Figura 6b).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 38/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

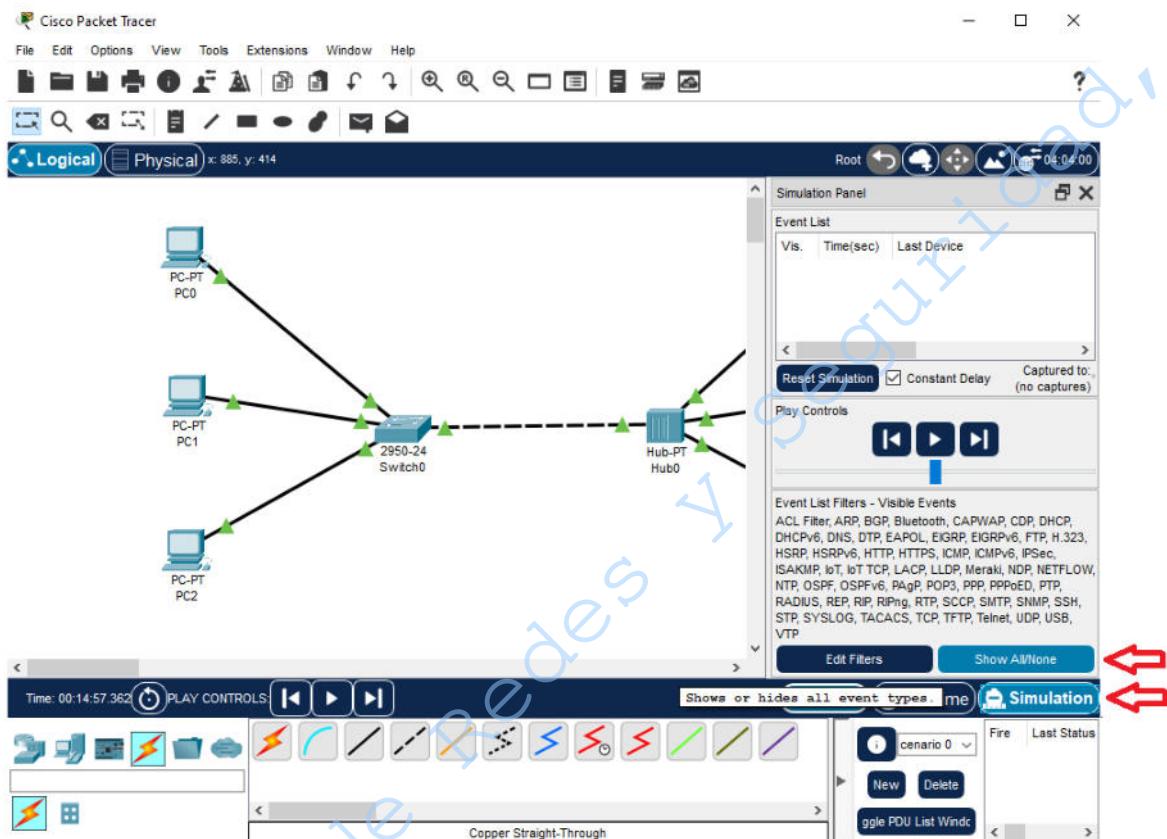


Figura No. 6a Pestaña de simulación de Packet Tracer.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 39/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

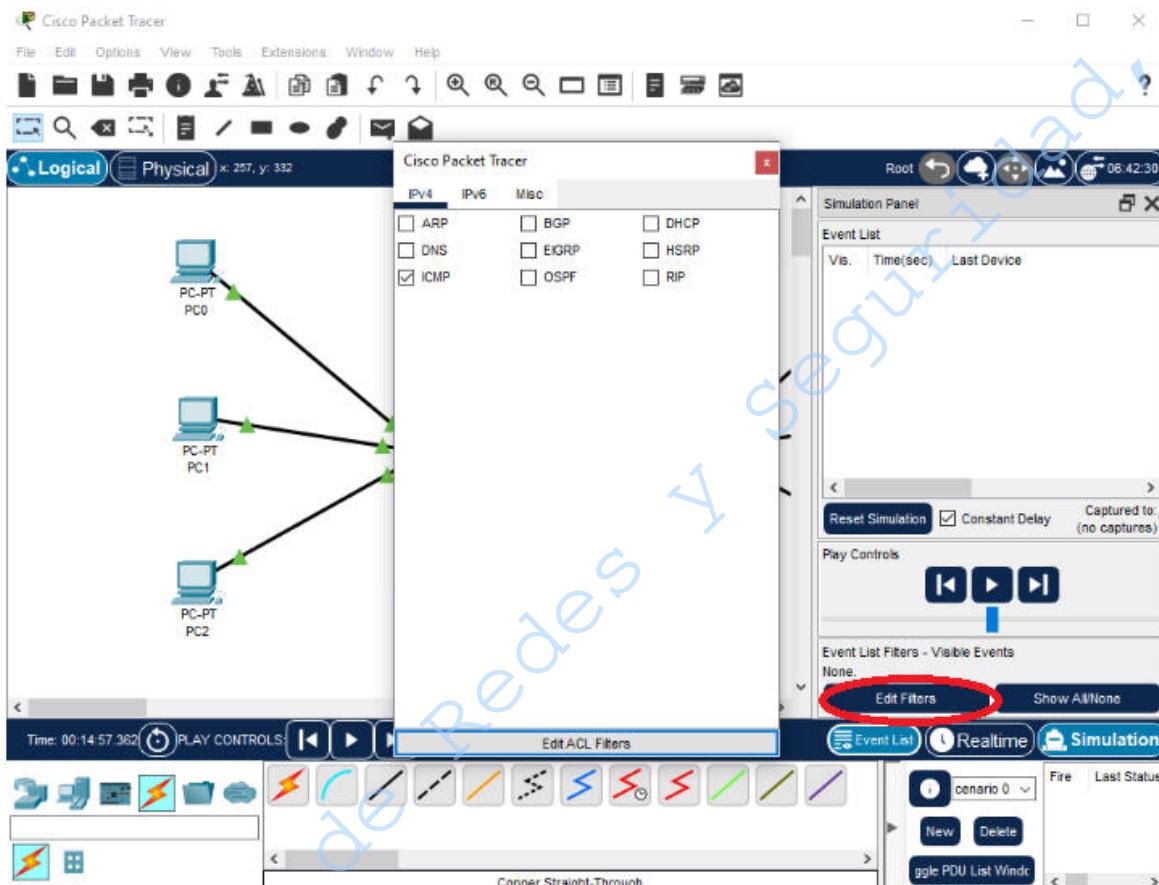


Figura No. 6b Edición de filtros.

4.1.10 En seguida dé clic sobre Add Simple PDU (P) que se encuentra en la barra de herramientas a la derecha del área de trabajo (Figura No. 7).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 40/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

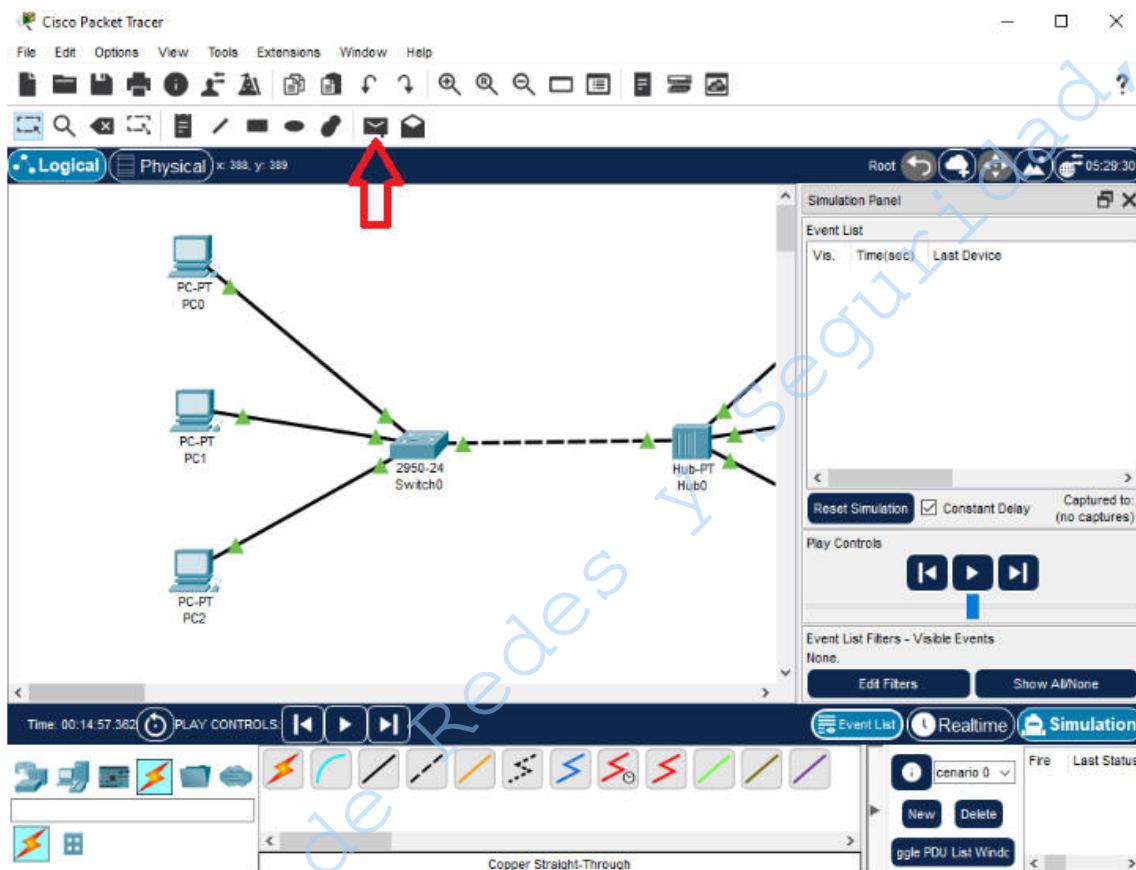


Figura No. 7 Add Simple PDU (P)

4.1.11 Dé clic sobre una PC y a continuación sobre otra PC diferente.

4.1.12 Presione el Botón If last evento, capture then forward en la sección Play controls para comenzar la simulación (ver figura No. 8).



Figura No. 8 Simulación de Packet Tracer en curso.

4.1.13 Repita los pasos 4.1.10 a 4.1.12 para comunicar diferentes parejas de PC simultáneamente. Comente lo que sucede cuando hay varias comunicaciones en el switch.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	41/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.1.14** Comente lo que sucede cuando hay varias comunicaciones en el hub. ¿Por qué sucede esto?

4.2 Configuración y análisis de una red cableada por medio de un switch y una red cableada por medio de un hub.

- 4.2.1** En este punto el laboratorio se dividirá en dos equipos según sea indicado por la profesora o el profesor, cada equipo realizará la siguiente actividad con el dispositivo que se le sea asignado.
- 4.2.2** Conecte el dispositivo asignado (hub o switch, según sea el caso) a una roseta
- 4.2.3** Conecte las PC al dispositivo asignado (hub o switch, según sea el caso)
- 4.2.4** Emplee la ventana de comandos para verificar mediante el comando ipconfig que todas las PC conectadas a dicho dispositivo tengan una dirección IP con el mismo segmento de red, así como con la misma máscara de subred.
- 4.2.5** Designe una máquina como servidor.
- 4.2.6** Abra el analizador de paquetes Wireshark, seleccione la opción Captura, luego Opciones y configure de la siguiente manera (Ver Figura No. 9):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 42/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

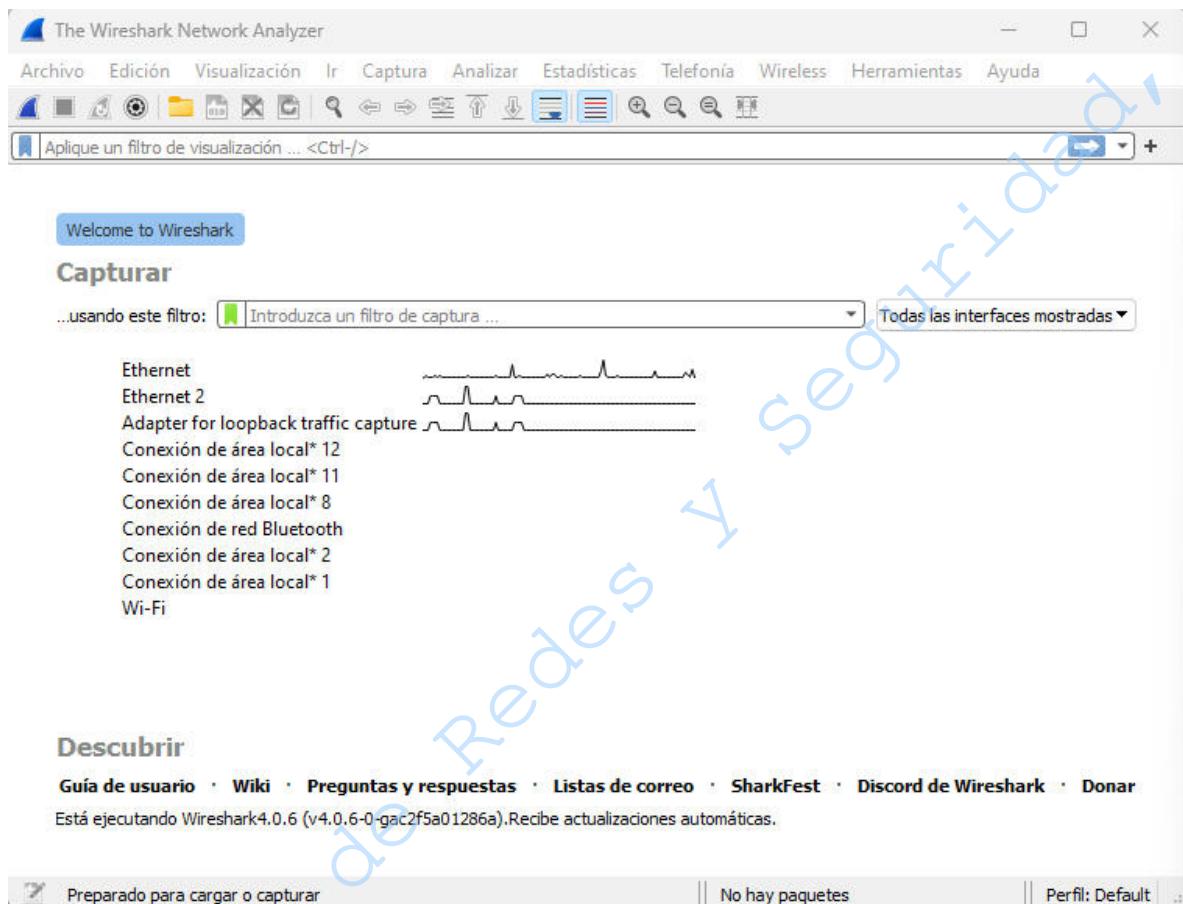


Figura No. 9 Iniciando una captura.

- 4.2.7** En la pantalla anterior seleccione y habilite la tarjeta de red que está usando (interface) dando doble clic sobre ella. Verifique que empiece a capturar el tráfico de la red (Figura No. 10) de no ser así, deberá seleccionar otra tarjeta de red, evite seleccionar aquellas que correspondan a las tarjetas inalámbricas o virtuales.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 43/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

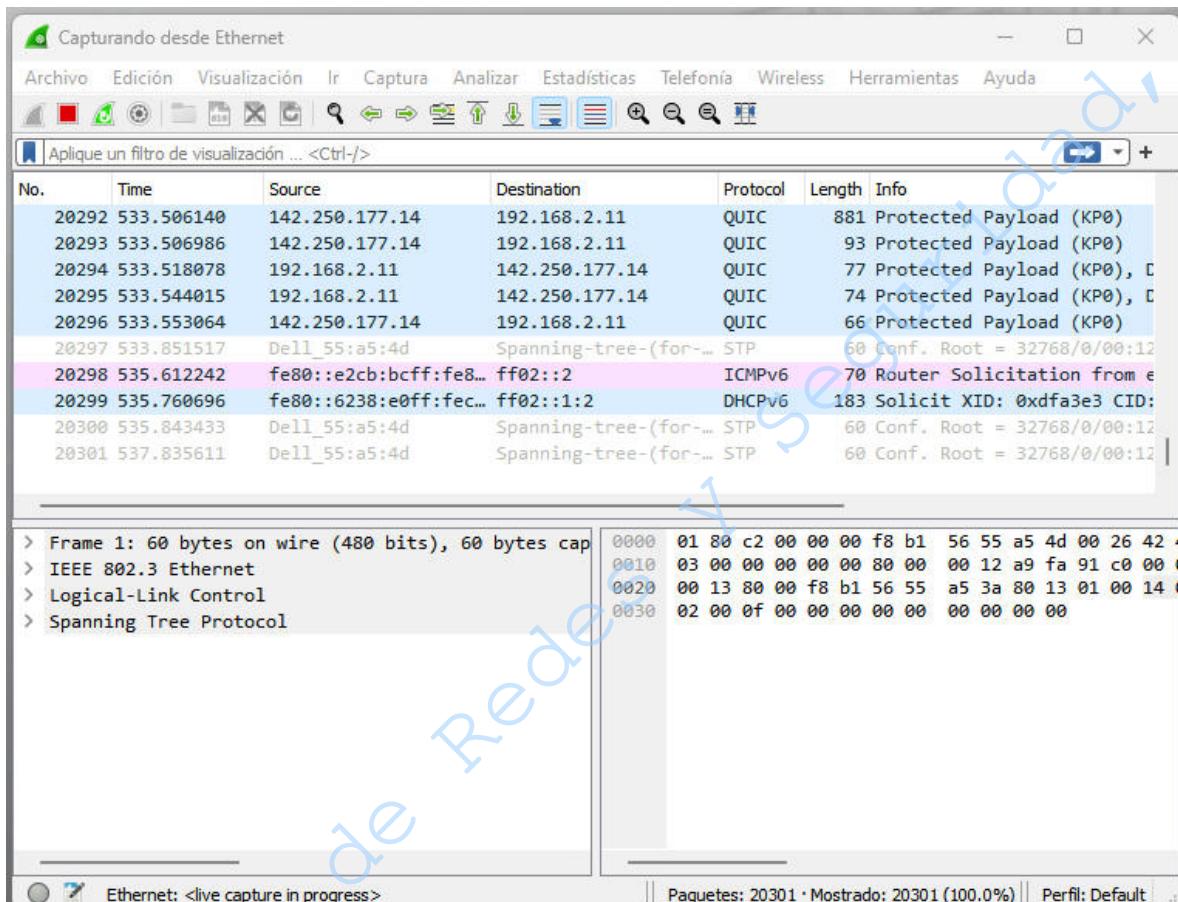


Figura No. 10 Iniciando una captura.

4.2.8 Despues de esto verifique que la captura en modo promiscuo esté activada, para ello seleccione la opción Edición, despues Preferencias y por ultimo Captura (Use Capturar paquetes en modo promiscuo) y presione start (Figura No. 11).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 44/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

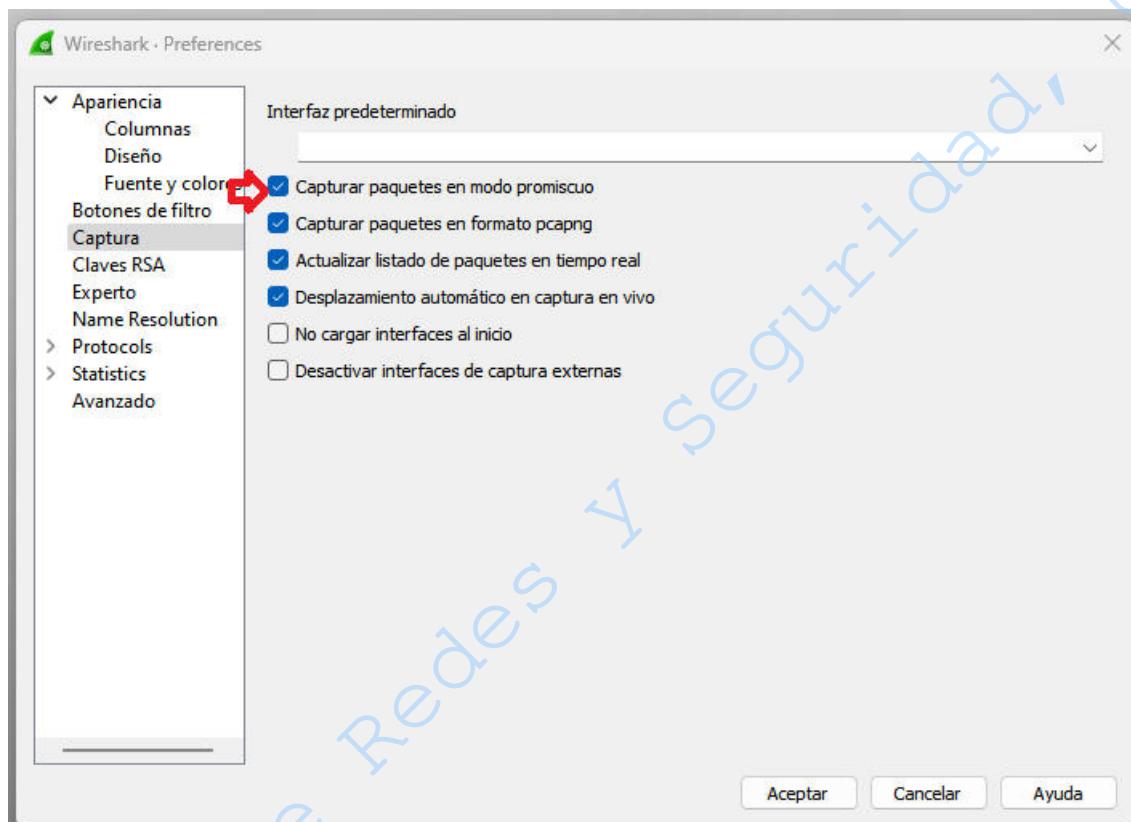


Figura No. 11. Modo Promiscuo.

4.2.9 Descargue una imagen o un video desde alguna otra computadora conectada al mismo dispositivo de la siguiente manera:

4.2.9.1 Cree una carpeta con el nombre que desee dentro de la unidad c:

4.2.9.2 Descargue una imagen o un video y guárdelo dentro de la carpeta que creó en el paso anterior.

4.2.9.3 Dé clic secundario en el ícono de la carpeta que acaba de crear, seleccione las propiedades.

4.2.9.4 Dé clic en la pestaña Uso compartido. Seleccione el botón que dice Compartir. (Ver Figura No. 12)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 45/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

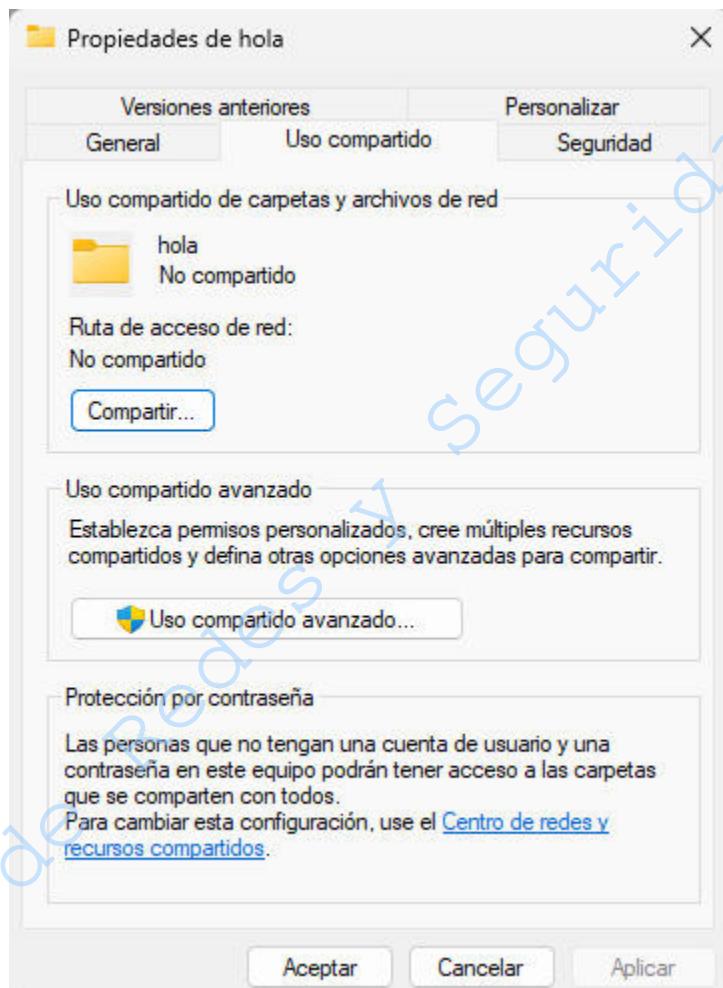


Figura No. 12. Propiedades de la carpeta

4.2.9.5 Seleccione Everyone o Todos y dé clic en el botón Agregar. (Ver Figura No. 13)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 46/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

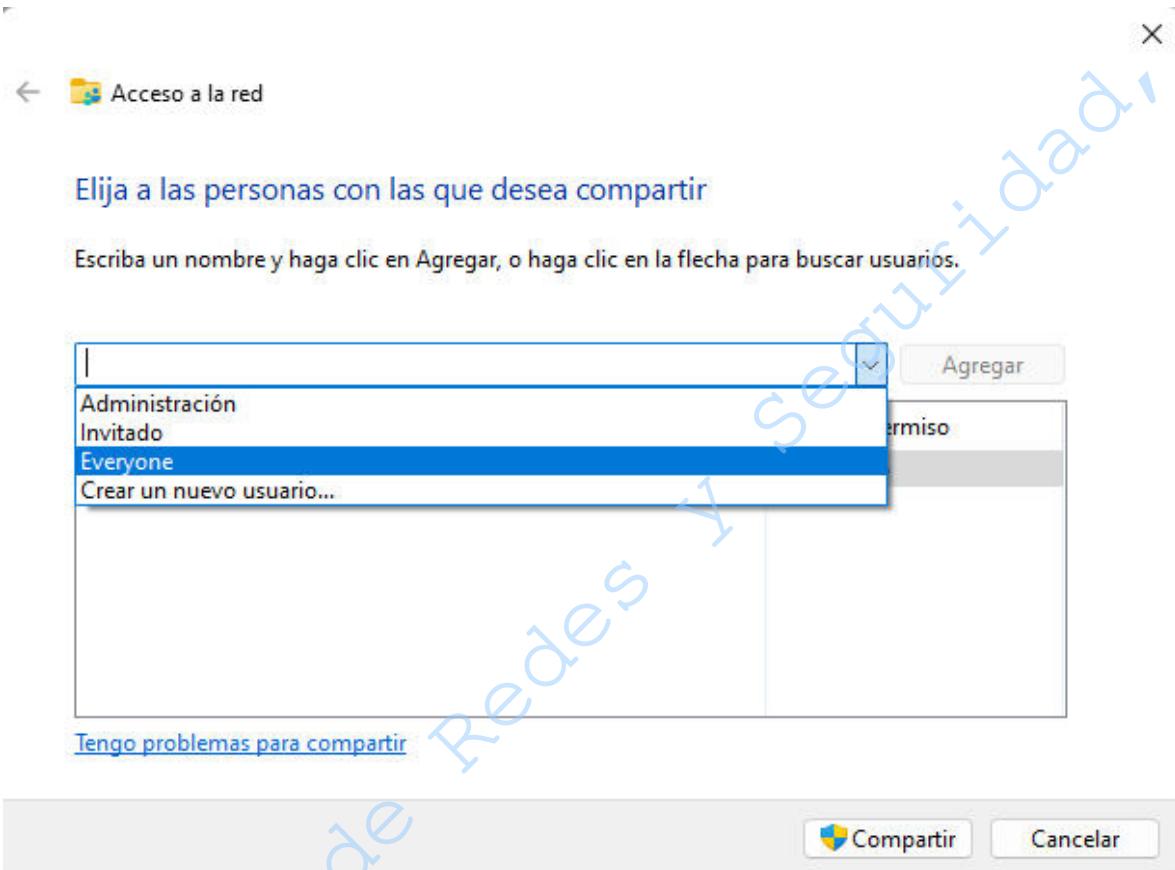


Figura No. 13. Permisos de la carpeta

4.2.9.6 En Nivel de permiso seleccione Lectura y escritura, dé clic en el botón Compartir. Se indicará que la carpeta está compartida, dar clic en el botón Listo (Figura No. 14).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	47/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

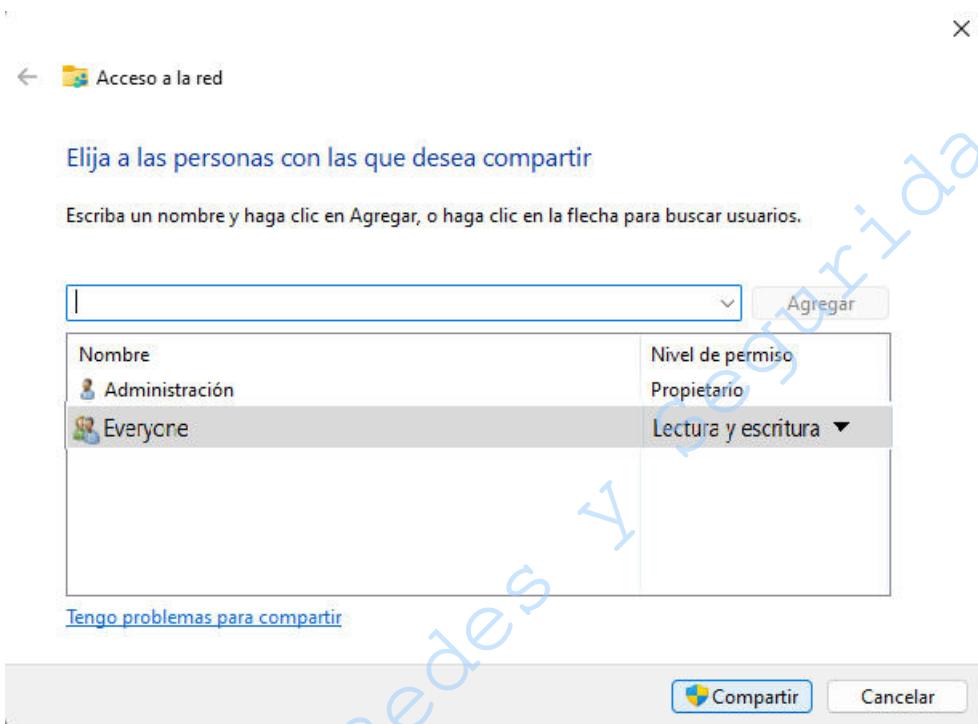


Figura No. 14. Nivel de permiso

4.2.9.7 Abra el menú principal y escriba en Buscar programas y archivos **\192.168.2.X\NombreDeLaCarpetaEnLaMáquinaRemota** (Ver Figura No. 15)

NOTA: X se sustituye por el número de la máquina remota desde donde descargará el archivo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	48/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

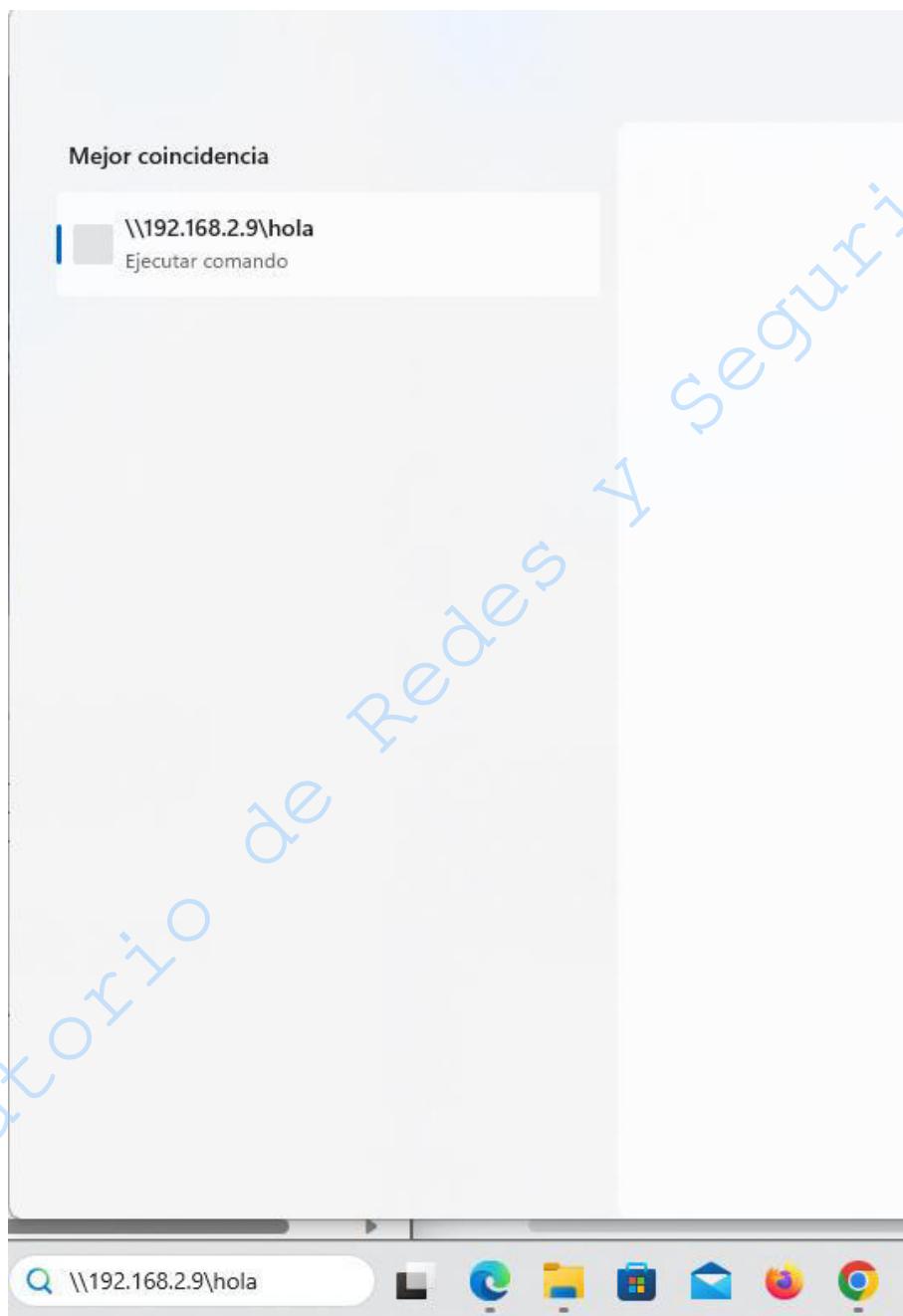


Figura No. 15 Ventana de búsqueda

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	49/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 4.2.10** Descargue la imagen o el video. Con el analizador de paquetes vea qué sucede y observe el tiempo de descarga entre dispositivos.

- 4.2.11** Elimine la carpeta que creó dentro de la unidad c:

- 4.2.12** A continuación mencione al menos tres de los protocolos que aparecen en la captura, investigue cuál es su función.

5.-Conclusiones.

Revise los objetivos planteados al inicio de la práctica y anote sus conclusiones

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	50/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 4
Manejo de Dispositivos de Interconectividad, hub y switch
Cuestionario Previo

1. Realice una tabla **comparativa** que contenga al menos cinco características de un hub y un switch.
2. ¿Cómo funciona el método de CSMA/CD?
3. ¿Qué es una colisión?
4. ¿Cuál es la importancia de la capa 2 del modelo OSI?
5. Describa los dos tipos de parámetros dúplex para las comunicaciones en una red Ethernet: Half dúplex y Full dúplex.
6. Investigue cómo es una conexión en cascada. Realice un diagrama y mencione las características de esta conexión, así como su funcionamiento.
7. Investigue cómo es una conexión en apilamiento. Realice un diagrama y mencione las características de esta conexión, así como su funcionamiento.
8. ¿Qué es un analizador de paquetes y cuál es su utilidad?
9. Mencione otras tres herramientas de análisis de paquetes y sus características.
10. Mencione otras tres herramientas de simulación de redes y sus características.
11. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 51/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 5

Instalación de una red básica en las plataformas: Windows de Microsoft y Linux distribución Debian

Capa 2 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 52/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

1.- Objetivos de Aprendizaje

- El alumno o la alumna al finalizar la práctica podrá configurar una tarjeta de red.
- El alumno o la alumna podrá instalar una LAN básica conectando dos computadoras utilizando un cable de conexión cruzada (crossover).

2.- Conceptos teóricos

Una tarjeta de Red, NIC (Network Interface Card) es el dispositivo que conecta a una estación, PC u otro equipo de red con el medio físico. El tipo de conector de la tarjeta de red dependerá de las características del medio de comunicación de la red: (par trenzado, coaxial, fibra óptica, aire) al cual se conecte. (Ver Figura No. 1)

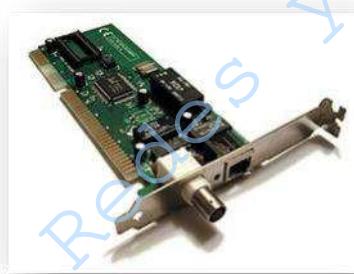


Figura No. 1. Tarjeta de red

Se define en la capa 2 del modelo OSI, debido a que tiene y reconoce direcciones MAC (subnivel de la capa de enlace). Contienen un código único en todo el mundo, que se llama dirección de Control de Acceso al Medio (MAC, Media Access Control). Esta dirección se utiliza para controlar la comunicación de datos para el host en la red.

La NIC es el componente de hardware básico en las comunicaciones de red. Traduce la señal producida por la computadora en un formato serie que se envía mediante el cable de red. La comunicación binaria (unos y ceros) se transforma en impulsos eléctricos, pulsos de luz, ondas de radio o cualquier esquema de transmisión de señales que usen los medios de comunicación en red, de manera que convierte el intercambio de señales a través de los medios de transmisión en una comunicación de datos efectiva.

Las funciones de la tarjeta de red son:

- Preparar los datos del equipo (formar tramas) para pasarlo a la capa física.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	53/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- En la salida transferir las tramas al medio físico de transmisión según el protocolo de comunicación.
- Recibir los datos que llegan por el cable y convertirlos en bytes para que puedan ser comprendidos por la unidad de procesamiento central del equipo (CPU).
- Controlar el flujo de datos entre el equipo y el sistema de cableado.

3.- Equipo y material necesario

Material del alumno o de la alumna:

- 1 cable de conexión directa (construido en la práctica 1).
- 1 cable de conexión cruzada (construido en la práctica 1).

Equipo del Laboratorio:

Primera Parte de la práctica:

- 2 computadoras con Windows
- Tarjeta de red
- Controlador de la tarjeta de red.

Segunda Parte de la práctica:

- 2 computadoras con Sistema Operativo Linux Debian.

4.- Desarrollo:

Modo de trabajar

La práctica se desarrollara en parejas.

Primera Parte: Plataforma Windows

4.1 Configuración de la tarjeta de red

Es importante señalar que existen cuatro tipos de componentes representados cada uno por un ícono distinto. (Ver Figura No. 1).



Figura No. 1. Íconos para los componentes de red.

- 4.1.1** Haga clic en el botón *Iniciar*, seleccione *Panel de control* y luego dé clic en *Redes e Internet->Centro de Redes y recursos compartidos->Cambiar configuración del adaptador*.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 54/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.1.2** Haga un clic con el botón derecho del mouse sobre el ícono en **Conexión de área local** y seleccione la opción **Propiedades**. (Ver Figura No. 2)

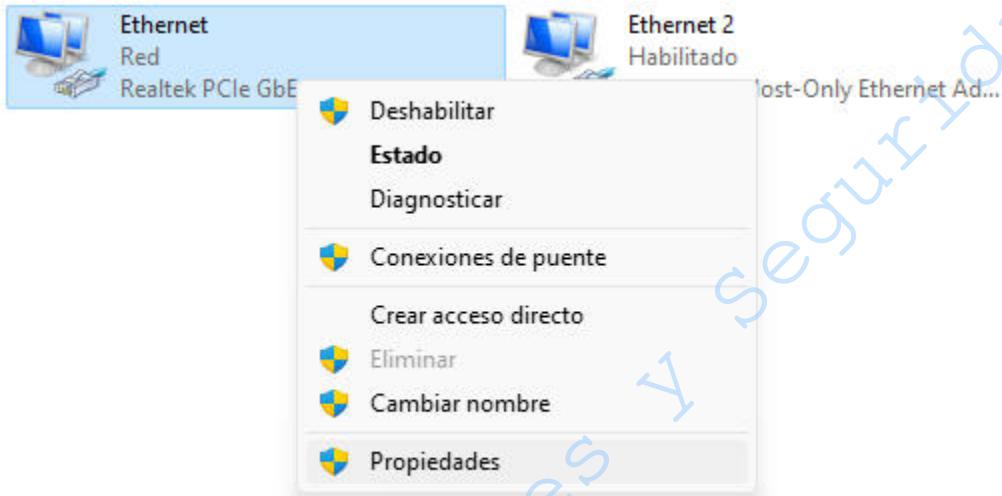


Figura No. 2. Conexión de área local

- 4.1.3** Seleccione la pestaña **Funciones de red**. Observe los elementos. (ver Figura No. 3)

Laboratorio de
Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 55/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

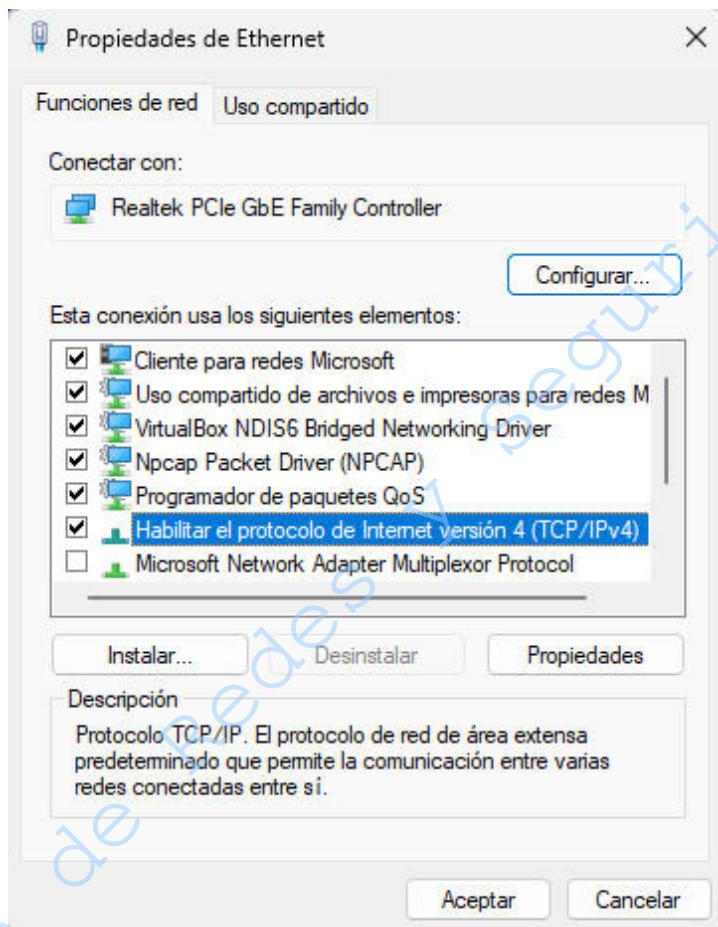


Figura No. 3. Propiedades de conexión de área local.

4.1.4 El protocolo TCP/IP, es un Protocolo de red de área extensa predeterminado que permite la comunicación entre varias redes conectadas entre sí. Es necesario configurarlo. Para ello dé un clic sobre el protocolo (**Protocolo de Internet versión 4**).

4.1.5 Dé clic en **Propiedades**. Aparecerá la pestaña **General**. Seleccione las opciones: Obtener una dirección IP automáticamente y Obtener la dirección del servidor DNS automáticamente. Dé clic en Aceptar.

4.1.6 Nuevamente dé clic en **Propiedades**. Aparecerá la pestaña **General**. Configure de acuerdo con los datos que indique su profesora o profesor (Dirección IP, Máscara de subred, Puerta de enlace predeterminada, Servidor DNS). (Ver Figura No. 4)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 56/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

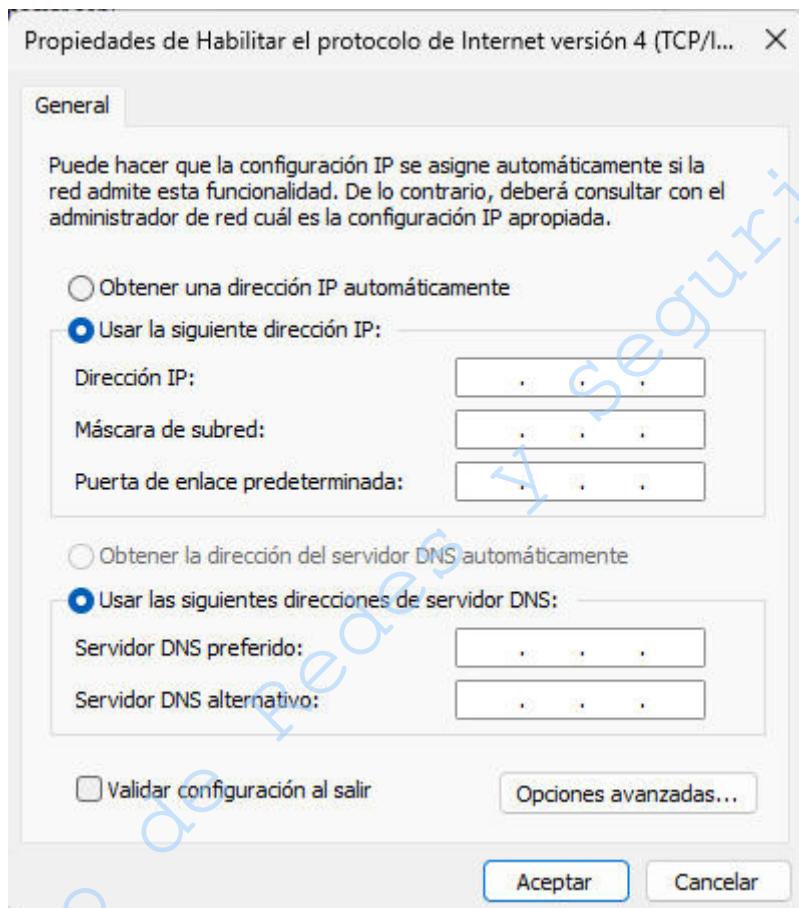


Figura No. 4. Propiedades del protocolo TCP/IP.

- 4.1.7** Coloque en las siguientes líneas lo que tomó en cuenta para colocar los parámetros adecuados (dirección IP, máscara de subred, puerta de enlace y direcciones DNS) en el punto anterior:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	57/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.1.8** Dibuje el diagrama lógico de la red del Laboratorio, desde la máquina en la cual está trabajando hasta la conexión con la red externa. Coloque las direcciones IP involucradas.



4.2 Pruebas y aplicaciones

- 4.2.1** Visualice la configuración de red del equipo. Ejecute el siguiente comando en una terminal de comandos:

C:/> ipconfig /all

- 4.2.2** Si la configuración no es la correcta, cámbiela y vuelva a ejecutar el comando.

- 4.2.3 Compartir documentos y recursos.**

- 4.2.3.1** Cree una carpeta con el nombre que desee dentro de la unidad c:

- 4.2.3.2** Cree un documento de texto y guárdelo dentro de la carpeta que creó en el paso anterior.

- 4.2.3.3** Dé clic secundario en el ícono de la carpeta que acaba de crear, seleccione las propiedades.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 58/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.3.4 Dé clic en la pestaña **Uso compartido** y oprima el botón **Compartir**. (Ver Figura No. 6)

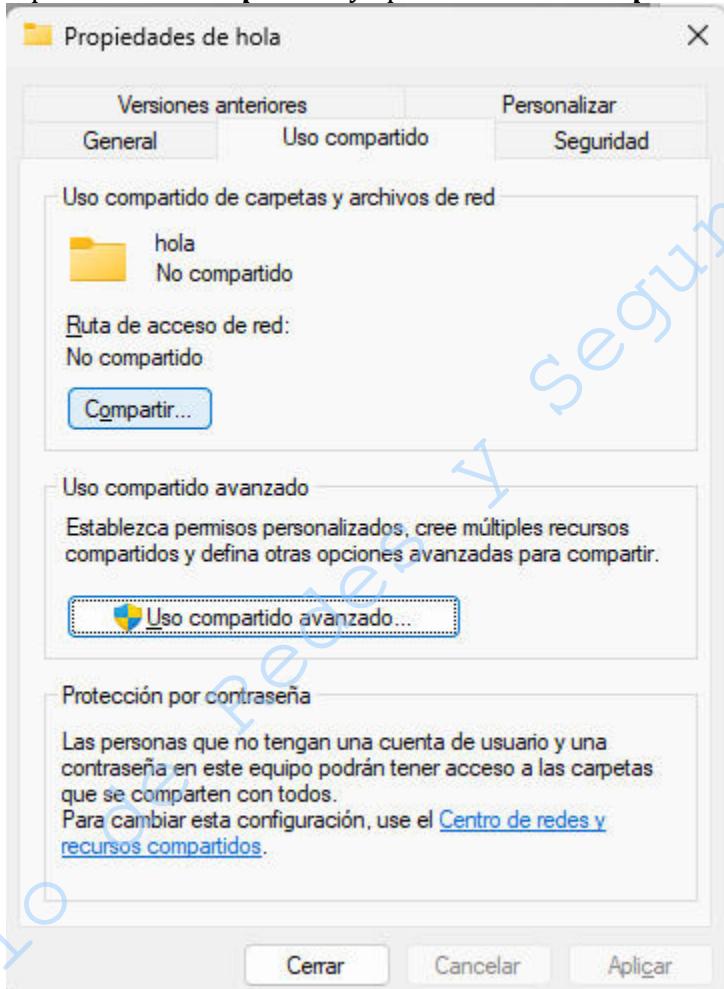


Figura No. 6. Propiedades de la carpeta

4.2.3.5 En la ventana **Elija a las personas con las que desea compartir** escriba **Everyone** y dé clic en el botón **Agregar**. (Ver Figura No. 7)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	59/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

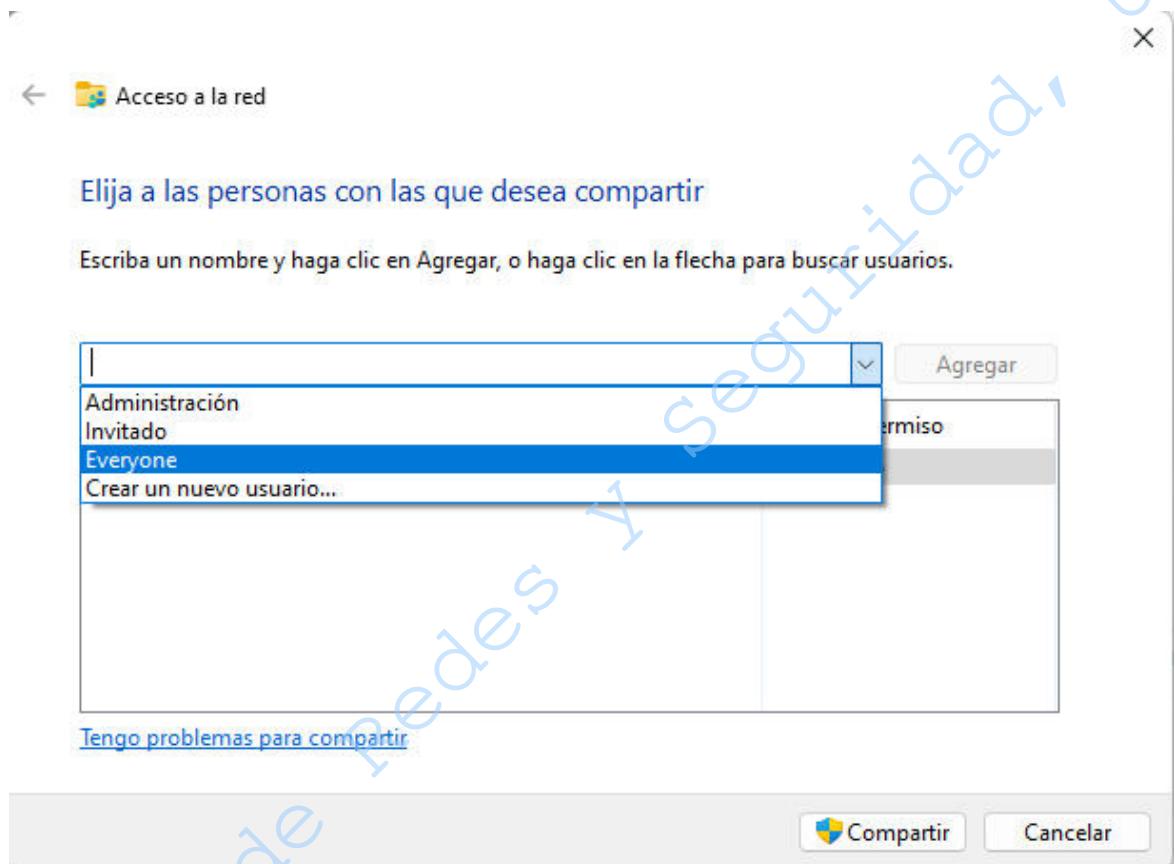


Figura No. 7. Permisos de la carpeta

4.2.3.6 Una vez agregado el sujeto, cambie los permisos (Nivel de permiso) a Lectura y escritura. Dé clic en **Compartir**. Dé clic en el botón **Listo** (Figura No. 8).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	60/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

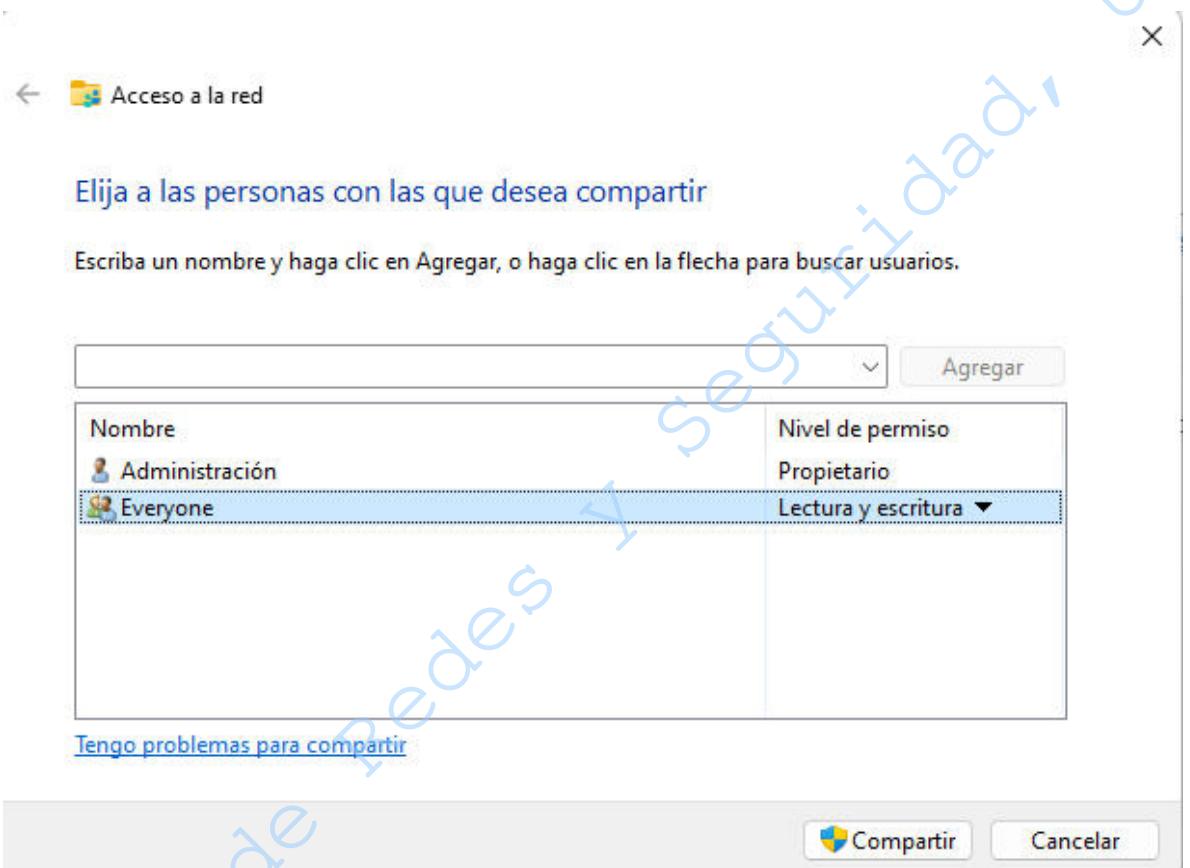


Figura No. 8. Selección de grupos, usuarios o equipos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	61/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.2.3.7 Dé clic en inicio y escriba en **Buscar programas y archivos** lo siguiente \\192.168.2.X\ (Ver Figura No. 9)

NOTA: X se sustituye por el número de la máquina remota



Figura No. 9 Ventana de comandos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	62/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

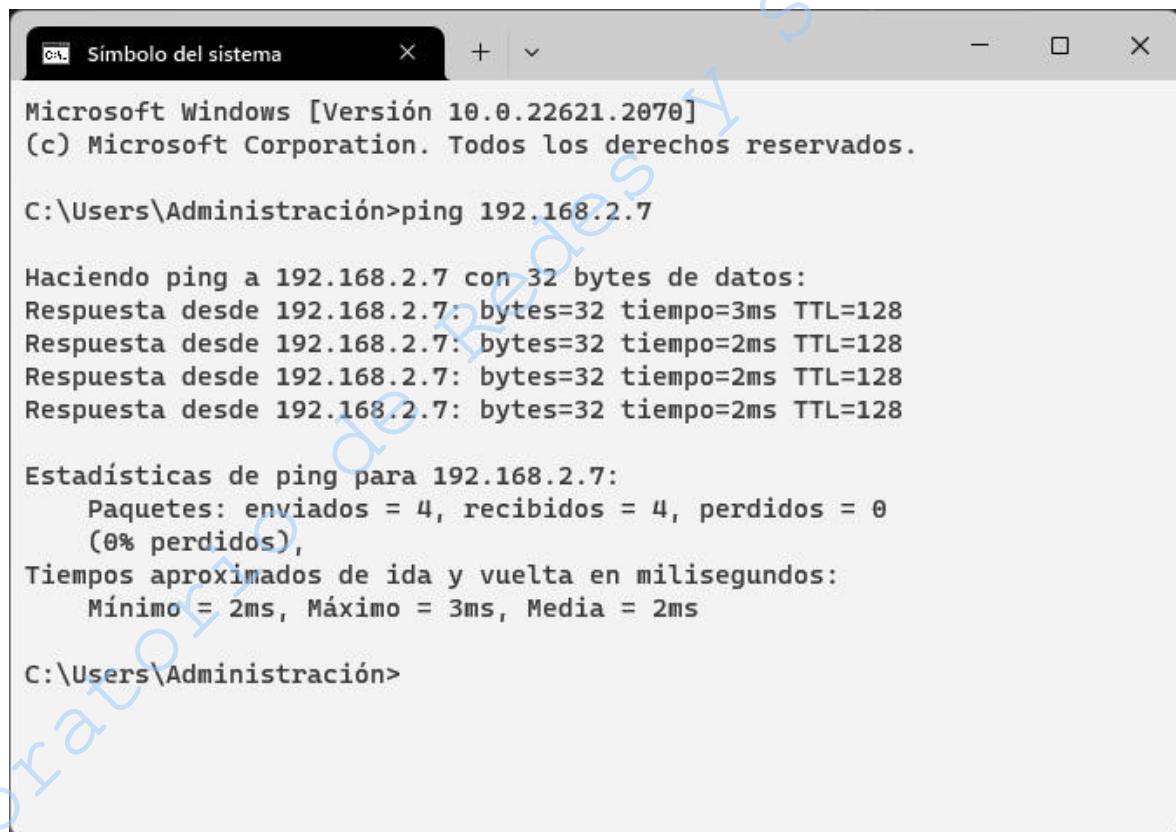
4.2.3.8 Indique si puede visualizar la carpeta compartida con los dispositivos de la red local.

4.2.4 Conecte el cable cruzado (crossover) a dos computadoras.

4.2.5 Para comprobar el funcionamiento de la red a través del cable cruzado ejecute el comando ping en una consola de comandos. (Ver Figura No. 10)

C:\>ping 192.168.2.X

NOTA: X se sustituye por el número de la máquina remota



```

Símbolo del sistema C:\> Microsoft Windows [Versión 10.0.22621.2070]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administración>ping 192.168.2.7

Haciendo ping a 192.168.2.7 con 32 bytes de datos:
Respuesta desde 192.168.2.7: bytes=32 tiempo=3ms TTL=128
Respuesta desde 192.168.2.7: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.2.7: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.2.7: bytes=32 tiempo=2ms TTL=128

Estadísticas de ping para 192.168.2.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 3ms, Media = 2ms

C:\Users\Administración>

```

Figura No. 10. Ejecución del comando ping

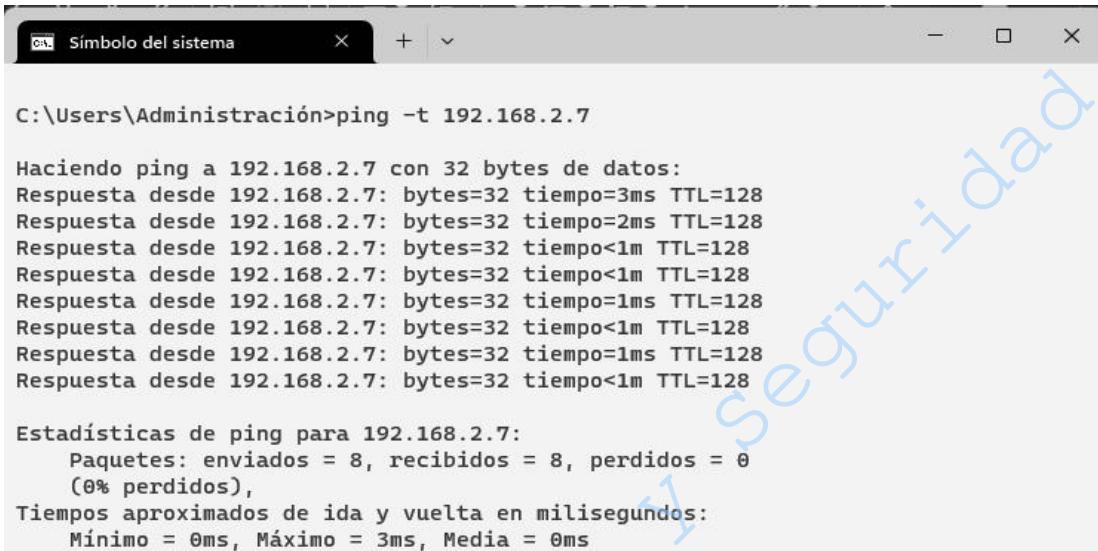
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	63/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

4.2.6 Explique cada una de las partes que conforman la respuesta afirmativa de conexión:

4.2.7 Si no existe una respuesta afirmativa, resuelva el problema y describa en las siguientes líneas el proceso que siguió:

4.2.8 Ejecute nuevamente el comando ping, pero ahora agregue el parámetro –t (Figura No. 11). Mientras se ejecuta, desconecte el cable de red y observe la salida del comando. Escriba a continuación el resultado y mencione la importancia del comando ping para realizar pruebas de conectividad en redes.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 64/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```
C:\Users\Administración>ping -t 192.168.2.7

Haciendo ping a 192.168.2.7 con 32 bytes de datos:
Respueta desde 192.168.2.7: bytes=32 tiempo=3ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo=2ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo<1ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo<1ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo=1ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo<1ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo=1ms TTL=128
Respueta desde 192.168.2.7: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.2.7:
Paquetes: enviados = 8, recibidos = 8, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 3ms, Media = 0ms
```

Figura No. 11. Ejecución del comando ping

4.2.9 Elimine la carpeta que creó en la unidad c:.

4.2.10 Conecte el cable que tenía originalmente la computadora (Conexión roseta – NIC de la computadora)

Segunda Parte: Plataforma Linux, distribución Debian

4.3 Verificación de la tarjeta

4.3.1 Abra la aplicación VirtualBox

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 65/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 12).

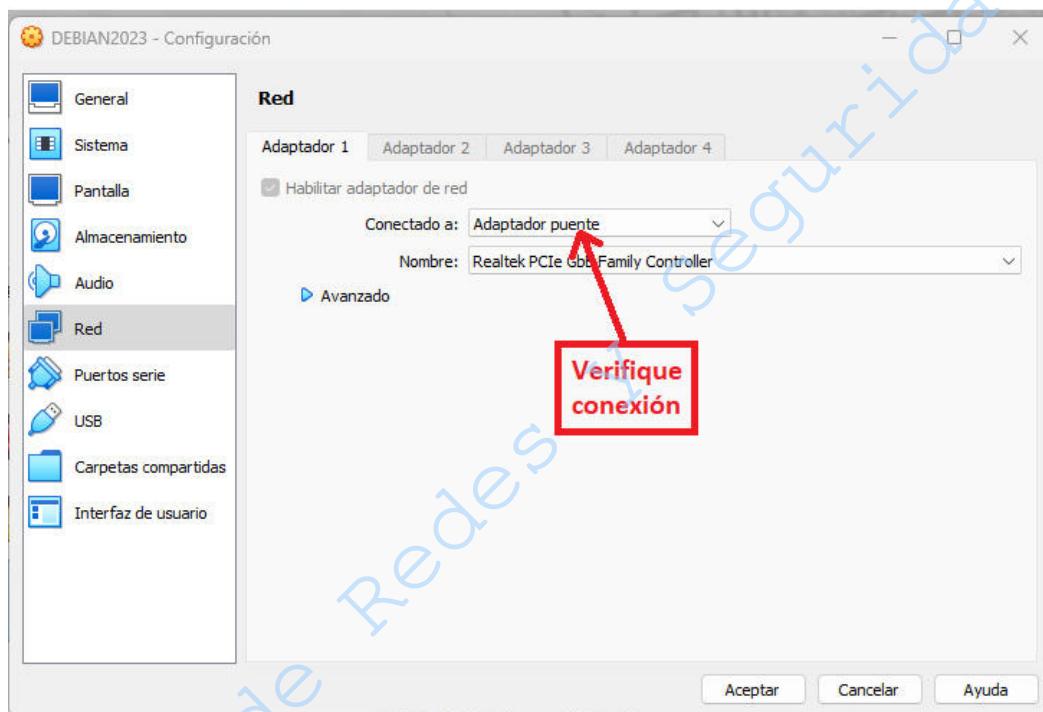


Figura No. 12. Conexión de red.

4.3.2 Encienda la máquina virtual

4.3.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete ifconfig.

4.3.4 Inicie sesión en la cuenta de *redes*.

4.3.5 Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 13)

NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root
redes@debian:~\$ su

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	66/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```
reedes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/reedes# rm /etc/network/interfaces
root@DEBIAN2023:/home/reedes# rm /etc/resolv.conf
```

Figura No. 13. Terminal de comandos como root.

4.3.6 Teclee los siguientes comandos para borrar cualquier configuración previa:

```
root@debian:/home/reedes# rm /etc/network/interfaces
root@debian:/home/reedes# rm /etc/resolv.conf
```

4.3.7 Liste los dispositivos de su computadora mediante el siguiente comando:

```
root@debian:/home/reedes# lspci
```

4.3.8 Verifique y anote la versión del kernel de su máquina. Teclee el siguiente comando: (Ver figura No.14)

```
root@debian:/home/reedes# uname -r
```



```
reedes@DEBIAN2023:~$ uname -r
5.10.0-23-amd64
root@DEBIAN2023:/home/reedes#
```

Figura No. 14 Visualización de la versión del kernel.

Versión del kernel:_____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	67/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.9** Explique el significado de cada parámetro de la versión del kernel obtenida en el paso anterior.

- 4.3.10** Liste el directorio correspondiente para buscar el módulo adecuado para la NIC. (Ver figura No. 15), para ello deberá teclear el siguiente comando considerando que en donde dice **versión_kernel** deberá sustituir por el número obtenido en el paso 4.3.8.

```
root@debian:/home/redes# ls /lib/modules/versión_kernel/kernel/drivers/net
```



```
root@DEBIAN2023:/home/redes# ls /lib/modules/5.10.0-23-amd64/kernel/drivers/net
appletalk gtp.ko      mdio          sb1000.ko        vmxnet3
arcnet    hamradio    mdio.ko       slip           vrf.ko
bonding   hippi       mii.ko        sungem_phy.ko  vsockmon.ko
can       hyperv      netconsole.ko  tap.ko         vxlan.ko
dummy.ko  ieee802154  net_failover.ko team          wan
eql.ko    ifb.ko       nlmon.ko     thunderbolt-net.ko wimax
ethernet  ipvlan     pcs           tun.ko        wireguard
fddi     macsec.ko    phy           usb            wireless
fjes      macvlan.ko  plip          veth.ko       xen-netback
geneve.ko macvtap.ko  ppp          virtio_net.ko xen-netfront.ko
```

Figura No. 15. Listado de drivers

- 4.3.11** Comente el resultado obtenido.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	68/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4 Configuración de la tarjeta de red.

4.4.1 Configuración de la NIC usando scripts

4.4.1.1 Edite el archivo **/etc/network/interfaces**, coloque lo siguiente: (Si los parámetros no aparecen en el archivo, tecléelos) (Ver Figura No. 16)

```
root@debian:/home/redes# nano /etc/network/interfaces
```

```
#The primary network interface
auto enp0s3
iface enp0s3 inet static
address 192.168.2.X
netmask 255.255.255.0
gateway 192.168.2.254
network 192.168.2.0
broadcast 192.168.2.255
```

NOTA: X se sustituye por la IP de su máquina+50.

Por ejemplo: si su máquina es 192.168.2.1 colocará 192.168.2.51

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 69/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

GNU nano 5.4                               redes@DEBIAN2023: ~
/etc/network/interfaces

#This file describes the network interfaces available on your system
#and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

#The loopback network interface
auto lo
iface lo inet loopback

#The primary network interface
auto enp0s3
iface enp0s3 inet static
address 192.168.2.61
netmask 255.255.255.0
gateway 192.168.2.254
network 192.168.2.0
broadcast 192.168.2.255

^G Help      ^O Write Out  ^W Where Is  ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File   ^\ Replace    ^U Paste     ^J Justify   ^

```

Figura No. 16 Configuración de la tarjeta de red.

4.4.1.2 Guarde y salga del editor

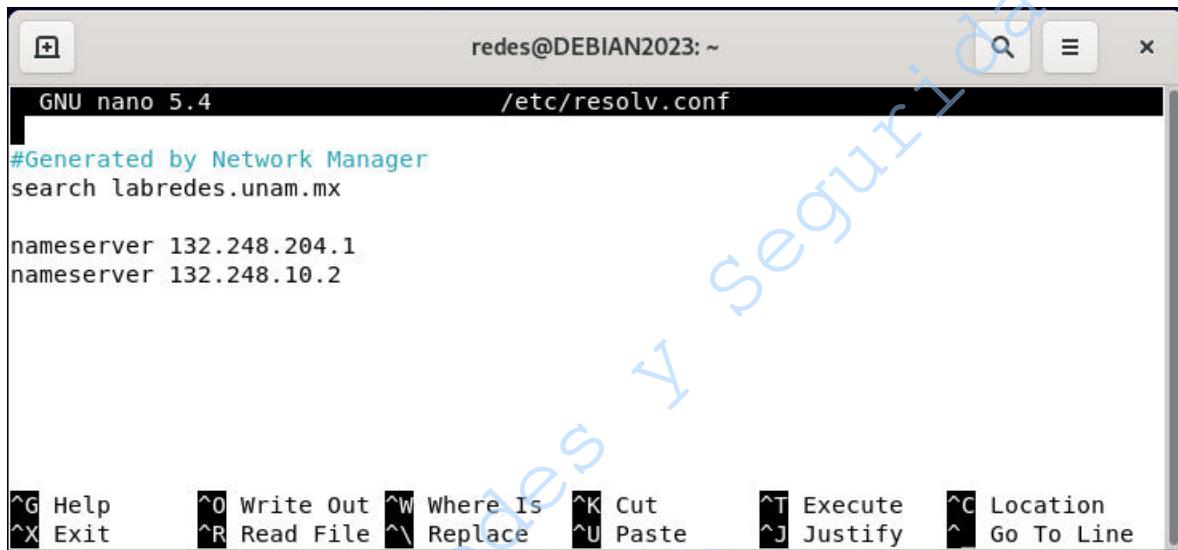
4.4.1.3 Explique el significado de cada uno de los parámetros agregados en la configuración:

auto:
iface **** inet:
address:
gateway:
netmask:
network:
broadcast:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	70/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4.1.4 Dentro del archivo **resolv.conf** coloque los DNS (Ver Figura No. 17)

```
root@debian:/home/redes# nano /etc/resolv.conf
```



```
redes@DEBIAN2023: ~
GNU nano 5.4          /etc/resolv.conf

#Generated by Network Manager
search labredes.unam.mx

nameserver 132.248.204.1
nameserver 132.248.10.2

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File   ^V Replace    ^U Paste      ^J Justify    ^
^L Location  ^P Paste      ^D Delete    ^F Find       ^B Backspace  ^H Home
```

Figura No. 17 Configuración de los DNS

4.4.1.5 Guarde y salga del editor

4.4.1.6 Finalmente, teclee una de las siguientes opciones:

```
root@debian:/home/redes# ifup enp0s3
```

```
root@debian:/home/redes# service networking restart
```

```
root@debian:/home/redes# /etc/init.d/networking restart
```

```
root@debian:/home/redes# ifconfig enp0s3 up
```

4.4.1.7 Mencione las diferencias que existen entre las instrucciones anteriores, si es necesario, ejecute cada una de ellas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 71/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.5 Pruebas y aplicaciones

4.5.1 Para comprobar la configuración actual de la NIC, utilice el siguiente comando(Ver Figura No. 18):

```
root@debian:/home/redes# ifconfig
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	72/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@DEBIAN2023:/home/redes# ifconfig enp3 up
enp3: ERROR while getting interface flags: No such device
root@DEBIAN2023:/home/redes# ifconfig enp0s3 up
root@DEBIAN2023:/home/redes# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.2.65 netmask 255.255.255.0 broadcast 192.168.2.255
        ether 08:00:27:cb:97:be txqueuelen 1000 (Ethernet)
          RX packets 5541 bytes 3780893 (3.6 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 1091 bytes 91326 (89.1 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 39 bytes 3581 (3.4 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 39 bytes 3581 (3.4 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@DEBIAN2023:/home/redes#

```

Figura No. 18. Ejecución del comando ifconfig

Anote la salida, sólo los **dos** primeros renglones y comente el resultado

4.5.2 Teclee el comando

root@debian:/home/redes # ifconfig enp0s3 192.168.2.X netmask 255.255.255.0 up

NOTA: X se sustituye por la IP de su máquina que utilizó para configurar el archivo en el paso 4.5.1.1

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	73/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.5.3** Teclee nuevamente el comando **ifconfig**. Compare con la salida del punto 4.5.1. ¿Se obtiene la misma información? ¿Por qué? Justifique su respuesta. ¿Para qué sirve el comando tecleado en el punto anterior empleando parámetros?



- 4.5.4** Conecte su máquina con otra del laboratorio por medio del cable cruzado.

- 4.5.5** Ejecute el comando ping para verificar la conexión anterior (Ver Figura No. 19)

root@debian:/home/redes ping 192.168.2.x

NOTA: X se sustituye por el número de la máquina remota

Pulse ctrl + c para detenerlo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	74/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

```

root@DEBIAN2023:/home/redes# ping 192.168.2.118
PING 192.168.2.118 (192.168.2.118) 56(84) bytes of data.
64 bytes from 192.168.2.118: icmp_seq=1 ttl=128 time=0.327 ms
64 bytes from 192.168.2.118: icmp_seq=2 ttl=128 time=0.607 ms
64 bytes from 192.168.2.118: icmp_seq=3 ttl=128 time=0.512 ms
64 bytes from 192.168.2.118: icmp_seq=4 ttl=128 time=0.521 ms
64 bytes from 192.168.2.118: icmp_seq=5 ttl=128 time=0.547 ms
64 bytes from 192.168.2.118: icmp_seq=6 ttl=128 time=0.388 ms
64 bytes from 192.168.2.118: icmp_seq=7 ttl=128 time=0.426 ms

```

Figura No. 19. Ejecución del comando ping

- 4.5.6** Conecte el cable directo que tenía originalmente la computadora y realice las pruebas de conectividad necesarias para verificar que la máquina tiene conexión hacia Internet (Conexión roseta-NIC de la computadora).

5.-Cuestionario

1. ¿Qué debe ser considerado cuando se selecciona una NIC para instalar en una computadora?

2. En el ambiente de las redes Microsoft ¿Qué es un dominio?

3. Explique detalladamente el procedimiento para instalar una tarjeta de red si el sistema operativo Linux no contiene los controladores adecuados para dicha tarjeta.

4. ¿Por qué es importante configurar la NIC a nivel de comandos?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 75/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.-Conclusiones

Revise los objetivos planteados al inicio de la práctica y escriba sus conclusiones

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 76/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

PRÁCTICA 5
Instalación de una red básica en las plataformas:
Windows de Microsoft y Linux distribución Debian
Cuestionario Previo

1. ¿Qué es un cliente, protocolo, adaptador y servicio en una red?
2. En el ámbito de las redes existen dos tipos de direcciones: físicas y lógicas. Describa las características de cada una.
3. Investigue las clases de direcciones lógicas.
4. ¿Qué es y qué funciones realiza una máscara de red?
5. Explique el funcionamiento de:
 - a. Un DNS
 - b. Una puerta de enlace
 - c. Un servidor DHCP
6. Investigue cómo se configura una tarjeta de red en modo gráfico en Linux Distribución Debian
7. Investigue el objetivo, funcionamiento y al menos 3 parámetros del comando ping
8. ¿Para qué se usa el comando apt-get install ifconfig o apt install ifconfig?
9. ¿Para qué se usa el comando ip addr y cuál es la sintaxis para usarlo?
10. ¿Con qué otros nombres se puede identificar a la NIC además de eth0?
11. ¿Para qué sirve el protocolo TCP/IP?
12. ¿Cuál es el significado e importancia de WINS?
13. ¿Por qué es importante conocer el modelo del chipset de la NIC?
14. ¿Qué significan cada uno de los parámetros en la versión del kernel (ejemplo: kernel 2.6.7.3)? Explique los 4 parámetros para las versiones actuales.
15. ¿Cómo se desactiva un firewall en el sistema operativo Linux?
16. ¿Cómo se desactiva un firewall en el sistema operativo Windows?
17. Investigar los pasos para instalar el controlador de tarjeta de red en Windows
18. En el administrador de dispositivos investigue los diferentes íconos que señalan los problemas en los dispositivos y su significado (Figura No. A)

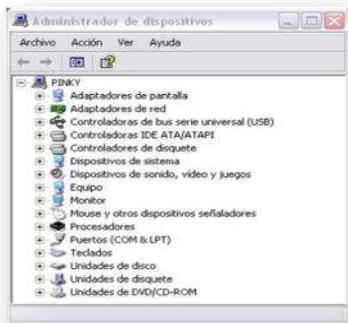


Figura No. A. Administrador de dispositivos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	77/479
		Sección ISO	8.3
Facultad de Ingeniería		Fecha de emisión	11 de agosto de 2023
		Área/Departamento:	Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada	

Práctica 6

Encaminamiento y análisis de paquetes

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	78/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno o la alumna al finalizar la práctica, se familiarizará con el manejo de algunas herramientas del Sistema Operativo Linux, como son route y traceroute, y sus similares en Windows, como son route y tracert, enfocadas al encaminamiento de paquetes a través de la red.
- El alumno o la alumna conocerá los fundamentos del monitoreo de redes.
- El alumno o la alumna aplicará filtros adecuados en el análisis de paquetes.
- El alumno o la alumna reafirmará los conocimientos teóricos acerca del protocolo ARP mediante observación de casos reales.

2.- Conceptos teóricos

Route

Este comando se utiliza para configurar las tablas de encaminamiento del núcleo de nuestro sistema. Generalmente en todo equipo de una red local tenemos al menos tres rutas: la de loopback, utilizando el dispositivo de bucle interno (lo, lo0...), la de red local (localnet), que utiliza la tarjeta de red para comunicarse con equipos dentro del mismo segmento de red, y una default que también utiliza la tarjeta para enviar a un router o gateway paquetes que no son para equipos de nuestro segmento.

Si route nos muestra una configuración sospechosa (esto es, las tablas no son las que en el sistema hemos establecido como administradores, aunque todo funcione correctamente) esto puede denotar un ataque de simulación: alguien ha desviado el tráfico por un equipo que se comporta de la misma forma que se comportaría el original, pero que seguramente analiza toda la información que pasa por él. Hemos de recalcar que esto suele ser transparente al buen funcionamiento del equipo (no notamos ni pérdida de paquetes, ni retardos excesivos, ni nada sospechoso), y que además el atacante puede modificar los archivos de arranque del sistema para, en caso de reinicio de la máquina, volver a tener configuradas las rutas a su gusto; estos archivos suelen ser del tipo /etc/rc.d/rc.inet1 o /etc/rc?.d/Sinet.

También es posible que alguien esté haciendo uso de algún elemento utilizado en la conexión entre nuestro sistema y otro (un router, una pasarela...) para amenazar la integridad de nuestro equipo; si queremos comprobar el camino que siguen los paquetes desde que salen de la máquina hasta que llegan al destino, podemos utilizar la orden traceroute. Sin embargo, este tipo de ataques es mucho más difícil de detectar, y casi la única herramienta factible para evitarlos es la criptografía.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	79/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Traceroute

La orden traceroute se utiliza para imprimir la ruta que los paquetes siguen desde nuestro sistema hasta otra máquina, realizar pruebas, medidas y administración de una red; introduce mucha sobrecarga, lo que evidentemente puede acarrear problemas de rendimiento, llegando incluso a negaciones de servicio por el elevado tiempo de respuesta que el resto de aplicaciones de red pueden presentar.

Traceroute es una herramienta que combina muy inteligentemente, dos características de los protocolos que hacen posible Internet. Éstos son:

a) TTL o expiración de los paquetes

Para proteger a Internet del efecto de paquetes atrapados en ciclos de encaminamiento, los diseñadores de TCP/IP dotaron a cada datagrama IP de un contador que llamaron TTL por las siglas de *Time To Live*. Esto es un número que limita cuántos *saltos* puede dar un datagrama, antes de ser descartado por la red.

Cuando se introduce un datagrama IP a la red, el campo TTL es poblado con el número máximo de saltos que define la vida de ese datagrama. Cada router por el que ese datagrama transita, resta uno a ese número. Cuando éste llega a cero, el datagrama es descartado.

b) Internet Control Message Protocol o ICMP

ICMP sirve para manejar mensajes de control. Esto son mensajes administrativos entre nodos de Internet. Los paquetes ICMP sirven para muchas cosas: avisar que un enlace o que un dispositivo están congestionados, que se escogió un camino sub-óptimo para enviar un paquete, que no se puede acceder a un sitio en particular, etcétera, uno de esos avisos es particularmente útil para traceroute: El aviso de que se excedió la vida útil del paquete.

Combinando estas dos herramientas, traceroute permite construir un mapa de la red tal como es vista desde un nodo en particular.

Aquí se muestra cada uno de los saltos que tiene que dar un paquete al recorrer el camino desde la computadora hasta www.unam.mx. La dirección del recorrido es muy importante, porque en Internet no necesariamente el camino de ida es igual al de regreso.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 80/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

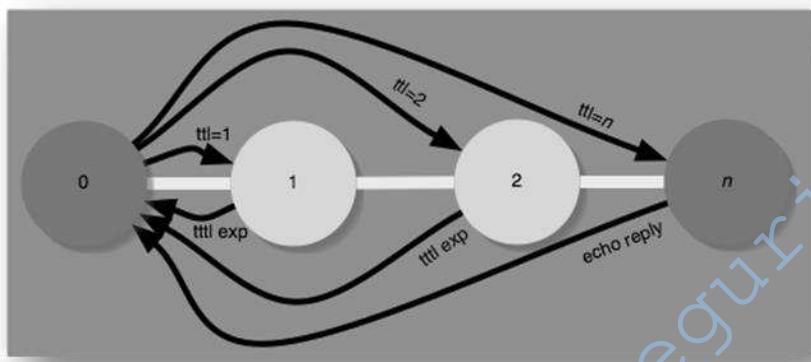


Figura No.1. Funcionamiento de traceroute

El ejemplo anterior permite ver mejor cómo funciona la herramienta. (Ver Figura No. 1). En el primer salto, hacia el nodo 1, traceroute pone el valor TTL en 1 y envía el paquete hacia el nodo de destino. Cuando el nodo 1 decrementa el valor del TTL y obtiene un cero, devuelve al nodo de origen un mensaje de error que dice que el TTL expiró mientras el paquete iba en tránsito. Este proceso se repite varias veces y los tiempos se registran.

Para el siguiente salto, traceroute aumenta en uno el valor del TTL y lo envía de nuevo hacia su destino. El nodo 1 decrementa el valor del TTL a uno y pasa el paquete hacia el nodo 2. El nodo 2 recibe el paquete con TTL uno y al decrementarlo, obtiene un TTL cero, enviando el correspondiente mensaje de error hacia el nodo de origen. Este proceso se va repitiendo con valores progresivamente más grandes de TTL, para ir encontrando los saltos cada vez más lejanos o hasta que se llega a un TTL muy grande. Típicamente este valor máximo es 30, aunque puede ser de hasta 255.

Análisis de paquetes

El análisis de paquetes resulta una herramienta fundamental en dos sentidos. Por un lado, permite apreciar de forma realista muchos de los conceptos fundamentales de las redes en general, y de los protocolos TCP/IP en particular (encapsulación, fragmentación, secuenciación de mensajes, etc). Por otro lado, permite realizar un diagnóstico muy preciso de las redes en funcionamiento, desde la detección de errores, la verificación de los mecanismos de seguridad y la evaluación de prestaciones de la red.

Es por ello que en esta práctica se estudiará una herramienta gratuita de análisis de paquetes, denominada Wireshark, que trabaja sobre una interfaz de red denominada WinPCap.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	81/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

La captura de tramas consiste en la obtención directa de tramas tal y como aparecen a nivel de LAN. Puesto que el medio de transmisión es generalmente, una línea de difusión, el monitoreo permite observar la totalidad de las comunicaciones que tienen lugar a través de la red, y por tanto resulta una herramienta muy potente, tanto desde el punto de vista positivo (diagnóstico de red) como el negativo (compromete la confidencialidad de las comunicaciones).

La cantidad de información obtenida de una captura de paquetes es enorme. Por tanto, es necesario establecer filtros de aceptación que permiten que las tramas no consideradas relevantes no se almacenen ni muestren al usuario.

El paquete Wireshark

Es una aplicación completamente configurable para el análisis mediante monitoreo de redes locales en entornos TCP/IP sobre cualquiera de las tecnologías soportadas por la interfaz WinPCap.

3.- Equipo y material necesario

Equipo del laboratorio:

- Computadora con sistema operativo Linux Debian y Windows
- Herramienta Wireshark instalada en el sistema Windows

4.- Desarrollo:

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Encaminamiento y análisis de paquetes bajo plataforma Linux

4.1.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 2)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 82/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

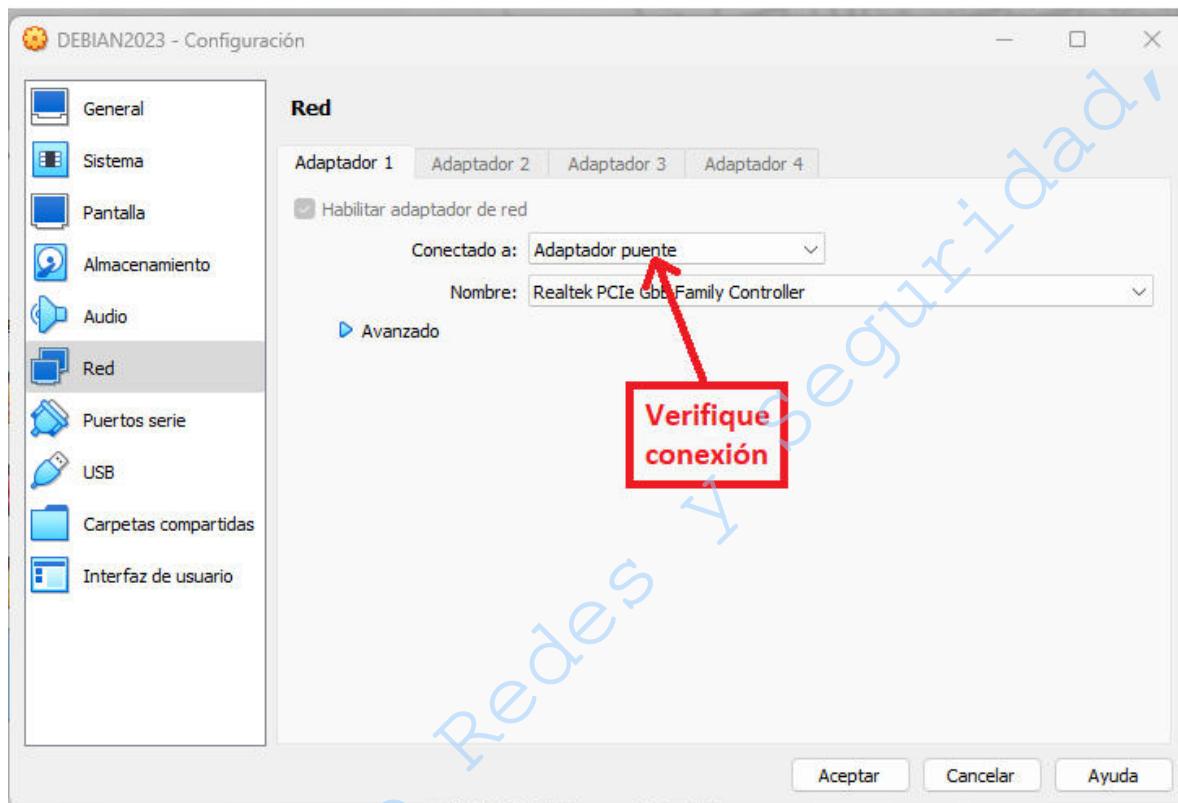
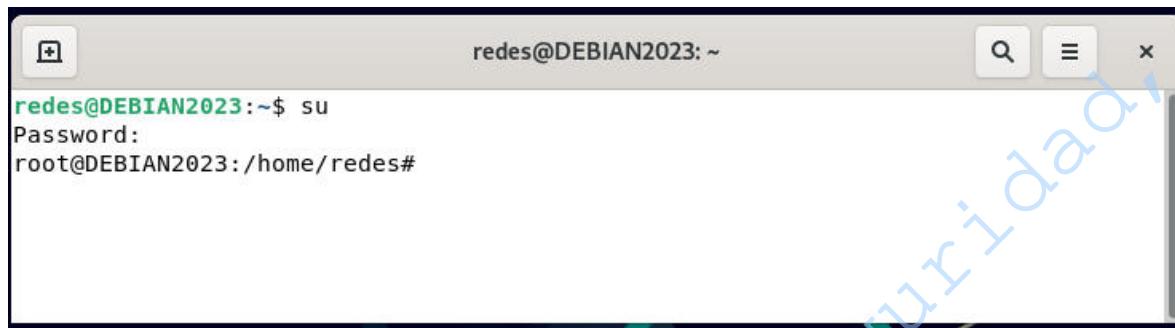


Figura No. 2. Conexión de red.

- 4.1.2 Encienda la máquina virtual
- 4.1.3 Elija la opción de cargar Linux, distribución Debian.
- 4.1.4 Inicie sesión como usuario redes. La profesora o el profesor le proporcionará la contraseña
- 4.1.5 Abra una terminal e ingrese como super usuario, teclee la contraseña de root. (Ver Figura No. 3)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 83/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```
redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes#
```

Figura No. 3. Terminal de comandos.

4.1.6 Verifique que la conexión a la red esté habilitada (Ver Figura No. 4).

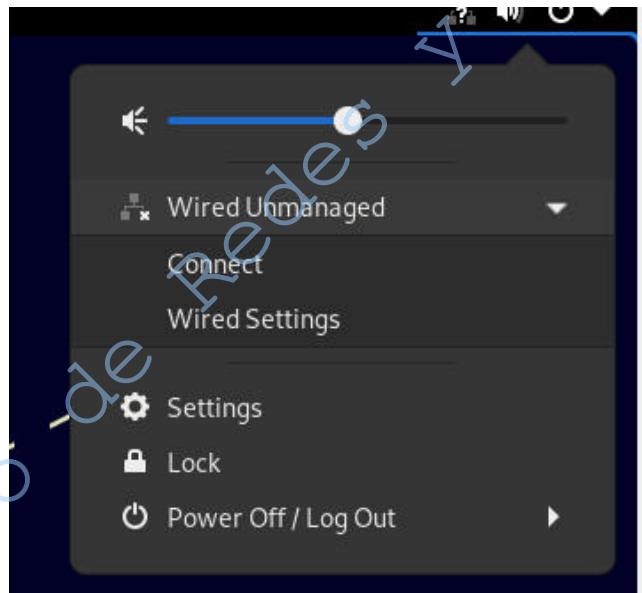


Figura No. 4. Conexión a la red.

4.1.7 Monitoree la interfaz de red, para ello teclee el siguiente comando (Figura No. 5)

NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete **tcpdump**.

```
root@debian:/home/redes# tcpdump -i enp0s3
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	84/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```
root@DEBIAN2023:/home/redes# tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:01:07.189653 STP 802.1d, Config, Flags [none], bridge-id 8000.00:12:a9:fa:91:c0.8018, length 35
13:01:08.618286 IP6 fe80::e2cb:bcff:fe8c:2739 > ip6-allrouters: ICMP6, router solicitation, length 16
13:01:08.689008 IP DEBIAN2023.56623 > dns1.unam.mx.domain: 41401+ PTR? 9.3.7.2.c.8.e.f.f.f.c.b.b.c.2.e.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
13:01:08.690689 IP dns1.unam.mx.domain > DEBIAN2023.56623: 41401 NXDomain* 0/1/0 (139)
13:01:08.793484 IP DEBIAN2023.46778 > dns1.unam.mx.domain: 36801+ PTR? 1.204.248.132.in-addr.arpa. (44)
13:01:08.794830 IP dns1.unam.mx.domain > DEBIAN2023.46778: 36801 1/2/4 PTR dns1.unam.mx. (194)
13:01:08.794916 IP DEBIAN2023.48792 > dns1.unam.mx.domain: 37828+ PTR? 65.2.168.192.in-addr.arpa. (43)
13:01:08.796534 IP dns1.unam.mx.domain > DEBIAN2023.48792: 37828 NXDomain* 0/1/0 (98)
13:01:09.188809 STP 802.1d, Config, Flags [none], bridge-id 8000.00:12:a9:fa:91:c0.8018, length 35
13:01:11.188484 STP 802.1d, Config, Flags [none], bridge-id 8000.00:12:a9:fa:91:c0.8018, length 35
13:01:12.618467 IP6 fe80::e2cb:bcff:fe8c:2739 > ip6-allrouters: ICMP6, router so
```

Figura No. 5. Tcpdump.

NOTA: Teclee ctrl+c para detener la captura

- 4.1.8** Analice la salida en pantalla y trate de identificar direcciones IP's, puertos, nombres, protocolos, etcétera y escríbalos a continuación:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	85/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- 4.1.9** Visualice la configuración actual de la tabla de encaminamiento. (Ver Figura No. 6)
Teclee lo siguiente:

```
root@debian:/home/redes# route
```



```
root@DEBIAN2023:/home/redes# route
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0        UG     0      0        0 enp0s3
192.168.2.0    0.0.0.0        255.255.255.0   U      0      0        0 enp0s3
root@DEBIAN2023:/home/redes#
```

Figura No. 6. Comando route

- 4.1.10** Analice la tabla y explique cada una de sus partes; así como la importancia de la misma.



- 4.1.11** Observe la ruta que sigue un paquete por la red. Teclee lo siguiente: (Ver Figura No. 7)

```
root@debian:/home/redes# traceroute www.google.com
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 86/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```
root@DEBIAN2023:/home/redes# traceroute www.google.com
traceroute to www.google.com (142.251.34.4), 30 hops max, 60 byte packets
 1 _gateway (192.168.2.254) 0.431 ms 0.404 ms 0.394 ms
 2 ve59.iimas.dist.unam.mx (132.248.59.254) 5.840 ms 5.830 ms 5.821 ms
 3 1010-iimas.redunam.unam.mx (132.247.237.101) 12.988 ms 12.977 ms 12.879 ms
 4 1006-arq.redunam.unam.mx (132.247.237.222) 1.011 ms 1.002 ms 0.994 ms
 5 132.248.133.49 (132.248.133.49) 0.987 ms 0.972 ms 0.955 ms
 6 192.180.200.82 (192.180.200.82) 1.065 ms 1.028 ms 0.997 ms
 7 178.201.148.69.bestelclientes.com.mx (201.148.69.178) 1.662 ms 1.628 ms 1.616 ms
 8 103.200.57.8.bestelclientes.com.mx (200.57.8.103) 3.869 ms 3.780 ms 3.765 ms
 9 105.200.57.8.bestelclientes.com.mx (200.57.8.105) 3.756 ms 3.746 ms 1.957 ms
10 107.200.57.8.bestelclientes.com.mx (200.57.8.107) 2.248 ms 2.738 ms 1.915 ms
11 58.189.204.203.bestelclientes.com.mx (189.204.203.58) 2.481 ms 2.234 ms 2.210 ms
12 74.125.48.146 (74.125.48.146) 10.816 ms 10.806 ms 10.798 ms
13 * * *
14 74.125.243.33 (74.125.243.33) 17.902 ms 142.251.235.42 (142.251.235.42) 16.918 ms 74.125.243.33 (74.125.243.33) 18.095 ms
15 142.251.78.51 (142.251.78.51) 10.464 ms 10.600 ms 10.590 ms
16 108.170.254.1 (108.170.254.1) 7.296 ms qro0ls27-in-f4.1e100.net (142.251.34.4) 16.842 ms 16.757 ms
root@DEBIAN2023:/home/redes#
```

Figura No. 7 Comando traceroute

4.1.12 Analice el resultado del paso anterior y comente al respecto.



4.1.13 Cierre la máquina virtual

4.2 Encaminamiento y análisis de paquetes bajo plataforma Windows.

4.2.1 Inicie en Windows

4.2.2 Inicie sesión como usuario privilegiado (administrador). La profesora o el profesor le proporcionará la contraseña.

4.2.3 Abra una terminal de comandos

4.2.4 Visualice la tabla de encaminamiento. Teclee lo siguiente:

C:\> route print

4.2.5 Analice la tabla y comente las diferencias con la obtenida en el sistema Linux

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 87/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.6 Observe el camino que sigue un paquete. Teclee lo siguiente:

C:\> tracert www.google.com

4.2.7 Analice el resultado del paso anterior y comente:

4.2.8 Utilización de la aplicación Wireshark

4.2.8.1 Abra la aplicación de Wireshark

4.2.8.2 Dé clic en el menú Capture y elija Options.

4.2.8.3 Seleccione y habilite la tarjeta de red que está usando (interface) dando doble clic sobre ella.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 88/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.8.4 Deshabilite la opción Activar modo promiscuo en todas las interfaces. Oprima Iniciar (Ver Figura No. 8)

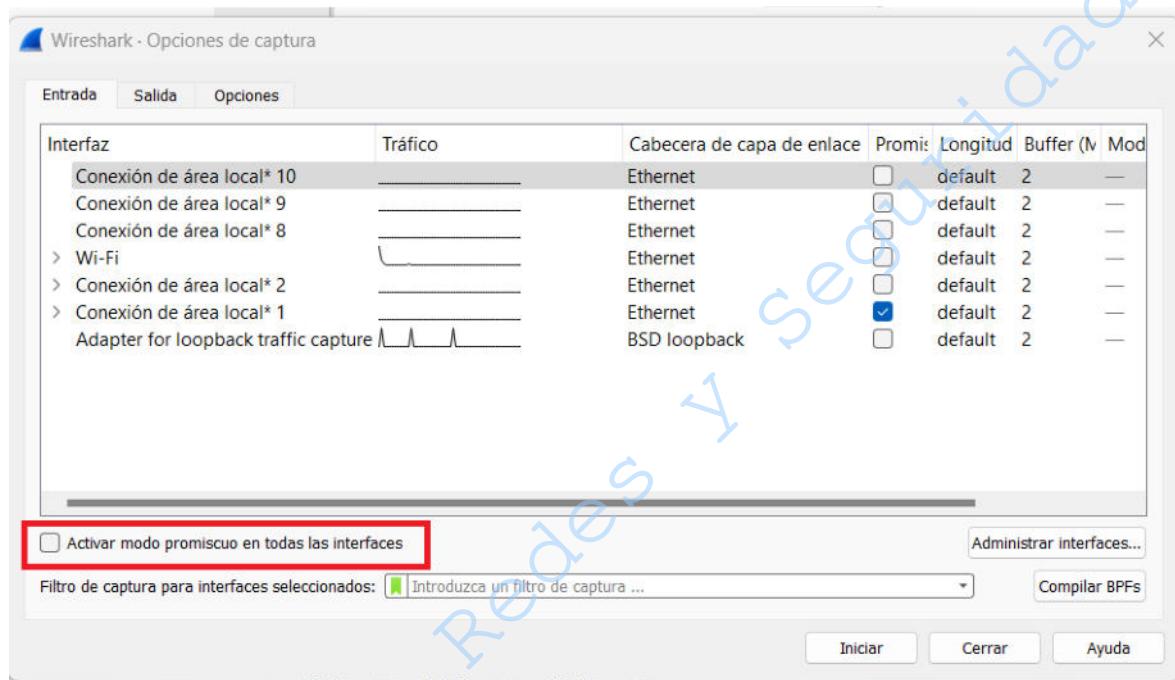


Figura No. 8. Opciones de captura.

4.2.8.5 Dé clic en la opción *Analizar* y seleccione del menú *Mostrar expresión de filtro* dar clic en la siguiente opción: *ARP/RARP – Address Resolution Protocol-> arp.proto.type-Protocol type*. Dé clic en *Aceptar* (Ver Figura No. 9)



Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 89/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada	

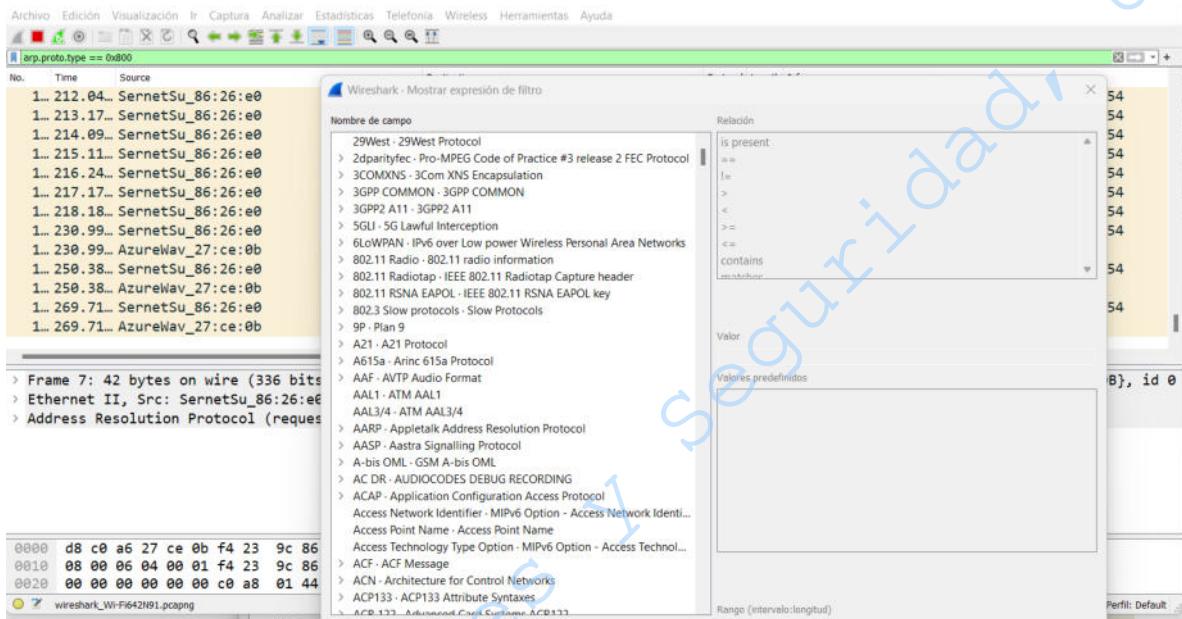


Figura No. 9. Filtro ARP.

4.2.8.6 Seleccione la flecha azul para aplicar el filtro seleccionado (Ver figura No. 10)

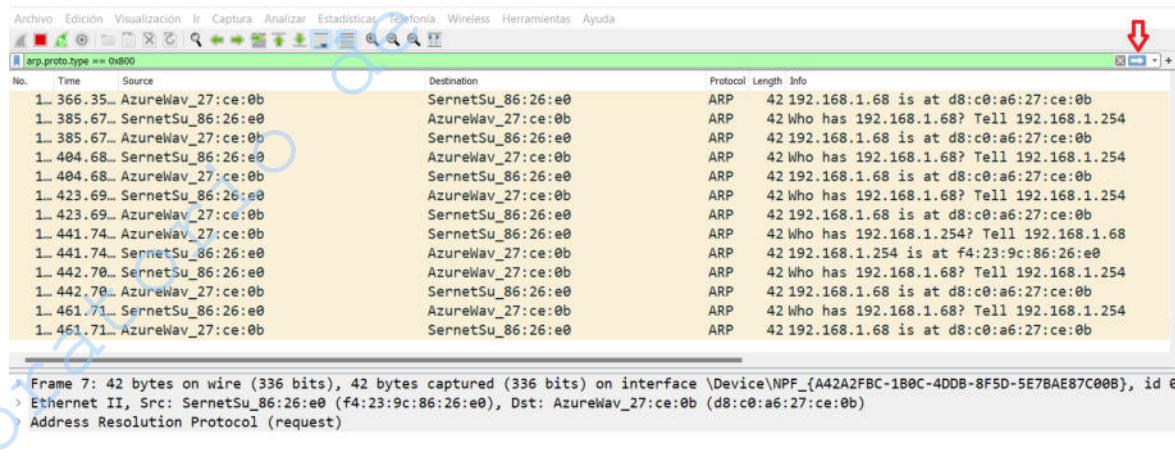


Figura No. 10. Aplicación del filtro ARP.

4.2.8.7 Borre la tabla arp, para ello, en la terminal de comandos ejecute el comando siguiente:

C:\> arp -d *

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	90/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

4.2.8.8 Visualice la tabla de ARP, para ello teclee lo siguiente:

C:\> arp -a

4.2.8.9 En la terminal de comandos ejecute el comando ping a 5 destinos diferentes, dos de ellos fuera de la red local y el resto a computadoras dentro de la red local.

4.2.8.10 Visualice la tabla de ARP, para ello teclee lo siguiente:

C:\> arp -a

4.2.8.11 Detenga la captura de Wireshark.

4.2.8.12 Realice una tabla con el contenido de la tabla del comando ARP del paso **4.2.8.10**.

4.2.8.13 Analice la información del paso anterior y comente

4.2.8.14 Vuelva a Wireshark y observe las tramas recibidas

4.2.8.15 Localice una trama ARP REQUEST y su correspondiente ARP REPLY. Analice las características de ambas tramas (Direcciones físicas y lógicas, de origen y destino) y escriba a continuación lo que observa para reconocer una trama ARP REQUEST y una trama ARP REPLY, indique cuál es el funcionamiento del protocolo ARP (Figura No. 11):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	91/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

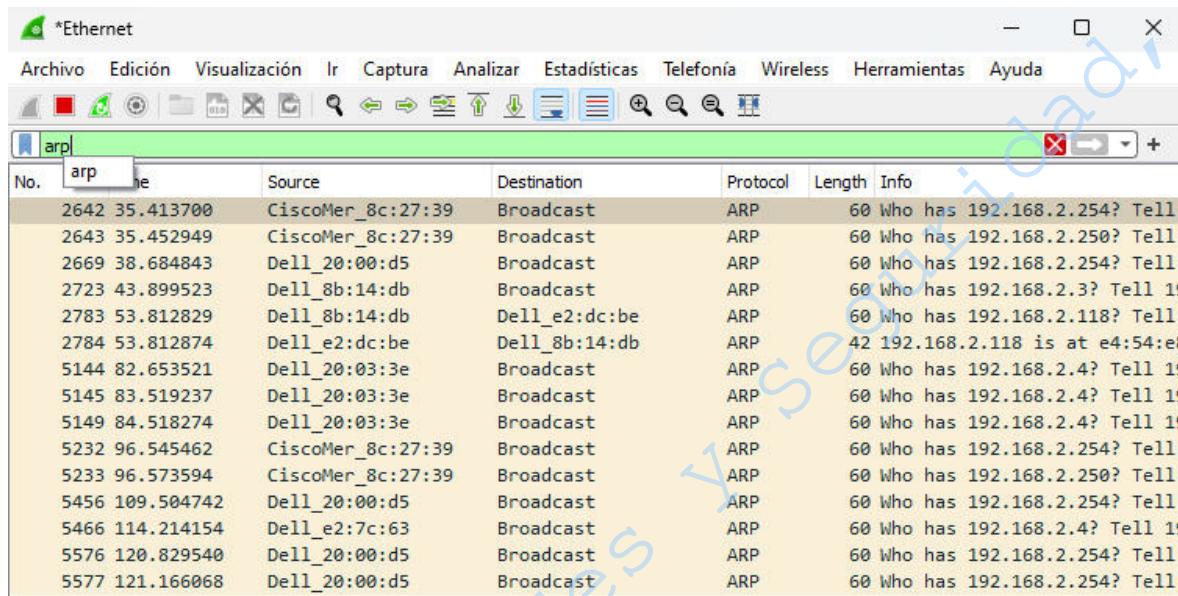


Figura No. 11 Tramas ARP REQUEST y ARP REPLY

4.2.9 Si la profesora o el profesor no indica lo contrario, cierre sesión.

5.-Cuestionario

1. ¿En qué casos utilizaría el comando *tcpdump*?

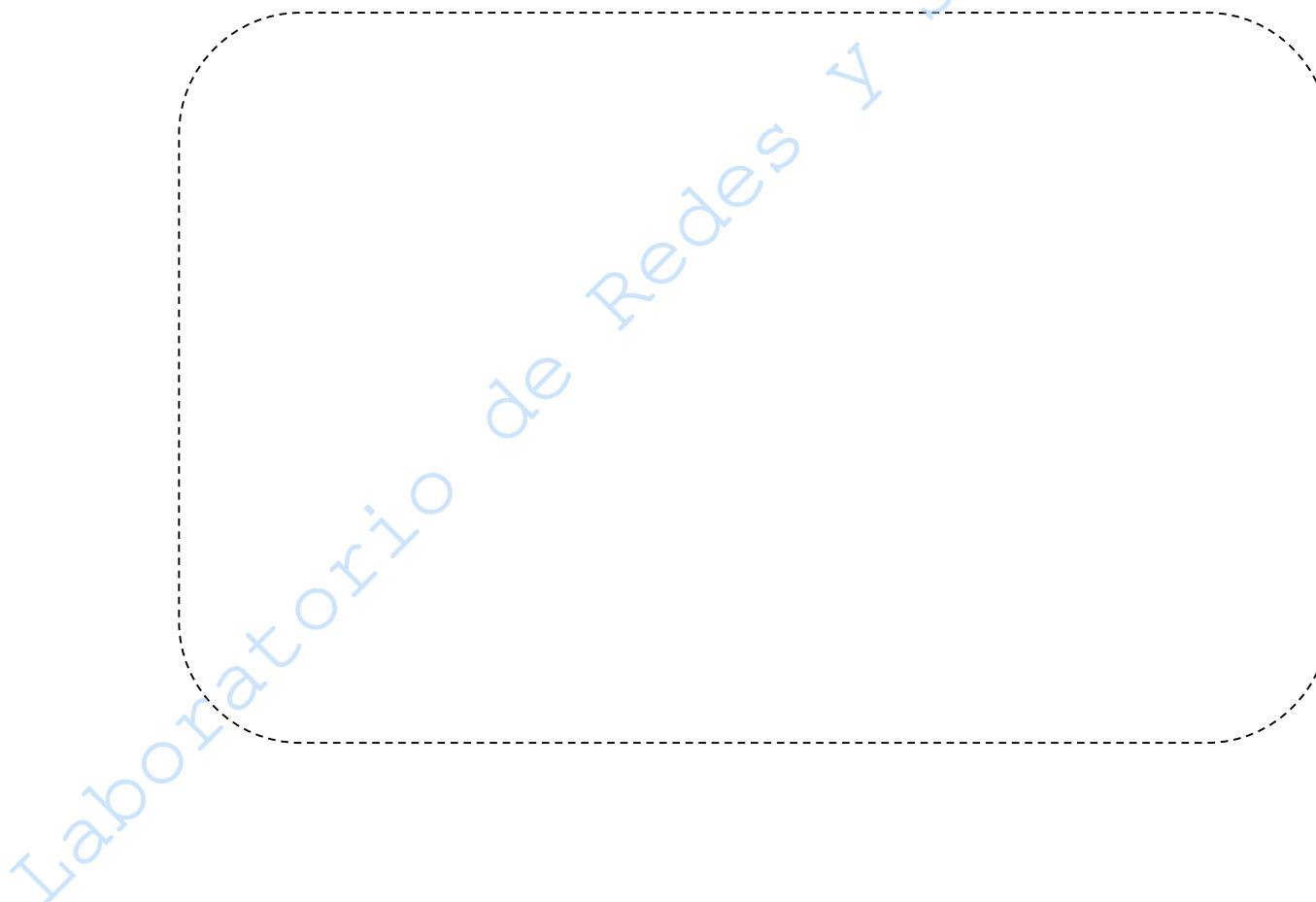
2. ¿En qué casos utilizaría el comando *traceroute* o *tracert*?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 92/479 8.3 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

3. De acuerdo con lo visto en la práctica ¿En qué casos utilizaría un analizador de paquetes?
-
-
-

6.-Conclusiones

Revise los objetivos planteados al inicio de la práctica y escriba sus conclusiones



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	93/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA 6
Encaminamiento y análisis de paquetes
Cuestionario Previo

1. Describa las funciones de la capa 3 (capa de red) del Modelo OSI
2. ¿Cuáles son los principales campos que forman la trama Ethernet?
3. ¿Cuáles son los principales campos que forman un paquete IP?
4. ¿Para qué se usa el comando apt-get install tcpdump o apt install tcpdump?
5. Defina el concepto de encaminamiento
6. Investigue el objetivo y funcionamiento del protocolo ARP
7. Descargue el software NeoTrace (o equivalente) y visualice en el modo Node View el camino que siguen los paquetes hacia un servidor localizado en:
 - a. www.google.com
 - b. www.youtube.com
 - c. wikipedia.com
 - d. Otra liga de su preferencia

Realice impresiones de pantalla e inclúyelas en la entrega de este previo.

8. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 94/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

Práctica 7

Configuración básica del router

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 95/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

1.- Objetivo de Aprendizaje

- El alumno o la alumna realizará la configuración básica y manipulará de manera lógica equipos de interconexión como lo son los routers, mediante el uso de la herramienta de simulación de redes: Packet Tracer.

2.- Conceptos teóricos

El router es un dispositivo hardware o bien un software corriendo sobre una computadora, encargado principalmente de tomar decisiones de paquetes de acuerdo con las tablas de ruteo almacenadas. Normalmente un router cuenta con al menos 2 interfaces de red, como pueden ser seriales o ethernet y puertos de consola auxiliar, ver Figura No. 1.

La principal responsabilidad de un router es dirigir los paquetes destinados a redes locales y remotas al:

- Determinar la mejor ruta para enviar paquetes
- Enviar paquetes hacia su destino



Figura No. 1 Router CISCO

En el caso de los routers Cisco, son dispositivos hardware con un sistema operativo propietario llamado IOS, Sistema Operativo de Red (Internetworking Operating System), que además de su función fundamental, es capaz de hacer filtrado de paquetes, firewalling, traducción de direcciones, priorización de tráfico, etc.

Cuando un router identifica la dirección IP de un paquete determina cuál es el camino que debe seguir, decidiendo si envía el paquete de información por cable o por satélite, dependiendo de la lejanía.

Es posible clasificar el encaminamiento:

- Encaminamiento estático: los cuales no determinan rutas, por lo que es necesario configurar la tabla de ruteo, especificando las rutas potenciales para los paquetes.
- Encaminamiento dinámico: que tienen la capacidad de determinar rutas y encontrar la más óptima de acuerdo con la información de los paquetes y de otros routers.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	96/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

En la comunicación existen dispositivos que mantienen el enlace WAN entre un dispositivo de envío y uno de recepción:

- Equipo de comunicación de datos (DCE): Un dispositivo que suministra los servicios de temporización a otro dispositivo. Habitualmente este dispositivo se encuentra en el extremo del enlace que proporciona el acceso WAN.
- Equipo terminal de datos (DTE): Un dispositivo que recibe los servicios de temporización desde otro dispositivo y se ajusta en consecuencia. Habitualmente este dispositivo se encuentra en el extremo del enlace del cliente WAN o del usuario.

3.- Equipo y material necesario

Equipo del Laboratorio:

- Software de simulación CISCO, Packet Tracer

4.- Desarrollo:

La práctica tiene por objetivo conocer los comandos básicos de un router Cisco empleando el simulador Packet Tracer, ésta es una herramienta que permite el diseño, construcción y configuración directa de varios dispositivos de una red.

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Conociendo al dispositivo

- 4.1.1** Indique los componentes de la vista posterior del router (ver Figura No. 2) en la Tabla No.1.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	97/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

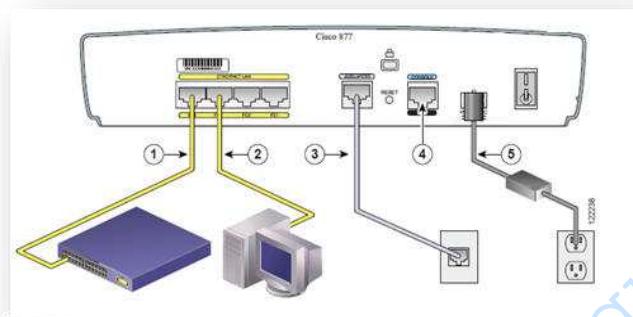


Figura No. 2. Componentes del router CISCO

Tabla No. 1. Relación de componentes del router CISCO

No.	Componente
1	
2	
3	
4	
5	

4.2 Conociendo la interfaz de Packet Tracer (PT)

4.2.1 Ejecute el software Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 3)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 98/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

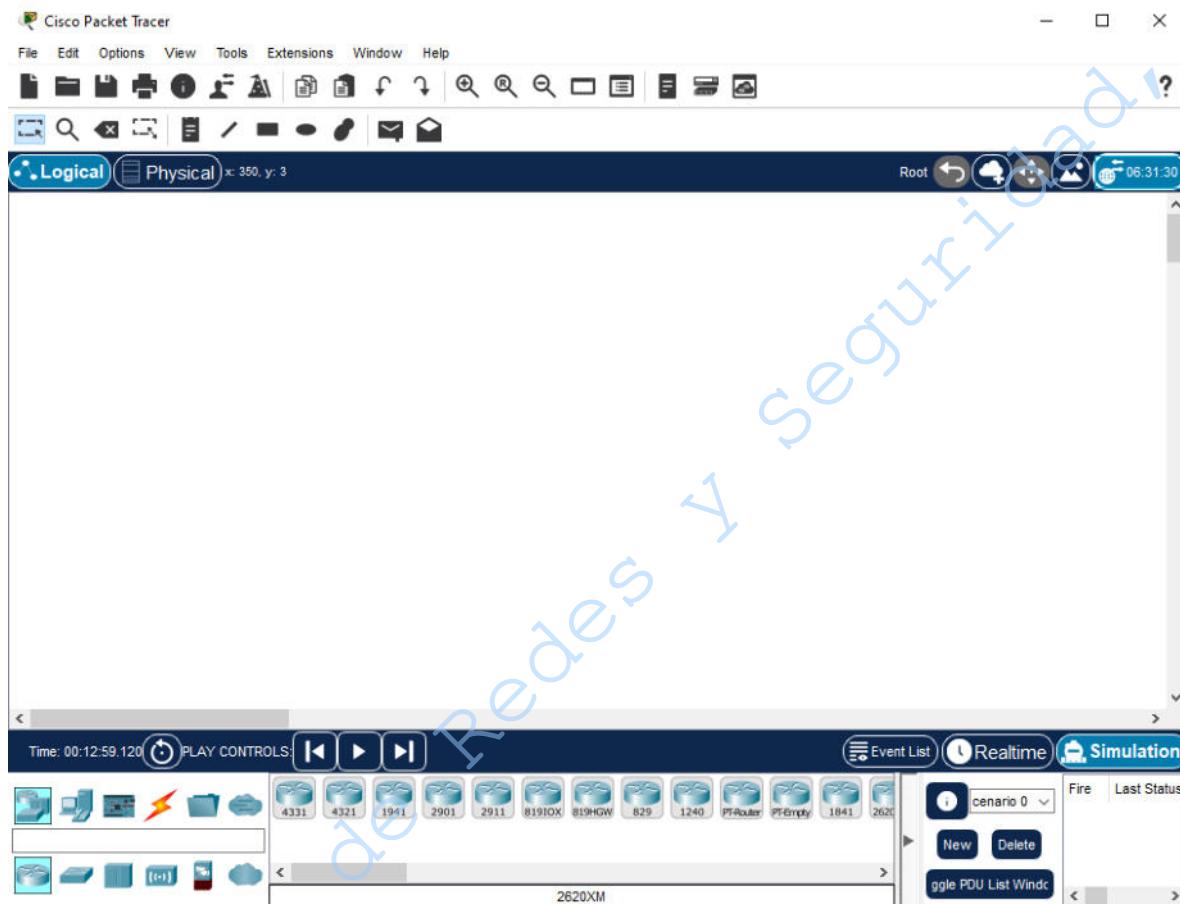


Figura No. 3. Interfaz gráfica de PT

- 4.2.2 Cuando Packet Tracer se inicia, muestra por default una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.
- 4.2.3 En la esquina inferior izquierda de la interfaz se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo (Ver figura No. 4.).



Figura No. 4. Secciones de dispositivos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 99/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.4** La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos, en el cuadro de texto del centro aparece el nombre de este grupo.
- 4.2.5** La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán.
- 4.2.6** La topología que deberá implementar se observa en la figura No. 5:

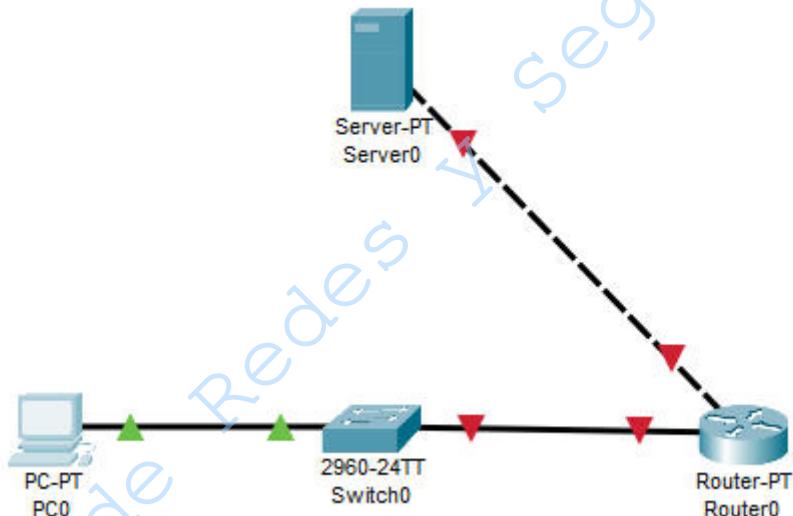


Figura No. 5 Topología

Arrastre al área lógica de trabajo los siguientes dispositivos: un servidor, una PC (el servidor y la PC pueden encontrarse en la opción End Devices, ver Figura No. 6), un router genérico (es decir, seleccione el router que diga Router-PT) y un switch 2960.

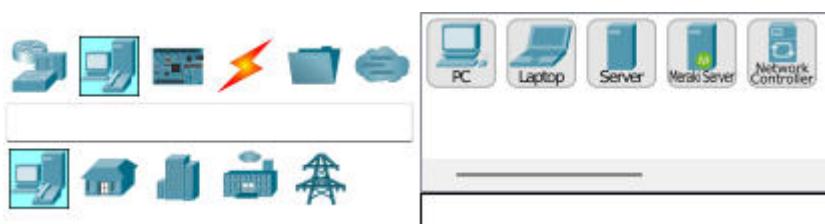


Figura No. 6 End Devices

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 100/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.7** Conecte la PC con el switch; para ello elija Connections en la sección de Grupos de Dispositivos. En el campo de Dispositivos Específicos, elija el tipo de cable Copper Straight-Through (Cable de Cobre Directo). (Ver figura No. 7)

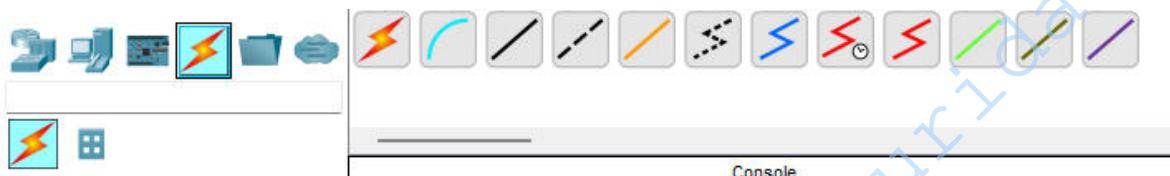


Figura No. 7. Tipos de cables de conexión.

- 4.2.8** Una vez elegido el tipo de conexión, dé clic izquierdo sobre el switch, con ello se desplegará una lista de los puertos a los que es posible conectar el cable; elija el puerto FastEthernet0/2 (Ver figura No. 8)

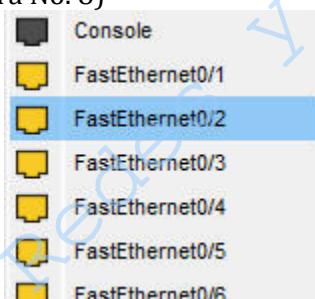


Figura No. 8. Puertos del switch

- 4.2.9** Para conectar el otro extremo del cable a la PC, dé clic sobre ésta. Igualmente aparecerá un listado de los puertos, seleccione el FastEthernet0.

- 4.2.10** A continuación, deberá conectar el resto de los dispositivos de la siguiente forma, indique qué tipo de cable empleará en cada caso:

- Switch (Puerto FastEthernet0/1) al Router (Puerto FastEthernet0/0)
Cable: _____
- Servidor (Puerto FastEthernet0) al Router (Puerto FastEthernet1/0)
Cable: _____

- 4.2.11** Para realizar las conexiones apropiadamente tendrá que elegir el tipo de cable adecuado, así como los puertos de los dispositivos. Muestre el resultado a su profesora o profesor.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 101/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.12** Una vez realizadas las conexiones adecuadas, para que la red esté completamente funcional se deberán hacer las configuraciones propias de cada dispositivo, lo cual será actividad de otra práctica.

4.3 Comandos básicos del router

- 4.3.1** Para configurar el router mediante la interfaz consola del dispositivo, dé doble clic sobre el router y aparecerá su ventana de gestión y dé clic en la pestaña CLI (Ver Figura No. 9). Espere unos segundos a que se cargue el sistema operativo del router.

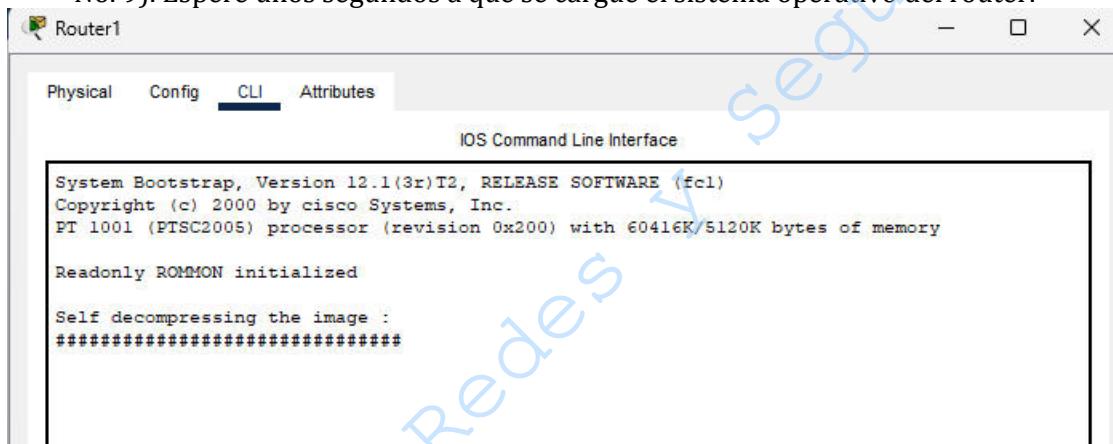


Figura No. 9. Interfaz de consola del router.

- 4.3.2** Una vez iniciado el sistema operativo del router, aparecerá un mensaje, si se desea continuar con el diálogo de configuración, escriba **no** y presione dos veces **enter**, con lo que aparecerá el prompt:

Router>

- 4.3.3** Haga uso de la función de ayuda, para ello teclee el comando de ayuda escribiendo **?**.

Router>?

- 4.3.4** Complete la Tabla No. 2 con cuatro comandos disponibles del router, que muestra el comando de ayuda. Escriba su descripción en español

Tabla No. 2. Comandos disponibles

Comando	Descripción
enable	
show	
resume	
terminal	

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	102/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

4.3.5 Los routers funcionan con tres modos básicos:

- a) **Modo de usuario**, en este modo se entra por defecto, permite pocas opciones, principalmente las relacionadas con estadísticas.
- b) **Modo privilegiado**, entramos en éste mediante el comando **enable** y es similar a un root en un sistema operativo Linux.
- c) **Modo de configuración**, entramos en él mediante el comando **configure terminal** y permite modificar la configuración del router.

4.3.6 Para cambiar a modo privilegiado, teclee **enable**, recuerde observar el prompt ahora finalizado con el símbolo #

Router>enable
Router#

4.3.7 Entre en el modo ayuda tecleando ?

Router# ?

4.3.8 Anote cinco comandos disponibles, sin descripción, del modo privilegiado del router.

4.3.9 Teclee el siguiente comando

Router# show ?

4.3.10 Anote cinco opciones disponibles y sus respectivas descripciones, que presenta el comando **show**

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	103/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.3.11 El comando **show running-config** o **show startup-config**, dentro del modo privilegiado, muestra la configuración del dispositivo cisco actual. La versión corta del comando anterior es **sh run**.

4.3.12 Muestre la configuración inicial del router. Tecleando el siguiente comando:

Router#show running-config

4.3.13 Anote una breve explicación de la salida del comando anterior:

4.3.14 Investigue las formas de acceso a un router CISCO

4.3.15 Para salir del modo privilegiado se pueden usar los comandos **disable** o **exit**. Pruebe ambos comandos y describa a continuación la diferencia entre ellos:

4.3.16 Para salir de la terminal ejecute el comando **logout** o **exit**.

NOTA: Siempre verifique el prompt antes de realizar algún cambio a la configuración de un router.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	104/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.3.17 Investigue los componentes internos de un router y descríbalos a continuación.

4.3.18 Para entrar en el modo configuración del router CISCO, es posible ejecutar cualquiera de las tres siguientes instrucciones en modo privilegiado:

- a) configure terminal.
- b) config t.
- c) configure

4.3.19 Ejecute el comando configure terminal en el modo privilegiado:

Router# configure terminal

4.3.20 Indique el nuevo formato del prompt

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	105/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.21** Dentro del modo configuración es posible manipular las interfaces de un router. Para realizar cambios sobre éstas, es necesario teclear el comando `interface` en modo configuración. Teclee el comando `interface ?` para conocer las opciones de la instrucción.

- 4.3.22** Anote cinco opciones disponibles que presenta el comando anterior
-
-
-
-
-

- 4.3.23** Es posible asignar un nombre a un router, el cual no afecta su funcionamiento ni comportamiento dentro de las redes, esto mediante la instrucción `hostname`, en el modo configuración.

Nota: NOMBRE se sustituirá por el nombre que deseé darle al dispositivo, colocar alguno de su elección, por ejemplo LabRD, sus_iniciales, R1, etcétera

Para ello teclee las siguientes instrucciones.

```
Router(config)#hostname NOMBRE
NOMBRE (config)#{
```

- 4.3.24 Configuración de las contraseñas**

Las contraseñas son las llaves del sistema, por lo que deben ser lo más seguras posibles para evitar inicios de sesión no autorizados, siendo éste el primer paso hacia problemas de seguridad mayores. El uso de contraseñas lo suficientemente fuertes como para minorizar un ataque, es un paso decisivo y a la vez sencillo que ahorra problemas en el futuro. Para configurar la contraseña del modo privilegiado, debe ejecutar la siguiente instrucción en la CLI en modo configuración, de esta manera cuando vuelva a iniciar el modo privilegiado, el IOS solicitará una contraseña.

- 4.3.24.1 Configuración de la contraseña del modo privilegiado del router.**

A esta contraseña también se le conoce como contraseña autorizada, para ello teclee los siguientes comandos:

```
NOMBRE (config)# enable password CONTRASEÑA
NOMBRE (config)#exit
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	106/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

NOTA: CONTRASEÑA se sustituirá por cualquier término que desee darle al dispositivo, colocar alguna de su elección, por ejemplo cisco, seguridad, etcétera

CONTRASEÑA _____

1. Para probar la nueva contraseña, es necesario salir del modo configuración, tecleando nuevamente el comando **exit**, hasta salir del modo privilegiado. Al iniciar sesión en el router presionando la tecla **Enter** y cambiando a modo privilegiado con el comando **enable**, el router solicita una contraseña, el siguiente paso será introducir la contraseña que estableció.
2. A continuación teclee el comando **show running-config**, y observe que la contraseña puede ser vista con este comando en la configuración del router.

4.3.24.2 Configuración de la contraseña del modo privilegiado del router (contraseña secreta autorizada)

1. Ingrese al modo configuración del router y teclee los siguientes comandos:

NOMBRE (config)#enable secret CONTRASEÑA_SECRETA_AUT
NOMBRE (config)#exit

Nota: CONTRASEÑA_SECRETA_AUT se sustituirá por cualquier palabra secreta que desee darle al dispositivo, colocar alguna de su elección, por ejemplo networking, secure55, etcétera.

CONTRASEÑA SECRETA AUTORIZADA _____

2. En el modo privilegiado, nuevamente escriba el comando **show running-config**. Observe los cambios realizados. Anote sus observaciones:

3. Use el comando **exit** para salir de modo privilegiado. Y reingrese con el comando **enable**. El router solicitará una contraseña, pruebe con la contraseña dada en el punto 4.3.24.1. Como puede observar, el router ya no acepta ese password, ahora intente con la palabra secreta dada en el punto 4.3.24.2.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	107/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4. ¿Qué diferencias hay entre la contraseña autorizada y la contraseña secreta autorizada?
(Anote sus observaciones e investigue el uso del comando **enable secret**)

4.3.24.3 Configuración de la contraseña de consola en el router

Para configurar la contraseña de la consola, ingrese al modo de configuración global y teclee los siguientes comandos:

```
NOMBRE(config)#line console 0
NOMBRE (config-line)#password cisco
NOMBRE (config-line)#login
NOMBRE (config-line)#exit
NOMBRE (config)#+
```

4.3.24.4 Configuración de la contraseña de las líneas de la terminal virtual

Para configurar la contraseña de una conexión tipo telnet se debe acceder a la configuración de las terminales virtuales a través de los siguientes comandos:

```
NOMBRE (config)# line vty 0 4
NOMBRE (config-line)#password cisco
NOMBRE (config-line)#login
NOMBRE (config-line)#exit
NOMBRE (config)#+
```

1. A qué se refiere cada uno de los componentes de la instrucción **line vty 0 4**

2. Cómo se debe configurar la contraseña de puerto AUXILIAR del router.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	108/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.3.25 Configuración de una interfaz FastEthernet

La configuración de las interfaces de un router, es el proceso más importante, debido a que sin ellas, el router es inservible, motivo por el cual su configuración debe estar activa al momento de comunicarse con otros dispositivos.

4.3.25.1 Introduzca el comando **interface FastEthernet ?** el cual proporcionará las etiquetas de las interfaces de red soportadas.

4.3.25.2 Seleccione la interfaz FastEthernet 0/0

NOMBRE (config)#int FastEthernet 0/0

4.3.25.3 Para configurar la interfaz FastEthernet del router, realice los siguientes pasos:

```
NOMBRE (config-if)#ip address 192.168.2.X 255.255.255.0
NOMBRE (config-if)#no shutdown
NOMBRE (config-if)#exit
NOMBRE (config)#exit
```

NOTA: La X deberá sustituirse por un número entre el 1 y el 254

4.3.25.4 Guarde la información de la configuración desde el modo de comandos de privilegiado.

NOMBRE #copy running-config startup-config

4.3.25.5 Se pedirá confirmación, teclee Enter.

4.3.25.6 Investigue para qué se emplea el comando **no shut** en los routers CISCO

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	109/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada	

4.3.25.7 Visualice la información de la configuración de la interfaz. Teclee lo siguiente:

NOMBRE # show interface FastEthernet 0/0

4.3.25.8 Escriba la información relacionada con los siguientes campos:

FastEthernet0/0 _____

Line protocolo _____

Internet address _____

Encapsulation _____

4.3.25.9 Cierre la ventana de configuración del router.

4.3.26 Configuración del host

4.3.26.1 Dé clic sobre la PC, en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.3.26.2 Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.

4.3.26.3 Se abrirá una ventana solicitando la dirección IP, máscara de red, el gateway y DNS. Ingrese los datos que se muestran en la Tabla No.3.

Tabla No.3. Datos para la configuración del host.

IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.X
DNS Server	

NOTA: La X deberá sustituirse por el número dado en el punto **4.3.25.3**

4.3.26.4 Cierre las dos ventanas de configuración de la PC.

4.4 Pruebas y aplicaciones

Existen diversas utilidades empleadas para verificar la conectividad del router, tales como:

1. ping.
2. traceroute.
3. telnet.
4. show interface.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	110/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- 4.4.1** Para comprobar que existe comunicación con el host, ingrese al CLI del router y teclee lo siguiente:

NOMBRE > ping 192.168.2.2

- 4.4.2** Anote la salida del comando anterior
-
-
-

- 4.4.3** Visualice la configuración final del router en el modo privilegiado a través del siguiente comando:

NOMBRE # show running-config

EJERCICIO OPCIONAL

4.5 Configuración entre routers

De manera opcional se procederá a completar la red, agregando y configurando otros elementos para lograr establecer comunicación entre las dos redes LAN. Para ello realice lo siguiente (Ver Figura 10):

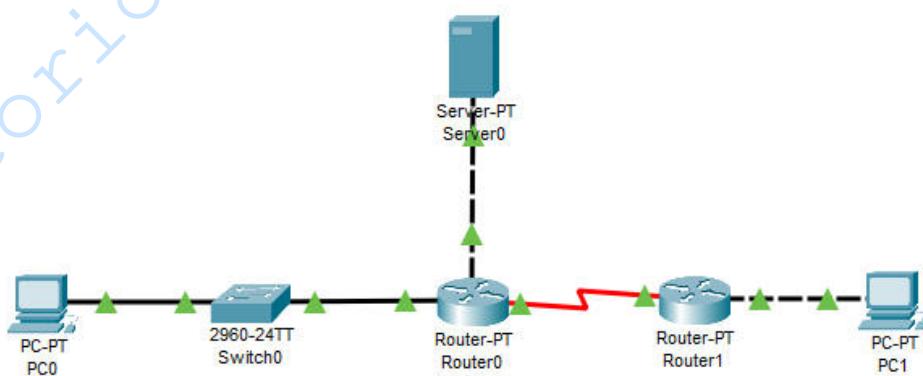


Figura No. 10 Topología de red final

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 111/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

4.5.1 Agregue al área de trabajo otro router genérico (seleccione el primero que aparece en la lista y que al colocarlo en el área lógica diga Router-PT) y otra PC.

4.5.2 Conecte los dispositivos de la siguiente manera :

- El Router0 (puerto Serial2/0) con Router1 (puerto Serial2/0) mediante el **cable Serial DCE**.
- Router1 (puerto FastEthernet0/0) con la PC (puerto FastEthernet).

NOTA: Tomar en cuenta el orden indicado de la conexión serial entre los routers, ya que el reloj será configurado en el Router0.

4.5.3 Ahora que los dispositivos han sido conectados adecuadamente, es necesario configurar las interfaces. Iniciaremos con la Serial2/0 del Router0, ingresando a la línea de comandos CLI.

4.5.4 Acceda al modo configuración y teclee lo siguiente:

```
NOMBRE (config)#interface Serial 2/0
NOMBRE (config-if)#ip address 192.168.3.150 255.255.255.0
NOMBRE (config-if)#clock rate 128000
NOMBRE (config-if)#no shutdown
NOMBRE (config-if)#exit
NOMBRE (config)#exit
```

4.5.5 Configure de la misma manera, el Router1 y PC1 con los siguientes datos:

a) Router1 Serial2/0 (Ver tabla No. 5):

Tabla No. 5. Configuración del Router1.

IP	192.168.3.151
Netmask	255.255.255.0

b) Router1 FastEthernet0/0(Ver tabla No. 6):

Tabla No. 6. Interfaz FastEthernet del router.

IP	192.168.4.1
Netmask	255.255.255.0

c) PC1 FastEthernet (Ver tabla No. 7):

Tabla No. 7. Configuración de la PC1.

IP Address	192.168.4.2
------------	-------------

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	112/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Default Gateway	192.168.4.1
Netmask	255.255.255.0

4.5.6 Finalmente se configurará la forma en que los routers encaminarán los paquetes. Para el Router0, en modo configuración, teclee los comandos adecuados para agregar las rutas estáticas correspondientes.

4.5.7 Anote a continuación los comandos ejecutados:

4.5.8 Realice el mismo procedimiento del paso anterior para el Router1. Anote los comandos ejecutados:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	113/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.5.9** Para comprobar la comunicación entre las PC's, realice un ping. Abra la ventana de configuración de la PC0 e ingrese a la pestaña Desktop. Dé doble clic sobre Command Prompt para abrir la línea de comandos (Ver Figura No. 11)



Figura No. 11. Command Prompt

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	114/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.5.10 Teclee:

PC> ping 192.168.4.2

4.5.11 ¿Se logró establecer la comunicación? Explique.

4.5.12 ¿Qué tipo de cable usó para interconectar el Router1 con la PC1? ¿Por qué?

5.-Conclusiones

Revise los objetivos planteados al inicio de la práctica y escriba sus conclusiones

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	115/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 7
Configuración básica del router
Cuestionario Previo

1. Investigue las siguientes 3 funciones de la capa de red:
 - a. Determinación del camino
 - b. Encaminamiento
 - c. Establecimiento de la llamada
2. ¿Qué es un router y cuál es su funcionamiento?
3. ¿Cuáles son los modos de configuración que maneja el router? Indique sus privilegios
4. Investigue las formas de acceso a un router CISCO
5. ¿Qué son los servicios ADSL y POTS?
6. ¿Qué es una tabla de encaminamiento?
7. Explique las características principales del encaminamiento estático.
8. Explique las características principales del encaminamiento dinámico.
9. ¿Cómo funcionan los protocolos por vector-distancia? Menciona dos ejemplos.
10. ¿Cómo funcionan los protocolos por estado-enlace? Menciona dos ejemplos.
11. Investigue la sintaxis de los comandos para configurar una ruta de encaminamiento estática en un router CISCO.
12. Investigue los componentes internos de un router y descríbalos a continuación
13. Investigue a qué se refieren cada uno de los componentes de la instrucción line vty 0 4
14. Investigue los comandos correspondientes que deben emplearse en el router para configurar el encaminamiento dinámico
15. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 116/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 8

TCP Y UDP

Capa 4 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	117/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno o la alumna podrá utilizar un programa que le permita enviar y recibir información utilizando los protocolos TCP y UDP y reafirmando conceptos teóricos.
- El alumno o la alumna creará un socket servidor y un socket cliente

2.- Conceptos teóricos

El programa Sock

El programa sock ofrece un modo de acceder a la interfaz de los sockets sin tener que programar. Conecta la entrada/salida estándar (teclado/pantalla) con un socket cuyas características se especifican mediante parámetros al ejecutar la orden. Mediante la redirección de la entrada o la salida se puede enviar el contenido de un archivo o almacenar en un archivo la información recibida.

Los sockets pueden ser de dos tipos: UDP o TCP, que se corresponden con un servicio sin conexión, que no garantiza ni la entrega ni el orden de entrega de la información (UDP) y otro servicio que garantiza la entrega ordenada y sin errores de la información (TCP).

Además, se sabe que una aplicación puede comenzar iniciando la comunicación (enviando información) o bien puede esperar pacientemente hasta que la otra le solicite el inicio de la comunicación (espera petición).

El programa sock va a permitir imitar cualquiera de estas situaciones entre otras.

3.- Equipo y material necesario

3.1 Material del alumno o de la alumna:

- Imagen extensión BMP con calidad de una imagen fotográfica.

3.2 Equipo del Laboratorio:

- Programa sock (sock-1.1.tar.tar).

4.- Desarrollo:

Modo de trabajar

- La práctica se desarrollará en parejas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 118/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1 Preparación del programa Sock

4.1.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 1)

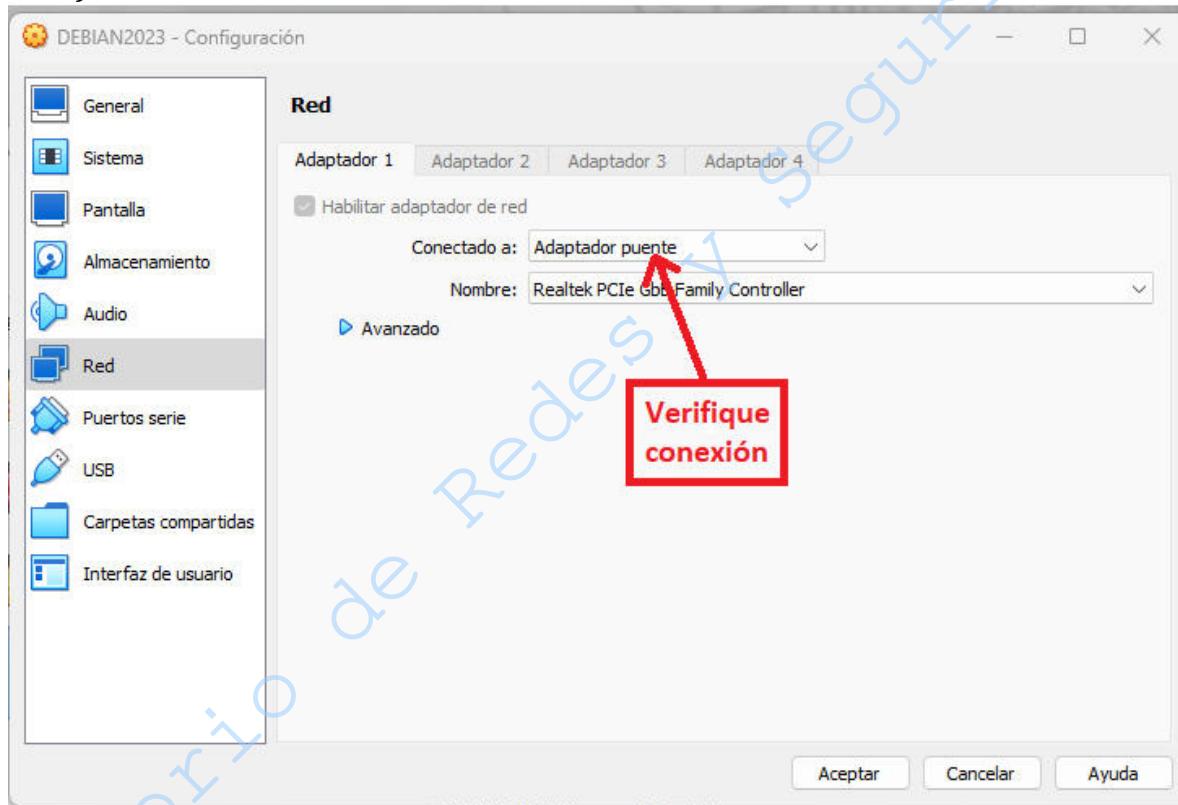


Figura No. 1. Conexión de red.

4.1.2 Elija la opción de cargar Linux, distribución Debian.

4.1.3 Inicie sesión como usuario **redes**.

4.1.4 Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 2)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	119/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```
redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes#
```

Figura No. 2. Super usuario

NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root

redes@debian:~\$ su

NOTA: Para realizar la práctica exitosamente debe tener instalado los paquetes ifconfig, gcc y ssh.

- 4.1.5** Verifique que la tarjeta de red esté debidamente configurada y que tenga asignada una dirección IP dentro del rango: 192.168.2.25-192.168.2.60. Emplee el comando ifconfig

root@debian:/home/redes# ifconfig

Anote la dirección IP _____

En caso de no cumplir con lo indicado en el punto 4.1.5, configure debidamente la tarjeta. Teclee:

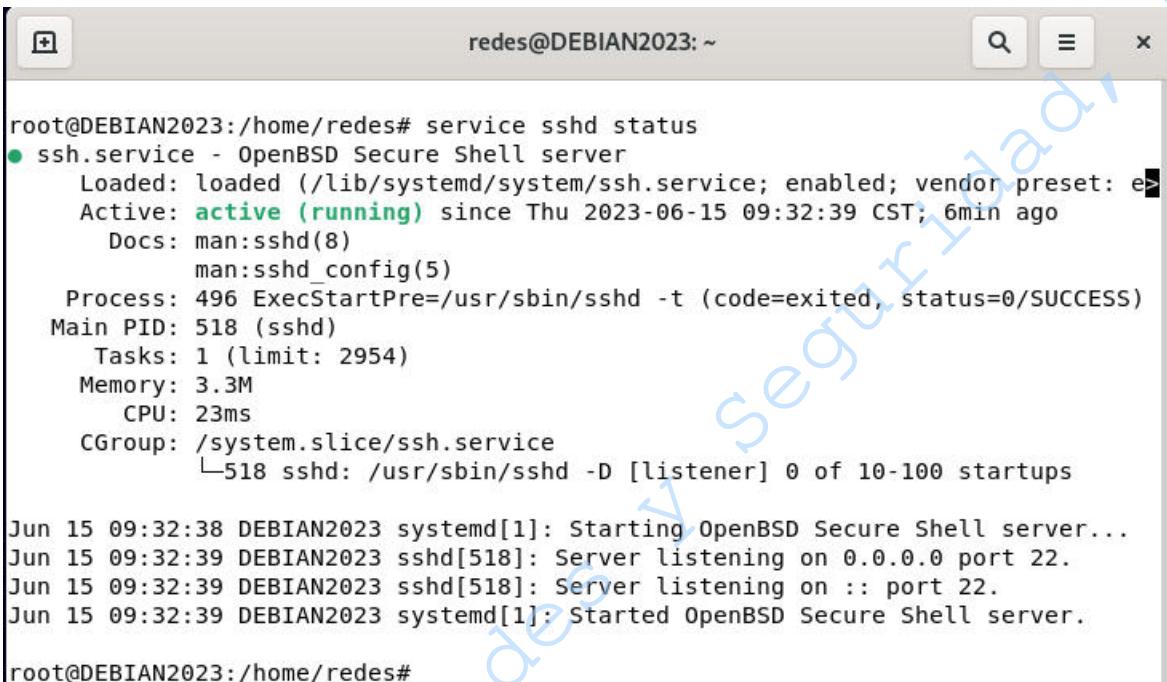
root@debian:/home/redes# ifconfig enp0s3 192.168.2.X netmask 255.255.255.0

NOTA: X se sustituye por una IP que se encuentre dentro del rango mencionado en el punto 4.1.5 para que esté dentro de la misma subred.

- 4.1.6** Verifique que la aplicación SSH se encuentre instalada (Active: active (running)) (Figura No. 3), para ello teclee:

root@debian:/home/redes# service sshd status

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	120/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			



```

root@DEBIAN2023:/home/redes# service sshd status
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
    Active: active (running) since Thu 2023-06-15 09:32:39 CST; 6min ago
      Docs: man:sshd(8)
             man:sshd_config(5)
   Process: 496 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 518 (sshd)
    Tasks: 1 (limit: 2954)
   Memory: 3.3M
      CPU: 23ms
     CGroup: /system.slice/ssh.service
             └─518 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Jun 15 09:32:38 DEBIAN2023 systemd[1]: Starting OpenBSD Secure Shell server...
Jun 15 09:32:39 DEBIAN2023 sshd[518]: Server listening on 0.0.0.0 port 22.
Jun 15 09:32:39 DEBIAN2023 sshd[518]: Server listening on :: port 22.
Jun 15 09:32:39 DEBIAN2023 systemd[1]: Started OpenBSD Secure Shell server.

root@DEBIAN2023:/home/redes#

```

Figura No. 3. Verificación de SSH

NOTA: En caso de que no se encuentre instalada, debe teclear el siguiente comando para instalarla (Figura No. 4):

root@debian:/home/redes# apt-get install ssh



```

root@DEBIAN2023:/home/redes# apt-get install ssh

```

Figura No. 4. Instalación de SSH

4.1.7 Teclee los siguientes comandos para eliminar cualquier archivo existente cuyo nombre inicie con **prac** (Figura No. 5)

root@debian:/home/redes# rm -rf prac*
root@debian:/home/redes# exit

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	121/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```
root@DEBIAN2023:/home/redes# rm -rf pract*
root@DEBIAN2023:/home/redes# exit
```

Figura No. 5. Eliminación de archivos

4.1.8 Salga de la cuenta de superusuario y emplee la cuenta de redes.

4.1.9 Cree el subdirectorio ***practica*** dentro del directorio actual (Ver Figura No. 6)

NOTA: Evite cambiarle el nombre al subdirectorio, deberá llamarse ***practica***, sin ningún número posteriormente ni abreviatura alguna, nombres como ***prac8***, ***p8***, ***practica8***, etcétera, serán inválidos.

redes@debian:~\$ mkdir practica



```
redes@DEBIAN2023:~$ mkdir practica
redes@DEBIAN2023:~$
```

Figura No. 6. Creación del subdirectorio practica

4.1.10 Copie el archivo ***sock-1.1.tar.tar*** dentro del subdirectorio ***practica***. (Ver figura No. 7)

redes@debian:~\$ cp sock-1.1.tar.tar /home/redes/practica



```
redes@DEBIAN2023:~$ cp sock-1.1.tar.tar /home/redes/practica/
redes@DEBIAN2023:~$
```

Figura No. 7. Copia del archivo sock

4.1.11 Cámbiese al subdirectorio ***practica*** y descomprima el archivo ***sock-1.1.tar.tar*** (Ver Figura No. 8)

redes@debian:~\$ cd practica
redes@debian:~/practica\$ tar xvf sock-1.1.tar.tar

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	122/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

redes@DEBIAN2023:~$ cd practica/
redes@DEBIAN2023:~/practica$ tar xvf sock-1.1.tar.tar
sock-1.1/
sock-1.1/ChangeLog
sock-1.1/Makefile.in
sock-1.1/config.h.in
sock-1.1/configure
sock-1.1/configure.in
sock-1.1/install-sh
sock-1.1/sock.c
sock-1.1/README
sock-1.1/sock.1
sock-1.1/sock.lsm
sock-1.1/debian/
sock-1.1/debian/changelog
sock-1.1/debian/control
sock-1.1/debian/copyright
sock-1.1/debian/rules
redes@DEBIAN2023:~/practica$ █

```

Figura No. 8. Archivos en sock antes comprimidos.

4.1.12 Sitúese dentro del subdirectorio sock-1.1 y ejecute la orden **./configure** con la que el programa quedará preparado para su compilación y montaje. (Ver Figura No.9)

```

redes@debian:~/practica$ cd sock-1.1
redes@debian:~/practica/sock-1.1$ ./configure

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	123/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

```

redes@DEBIAN2023:~/practica$ cd sock-1.1/
redes@DEBIAN2023:~/practica/sock-1.1$ ./configure
creating cache ./config.cache
checking for gcc... gcc
checking whether the C compiler (gcc ) works... yes
checking whether the C compiler (gcc ) is a cross-compiler... no
checking whether we are using GNU C... yes
checking whether gcc accepts -g... yes
checking whether warnings should be enabled... yes
checking for a BSD compatible install... /usr/bin/install -c
checking for gethostbyname in -lresolv... yes
checking for socket in -lsocket... no
checking for gethostbyname in -lnsl... yes
checking how to run the C preprocessor... gcc -E
checking for ANSI C header files... yes
checking for pid_t... yes
checking return type of signal handlers... void
updating cache ./config.cache
creating ./config.status
creating Makefile
creating config.h
redes@DEBIAN2023:~/practica/sock-1.1$
```

Figura No. 9. Configuración de archivos y creación de un “Makefile”

4.1.13 Compile el programa. Ahora ya se dispone del programa sock ejecutable. (Ver figura No. 10)

redes@debian:~/practica/sock-1.1\$ make



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	124/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

```
redes@DEBIAN2023:~/practica/sock-1.1$ make
gcc -g -O2 -Wall -Wno-parentheses -Wstrict-prototypes -Wno-unused -lssl
-lresolv  sock.c  -o sock
sock.c: In function 'main':
sock.c:461:37: warning: pointer targets in passing argument 3 of 'accept' differ in signedness [-Wpointer-sign]
  461 |     int ns = accept(sk, sa_incoming, &l);
                  ^~
                  |
                  int *
In file included from sock.c:18:
/usr/include/x86_64-linux-gnu/sys/socket.h:233:28: note: expected 'socklen_t * restrict' {aka 'unsigned int * restrict'} but argument is of type 'int *'
  233 |     socklen_t * __restrict __addr_len);
                                         ^~~~~~
```

Figura No. 10. Compilación de archivos

4.2 Clientes TCP

4.2.1 Observe qué sucede cuando un navegador se dirige a un servidor de web y le solicita una página. En el shell teclee lo siguiente y después de pulsar la tecla “ENTER”, escriba el texto GET / HTTP/1.0 Finalice presionando dos veces “ENTER” (Ver figura No. 11).

```
redes@debian:~/practica/sock-1.1$ ./sock -e www.fi-b.unam.mx:80  
GET / HTTP/1.0
```

```
redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -e www.fi-b.unam.mx:80  
GET / HTTP/1.0
```

Figura No. 11. Socket hacia www.fi-b.unam.mx

Con esto se está conectando al servidor www.fi-b.unam.mx (que es el servidor web de la DIE) al puerto 80, que es donde se encuentra este servicio habitualmente (well-known port) y se utiliza el protocolo TCP. Lo que se está haciendo es crear un socket en nuestra computadora. Ese socket, que actúa como cliente, lo conectamos al servidor de web de la DIE y le solicitamos que nos envíe el contenido de su página web inicial. La conexión iniciada por el programa `sock` se realiza al puerto 80 del servidor www.fi-b.unam.mx y dura sólo lo indispensable hasta que se entrega la página web solicitada. Es importante destacar que la respuesta del servidor contiene una información del protocolo HTTP (o cabecera) a la que

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	125/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

sigue, después de una línea en blanco, el código HTML de la página solicitada. Tras enviar esa información el servidor cierra la conexión, con lo cual la ejecución de la orden sock finaliza.

4.2.2 En la terminal teclee lo siguiente:

```
redes@debian:~/practica/sock-1.1$ ./sock :22
```

Deberá obtener como resultado algo similar a: (Ver figura No. 12).



```
redes@DEBIAN2023: ~/practica/sock-1.1$ ./sock :22
SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1
```

Figura No. 12. Socket usando el puerto 22

Observará que el programa no finaliza, para que lo haga pulse las teclas <CTRL>+<c>.

En este ejercicio se está conectando con el servidor SSH local que se está ejecutando en la misma computadora desde el que ejecuta la orden. Esto es así porque al no especificar un servidor y sólo un puerto (22) se entiende que nos referimos a la computadora local.

El servidor SSH comienza enviando una cadena que identifica la versión del programa, y eso es lo que obtenemos como resultado.

4.3 Servidor TCP

Los programas pueden esperar pacientemente a que se les solicite algo antes de enviar alguna información. Éste es el comportamiento de muchos servidores. Utilizando el programa sock va a crear un servidor cuya única función es esperar a que un cliente se conecte y luego conecta la entrada y salida estándar con ese cliente.

4.3.1 Para crear un socket servidor, teclee lo siguiente en el shell:

NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535.

```
redes@debian:~/practica/sock-1.1$ ./sock -le :PUERTO
```

4.3.2 Ahora, abra un nuevo shell, sitúese en el subdirectorio sock-1.1 y ejecute la siguiente orden: (Ver figura No. 13).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	126/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535 e igual al del punto 4.3.1

redes@debian:~/practica/sock-1.1\$./sock -e :PUERTO



```
redes@DEBIAN2023: ~/practica/sock-1.1$ ./sock -e :PUERTO
```

Figura No. 13. Creación de un socket servidor y de un socket cliente

4.3.3 Escriba en el Shell cliente y después teclee “ENTER” observe los que sucede en el Shell servidor. Seguidamente escriba en el Shell servidor, ¿qué sucede en el Shell cliente? (Ver figura No. 14).



```
redes@DEBIAN2023: ~/practica/sock-1.1$ ./sock -le :PUERTO
Hola donde estás?
Estoy en el laboratorio de redes

```

Figura No. 14. Comunicación entre terminales

Salga con CTRL + C

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	127/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

La orden del punto 4.3.2 es equivalente a: *telnet localhost PUERTO*

El parámetro -l hace que la aplicación configure el socket en modo escucha (*listen*) y acepte peticiones. Por tanto, en el punto 4.3.1 ha puesto en marcha, en su computadora, un servidor que escucha en el puerto seleccionado Mientras que las órdenes de los pasos 4.3.2 y 4.3.3 han arrancado clientes TCP que se han conectado a ese puerto.

- 4.3.4** En un shell, sitúese en el subdirectorio sock-1.1 y cree un socket servidor tecleeando lo siguiente:

NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535.

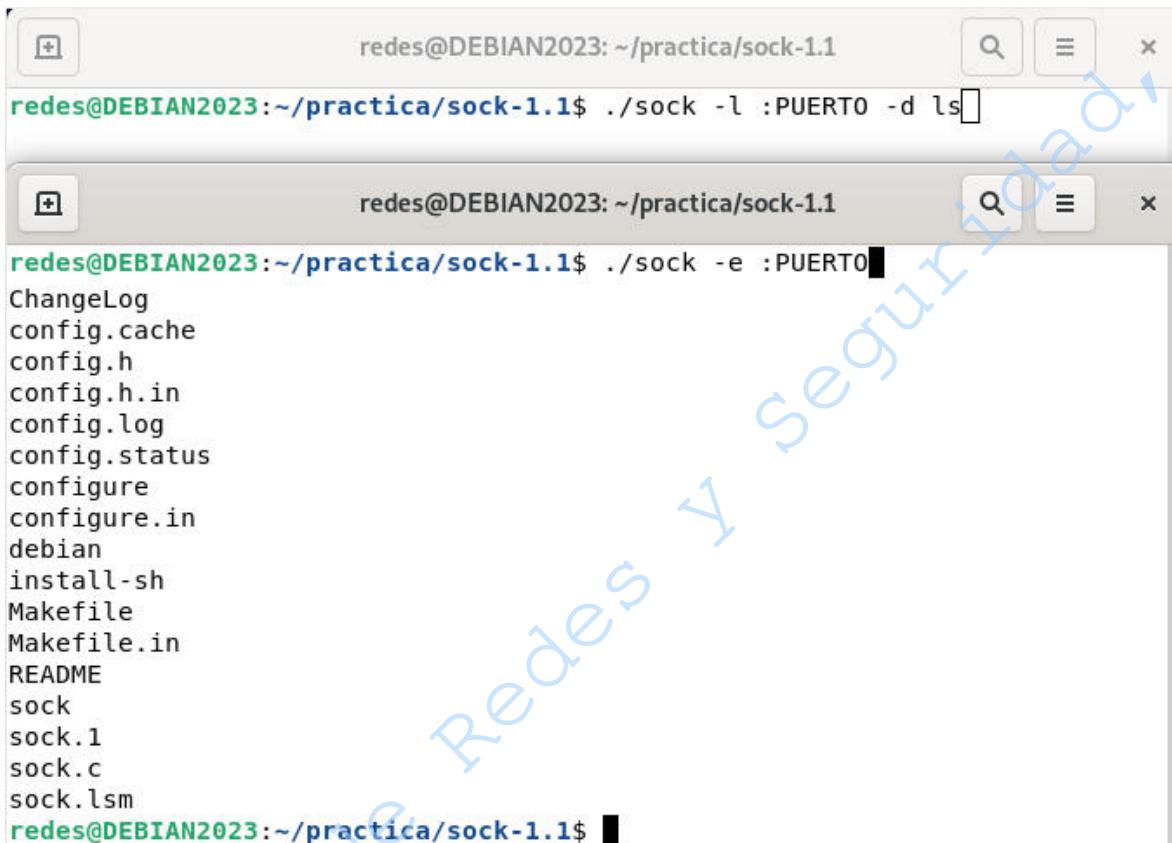
redes@debian:~/practica/sock-1.1\$./sock -l :PUERTO -d ls

- 4.3.5** Ahora, en otro shell, sitúese en el subdirectorio sock-1.1 y cree un socket cliente ejecutando la orden: (Ver figura No. 15).

NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535 e igual al del punto 4.3.4

redes@debian:~/practica/sock-1.1\$./sock -e :PUERTO

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	128/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



The screenshot shows two terminal windows side-by-side. Both windows have a title bar 'redes@DEBIAN2023: ~/practica/sock-1.1'. The left window contains the command 'redes@DEBIAN2023:~/practica/sock-1.1\$./sock -l :PUERTO -d ls' and its output, which lists several files: ChangeLog, config.cache, config.h, config.h.in, config.log, config.status, configure, configure.in, debian, install-sh, Makefile, Makefile.in, README, sock, sock.1, sock.c, and sock.lsm. The right window contains the command 'redes@DEBIAN2023:~/practica/sock-1.1\$./sock -e :PUERTO'.

```

redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -l :PUERTO -d ls
ChangeLog
config.cache
config.h
config.h.in
config.log
config.status
configure
configure.in
debian
install-sh
Makefile
Makefile.in
README
sock
sock.1
sock.c
sock.lsm
redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -e :PUERTO

```

Figura No. 15. Creación de un socket servidor y cliente

4.3.6 Observe lo que sucede.

En este experimento se ha construido un “miniservidor”. Lo que hace el programa es esperar la conexión de un usuario al puerto indicado y cuando el cliente se conecta (mediante la orden `sock` o el programa `telnet`) entonces ejecuta la orden `ls` que lista el contenido del directorio y lo envía a través del socket. Una vez finalizada la orden `ls` el servidor corta la conexión del cliente `telnet`, pero sigue escuchando en el puerto para atender nuevas peticiones de otros clientes.

Si se sustituye la orden ‘`ls`’ por la orden ‘`date`’ en el punto 4.3.4 tendrá un miniservidor de fecha y hora.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	129/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4 El protocolo UDP

Del mismo modo que en los ejemplos anteriores ha utilizado el protocolo TCP, ahora va a ver cómo se puede enviar información mediante el protocolo UDP. Para ello mantendrá los dos shells que tiene abiertos.

4.4.1 En un shell cree un socket servidor tecleando lo siguiente:

NOTA: *PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535.*

```
redes@debian:~/practica/sock-1.1$ ./sock -ul :PUERTO
```

4.4.2 Y en otro shell ejecute la orden: (Ver Figura No. 16).

NOTA: *PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535 e igual al del punto 4.4.1*

```
redes@debian:~/practica/sock-1.1$ ./sock -u :PUERTO
```

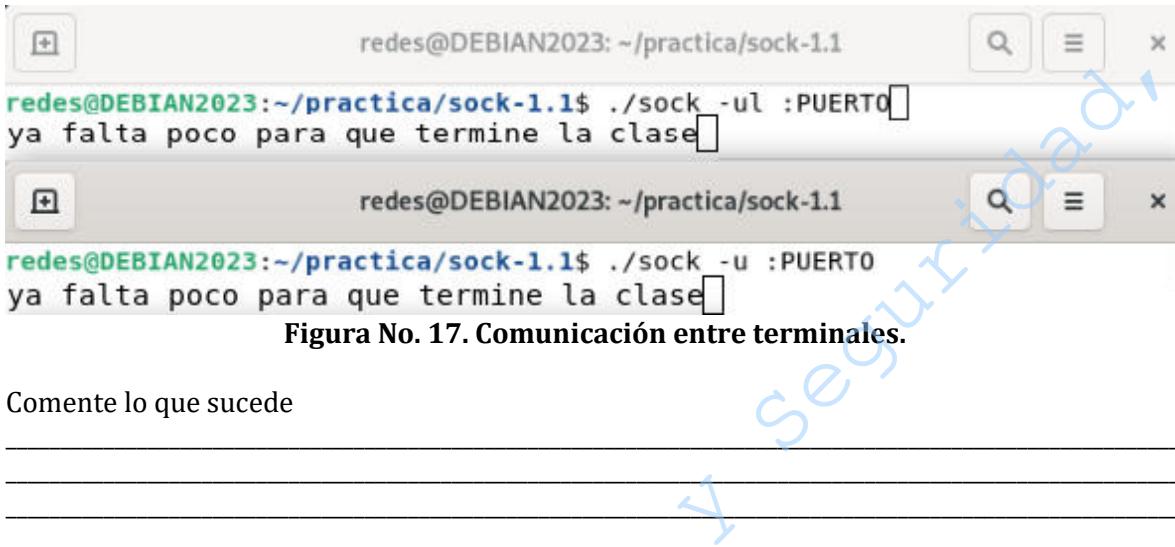


```
redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -ul :PUERTO
redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -u :PUERTO
```

Figura No.16. Socket servidor y cliente.

4.4.3 Escriba en el Shell cliente y después del ENTER observe lo que sucede en el Shell servidor. (Ver figura No. 17). Realice la prueba del shell servidor hacia el cliente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	130/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



redes@DEBIAN2023:~/practica/sock-1.1\$./sock -ul :PUERTO
ya falta poco para que termine la clase

redes@DEBIAN2023:~/practica/sock-1.1\$./sock -u :PUERTO
ya falta poco para que termine la clase

Figura No. 17. Comunicación entre terminales.

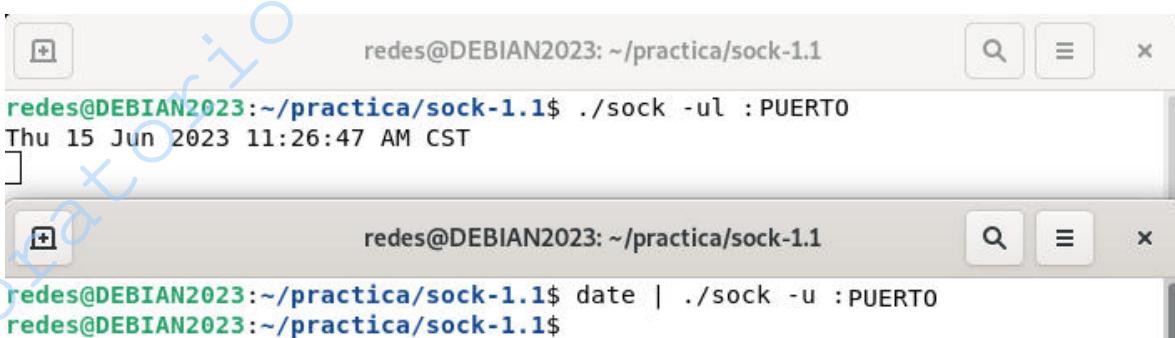
Comente lo que sucede

Salga con CTRL + C, en el Shell del cliente.

4.4.4 Ahora en el Shell cliente cambie la orden del paso número 4.4.2 por la siguiente: (Ver figura No. 18).

NOTA: *PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535 e igual al del punto 4.4.1*

redes@debian:~/practica/sock-1.1\$ date | ./sock -u :PUERTO



redes@DEBIAN2023:~/practica/sock-1.1\$./sock -ul :PUERTO
Thu 15 Jun 2023 11:26:47 AM CST

redes@DEBIAN2023:~/practica/sock-1.1\$ date | ./sock -u :PUERTO
redes@DEBIAN2023:~/practica/sock-1.1\$

Figura No. 18. Comunicación entre terminales.

Como ve el funcionamiento es bastante similar, pero al carecer UDP del concepto de conexión no se puede construir un servidor de manera tan sencilla.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	131/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Pero la razón que hace que UDP tenga utilidad para muchas aplicaciones es su capacidad para hacer difusiones (enviando a la dirección 255.255.255.255 realmente se envía un datagrama que será recibido por todas las computadoras de la misma red IP). Sin embargo, y por motivos de seguridad, el uso de esta característica está restringido y no se empleará en esta práctica.

Una forma de evitar esta restricción es emplear la dirección IP de multicast que esté configurada en todos sus equipos como si se tratara de una dirección de difusión.

4.5 Transferencia de archivos

En los ejercicios anteriores ha visto algunos de los usos que nos permite un socket. Ahora va a utilizar los servicios de TCP y UDP para el envío de archivos entre dos computadoras.

En el siguiente ejercicio se mostrará cómo transferir un archivo empleando el programa sock:

4.5.1 Copie una imagen (por ejemplo dibujo.bmp) al subdirectorio /home/redes/practica/sock-1.1

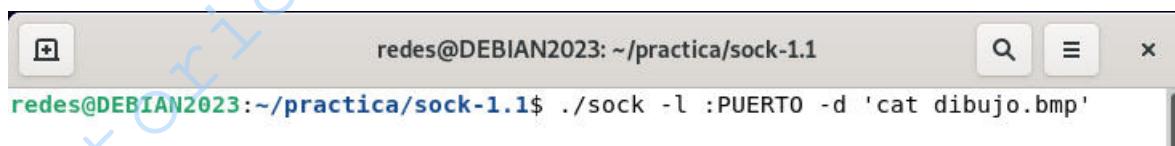
4.5.2 Ahora va a enviar la imagen tecleando en el Shell emisor (Ver figura No. 19):

NOTA 1: *cat* es un comando que no puede ser omitido.

NOTA 2: “dibujo.bmp” es el nombre original de la imagen.

NOTA 3: *PUERTO* deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535.

```
redes@debian:~/practica/sock-1.1$ ./sock -l :PUERTO -d 'cat dibujo.bmp'
```



```
redes@DEBIAN2023: ~/practica/sock-1.1$ ./sock -l :PUERTO -d 'cat dibujo.bmp'
```

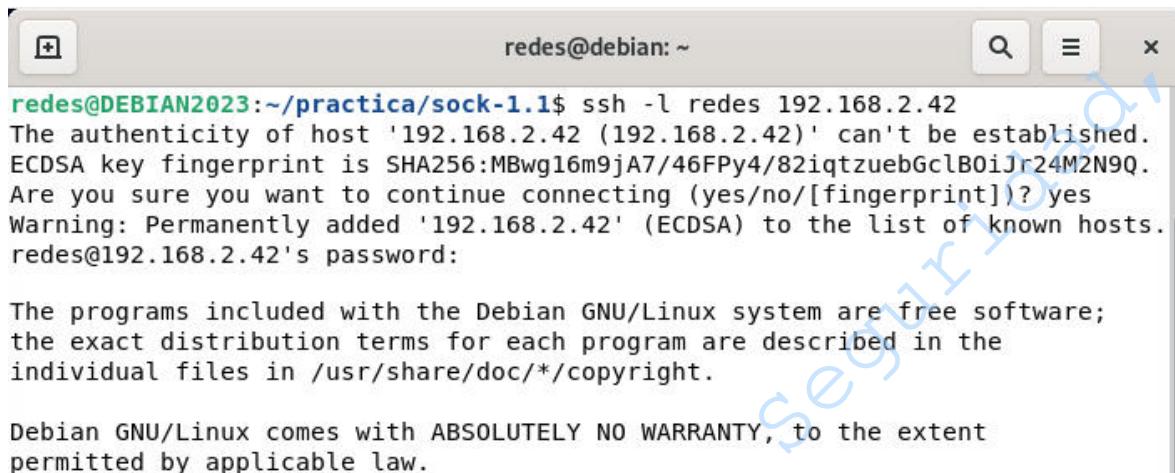
Figura No.19. Envío de la imagen desde el Shell emisor.

4.5.3 Conéctese a la máquina que le indique su profesora o profesor con la cuenta **redes** desde uno de los shells tecleando: (Ver figura No. 20).

```
redes@debian:~/practica/sock-1.1$ ssh -l redes 192.168.2.X
```

NOTA: X se sustituirá por la IP de la computadora.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	132/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```

redes@DEBIAN2023:~/practica/sock-1.1$ ssh -l redes 192.168.2.42
The authenticity of host '192.168.2.42 (192.168.2.42)' can't be established.
ECDSA key fingerprint is SHA256:MBwg16m9jA7/46FPy4/82iqtzuebGclB0iJr24M2N9Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.42' (ECDSA) to the list of known hosts.
redes@192.168.2.42's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

```

Figura No. 20. Conexión por medio de ssh en el Shell receptor

4.5.4 En el Shell del paso anterior, sitúese en el subdirectorio sock-1.1 y teclee: (Ver figura No. 21).

NOTA 1: *PUERTO* deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535 e igual al del punto 4.5.2

```

redes@debian:~$ cd practica/sock-1.1
redes@debian:~/practica/sock-1.1$ ./sock -e 192.168.2.X:PUERTO>imagen2.bmp

```

NOTA 2: X se sustituirá por la IP de su computadora



```

redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -e 192.168.2.56:PUERTO>imagen2.bmp

```

Figura No. 21. Recepción de la imagen en el Shell receptor

NOTA 3: "imagen2.bmp" es un segundo nombre para la imagen

4.5.5 Compruebe que el archivo recibido en la máquina con la cual se conectó tiene el mismo tamaño que el original, utilice el comando: *ls -la*. (Ver figura No. 22).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 133/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

redes@DEBIAN2023:~/practica/sock-1.1$ ls -la
total 184
drwxr-xr-x 3 redes redes 4096 Aug  8 11:57 .
drwxr-xr-x 3 redes redes 4096 Aug  8 10:20 ..
-rw-r--r-- 1 redes redes 1134 Jun 12 2001 ChangeLog
-rw-r--r-- 1 redes redes 1413 Aug  8 10:27 config.cache
-rw-r--r-- 1 redes redes 460 Aug  8 10:27 config.h
-rw-r--r-- 1 redes redes 386 Jun 19 1998 config.h.in
-rw-r--r-- 1 redes redes 4234 Aug  8 10:27 config.log
-rwrxr-xr-x 1 redes redes 7920 Aug  8 10:27 config.status
-rwrxr-xr-x 1 redes redes 50279 Jun 12 2001 configure
-rw-r--r-- 1 redes redes 493 Jun 12 2001 configure.in
drwxr-xr-x 2 redes redes 4096 Jun 12 2001 debian
-rw-r--r-- 1 redes redes 0 Aug  8 11:31 dibujo.bmp
-rwxr-xr-x 1 redes redes 4771 Jun 19 1998 install-sh
-rw-r--r-- 1 redes redes 823 Aug  8 10:27 Makefile
-rw-r--r-- 1 redes redes 714 Jun 12 2001 Makefile.in
-rw-r--r-- 1 redes redes 826 Jun 12 2001 README
-rwrxr-xr-x 1 redes redes 44416 Aug  8 10:31 sock
-rw-r--r-- 1 redes redes 2876 Jun 12 2001 sock.1
-rw-r--r-- 1 redes redes 9612 Jun 12 2001 sock.c
-rw-r--r-- 1 redes redes 498 Jun 12 2001 sock.lsm
redes@DEBIAN2023:~/practica/sock-1.1$ ls -la
total 184
drwxr-xr-x 3 redes redes 4096 Aug  8 11:57 .
drwxr-xr-x 3 redes redes 4096 Aug  8 10:20 ..
-rw-r--r-- 1 redes redes 1134 Jun 12 2001 ChangeLog
-rw-r--r-- 1 redes redes 1413 Aug  8 10:27 config.cache
-rw-r--r-- 1 redes redes 460 Aug  8 10:27 config.h
-rw-r--r-- 1 redes redes 386 Jun 19 1998 config.h.in
-rw-r--r-- 1 redes redes 4234 Aug  8 10:27 config.log
-rwrxr-xr-x 1 redes redes 7920 Aug  8 10:27 config.status
-rwrxr-xr-x 1 redes redes 50279 Jun 12 2001 configure
-rw-r--r-- 1 redes redes 493 Jun 12 2001 configure.in
drwxr-xr-x 2 redes redes 4096 Jun 12 2001 debian
-rw-r--r-- 1 redes redes 0 Aug  8 11:57 imagen2.bmp
-rwxr-xr-x 1 redes redes 4771 Jun 19 1998 install-sh
-rw-r--r-- 1 redes redes 823 Aug  8 10:27 Makefile
-rw-r--r-- 1 redes redes 714 Jun 12 2001 Makefile.in
-rw-r--r-- 1 redes redes 826 Jun 12 2001 README
-rwrxr-xr-x 1 redes redes 44416 Aug  8 10:31 sock
-rw-r--r-- 1 redes redes 2876 Jun 12 2001 sock.1
-rw-r--r-- 1 redes redes 9612 Jun 12 2001 sock.c
-rw-r--r-- 1 redes redes 498 Jun 12 2001 sock.lsm
redes@DEBIAN2023:~/practica/sock-1.1$ 

```

Figura No. 22. Comparación de los archivos.

En este ejercicio se ha realizado la transferencia del archivo mediante el protocolo TCP. Su computadora ha quedado a la espera de un cliente en el paso 4.5.2. Y desde la máquina de al lado se ha conectado como tal cliente en el paso 4.5.4.

Es interesante resaltar que aunque el archivo resultante tenga el mismo tamaño, eso no garantiza que la transferencia ha tenido éxito (¿y si el contenido fuera diferente?). Ahora enviará el archivo de vuelta para poderlo comprobar, pero empleando el protocolo UDP.

Escriba "exit" en ambos Shells hasta cerrarlos.

4.5.6 Abra un shell, sitúese en el subdirectorio sock-1.1 y teclee (Ver figura No. 23):

NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535.

```

redes@debian:~$ cd practica/sock-1.1
redes@debian:~/practica/sock-1.1$ ./sock -ul :PUERTO>dibujo2.bmp

```

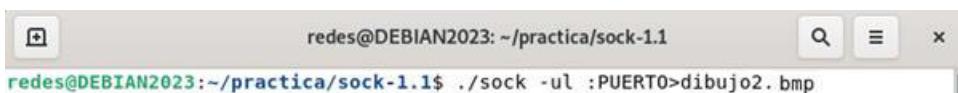


Figura No.23. Recepción del archivo

Lo que le prepara para recibir el archivo, -u indica UDP

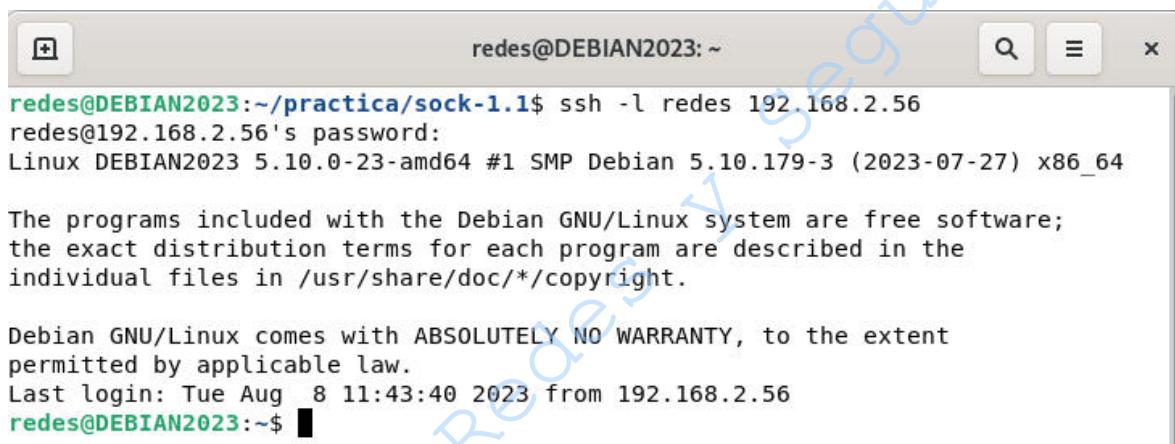
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	134/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA: “dibujo2.bmp” es un tercer nombre para la imagen para diferenciarlo de los anteriores.

- 4.5.7** Abra un segundo Shell y conéctese con la cuenta redes a la máquina con la que realizó la conexión anterior desde un shell tecleando: (Ver figura No. 24).

redes@debian:~\$ ssh -l redes 192.168.2.X

NOTA: X se sustituirá por la IP de la computadora remota.



```
redes@DEBIAN2023:~/practica/sock-1.1$ ssh -l redes 192.168.2.56
redes@192.168.2.56's password:
Linux DEBIAN2023 5.10.0-23-amd64 #1 SMP Debian 5.10.179-3 (2023-07-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug  8 11:43:40 2023 from 192.168.2.56
redes@DEBIAN2023:~$
```

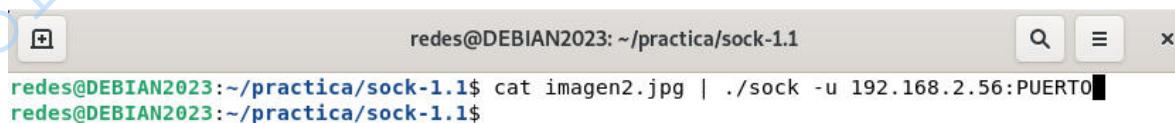
Figura No. 24. Conexión por medio de ssh

- 4.5.8** En el mismo Shell del paso anterior, sitúese en el subdirectorio sock-1.1 y teclee lo siguiente para enviar el archivo: (Ver figura No. 25).

NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535 e igual al del punto 4.5.6

**redes@debian:~\$ cd practica/sock-1.1
redes@debian:~/practica/sock-1.1\$ cat imagen2.bmp | ./sock -u 192.168.2.X:PUERTO**

NOTA: XX se sustituirá por la IP de su computadora



```
redes@DEBIAN2023:~/practica/sock-1.1$ cat imagen2.jpg | ./sock -u 192.168.2.56:PUERTO
```

Figura No.25. Envío del archivo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 135/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.5.9** A continuación, finalice la orden del paso 4.5.8 pulsando <Ctrl>+<c> en el primer shell (asegúrese de que la ha seleccionado primero, haciendo clic con el ratón). (Ver figura No. 26).

```
redes@DEBIAN2023: ~/practica/sock-1.1
redes@DEBIAN2023:~/practica/sock-1.1$ ./sock -ul :PUERTO>dibujo2.bmp
```

Figura No. 26. Final de la instrucción

- 4.5.10** Compruebe que los archivos “imagen2.bmp” (enviado) y “dibujo2.bmp” (recibido) son iguales con la orden *ls -la*. (Ver figura No. 27).

```
redes@DEBIAN2023:~/practica/sock-1.1$ ls -la
total 184
drwxr-xr-x 3 redes redes 4096 Aug  8 12:26 .
drwxr-xr-x 3 redes redes 4096 Aug  8 10:20 ..
-rw-r--r-- 1 redes redes 1134 Jun 12 2001 ChangeLog
-rw-r--r-- 1 redes redes 1413 Aug  8 10:27 config.cache
-rw-r--r-- 1 redes redes 460 Aug  8 10:27 config.h
-rw-r--r-- 1 redes redes 386 Jun 19 1998 config.h.in
-rw-r--r-- 1 redes redes 4234 Aug  8 10:27 config.log
-rw-r--r-x 1 redes redes 7920 Aug  8 10:27 config.status
-rw-r--r-x 1 redes redes 50279 Jun 12 2001 configure
-rw-r--r-- 1 redes redes 493 Jun 12 2001 configure.in
drwxr-xr-x 2 redes redes 4096 Jun 12 2001 debian
-rw-r--r-- 1 redes redes 0 Aug  8 12:26 dibujo2.bmp
-rw-r--r-x 1 redes redes 4771 Jun 19 1998 install-sh
-rw-r--r-- 1 redes redes 823 Aug  8 10:27 Makefile
-rw-r--r-- 1 redes redes 714 Jun 12 2001 Makefile.in
-rw-r--r-- 1 redes redes 826 Jun 12 2001 README
-rw-r--r-x 1 redes redes 44416 Aug  8 10:31 sock
-rw-r--r-- 1 redes redes 2876 Jun 12 2001 sock.1
-rw-r--r-- 1 redes redes 9612 Jun 12 2001 sock.c
-rw-r--r-- 1 redes redes 498 Jun 12 2001 sock.lsm
redes@DEBIAN2023:~/practica/sock-1.1$ ls -la
total 184
drwxr-xr-x 3 redes redes 4096 Aug  8 12:26 .
drwxr-xr-x 3 redes redes 4096 Aug  8 10:20 ..
-rw-r--r-- 1 redes redes 1134 Jun 12 2001 ChangeLog
-rw-r--r-- 1 redes redes 1413 Aug  8 10:27 config.cache
-rw-r--r-- 1 redes redes 460 Aug  8 10:27 config.h
-rw-r--r-- 1 redes redes 386 Jun 19 1998 config.h.in
-rw-r--r-- 1 redes redes 4234 Aug  8 10:27 config.log
-rw-r--r-x 1 redes redes 7920 Aug  8 10:27 config.status
-rw-r--r-x 1 redes redes 50279 Jun 12 2001 configure
-rw-r--r-- 1 redes redes 493 Jun 12 2001 configure.in
drwxr-xr-x 2 redes redes 4096 Jun 12 2001 debian
-rw-r--r-- 1 redes redes 0 Aug  8 11:57 imagen2.bmp
-rw-r--r-x 1 redes redes 4771 Jun 19 1998 install-sh
-rw-r--r-- 1 redes redes 823 Aug  8 10:27 Makefile
-rw-r--r-- 1 redes redes 714 Jun 12 2001 Makefile.in
-rw-r--r-- 1 redes redes 826 Jun 12 2001 README
-rw-r--r-x 1 redes redes 44416 Aug  8 10:31 sock
-rw-r--r-- 1 redes redes 2876 Jun 12 2001 sock.1
-rw-r--r-- 1 redes redes 9612 Jun 12 2001 sock.c
-rw-r--r-- 1 redes redes 498 Jun 12 2001 sock.lsm
redes@DEBIAN2023:~/practica/sock-1.1$
```

Figura No. 27. Comparación de la imagen enviada y recibida

Si ambos archivos son iguales entonces podrá concluir que tanto la transmisión desde su computadora a la de al lado, empleando TCP, como la vuelta, empleando UDP, no han sufrido errores. Si repite la operación con un archivo mayor (por ejemplo, el enunciado de esta práctica en pdf) encontrará que la transmisión por TCP no tiene problemas pero la de UDP fallará eventualmente, aunque este punto no se realizará.

- 4.5.11** Cierre el shell que está conectado a la sesión remota. (Ver figura No. 28).

- 4.5.12**

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	136/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```
redes@DEBIAN2023:~$ cd practica/sock-1.1/
redes@DEBIAN2023:~/practica/sock-1.1$ exit
logout
Connection to 192.168.2.56 closed.
redes@DEBIAN2023:~/practica/sock-1.1$ █
```

Figura No. 28. Cierre de la conexión por ssh.

4.5.13 Cierre sesión.

5.-Cuestionario

- De acuerdo con lo visto en el desarrollo de la práctica ¿qué diferencias sustanciales existen entre TCP y UDP?
-
-
-

- ¿Por qué la conexión iniciada por el socket al servidor sólo dura lo necesario para recibir la información requerida?
-
-
-

- Mencione algunos ejemplos de los usos de TCP y UDP
-
-
-

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	137/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Conclusiones.

Revise los objetivos planteados al inicio de la práctica y concluya.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 138/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 8
TCP y UDP
Cuestionario Previo

1. Mencione al menos 2 funciones de la capa de transporte del Modelo OSI
2. Mencione algunos protocolos de transporte (no incluya TCP ni UDP).
3. ¿Qué es el protocolo de transporte TCP?
4. ¿Qué es el protocolo de transporte UDP?
5. Dibuje un datagrama UDP.
6. Dibuje un segmento TCP.
7. ¿Qué es un socket y qué se necesita para crearlo?
8. ¿Para qué se usa el comando apt-get install gcc o apt install gcc?
9. ¿Para qué se usa el comando apt-get install ssh o apt install ssh?
10. ¿Qué es un puerto?
11. ¿Cuáles son los rangos de puertos existentes?
12. ¿Qué rangos de puertos pueden utilizarse para establecer comunicaciones?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 139/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 9

SSH: Secure Shell

Capa 6 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	140/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

1.- *Objetivo de aprendizaje*

- El alumno o la alumna al finalizar la práctica, conocerá la importancia de utilizar el protocolo SSH (Secure Shell) y su herramienta OpenSSH.
- El alumno o la alumna iniciará una sesión remota a través de SSH, utilizando autenticación por contraseña.
- El alumno o la alumna iniciará una sesión remota con clave pública, generando las claves.
- El alumno o la alumna podrá transferir claves públicas al servidor.

2.- *Conceptos teóricos*

SSH™ permite a los usuarios registrarse en sistemas de host remotamente. A diferencia de *FTP* o *Telnet*, *SSH* cifra la sesión de registro imposibilitando que alguien pueda obtener contraseñas no cifradas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través del shell de comando, tales como *telnet* o *rsh*. Un programa relacionado, el *scp*, reemplaza otros programas diseñados para copiar archivos entre hosts como *rcp*. Ya que estas aplicaciones antiguas no cifran contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas hará disminuir los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

Características de SSH

SSH (o *Secure SHell*) es un protocolo para crear conexiones seguras entre dos sistemas usando una arquitectura cliente/servidor.

El *protocolo SSH* proporciona los siguientes tipos de protección:

- Despues de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando un cifrado robusto de 128 bits.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de un cifrado de 128 bits, lo cual los hacen extremadamente difícil de descifrar y leer.
- El cliente tiene la posibilidad de enviar aplicaciones X11 lanzadas desde el intérprete de comandos del shell. Esta técnica proporciona una interfaz gráfica segura (llamada *reenvío por X11*) que proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	141/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

Ya que el protocolo *SSH* cifrado todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor *SSH* puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada *reenvío por puerto*, como por ejemplo *POP*, incrementando la seguridad del sistema en general y de los datos.

Linux contiene el paquete general de *OpenSSH* (*openssh*), el servidor de *OpenSSH* (*openssh-server*) y los paquetes de clientes (*openssh-clients*). Los paquetes OpenSSH requieren el paquete OpenSSL (*openssl*). OpenSSL instala varias librerías criptográficas importantes que ayudan a OpenSSH a proporcionar comunicaciones cifradas.

Una gran cantidad de programas de cliente y servidor pueden usar el protocolo *SSH*. Muchas aplicaciones *SSH* cliente están disponibles para casi todos los principales sistemas operativos en uso hoy día.

¿Por qué usar *SSH*?

Los usuarios maliciosos tienen a su disposición una variedad de herramientas para interceptar y dirigir el tráfico de la red para ganar acceso al sistema. En términos generales, estas amenazas se pueden catalogar del siguiente modo:

- *Intercepción de la comunicación entre dos sistemas*: En este escenario, existe un tercero en algún lugar de la red entre entidades en comunicación que hace una copia de la información que pasa entre ellas. La parte interceptora puede interceptar y conservar la información o puede modificar la información y luego enviarla al receptor al cual estaba destinado. Este ataque se puede articular a través del uso de un paquete sniffer — una utilidad de red muy común.
- *Personificación de un determinado host*: Con esta estrategia, un sistema interceptor finge ser el receptor a quien está destinado un mensaje. Si funciona la estrategia, el cliente no se da cuenta del engaño y continúa la comunicación con el interceptor como si su mensaje hubiese llegado a su destino satisfactoriamente. Esto se produce con técnicas como el envenenamiento del DNS o spoofing de IP.

Ambas técnicas causan que se intercepte información, posiblemente con propósitos hostiles. El resultado puede ser catastrófico.

Si se utiliza *SSH* para inicios de sesión de shell remota y para copiar archivos, estas amenazas a la seguridad se pueden disminuir notablemente. Esto es porque el cliente *SSH* y el servidor usan firmas digitales para verificar su identidad. Adicionalmente, toda la comunicación entre los sistemas cliente y servidor es cifrada. No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	142/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Capa de Presentación

El papel principal de la capa de presentación es facilitar una comunicación segura entre los dos hosts en el momento y después de la autenticación. La capa de presentación lleva esto a cabo manejando la encriptación y decodificación de datos y proporcionando protección de integridad de los paquetes de datos mientras son enviados y recibidos. Además, la capa de presentación proporciona compresión de datos, lo que acelera la transmisión de información.

Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de presentación correctamente. Durante el intercambio se producen los siguientes pasos:

- Intercambio de claves.
- Se determina el algoritmo de cifrado de la clave pública.
- Se determina el algoritmo de cifrado simétrico.
- Se determina el algoritmo autenticación de mensajes.
- Se determina el algoritmo de hash que hay que usar.

3.- Equipo y material necesario

3.1 Equipo del Laboratorio

- 1 Computadora con Sistema Operativo Linux

4.- Desarrollo

4.1 Sistema Operativo Linux Debian

Modo de trabajar

La realización de la práctica se hará por equipos de dos personas por computadora y se trabajará conjuntamente, un equipo hará la función de servidor y el otro de cliente.

4.2 Ejercicio

NOTA: Para ejemplificar el siguiente ejercicio se muestra la siguiente Figura No. 1.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 143/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 1 Computadoras trabajando conjuntamente

4.2.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 2).

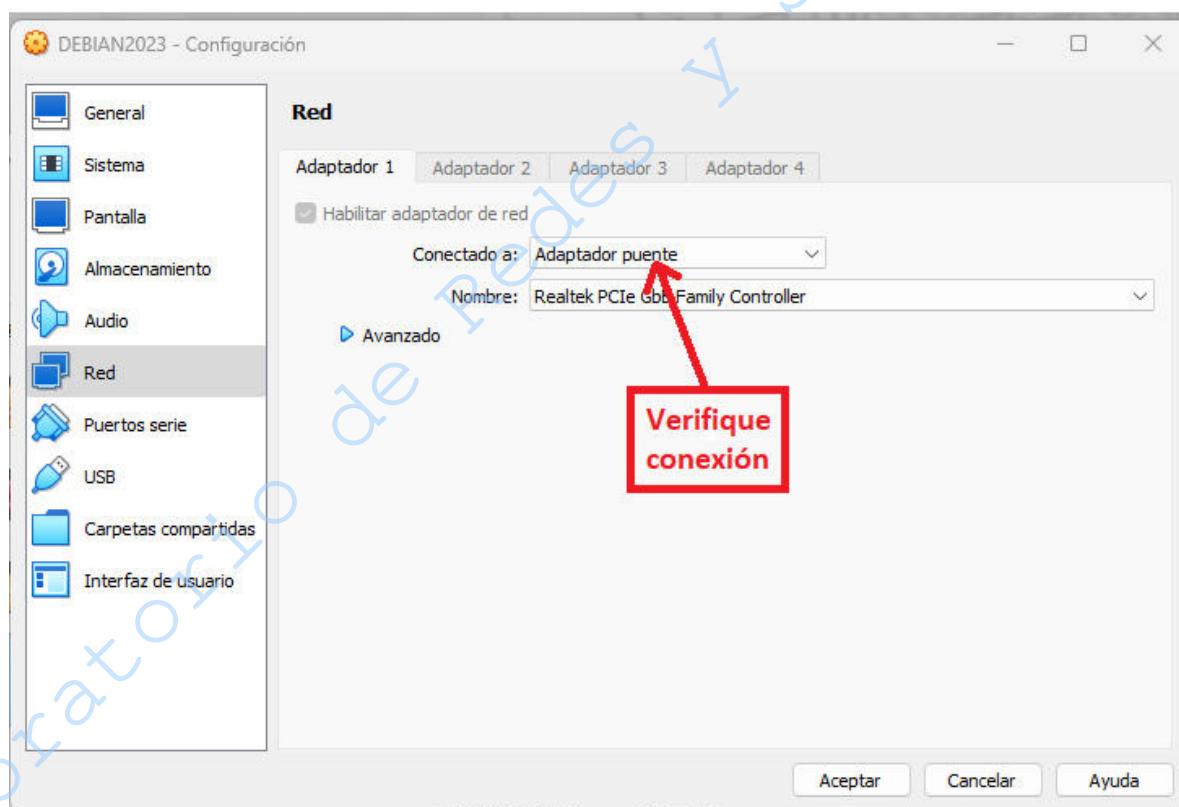


Figura No. 2. Conexión de red.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 144/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.2 Encienda la máquina virtual.

4.2.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: Para realizar la práctica exitosamente debe tener instalado los paquetes ifconfig y ssh.

4.2.4 Entre a sesión como usuario redes (cliente) o estudiante (servidor), según le indique su profesora o profesor. La cuenta y la contraseña serán proporcionadas por la profesora o el profesor del laboratorio.

4.2.5 Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 3)

NOTA: su significa super usuario, por lo que se emplea la misma contraseña de root
redes@debian:~\$ su



```
redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes#
```

Figura No. 3. Terminal de comandos como root.

4.2.6 Teclee la contraseña de root. (Ver Figura No. 4)



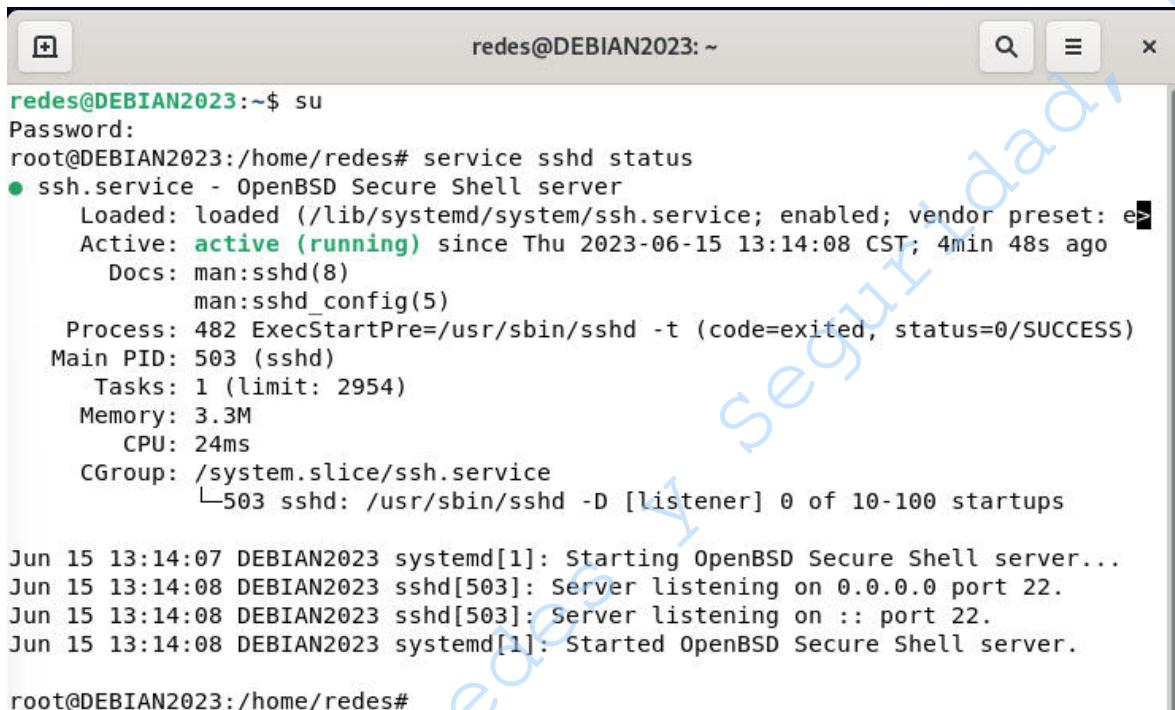
```
redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes#
```

Figura No. 4. Cambio de sesión con privilegios

4.2.7 Verifique que la aplicación SSH se encuentre instalada (Active: active (running)) (Figura No. 5), para ello teclee:

root@debian:/home/redes# service sshd status

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	145/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```

redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes# service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2023-06-15 13:14:08 CST; 4min 48s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 482 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 503 (sshd)
   Tasks: 1 (limit: 2954)
     Memory: 3.3M
        CPU: 24ms
      CGroup: /system.slice/sshd.service
              └─503 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Jun 15 13:14:07 DEBIAN2023 systemd[1]: Starting OpenBSD Secure Shell server...
Jun 15 13:14:08 DEBIAN2023 sshd[503]: Server listening on 0.0.0.0 port 22.
Jun 15 13:14:08 DEBIAN2023 sshd[503]: Server listening on :: port 22.
Jun 15 13:14:08 DEBIAN2023 systemd[1]: Started OpenBSD Secure Shell server.

root@DEBIAN2023:/home/redes#

```

Figura No. 5. Verificación de SSH

NOTA: En caso de que no se encuentre instalada, debe teclear el siguiente comando para instalarla (Figura No. 6)

```
root@debian:/home/redes# apt-get install ssh
```



```

root@DEBIAN2023:/home/redes# apt-get install ssh
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ssh is already the newest version (1:8.4p1-5+deb11u1).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
root@DEBIAN2023:/home/redes#

```

Figura No. 6. Descarga del paquete SSH

4.2.8 Visualice el archivo *sshd_config*. (Ver figura No. 7). Teclee lo siguiente:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	146/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

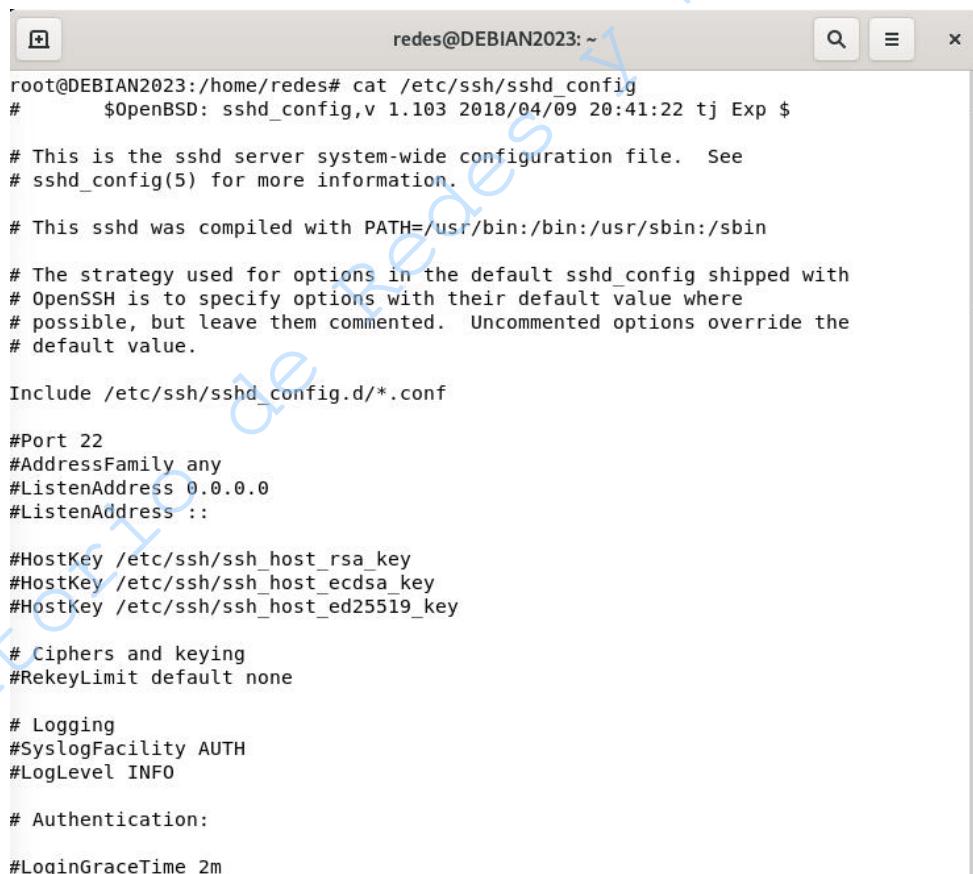
root@debian:/home/redes# cat /etc/ssh/sshd_config



```
redes@DEBIAN2023: ~
root@DEBIAN2023:/home/redes# cat /etc/ssh/sshd_config
```

Figura No. 7. Archivo sshd_config

La salida del comando dará algo similar a lo siguiente (Ver figura No. 8). Comente la información obtenida en la pantalla.



```
redes@DEBIAN2023: ~
root@DEBIAN2023:/home/redes# cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
```

Figura No. 8 Archivo sshd_config

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	147/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.9 Teclee el comando ifconfig y anote la dirección IP que tiene asignada su máquina

Dirección IP _____

4.2.10 Cierre la sesión de root, colocando *exit*.

4.3 Iniciando una sesión remota con contraseña

4.3.1 El primer ejemplo que se analizará será el inicio de una sesión remota a través de SSH, utilizando autenticación por contraseña. Para ello, ingrese como usuario “estudiante” en el servidor (su propia máquina).

Abra una segunda terminal en el cliente (cuenta de redes) e introduzca el siguiente comando (Ver figura No. 9):

```
redes@debian:~$ ssh estudiante@192.168.2.x
```

NOTA: El valor X será de acuerdo con la máquina que esté utilizando como servidor.



```
estudiante@debian: ~
redes@DEBIAN2023:~$ ssh estudiante@192.168.2.42
```

Figura No. 9 Conexión con equipo remoto

Al ser la primera vez que se conecta al servidor, si previamente no ha agregado la clave pública del mismo en */home/redes/.ssh/known_hosts*, aparecerá un mensaje similar al siguiente: (Ver figura No. 10).



```
redes@debian: ~
redes@DEBIAN2023:~/practica/sock-1.1$ ssh -l redes 192.168.2.42
The authenticity of host '192.168.2.42 (192.168.2.42)' can't be established.
ECDSA key fingerprint is SHA256:MBwg16m9jA7/46FPy4/82iqtzuebGclB0iJr24M2N9Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

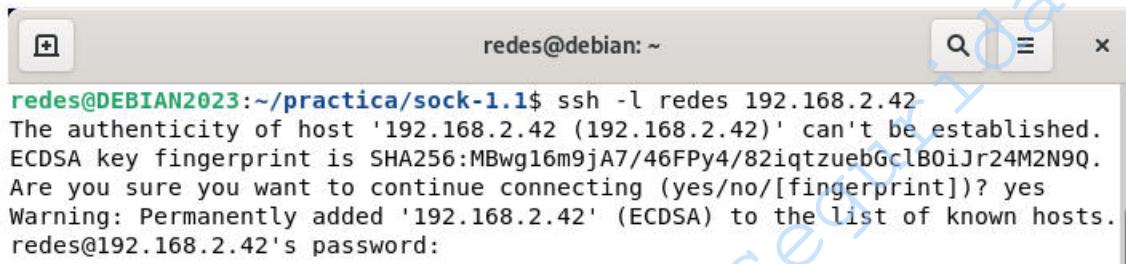
Figura No. 10 Confirmación de la sesión con equipo remoto

4.3.2 Debido a que se confía que ésa es la verdadera clave pública del servidor. Teclee yes. Luego el cliente informará algo similar a lo siguiente:

Warning: Permanently added '192.168.2.x' (RSA) to the list of known hosts.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	148/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

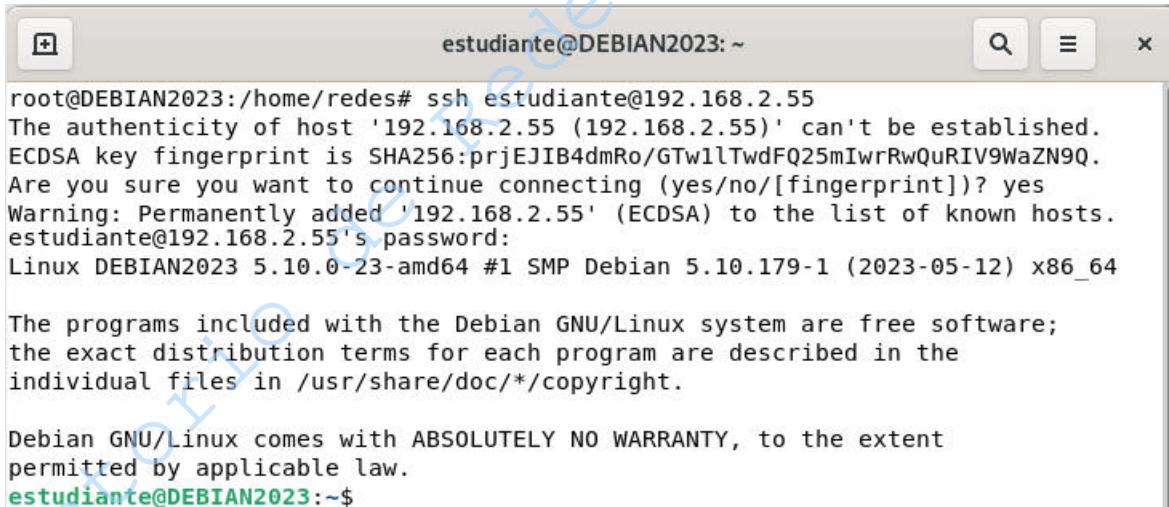
Lo que significa que se ha agregado la clave pública del servidor en `/home/redes/.ssh/known_hosts`. (Ver figura No. 11). Luego el cliente solicitará el ingreso de la contraseña:



```
redes@DEBIAN2023:~/practica/sock-1.1$ ssh -l redes 192.168.2.42
The authenticity of host '192.168.2.42 (192.168.2.42)' can't be established.
ECDSA key fingerprint is SHA256:MBwg16m9jA7/46FPy4/82iqtzuebGclB0iJr24M2N9Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.42' (ECDSA) to the list of known hosts.
redes@192.168.2.42's password:
```

Figura No. 11 Acceso al equipo remoto

4.3.3 Teclee la contraseña de la cuenta estudiante, que será proporcionada por la profesora o el profesor. Finalmente, si la contraseña ingresada es correcta, aparecerá algo similar a lo siguiente: (Ver figura No. 12).



```
estudiante@DEBIAN2023:~$ ssh estudiante@192.168.2.55
The authenticity of host '192.168.2.55 (192.168.2.55)' can't be established.
ECDSA key fingerprint is SHA256:prjEJIB4dmRo/GTw1lTwdFQ25mIwrRwQuRIV9WaZN9Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.55' (ECDSA) to the list of known hosts.
estudiante@192.168.2.55's password:
Linux DEBIAN2023 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
estudiante@DEBIAN2023:~$
```

Figura No. 12 Sesión iniciada en el equipo remoto

Con lo cual se ha iniciado una sesión en el servidor como el usuario estudiante.

4.3.4 Cierre la sesión remota. Teclee exit: (Ver figura No. 13).

`estudiante@debian:~$ exit`

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	149/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
estudiante@DEBIAN2023:~$ exit
logout
Connection to 192.168.2.55 closed.
root@DEBIAN2023:/home/redes# █
```

Figura No. 13 Sesión terminada en el equipo remoto

4.4 Iniciando una sesión remota con clave pública

- 4.4.1** El primer paso para utilizar la autenticación mediante clave pública es modificar el archivo de configuración de SSH en la computadora cliente (sesión redes). Debe estar en la cuenta *root* para poder modificar el archivo.

Para ello, edite el archivo *sshd_config* borrando el símbolo # de las siguientes líneas y verificando que estén escritas como se ve a continuación, si alguna falta inclúyala: (Ver Figura No. 14)

```
root@debian:/home/redes# nano /etc/ssh/sshd_config
```

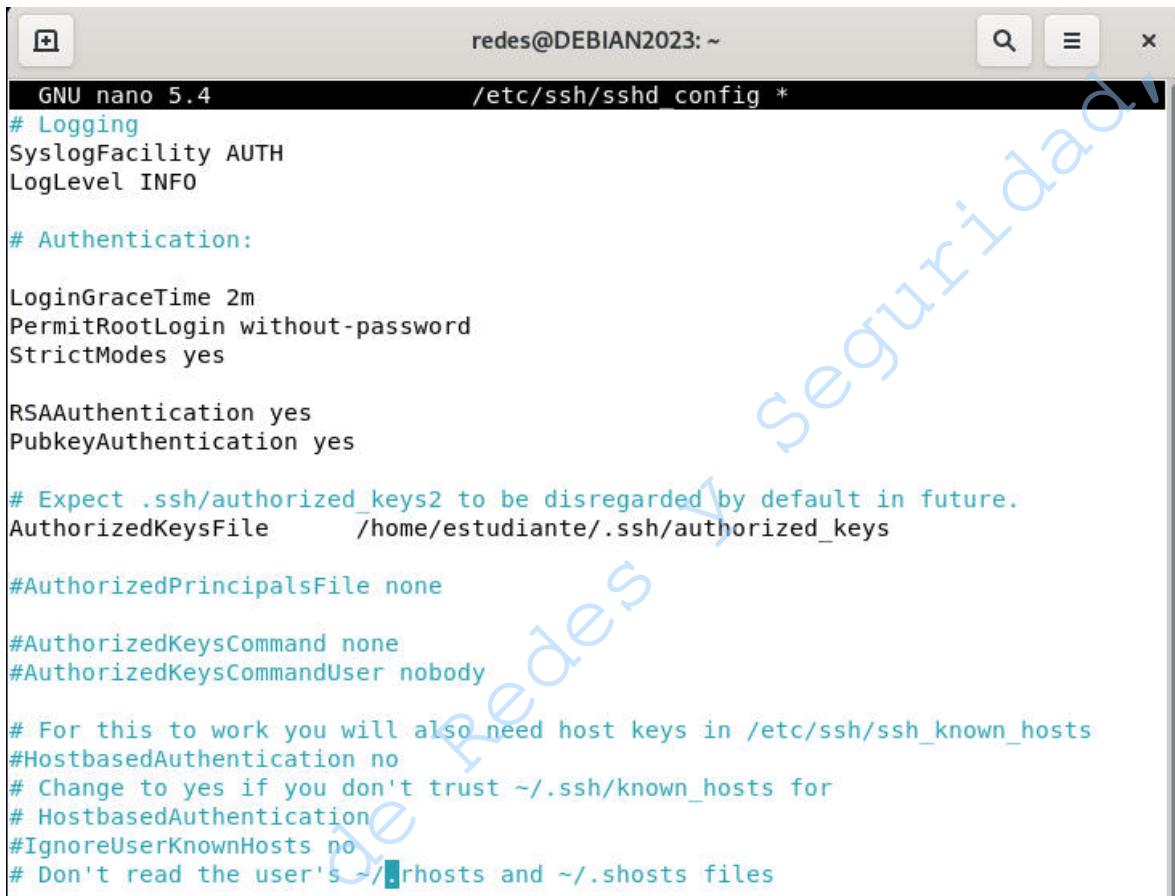
```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile /home/estudiante/.ssh/authorized_keys
```



```
redes@DEBIAN2023: ~
root@DEBIAN2023:/home/redes# nano /etc/ssh/sshd_config
```



Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
	Versión:	06
	Página	150/479
	Sección ISO	8.3
	Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

GNU nano 5.4                               /etc/ssh/sshd_config *

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:

LoginGraceTime 2m
PermitRootLogin without-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      /home/estudiante/.ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files

```

Figura No. 14 Archivo de configuración

Guarde los cambios (ctrl+o), salga del editor (ctrl+x) y reinicie el servicio (Ver Figura No. 15).

root@debian:/home/redes# /etc/init.d/ssh restart



```

root@DEBIAN2023:/home/redes# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
root@DEBIAN2023:/home/redes#

```

Figura No. 15 Reiniciando el servicio de SSH

Cierre la sesión de root (Figura No. 16).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	151/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				



```
root@DEBIAN2023:/home/redes# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
root@DEBIAN2023:/home/redes# exit
exit
root@DEBIAN2023:/home/redes#
```

Figura No. 16. Cerrando sesión de root

Generando las claves

4.4.2 Genere el par de claves de RSA que se utilizarán.

Para ello, ejecute el siguiente comando en el Shell de la cuenta de redes: (Ver figura No. 17).

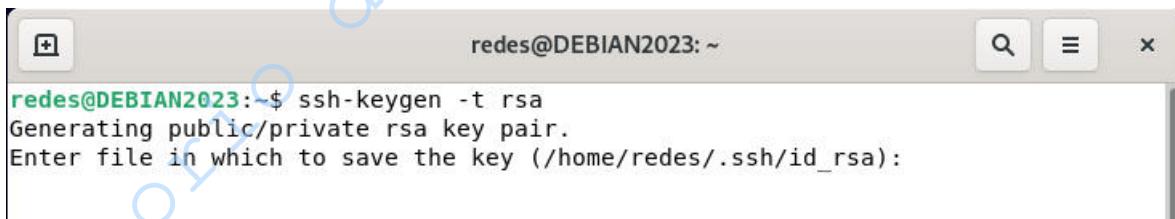
redes@debian:~\$ ssh-keygen -t rsa



```
redes@DEBIAN2023:~$ ssh-keygen -t rsa
```

Figura No. 17 Comando para generar las claves

El programa responderá algo similar a lo siguiente: (Ver figura No. 18).



```
redes@DEBIAN2023:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/redes/.ssh/id_rsa):
```

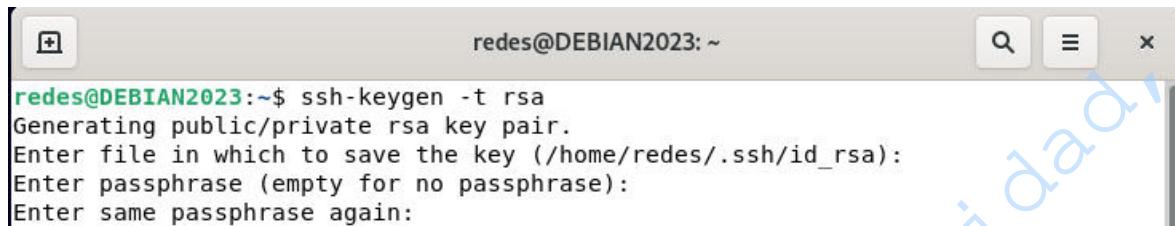
Figura No. 18 Generando las claves

4.4.3 Solicita que se ingrese el nombre del archivo en donde se almacenará la clave privada, asegúrese que la ruta sea */home/redes/.ssh/id_rsa*, de no ser así introduzca la ruta para que concuerde con la configuración del cliente SSH. Presione <Enter>. Luego solicitará una frase clave: (Ver figura No. 19).

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	152/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				



```
redes@DEBIAN2023:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/redes/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

Figura No. 19 Colocando la frase

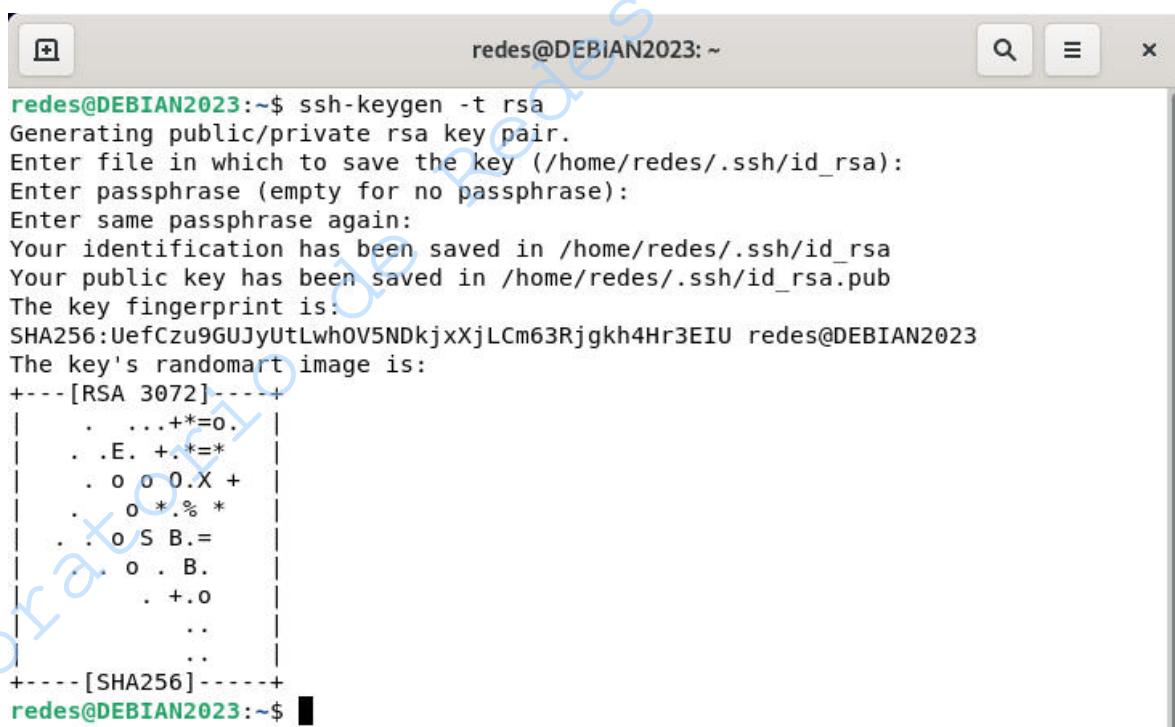
- 4.4.4** Presione dos veces <Enter> para omitir el uso de una frase clave. Más adelante se realizará esto. Finalmente informa: (Ver figura No. 20).

Your identification has been saved in /home/redes/.ssh/id_rsa.

Your public key has been saved in /home/redes/.ssh/id_rsa.pub.

The key fingerprint is:

13:8b:23:74:53:e4:0f:b3:16:49:1b:79:64:60:7c:38 redes@cliente



```
redes@DEBIAN2023:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/redes/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/redes/.ssh/id_rsa
Your public key has been saved in /home/redes/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:UefCzu9GUJyUtLwh0V5NDkjxXjLCm63Rjgkh4Hr3EIU redes@DEBIAN2023
The key's randomart image is:
+--- [RSA 3072] ---+
|   . .+*=0. |
|   ..E. +.*=*
|   . o o 0.X +
|   o * .% *
|   . : o S B.=
|   o . B.
|   . +.o
|   ..
|   ..
+--- [SHA256] ---+
redes@DEBIAN2023:~$
```

Figura No. 20 Claves generadas satisfactoriamente

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	153/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.5 Transfiriendo la clave pública al servidor

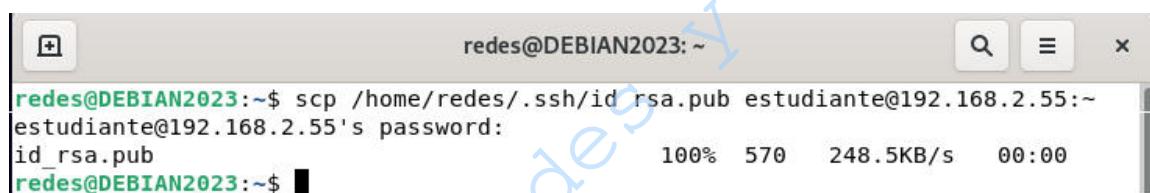
Luego, se debe transferir la clave pública del usuario *redes* (*/home/redes/.ssh/id_rsa.pub*) al directorio *home* del usuario estudiante en servidor y añadirla al final del archivo */home/estudiante/.ssh/authorized_keys*.

4.5.1 Desde la terminal teclee sin omitir la tilde: (Ver figura No. 21).

```
redes@debian:~$ scp /home/redes/.ssh/id_rsa.pub estudiante@192.168.2.x:~
```

NOTA: El valor X será de acuerdo con la máquina que esté utilizando como servidor.

Teclee la contraseña de la cuenta estudiante y la transferencia finalizará



```
redes@DEBIAN2023:~$ scp /home/redes/.ssh/id_rsa.pub estudiante@192.168.2.55:~
estudiante@192.168.2.55's password:
id_rsa.pub                                         100%   570    248.5KB/s   00:00
redes@DEBIAN2023:~$
```

Figura No. 21 Trasferencia de la clave

4.5.2 Para añadir la clave pública al archivo *authorized_keys* realice lo siguiente en el servidor

- Realice lo siguiente en el servidor (sesión estudiante):

Teclee:

```
estudiante@debian:~$su
```

NOTA: su significa super usuario, por lo que se emplea la misma contraseña de root

Ahora teclee el siguiente comando para crear la carpeta *.ssh* en */home/estudiante*

```
root@debian:/home/estudiante# mkdir .ssh
```

A continuación teclee lo siguiente (Figura No. 22):

```
root@debian:/home/estudiante# cat /home/estudiante/id_rsa.pub>
/home/estudiante/.ssh/authorized_keys
```

```
root@DEBIAN2023:/home/estudiante# cat /home/estudiante/id_rsa.pub >/home/estudiante/.s
sh/authorized_keys
```

Figura No. 22 Añadiendo la clave al archivo *authorized_keys*

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	154/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- b) Ahora diríjase al cliente (sesión redes) y agregue la clave (Figura No. 23)

```
root@debian:/home/redes# ssh-add /home/redes/.ssh/id_rsa
```



```
redes@DEBIAN2023:~$ ssh-add /home/redes/.ssh/id_rsa
Identity added: /home/redes/.ssh/id_rsa (redes@DEBIAN2023)
redes@DEBIAN2023:~$
```

Figura No. 23 Agregando la clave

Salga de la sesión de root

4.6 Iniciando la sesión

4.6.1 Ingrese el siguiente comando:

```
redes@debian:~$ ssh estudiante@192.168.2.x
```

NOTA: El valor X será de acuerdo con la máquina que esté utilizando como servidor.

El servidor nuevamente envía su clave pública de RSA, la cual es comparada con la almacenada en *known_hosts*, y si coincide, el proceso continúa.

El cliente de SSH, al encontrar el archivo */home/redes/.ssh/id_rsa*, primero intentará la autenticación con clave pública. El servidor le enviará el *challenge* cifrado con la clave pública encontrada en */home/estudiante/authorized_keys* (en el directorio *home* del usuario estudiante) y el cliente deberá devolverla descifrada (usando la clave */home/redes/.ssh/id_rsa* en el directorio *home* del usuario redes).

NOTA: Esto se realiza automáticamente, sin la intervención del usuario.

Si esto se realiza correctamente, se iniciará la sesión remota (Ver figura No. 24).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	155/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
redes@DEBIAN2023:~$ ssh estudiante@192.168.2.55
estudiante@192.168.2.55's password:
Linux DEBIAN2023 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64
```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Thu Aug 3 11:05:38 2023 from 192.168.2.56

```
estudiante@DEBIAN2023:~$ █
```

Figura No. 24 Sesión iniciada con el equipo remoto

- 4.6.2** Si la autenticación con clave pública hubiera fallado, el cliente intentará con la autenticación con contraseña. Después de conectarse al servidor, salga de este. (Ver figura No. 25).

```
estudiante@DEBIAN2023:~$ exit
logout
Connection to 192.168.2.55 closed.
redes@DEBIAN2023:~$
```

Figura No. 25 Cerrando la sesión remota

4.7 Asegurando la clave privada en el cliente

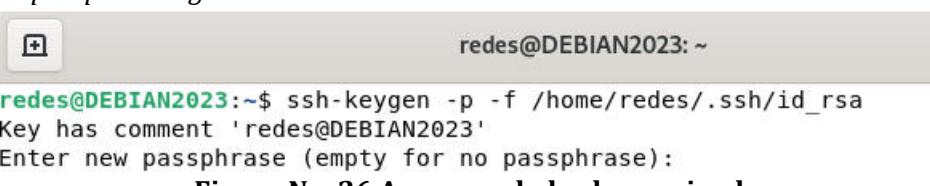
- 4.7.1** Cuando creó el par de claves usando ssh-keygen, se omitió especificar la frase clave que se usaría a tal efecto. Usando nuevamente ssh-keygen se asignará una nueva. Teclee lo siguiente:

```
redes@debian$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
```

Pedirá ingresar la nueva frase clave: (Ver figura No. 26).

Enter new passphrase (empty for no passphrase):

Enter same passphrase again:



```
redes@DEBIAN2023:~$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
Key has comment 'redes@DEBIAN2023'
Enter new passphrase (empty for no passphrase):
```

Figura No. 26 Asegurando la clave privada

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	156/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.7.2 Ingrese la frase clave, usted seleccione una y escriba esta misma en ambas ocasiones.

Frase clave empleada: _____

4.7.3 Finalmente informa: (Ver figura No. 27).



```
redes@DEBIAN2023:~$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
Key has comment 'redes@DEBIAN2023'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
redes@DEBIAN2023:~$
```

Figura No. 27 Ingresando clave, para la conexión remota

4.8 Usando ssh-agent en el shell

4.8.1 En la sesión redes, ejecute el ssh-agent de la siguiente forma: (Ver figura No. 28).

redes@debian:~\$ eval 'ssh-agent'



```
redes@DEBIAN2023:~$ eval 'ssh-agent'
SSH_AUTH_SOCK=/tmp/ssh-wBfn1gJakG37/agent.2561; export SSH_AUTH_SOCK;
SSH_AGENT_PID=2562; export SSH_AGENT_PID;
echo Agent pid 2562;
redes@DEBIAN2023:~$
```

Figura No. 28 Utilizando el ssh-agent

4.8.2 Agregue la clave privada de RSA. (Ver figura No. 29). Para ello use el comando *ssh-add*:

redes@debian:~\$ ssh-add /home/redes/.ssh/id_rsa

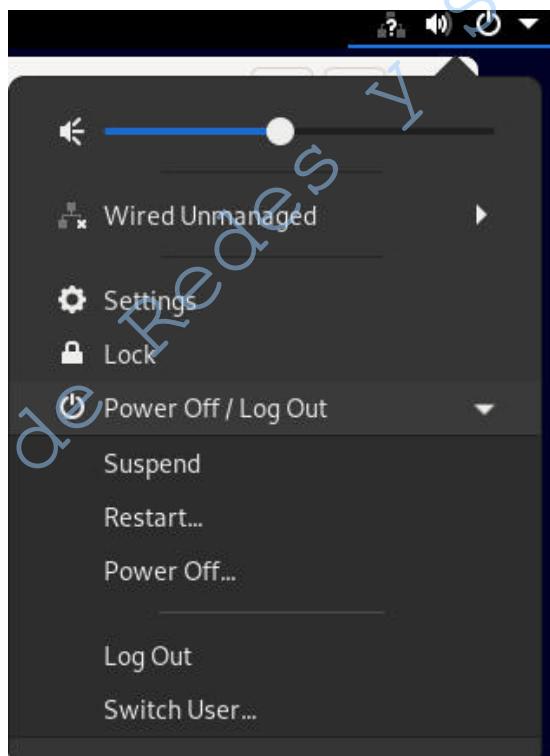
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 157/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```
redes@DEBIAN2023:~$ ssh-add /home/redes/.ssh/id_rsa
Enter passphrase for /home/redes/.ssh/id_rsa:
Identity added: /home/redes/.ssh/id_rsa (redes@DEBIAN2023)
redes@DEBIAN2023:~$
```

Figura No. 29 Agregando la clave privada de RSA

Este procedimiento puede repetirse si se tienen varias claves privadas. Luego, al ejecutar ssh éste le solicitará al ssh-agent la clave privada.

Reinicie la sesión del cliente (sesión redes) (cierra la sesión e ingrese nuevamente) (Figura No. 30).



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	158/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura No. 31 Cierre e inicio de sesión en redes

Una vez estando dentro de la sesión cliente y empleando una terminal, conéctese de manera remota al servidor (sesión estudiante) y comente lo que sucede, para ello teclee:

redes@debian\$ ssh estudiante@192.168.2.x

Cierre la sesión de estudiante.

4.9 Restaurando la configuración de las máquinas

4.9.1 Eliminación de los archivos

Teclee lo siguiente para eliminar los archivos generados en el servidor (sesión estudiante), recuerde que debe estar como superusuario.

root@debian:/home/estudiante# rm /home/estudiante/id_rsa.pub

Teclee lo siguiente para eliminar los archivos generados en el cliente (sesión redes) recuerde que debe estar como superusuario.

root@debian:/home/redes# rm /home/redes/.ssh/id_rsa.pub
root@debian:/home/redes# rm /home/redes/.ssh/id_rsa

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	159/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.9.2 Borrado del contenido de los archivos

Debe borrar el contenido de los archivos y dejarlos en blanco completamente, como estaban originalmente, recuerde que debe encontrarse en modo superusuario.

Teclee lo siguiente y borre el contenido de cada archivo, dentro del archivo puede oprimir ctrl+k para eliminar cada línea rápidamente, guarde el archivo en blanco:

```
root:/home/redes# nano /home/redes/.ssh/known_hosts
```

4.9.3 Cierre la sesión.

4.9.4 Cuestionario

1. ¿Qué sucedería si escribiera mal la contraseña al querer hacer una conexión remota con ssh?

2. Investigue las características de los algoritmos de cifrado RSA y 3DES



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	160/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

5. Anote sus Conclusiones u Observaciones; revisando los objetivos planteados al inicio de la práctica:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	161/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA 9
SSH: Secure Shell
Cuestionario Previo

1. ¿Qué es el reenvío por X11?
2. ¿Qué es un sniffer?
3. Mencione cuáles son las versiones del protocolo SSH y explique sus características.
4. ¿Cuáles son las secuencias de eventos a llevar a cabo en una conexión SSH?
5. ¿A qué nos referimos con la Autenticación?
6. Explique detalladamente los pasos que se producen cuando un cliente contacta a un servidor a través del protocolo SSH.
7. ¿Qué algoritmo de cifrado emplea el protocolo SSH?
8. ¿En dónde es conveniente utilizar SSH?
9. ¿Cuáles son los objetivos principales de la capa 6 del modelo OSI?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 162/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 10

Funciones de la capa de presentación

Capa 6 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 163/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

1.- Objetivo de Aprendizaje

- El alumno o la alumna al finalizar la práctica, conocerá algunos de los conceptos básicos de la Capa 6 del Modelo OSI (Capa de Presentación), utilizando algunos programas de uso común.
- El alumno o la alumna conocerá las funciones principales de la Capa de Presentación, y utilizará adecuadamente estas características según las situaciones que se le presenten.

2.- Conceptos Teóricos

La capa de presentación se encarga del formato y representación de los datos. De ser necesario, esta capa puede servir de intermediario entre distintos formatos.

La capa 6, o capa de presentación, cumple tres funciones principales (ver Figura No. 1). Estas funciones son las siguientes:

- Formateo de datos (presentación)
- Cifrado de datos
- Compresión de datos

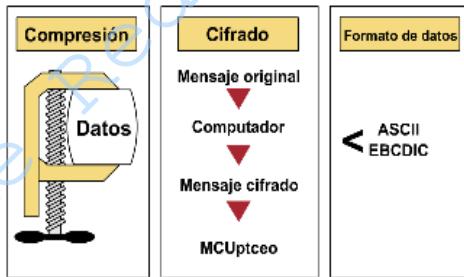


Figura No. 1. Funciones principales de la Capa 6.

Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta una de sus funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión. En la estación receptora, la capa de presentación toma los datos de la capa de sesión y ejecuta las funciones requeridas antes de pasarlos a la capa de aplicación.

Los estándares de la Capa 6 también determinan la presentación de las imágenes gráficas. A continuación, se presentan tres de estos estándares:

- *PICT*: Un formato de imagen utilizado para transferir gráficos QuickDraw entre programas del sistema operativo MAC
- *TIFF* (Formato de archivo de imagen etiquetado): Un formato para imágenes con asignación de bits de alta resolución

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	164/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- *JPEG* (Grupo conjunto de expertos fotográficos): Formato gráfico utilizado con frecuencia para comprimir imágenes fijas de ilustraciones o fotografías complejos
- Otros estándares de la Capa 6 regulan la presentación de sonido y películas. Entre estos estándares se encuentran:

- *MIDI* (Interfaz digital para instrumentos musicales): para música digitalizada
- *MPEG* (Grupo de expertos en películas): Estándar para la compresión y codificación de vídeo con movimiento para el almacenamiento en CD y digital
- *QuickTime*: Estándar para el manejo de audio y vídeo para los sistemas operativos de los MAC y de los PC

También existen estándares para el formato del texto, éstos son:

- *EBCDIC* (Código de caracteres decimal codificados en binario): Es un código estándar de 8 bits usado por computadoras *mainframe IBM*.
- *ASCII* (Código americano normalizado para el intercambio de información): Es un código de caracteres basado en el alfabeto latino tal como se usa en inglés moderno y en otras lenguas occidentales.

Otro formato de archivo común es el formato binario. Los archivos binarios contienen datos codificados especiales que sólo se pueden leer con aplicaciones de software específicas. Programas como FTP utilizan el tipo de archivo binario para transferir archivos.

Otro tipo de formato de archivo es el lenguaje de etiquetas. Este formato actúa como un conjunto de instrucciones que le indican al navegador de Web cómo mostrar y administrar los documentos. El Lenguaje de etiquetas por hipertexto (HTML) es el lenguaje de Internet. Las direcciones HTML le indican al navegador dónde mostrar texto o un hipervínculo con otro URL. El formato HTML no es un lenguaje de programación sino un conjunto de direcciones para la visualización de una página.

La capa 6 también es responsable por el cifrado de datos. El cifrado de los datos protege la información durante la transmisión.

La capa de presentación también se ocupa de la compresión de los archivos. La compresión funciona mediante el uso de algoritmos (fórmulas matemáticas complejas) para reducir el tamaño de los archivos.

3.- Equipo y material necesario

Computadora con Sistema Operativo Windows, acceso a Internet, y las siguientes herramientas instaladas:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 165/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- Paint
- Mozilla Firefox
- AESCrypt

4.- Desarrollo

Modo de trabajar

Se trabajará por parejas

4.1. Realización de la práctica

4.1.1 Encienda la computadora y acceda a Windows

4.2. Formato de texto

4.2.1 Abra las aplicaciones de Mozilla Firefox, Edge y Chrome.

4.2.2 Ingrese a la página [http://es.wikipedia.org/wiki/Facultad_de_Ingenieria_\(UNAM\)](http://es.wikipedia.org/wiki/Facultad_de_Ingenieria_(UNAM)) (ver Figura No. 2.) en los navegadores.



Figura No. 2. Página de Internet

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	166/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.2.3** Observe la página detenidamente en los diferentes navegadores. ¿Existe alguna diferencia de la manera en cómo se observa la información? Justifique su respuesta

- 4.2.4** Investigue ¿Qué es la codificación Unicode?

- 4.2.5** Investigue ¿Qué es la codificación ISO?

- 4.2.6** Busque en Internet una tabla de caracteres ISO

- 4.2.7** Escriba 5 caracteres ISO y su número correspondiente

- 4.2.8** Repita la actividad con una codificación diferente

- 4.2.** Emplee cualquiera de los navegadores y elija la opción correspondiente para visualizar el Código fuente de esta página.

- 4.2.10** Observe el código fuente de la página de Internet. Y describa el funcionamiento de algunas etiquetas de HTML.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 167/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.11 Mencione cuál es la relación entre el formato HTML y la capa de presentación.

4.3 Compresión de datos

4.3.1 Busque y descargue de Internet una imagen de formato bmp, con un tamaño que exceda los 2000 píxeles por 2000 píxeles, y que de preferencia maneje varias tonalidades de colores.

4.3.2 Abra la imagen con el programa Paint y guárdela, pero esta vez con formato jpg (Figura No. 3)

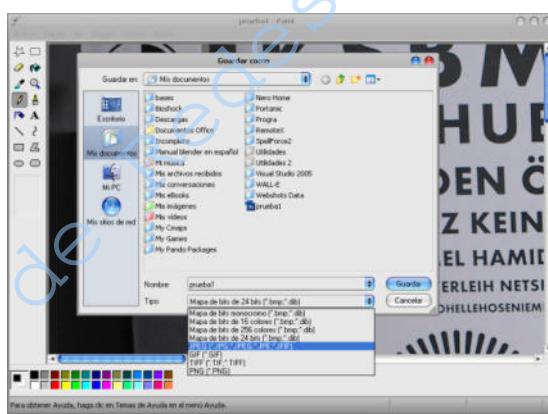


Figura No. 3. Guardando la imagen bmp a jpg.

4.3.3 Abra ambas imágenes en ventanas diferentes. Reajuste las ventanas para poder comparar las imágenes. (ver Figura No. 4)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 168/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

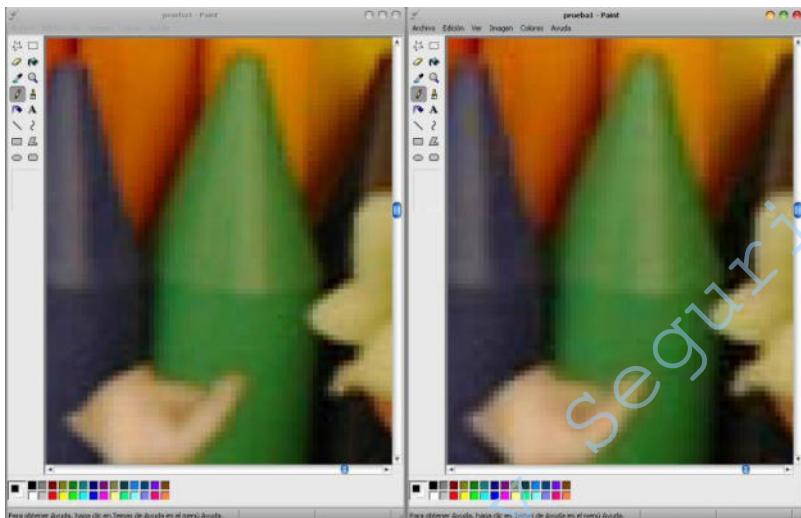


Figura No. 4. Imagen bmp e imagen jpg.

4.3.4 ¿Qué diferencias hay entre las imágenes?

Nota: Se sugiere que para observar algunas diferencias se haga un acercamiento en ambas imágenes.

4.3.5 ¿Qué diferencias hay entre los formatos bmp y jpg? (Observe el tamaño de ambos archivos y la calidad de las imágenes).

4.3.6 Tras haber hecho el análisis anterior, ¿Cómo se podría considerar al formato jpg respecto al bmp, un formato de compresión con pérdida o sin pérdida de datos? (Justifique su respuesta).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 169/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.3.7 Repita la actividad guardando esta vez la imagen en formato tiff.

4.4 Cifrado de Datos

4.4.1 Cree un archivo de texto en el bloc de notas con un mensaje genérico, y guárdelo.

4.4.2 Dé clic derecho sobre el archivo, y elija la opción *AESCrypt Encrypt*. (ver Figura No. 5)

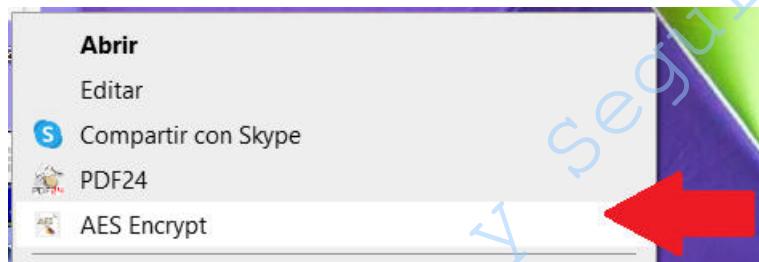


Figura No. 5. Opción de cifrar archivo tras haber instalado AESCrypt.

4.4.3 Introduzca la clave con la que será encriptado el archivo. Tendrá que recordar la clave para descifrar posteriormente el archivo. (ver Figura No. 6).

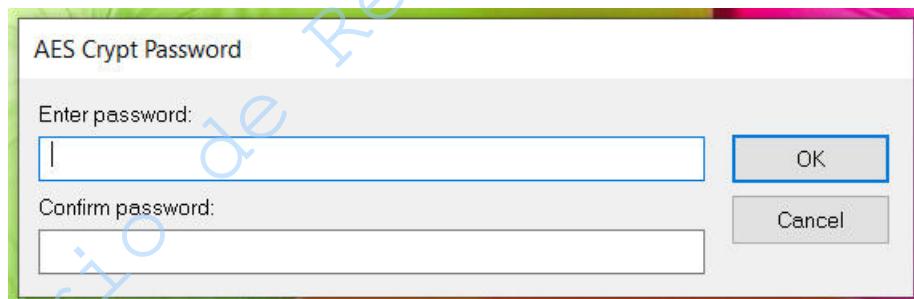


Figura No. 6. Ingreso de clave.

4.4.4 Ahora el archivo ha sido reemplazado por un archivo protegido de AESCrypt. Intercambie vía memoria usb o e-mail con uno de sus compañeros, el archivo creado.

4.4.5 Abra con block de notas el archivo que le proporcionó su compañero. ¿Qué observa? ¿Es legible el mensaje que muestra el bloc de notas? (Justifique su respuesta).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	170/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.4.6 Ahora dé clic derecho sobre el archivo, y elija la opción *AESCrypt Decrypt*. Solicite a su compañero la clave de acceso y vuelva a abrir con block de notas el archivo. ¿Es ahora legible el texto? Describa la función que realiza AESCrypt.

4.4.7 Investigue qué tipo de cifrado emplea AESCrypt

4.4.8 ¿Esta actividad simula un tipo de cifrado con Clave Pública o Privada? (Justifique su respuesta).

4.4.9 Realice la actividad extra que le deje la profesora o el profesor

4.4.10 Cierre la sesión.

5.- Cuestionario

1. ¿Para qué sirve el programa AESCrypt?

2. Mencione algunas aplicaciones de la criptografía.

3. Mencione algunas aplicaciones de la compresión de datos y en qué situaciones se usaría compresión con pérdida de datos.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	171/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

4. Menciona en qué situaciones se usaría compresión sin pérdida de datos.

ANSWER

5. Investigue la relación entre las formas de codificación de texto que maneja Mozilla Firefox y el código ASCII.

S Y

6.- Anote sus Conclusiones u Observaciones; revisando los objetivos planteados al inicio de la práctica:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	172/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 10
Funciones de la capa de presentación
Cuestionario Previo

1. ¿Cuál es la capa 6 del modelo OSI? (Dé una descripción general).
2. ¿Cuáles son las funciones principales de la Capa de Presentación?
3. Mencione algunos formatos de sonido, imágenes, películas y texto.
4. ¿Qué es la compresión de datos?
5. ¿Qué es la compresión con pérdida de datos y qué es la compresión sin pérdida?
6. ¿Qué es criptografía?
7. Describa en qué consiste la criptografía simétrica.
8. Describa en qué consiste la criptografía asimétrica.
9. Menciona algunos algoritmos de cifrado.
10. ¿De qué forma interactúa la capa 6 con sus capas aledañas (capa 5 y 7)?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO Fecha de emisión	MADO-31 06 173/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 11

Servidor DHCP

Capa 7 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	174/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- Al finalizar la práctica, el alumno o la alumna habrá configurado un servidor DHCP bajo una plataforma Linux.
- El alumno o la alumna configurará el servidor en sus tres modos de asignación de parámetros.

2.- Conceptos teóricos

Servidor DHCP

“Dynamic Host Configuration Protocol” sus especificaciones se encuentran en los RFC 1541 y 1533.

Es un protocolo que proporciona un entorno de trabajo que tiene como objetivo asignar los parámetros de configuración a los diferentes hosts dentro de una red bajo TCP/IP. DHCP se basa en el protocolo BOOTP, añadiendo la capacidad de asignar automáticamente direcciones de red reutilizables y opciones de configuración adicionales.

DHCP es un protocolo que funciona en una arquitectura cliente/servidor y hace uso de los puertos 67 y 68 con protocolo de transporte UDP.

El protocolo soporta tres modos de asignación de direcciones IP:

- Manual
- Automática
- Dinámica

Funcionamiento:

El servidor DHCP tiene la característica de que cuenta con una dirección IP fija. Cuando la computadora cliente se conecta a la red lo hace por medio del protocolo BOOTP, durante el proceso de arranque de la máquina. Como el cliente no cuenta con la información necesaria sobre la configuración de red a la cual está conectada, inicia una técnica en la cual busca, encuentra y se comunica con el servidor DHCP solicitándole los parámetros de configuración. Cuando el DHCP recibe la solicitud, éste responderá con la información solicitada.

Algunos de los mensajes que se transmiten entre el servidor y el cliente son: DHCP Discovery, DHCP Offer, DHCP Request, y DHCP Acknowledge.

3.- Equipo y material necesario

3.1 Material del alumno o de la alumna:

- Cables construidos en la práctica 1

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	175/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

3.2 Equipo del Laboratorio:

- 1 Dispositivo de interconexión Switch
- 1 Computadora con Sistema Operativo Linux (Debian)
- 1 Computadora con Sistema Windows.
- Analizador de paquetes Wireshark.

4.- Desarrollo:

Modo de trabajar

La práctica se desarrollará entre dos equipos de dos integrantes cada uno como máximo. Cada equipo manipulará ambas computadoras en turnos. La computadora con sistema operativo Linux será el servidor y la otra con sistema operativo Windows será el cliente

4.1 Ejercicio

4.1.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 1).

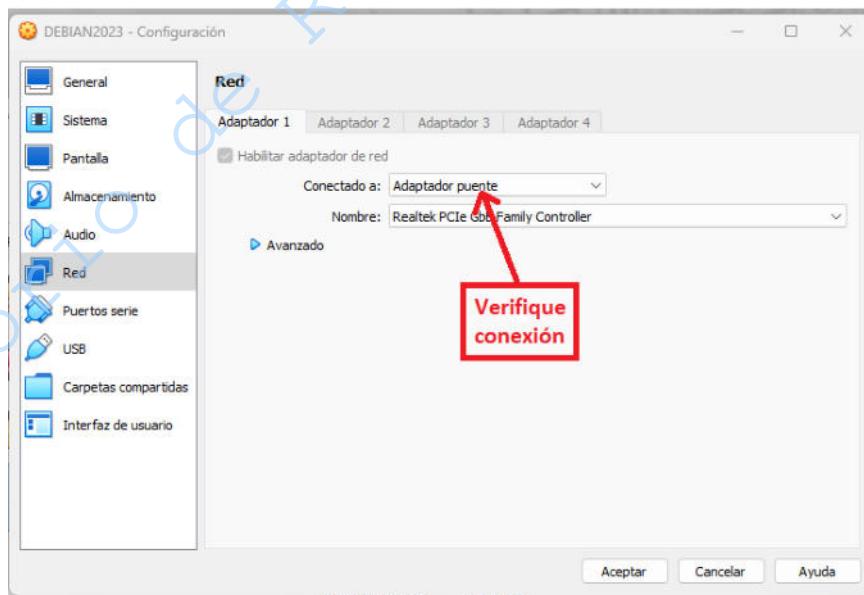


Figura No. 1. Conexión de red.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	176/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.2 Encienda la máquina virtual

4.1.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete ifconfig.

4.1.4 Inicie sesión en la cuenta de *redes*.

4.1.5 Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 2)

NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root
redes@debian:~\$ su



```
redes@DEBIAN2023: ~
redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes#
```

Figura No 2. Cambio de sesión con privilegios

4.1.6 Verifique que la computadora servidor tenga conexión a Internet. En caso contrario realice lo necesario para poder obtenerla.

4.1.7 Teclee los siguientes comandos para restaurar el sistema antes de realizar la instalación del servidor

```
root@debian:/home/redes# apt-get autoremove --purge isc-dhcp-server
root@debian:/home/redes# apt-get remove isc-dhcp-server
root@debian:/home/redes# apt-get purge isc-dhcp-server
root@debian:/home/redes # rm -rf /etc/dhcp/dhcpd.conf.*
```

4.2 Instalación del servidor DHCP

4.2.1 En el Shell, teclee lo siguiente (ver Figura No. 3)

```
root@debian:/home/redes# apt install isc-dhcp-server
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	177/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

```

root@DEBIAN2023:/home/redes# apt install isc-dhcp-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libirs-export161 libisccfg-export163 policycoreutils selinux-utils
Suggested packages:
  isc-dhcp-server-ldap
The following NEW packages will be installed:
  isc-dhcp-server libirs-export161 libisccfg-export163 policycoreutils
  selinux-utils
0 upgraded, 5 newly installed, 0 to remove and 1 not upgraded.
Need to get 1,703 kB of archives.
After this operation, 6,915 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libisccfg-export163 amd64
 1:9.11.19+dfsg-2.1 [272 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libirs-export161 amd64 1:
 9.11.19+dfsg-2.1 [245 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 isc-dhcp-server amd64 4.4
  .1-2.3+deb11u2 [554 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 selinux-utils amd64 3.1-3
  [142 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 policycoreutils amd64 3.1
  -3 [491 kB]
Fetched 1,703 kB in 10s (163 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libisccfg-export163.
(Reading database ... 168395 files and directories currently installed.)
Preparing to unpack .../libisccfg-export163_1%3a9.11.19+dfsg-2.1_amd64.deb ...
Unpacking libisccfg-export163 (1:9.11.19+dfsg-2.1) ...
Selecting previously unselected package libirs-export161.
Preparing to unpack .../libirs-export161_1%3a9.11.19+dfsg-2.1_amd64.deb ...
Unpacking libirs-export161 (1:9.11.19+dfsg-2.1) ...
Selecting previously unselected package isc-dhcp-server.
Preparing to unpack .../isc-dhcp-server_4.4.1-2.3+deb11u2_amd64.deb ...
Unpacking isc-dhcp-server (4.4.1-2.3+deb11u2) ...

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	178/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

Setting up libisccfg-export163 (1:9.11.19+dfsg-2.1) ...
Setting up libirs-export161 (1:9.11.19+dfsg-2.1) ...
Setting up isc-dhcp-server (4.4.1-2.3+deb11u2) ...
Generating /etc/default/isc-dhcp-server...
Job for isc-dhcp-server.service failed because the control process exited with error code.
See "systemctl status isc-dhcp-server.service" and "journalctl -xe" for details.
invoke-rc.d: initscript isc-dhcp-server, action "start" failed.
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: failed (Result: exit-code) since Mon 2023-10-30 11:44:01 CST; 21ms ago
     Docs: man:systemd-sysv-generator(8)
   Process: 1962 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=1/FAILURE)
             CPU: 34ms

Oct 30 11:43:59 DEBIAN2023 dhcpd[1978]: before submitting a bug. These pages explain the proper
Oct 30 11:43:59 DEBIAN2023 dhcpd[1978]: process and the information we find helpful for debugging.
Oct 30 11:43:59 DEBIAN2023 dhcpd[1978]:
Oct 30 11:43:59 DEBIAN2023 dhcpd[1978]: exiting.
Oct 30 11:44:01 DEBIAN2023 isc-dhcp-server[1962]: Starting ISC DHCPv4 server: dhcpdcheck syslog for diagnostics. ...
Oct 30 11:44:01 DEBIAN2023 isc-dhcp-server[1983]: failed!
Oct 30 11:44:01 DEBIAN2023 isc-dhcp-server[1984]: failed!
Oct 30 11:44:01 DEBIAN2023 systemd[1]: isc-dhcp-server.service: Control process exited, code=exited, status=1/FAILURE
Oct 30 11:44:01 DEBIAN2023 systemd[1]: isc-dhcp-server.service: Failed with result 'exit-code'.
Oct 30 11:44:01 DEBIAN2023 systemd[1]: Failed to start LSB: DHCP server.
Processing triggers for libc-bin (2.31-13+deb11u6) ...
Processing triggers for man-db (2.9.4-2) ...
root@DEBIAN2023:/home/redes#

```

Figura No. 3. Instalación del servidor DHCP

NOTA: El error que se observa se debe a que aún no se configura el servidor DHCP, aunque los paquetes ya estén descargados.

4.3 Configuración del cliente y servidor DHCP

4.3.1 Tome nota de la configuración de red actual de la máquina cliente y del servidor antes de realizar algún cambio.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 179/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.3.2** Configure la tarjeta de red del cliente de tal forma que sus parámetros sean asignados de forma automática. Recuerde asignar en la máquina cliente, la cual está empleando el sistema operativo Windows, la obtención de una dirección IP automáticamente y la obtención del servidor DNS automáticamente como se observa en la Figura 4.

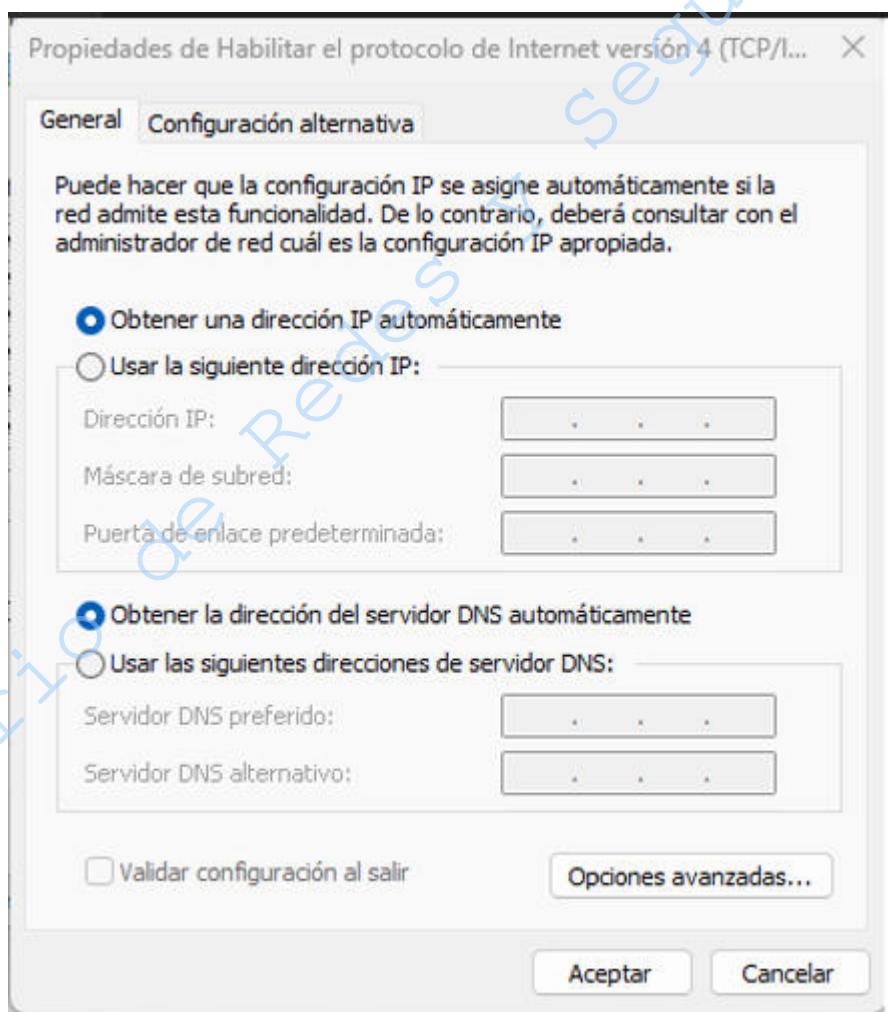


Figura No. 4. Configuración automática

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	180/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.3** Configure la tarjeta de red del servidor con los siguientes datos (no emplee la forma gráfica sino vía comandos), vea la Figura 5:

Dirección IP: 192.168.1.8
Máscara de red: 255.255.255.0
Red: 192.168.1.0
Broadcast: 192.168.1.255
Gateway: 192.168.1.1

```
GNU nano 5.4                               /etc/network/interfaces *

#This file describes the network interfaces available on your system
#and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

#The loopback network interface
auto lo
iface lo inet loopback

#The primary network interface
auto enp0s3
iface enp0s3 inet static
address 192.168.1.8
netmask 255.255.255.0
gateway 192.168.1.1
network 192.168.1.0
broadcast 192.168.1.255
```

Figura No. 5. Parámetros

- 4.3.4** Reinicie los servicios de la tarjeta de red, ingrese el siguiente comando (Figura No. 6)

```
root@debian:/home/redes# /etc/init.d/networking restart
```

```
redes@DEBIAN2023: ~

root@DEBIAN2023:/home/redes# /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.
root@DEBIAN2023:/home/redes#
```

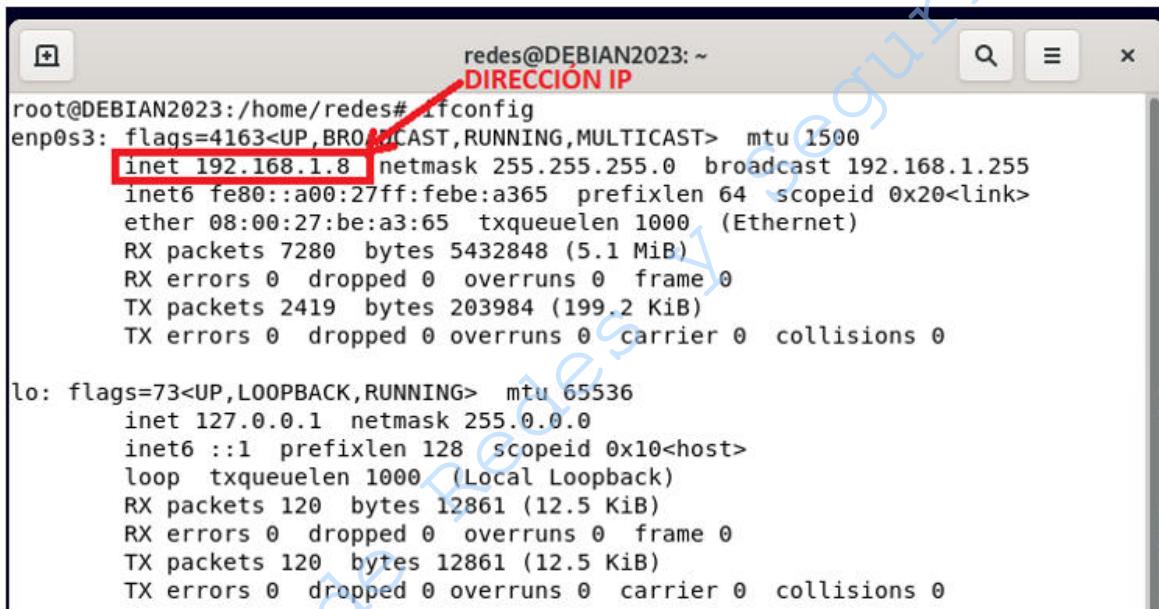
Figura No. 6. Reinicio del servicio

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 181/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.3.5** Verifique que pertenezca al mismo segmento de red (Ver la Figura No. 7), ingrese el comando siguiente:

```
root@debian:/home/redes# ifconfig
```

Coloque el nombre de la interfaz observada_____



```
root@DEBIAN2023:/home/redes# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.8 brd 192.168.1.255 netmask 255.255.255.0 broadcast 192.168.1.255
        ether 08:00:27:be:a3:65 txqueuelen 1000 (Ethernet)
        RX packets 7280 bytes 5432848 (5.1 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 2419 bytes 203984 (199.2 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 120 bytes 12861 (12.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 120 bytes 12861 (12.5 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura No. 7 Verificación de la dirección IP.

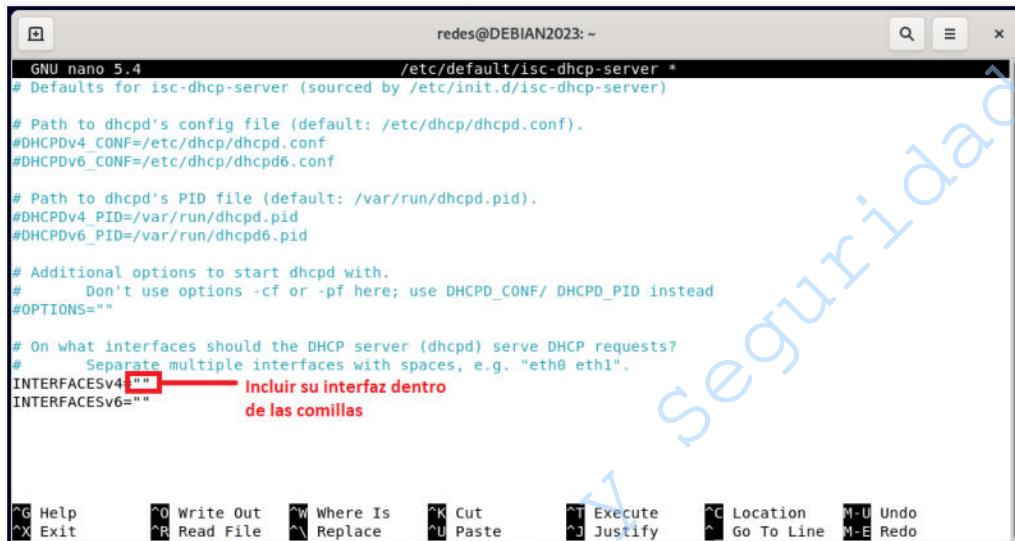
- 4.3.6** Ingrese al archivo de configuración de interfaces de red, para ello teclee el comando siguiente:

```
root@debian:/home/redes# nano /etc/default/isc-dhcp-server
```

- 4.3.7** Coloque el nombre de la interfaz observado en el punto 4.3.5 entre las comillas de la línea INTERFACESv4= “ ”(Figuras No. 8 y 9).

Por ejemplo: INTERFACESv4= “enp0s3”

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	182/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			



```

GNU nano 5.4          /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDv4_PID=/var/run/dhcpcd.pid
#DHCPDv6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#   Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#   Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4=""      Incluir su interfaz dentro
INTERFACESv6=""


```

Figura No. 8 Ingreso de la interfaz de red



```

GNU nano 5.4          /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDv4_PID=/var/run/dhcpcd.pid
#DHCPDv6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#   Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#   Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"  CORRECTA
INTERFACESv6=""


```

Figura No. 9 Interfaz de red ingresada

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	183/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- 4.3.8** Copie el archivo de configuración original del servidor. Teclee lo siguiente (Figura No. 10):

```
root@debian:/home/redes# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.old
```



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.old
```

Figura No. 10 Cambio de nombre del archivo de configuración

- 4.3.9** Ingrese al archivo de configuración, para ello teclee lo siguiente:

```
root@debian:/home/redes# nano /etc/dhcp/dhcpd.conf
```

- 4.3.10** Dentro del archivo ubique la siguiente sección option domain-name y option domain-name-servers (ver Figura No. 11) y modifique con los datos indicados a continuación:

```
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;
```

Figura No. 11. Configuración

```
option domain-name "lab.redes";
option domain-name-servers 132.248.204.1, 132.248.10.2;
```

Explique el significado de las líneas agregadas anteriormente

- 4.3.11** Dentro del mismo archivo ubique las líneas **default-lease-time 600;** y **max-lease-time 720;** anteponga el símbolo de #

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	184/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
#default-lease-time 600;
#max-lease-time 720;
```

4.3.12 Ahora vaya al final del archivo e incluya las líneas siguientes

```
subnet 192.168.1.0 netmask 255.255.255.0 {
}
```

Explique el significado de las líneas agregadas anteriormente

4.3.13 Guarde y salga del editor

4.3.14 Reinicie el servicio DHCP. Teclee lo siguiente

```
root@debian:/home/redes# systemctl restart isc-dhcp-server
```

Para verificar que el servidor funciona de manera correcta teclee el comando (Figura No. 12):

```
root@debian:/home/redes# systemctl status isc-dhcp-server.service
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	185/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```
root@DEBIAN2023:/home/redes# systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - LSB: DHCP server
  Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
  Active: active (running) since Thu 2023-08-10 13:43:04 CST; 5min ago
    Docs: man:systemd-sysv-generator(8)
 Process: 1769 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, sta>
  Tasks: 4 (limit: 2954)
 Memory: 2.3M
      CPU: 35ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─1785 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s3

Aug 10 13:44:08 DEBIAN2023 dhcpd[1785]: Ignoring empty DHO_HOST_NAME option
Aug 10 13:44:08 DEBIAN2023 dhcpd[1785]: BOOTREQUEST from f8:b1:56:55:a5:3a via >
Aug 10 13:45:08 DEBIAN2023 dhcpd[1785]: Ignoring empty DHO_HOST_NAME option
Aug 10 13:45:08 DEBIAN2023 dhcpd[1785]: BOOTREQUEST from f8:b1:56:55:a5:3a via >
Aug 10 13:46:08 DEBIAN2023 dhcpd[1785]: Ignoring empty DHO_HOST_NAME option
Aug 10 13:46:08 DEBIAN2023 dhcpd[1785]: BOOTREQUEST from f8:b1:56:55:a5:3a via >
Aug 10 13:47:07 DEBIAN2023 dhcpd[1785]: Ignoring empty DHO_HOST_NAME option
Aug 10 13:47:07 DEBIAN2023 dhcpd[1785]: BOOTREQUEST from f8:b1:56:55:a5:3a via >
Aug 10 13:47:08 DEBIAN2023 dhcpd[1785]: DHCPDISCOVER from e4:54:e8:e2:7d:99 via >
```

Figura No. 12. Verificación del servicio de DHCP

NOTA: En caso de que no aparezca la figura anterior, debe repetir todo el proceso que ha realizado hasta ahora.

Hasta el momento, el servidor está funcionando correctamente, pero aún no asigna direcciones. Para ello realice lo siguiente:

4.4 Asignación Manual

4.4.1 Vaya a la máquina cliente y averigüe su dirección MAC.

4.4.2 Regrese a la máquina servidor y edite el archivo de configuración:

root@debian:/home/redes# nano /etc/dhcp/dhcpd.conf

4.4.3 Diríjase al final del archivo y ubique la parte donde incluyó el segmento de red, agregue la información que se muestra a continuación: (ver Figura No. 13)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 186/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

```

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.200;
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.255;
}

#####
##Asignación Manual #####
host Equipo1 {
    hardware ethernet MAC_del_cliente;
    fixed-address 192.168.1.101;
}

```

NOTA: Donde MAC_del_cliente debe sustituirse por la dirección MAC del dispositivo que es el cliente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	187/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

```

GNU nano 5.4                               redes@DEBIAN2023: ~
                                              /etc/dhcp/dhcpd.conf

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.200;
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.255;
}

#####
##Asignacion Manual##
host Equipo1 {
  hardware ethernet E4:54:E8:E3:DF:5A;
  fixed-address 192.168.1.101;
}

```

Figura No. 13 Asignación Manual

Explique el significado de las líneas agregadas anteriormente

4.4.4 Guarde y salga del editor

4.4.5 Reinicie el servicio

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	188/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

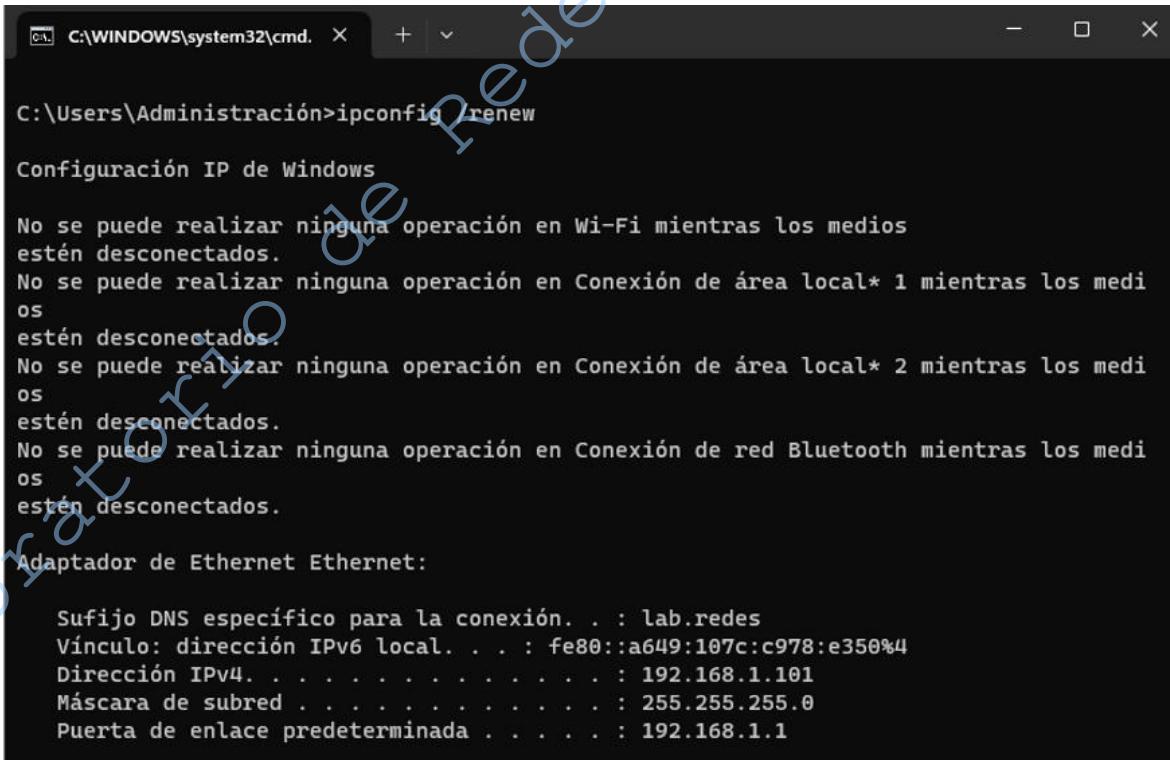
```
root@debian:/home/redes# /etc/init.d/isc-dhcp-server restart
root@debian:/home/redes# systemctl restart isc-dhcp-server.service
```

4.4.6 Vaya a la computadora cliente y renueve la configuración de la tarjeta de red con alguna de las siguientes acciones:

- a) Desactive y vuelva a activar la conexión de área local
- b) Abra un CMD y ejecute las dos siguientes instrucciones:
 ipconfig /release
 ipconfig /renew

NOTA: Es probable que tenga que realizar ambos incisos durante las pruebas de asignación.

4.4.7 Visualice la configuración de red de la computadora cliente (Ver Figura No. 14)



```
C:\WINDOWS\system32\cmd. x + v
C:\Users\Administración>ipconfig /renew

Configuración IP de Windows

No se puede realizar ninguna operación en Wi-Fi mientras los medios
estén desconectados.
No se puede realizar ninguna operación en Conexión de área local* 1 mientras los medi
os
estén desconectados.
No se puede realizar ninguna operación en Conexión de área local* 2 mientras los medi
os
estén desconectados.
No se puede realizar ninguna operación en Conexión de red Bluetooth mientras los medi
os
estén desconectados.

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . : lab.redes
Vínculo: dirección IPv6 local. . . : fe80::a649:107c:c978:e350%4
Dirección IPv4. . . . . : 192.168.1.101
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Figura No. 14. Configuración en la computadora cliente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	189/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.4.8 Escriba a continuación lo obtenido en el paso anterior y analice y comente al respecto

(Este espacio es para la respuesta)

4.5 Asignación Automática

4.5.1 Copie el archivo de configuración con el nombre ***dhcpd.conf.manual*** Teclee lo siguiente:

```
root@debian:/home/redes# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.manual
```

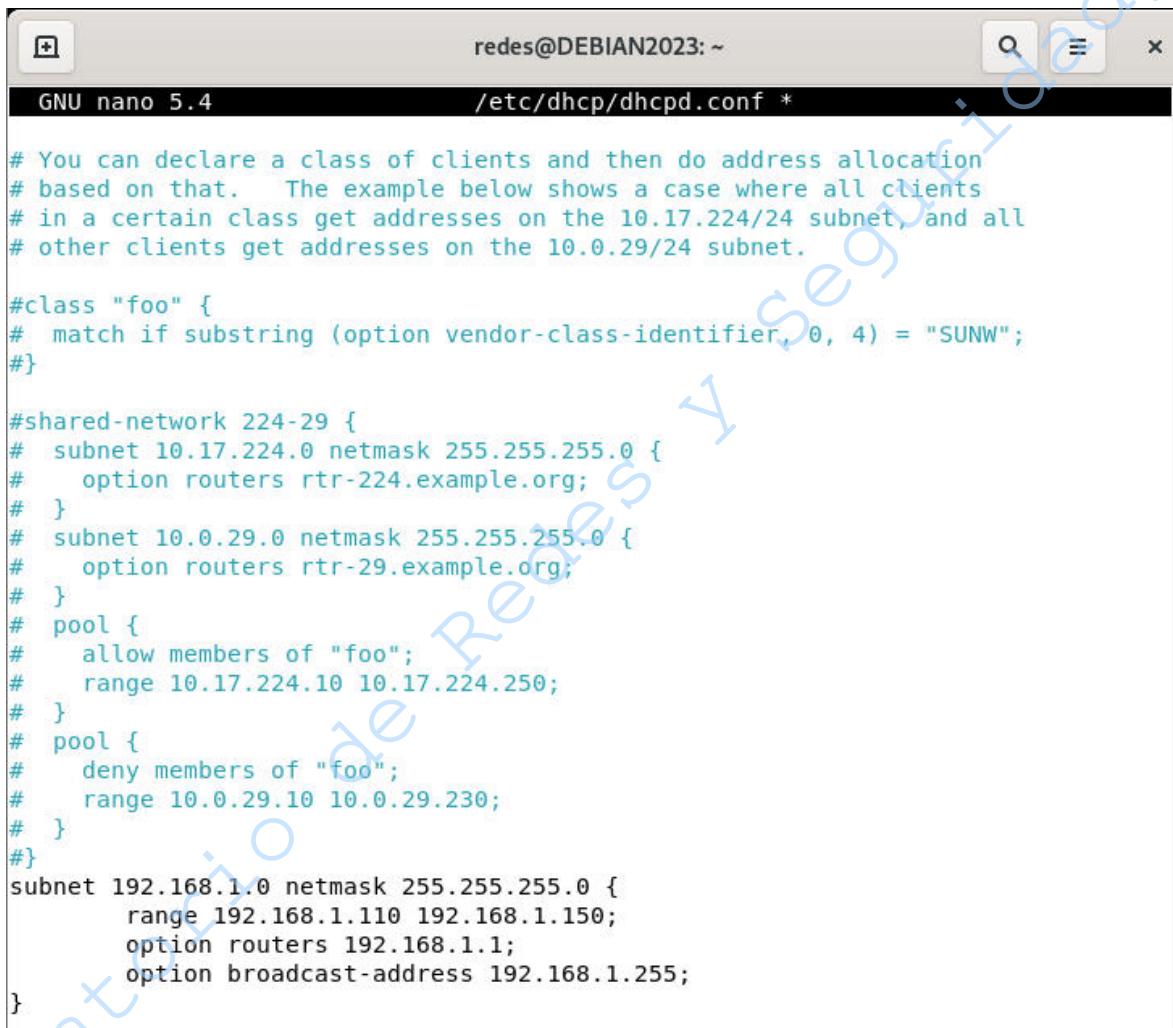
4.5.2 Ingrese al archivo de configuración empleando el archivo siguiente:

```
root@debian:/home/redes# nano /etc/dhcp/dhcpd.conf
```

4.5.3 Edite el archivo de configuración. Vaya al final del archivo y realice lo siguiente (Ver Figura No. 15):

- a) Borre la configuración manual.
- b) El rango de direcciones cámbielo por: 192.168.1.110 a 192.168.1.150

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	190/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```

GNU nano 5.4          redes@DEBIAN2023: ~
/etc/dhcp/dhcpd.conf *

# You can declare a class of clients and then do address allocation
# based on that. The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

"class \"foo\" {
# match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
}

#shared-network 224-29 {
# subnet 10.17.224.0 netmask 255.255.255.0 {
#   option routers rtr-224.example.org;
# }
# subnet 10.0.29.0 netmask 255.255.255.0 {
#   option routers rtr-29.example.org;
# }
# pool {
#   allow members of "foo";
#   range 10.17.224.10 10.17.224.250;
# }
# pool {
#   deny members of "foo";
#   range 10.0.29.10 10.0.29.230;
# }
#
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.110 192.168.1.150;
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.255;
}

```

Figura No. 15. Asignación Automática.

- 4.5.4 Guarde y salga del editor
- 4.5.5 Reinicie el servidor DHCP

root@debian:/home/redes# systemctl restart isc-dhcp-server

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	191/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 4.5.6** Vaya a la computadora cliente y renueve la configuración de la tarjeta de red con las siguientes acciones:

En un CMD y ejecute las dos siguientes instrucciones:

```
ipconfig /release
ipconfig /renew
```

Escriba a continuación la configuración obtenida en la máquina cliente:

Analice lo obtenido en el paso anterior y comente al respecto

4.6 Asignación Dinámica

- 4.6.1** Copie el archivo de configuración con el nombre ***dhcpd.conf.automatic*** Teclee lo siguiente:

```
root@debian:/home/redes# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.automatic
```

- 4.6.2** Edite el archivo de configuración. Vaya al final del archivo y realice lo siguiente (Ver Figura No. 16):

- a) Localice las líneas que se muestran a continuación y elimine el #

```
#default-lease-time 600;
#max-lease-time 720;
```

Figura No. 16 Asignación Dinámica

- b) Cambie los valores por los siguientes:

```
default-lease-time 120;
max-lease-time 122;
```

- c) Cambie los valores del rango por los siguientes (figura 17):
Range 192.168.1.120 192.168.1.150

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	192/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

GNU nano 5.4          redes@DEBIAN2023: ~
/etc/dhcp/dhcpd.conf *

# You can declare a class of clients and then do address allocation
# based on that. The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.120 192.168.1.150;
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.255;
}

```

Figura No. 17. Asignación Dinámica

Analice las líneas agregadas anteriormente y explique su significado:

4.6.3 Guarde y salga del editor.

4.6.4 Reinicie el servidor

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	193/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

root@debian:/home/redes# systemctl restart isc-dhcp-server

4.6.5 Escriba a continuación la configuración obtenida en la máquina cliente:

Analice lo obtenido en el paso anterior, observe el tiempo de concesión y comente al respecto

EJERCICIO OPCIONAL

4.7 Análisis del funcionamiento del servidor DHCP

4.7.1 Visualice el contenido del archivo dhcpd.leases Teclee lo siguiente:

root@debian:/home/redes# cat /var/lib/dhcp/dhcpd.leases | more

Analice el contenido de dicho archivo y comente al respecto

4.7.2 Detenga el servidor DHCP. Teclee lo siguiente:

root@debian:/home/redes# /etc/init.d/isc-dhcp-server stop

4.7.3 Renueve la configuración en la tarjeta cliente (Paso 4.4.6) y Visualice la configuración actual de la máquina cliente

NOTA: Al estar parado el servidor, el cliente no podrá obtener una configuración, por lo que la máquina asignará una configuración provisional. Si no logra lo anterior ejecute varias veces el Paso 4.4.6 hasta lograrlo.

4.7.4 En la computadora cliente ejecute el software analizador de paquetes **Wireshark**.

4.7.5 Configure una nueva captura: elija la tarjeta de red adecuada, desactive el modo promiscuo y elija el filtro **IP** (ver Figura No. 18), para ello escriba ip. **No inicie la captura**

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 194/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

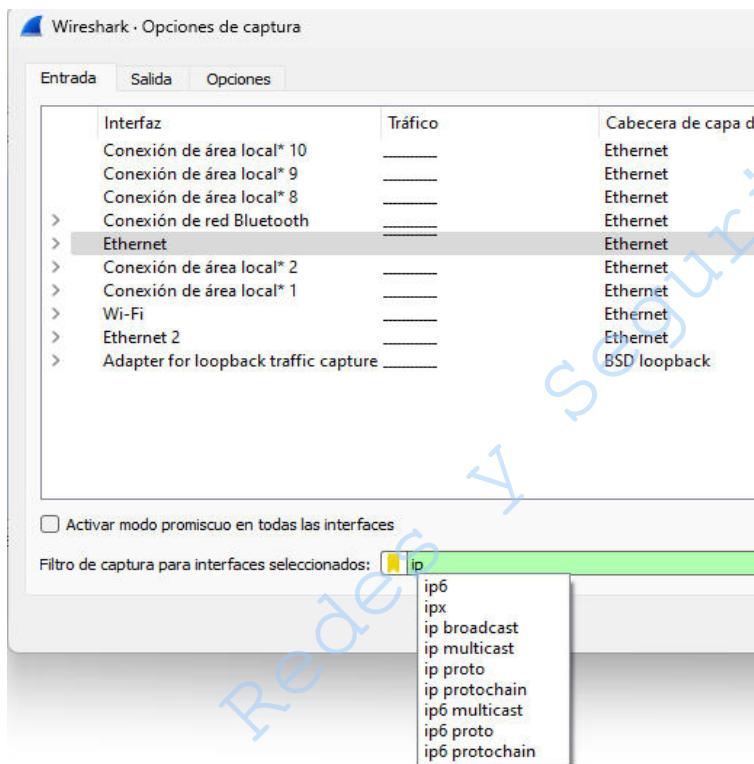


Figura No. 18. Configuración de la captura

¡ATENCIÓN! EL SIGUIENTE PASO (4.7.6) SE COMPONE DE 3 ACCIONES QUE DEBERÁN EJECUTARSE LO MÁS RÁPIDO POSIBLE, UNA SEGUIDA DE LA OTRA, PARA PODER LOGRAR LA CAPTURA. SI NO LO LOGRA LA PRIMERA VEZ REPITA DESDE EL PASO 4.7.2

- 4.7.6** Nuevamente repita el paso 4.4.6, inmediatamente inicie la captura y reinicie el servidor
- 4.7.7** Cuando la máquina cliente haya obtenido la configuración, detenga la captura de Wireshark
- 4.7.8** En la captura busque los paquetes relacionados con el establecimiento de la sesión del servidor DHCP con el cliente (Ver Figura No. 19)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	195/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

No.	Time	Source	Destination	Protocol	Length	Info
447	52.650593	0.0.0.0	255.255.255.255	BOOTP	342	Boot Request from f8:b1:56:55:a5:3
676	72.253680	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x9
791	73.254043	192.168.1.8	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x9
792	73.254929	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x9
793	73.265381	192.168.1.8	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x9
1063	82.374966	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x7
1064	82.375251	192.168.1.8	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x7
1065	82.376049	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x7
1066	82.378274	192.168.1.8	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x7
1649	112.413078	0.0.0.0	255.255.255.255	BOOTP	342	Boot Request from f8:b1:56:55:a5:3

Figura No. 19. Captura de paquetes.

4.7.9 Explore los detalles de cada uno de los paquetes involucrados y comente al respecto:

4.7.10 Inicie una nueva captura con las características de la anterior y busque entre los paquetes capturados la petición de la máquina cliente hacia el servidor DHCP cada vez que su concesión se termina. (Ver Figura No. 20)

No.	Time	Source	Destination	Protocol	Length	Info
333	22.360974	0.0.0.0	255.255.255.255	BOOTP	342	Boot Request from f8:b1:56:55:a5:3
352	23.430880	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xc
353	23.431182	192.168.1.8	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xc
354	23.432075	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xc
356	23.446679	192.168.1.8	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xc

Figura No. 20. Paquetes de actualización de concesión.

4.7.11 Analice lo obtenido en el paso anterior observando los detalles de los paquetes capturados. Comente al respecto.

4.7.12 Regrese a la configuración inicial tanto de la máquina servidor como de la máquina cliente con los datos del paso 4.3.1.

4.7.13 Desinstale el servidor tecleando lo siguiente:

```
root@debian:/home/redes# apt-get autoremove --purge isc-dhcp-server
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	196/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.7.14 Si la profesora o el profesor no indica lo contrario, cierre sesión.

5.-Cuestionario

1. Comente en qué casos es recomendable el uso de un servidor DHCP

2. Investigue cuáles son los requerimientos y el procedimiento para instalar un servidor DHCP bajo plataforma Windows.

3. Describa un ejemplo de aplicación para cada uno de los diferentes modos de asignación de direcciones del servidor DHCP (Manual, Automática y Dinámica)

6.- Anote sus Conclusiones u Observaciones revisando los objetivos planteados al inicio de la práctica:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	197/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 11
Servidor DHCP
Cuestionario Previo

1. Investigue los pasos que se llevan a cabo para el establecimiento de la sesión entre un servidor DHCP y una máquina cliente.
2. Investigue las características de funcionamiento del protocolo BOOTP
3. Investigue las características de los diferentes modos de asignación de direcciones de un servidor DHCP.
4. Explique el concepto de “concesión”

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 198/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Manual de prácticas complementarias y obligatorias para la clase de teoría de Redes de Datos Seguras

Elaborado por:	Revisado por:	Autorizado por:	Vigente desde:
Ing. María Eugenia Bautista González Ing. Edgar Martínez Meza Ing. Javier León Cotonieto M.C. Cintia Quezada Reyes Ing. Magdalena Reyes Granados	M.C. Ma. Jaquelina López Barrientos Ing. Edgar Martínez Meza M.C. Cintia Quezada Reyes	Dra. Rocío Alejandra Aldeco Pérez	11 de agosto de 2023

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	199/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

Índice de prácticas complementarias y obligatorias

Estándares y arquitecturas

Práctica complementaria y obligatoria 1. Normatividad

200

Capa 1 del Modelo OSI

Práctica complementaria y obligatoria 2. Instalación y cambio de módulos en routers

211

Práctica complementaria y obligatoria 3. Cableado estructurado

231

Capa 2 del Modelo OSI

Práctica complementaria y obligatoria 4. Compartición de archivos por Hub y Switch en Linux

240

Práctica complementaria y obligatoria 5. Políticas de seguridad en las interfaces del switch

260

Práctica complementaria y obligatoria 6. EtherChannel y port security

278

Capa 3 del Modelo OSI

Práctica complementaria y obligatoria 7. Enrutamiento estático

307

Práctica complementaria y obligatoria 8. HSRP – Hot Spot Router Protocol

327

Capa 4 del Modelo OSI

Práctica complementaria y obligatoria 9. Uso de protocolos TCP y UDP

351

Capa 5 del Modelo OSI

Práctica complementaria y obligatoria 10. Sistema Operativo de Router

377

Capa 6 del Modelo OSI

Práctica complementaria y obligatoria 11. VPN

394

Capa 7 del Modelo OSI

Práctica complementaria y obligatoria 12. Firewall básico

409

Práctica complementaria y obligatoria 13. Configuración básica de una comunicación de Voz IP

426

Práctica complementaria y obligatoria 14. Web DNS e IP Helper

452

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO Fecha de emisión	MADO-31 06 200/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 1

Normatividad

Estándares y Arquitecturas

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	201/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivos de aprendizaje

- El alumno o la alumna investigará organismos de estandarización.
- El alumno o la alumna investigará las normas y estándares para el cableado estructurado.

2.- Conceptos teóricos

Las normas de redes son descripciones técnicas con el fin de lograr una intercomunicación uniforme entre diferentes dispositivos.

En la actualidad existen organismos encargados de crear normas y estándares para la construcción y creación del cableado estructurado.

- a) **ANSI (American National Standards Institute).** Es la encargada de supervisar el desarrollo para productos, servicios, procesos y sistemas en los Estados Unidos.
- b) **TIA (Telecommunications Industry Association).** Encargada de mejorar el entorno de las diferentes industrias de la comunicación.
- c) **EIA (Electronic Industries Alliance).** Encargada de promover el mercado y la alta tecnología en los Estados Unidos.
- d) **ISO (International Organization for Standardization).** Es una organización la cual se encarga de promover estándares a nivel internacional de creación, construcción y aplicación de las ramas de servicios de telecomunicaciones, construcciones, entre otras.

Existen más normas encargadas de la creación de manuales, documentos y estándares para la calidad y seguridad de servicios.

3.- Equipo y material necesario

Equipo del laboratorio:

- Computadora con un sistema operativo Windows.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 202/479 8.3 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

4.1 Ejercicio

- 4.1.1** Investigue qué es un organismo de estandarización

- 4.1.2** Investigue cuáles son los organismos de estandarización en redes, descríbalos brevemente.

- 4.1.3** Investigue cuál es la definición de Request for Comments, más conocido por sus siglas RFC.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	203/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.4 Investigue cuáles son las características principales de un Request for Comments.

4.1.5 Indique cuál es la importancia de un Request for Comments.

4.1.6 Defina IETF y cuál es su objetivo principal.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO Fecha de emisión	MADO-31 06 204/479 8.3 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

4.1.7 El comité Internet Architecture Board (IAB) del IETF, mantiene una lista de RFC que describen la familia de protocolos y los clasifica con base en su estado de dos formas independientes, indique qué describe cada una.

4.1.8 Con base en el punto anterior describa cada uno de los siguientes puntos:

- a) Estándar
- b) Estándar borrador
- c) Estándar propuesto
- d) Experimental Informativo
- e) Histórico
- f) Requerido
- g) Recomendado

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	205/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.1.9** Investigue y describa otras normas existentes en el área de las redes de datos y telecomunicaciones.

- 4.1.10** Discuta y reflexione con su equipo sobre cuál es la importancia del uso de las normas y estándares

- 4.1.11** Investigue qué es IANA.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	206/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.12 Investigue y describa la función de la IANA.

4.1.13 Visite la página www.ietf.org e indique cuál es su función.

4.1.14 Mencione qué norma hace referencia a la codificación de colores, etiquetado y documentación de un sistema de cableado instalado y descríbala brevemente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	207/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.15 Con base en la norma del punto anterior, describa cuál es el uso de cada color.

4.1.16 En el laboratorio de redes y seguridad, indique en qué puntos se debe usar la norma ANSI/EIA/TIA 606.

4.1.17 Investigue a qué se refiere la serie ISO 27000.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	208/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- 4.1.18** Con base en los estándares vistos qué consideraciones deben hacerse para que una red sea segura

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 209/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	210/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 1

Normatividad **Cuestionario Previo**

1. Defina el término norma.
2. Defina el término estándar.
3. Indique si existe alguna diferencia entre normas y estándares. Justifique su respuesta.
4. Mencione las ventajas y desventajas de utilizar normas.
5. ¿Qué nomenclatura emplean las normas en México? , describa la diferencia entre cada una de ellas.
6. ¿Cuáles son las normas y estándares que se utilizan en México?
7. ¿Qué nomenclatura emplea una norma internacional?
8. Indique las normas internacionales que se emplean para el cableado estructurado.

Laboratorio de Redes Y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO Fecha de emisión	MADO-31 06 211/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 2

Instalación y cambio de módulos en routers

Capa 1 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 212/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

1.- Objetivos de aprendizaje

- El alumno o la alumna conocerá y simulará módulos que pueden tener los routers modelo 1841 WIC-2T, 281 IOS15 e ISR 4331.

2.- Conceptos teóricos

Un router es un dispositivo intermedio que recibe y envía datos en redes informáticas, combinando funciones de switch, módem y concentradores de red para mejorar el acceso a Internet o ayudar a crear redes empresariales.

Físicamente, un router tiene módulos con puertos donde se conectan los cables ethernet, seriales, consola, etc., a su vez, estos módulos son modificables con la finalidad de poder conectar al router distintos dispositivos.

El modelo 1841 visto por detrás luce como se muestra en la Figura No. 1.

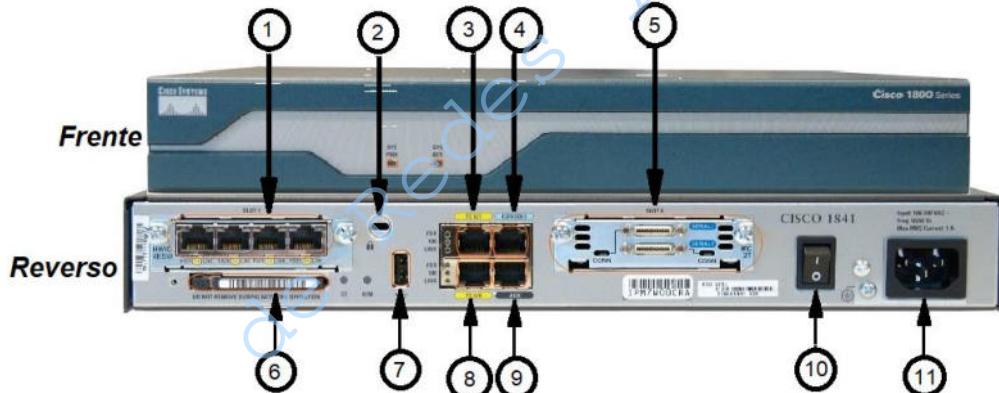


Figura No. 1. Modelo 1841.

Donde:

1. Primer slot o ranura de instalación de módulos adicionales.
2. Conector de seguridad Kensington.
3. Interfaz Fast Ethernet 0/1.
4. Puerto de consola para administración inicial.
5. Segundo slot o ranura de instalación de módulos adicionales.
6. Unidad de tarjeta flash compacta.
7. Puerto USB.
8. Interfaz Fast Ethernet 0/0.
9. Puerto auxiliar para acceso mediante Módem.
10. Botón encendido/apagado.
11. Entrada de corriente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 213/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

El modelo 2811 IOS15 luce como se muestra en la Figura No. 2.

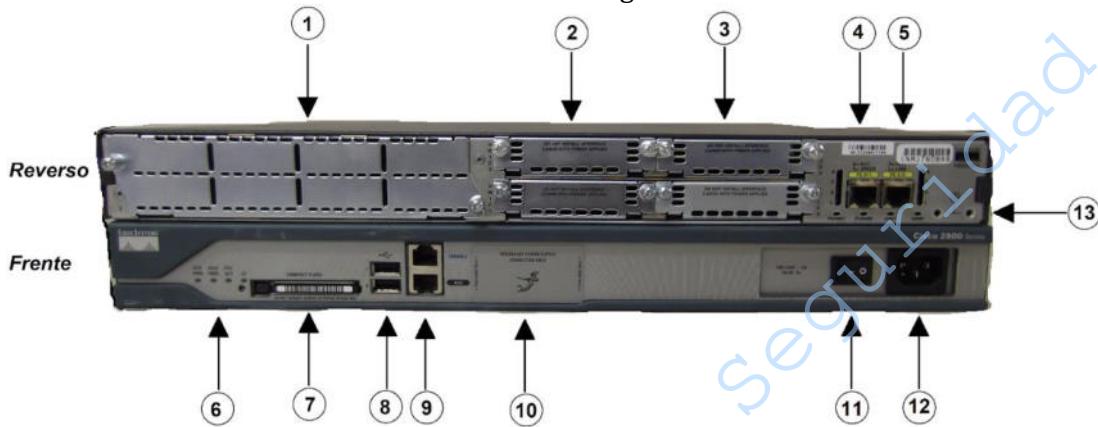


Figura 2. Modelo 2811 IOS15.

Donde:

1. Slot o ranura de instalación de módulos adicionales.
2. Slots o ranuras de instalación de módulos adicionales.
3. Slots o ranuras de instalación de módulos adicionales.
4. Interfaz Fast Ethernet 0/1.
5. Interfaz Fast Ethernet 0/0.
6. Indicadores LED.
7. Unidad de tarjeta flash compacta.
8. Puertos USB.
9. Puertos de Consola (arriba) y Auxiliar(abajo)
10. Sistema Cisco de alimentación redundante (cubierto si no es usado)
11. Botón Encendido/Apagado.
12. Entrada de corriente.

El modelo ISR 4331 luce como se muestra en la Figura No. 3.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 214/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

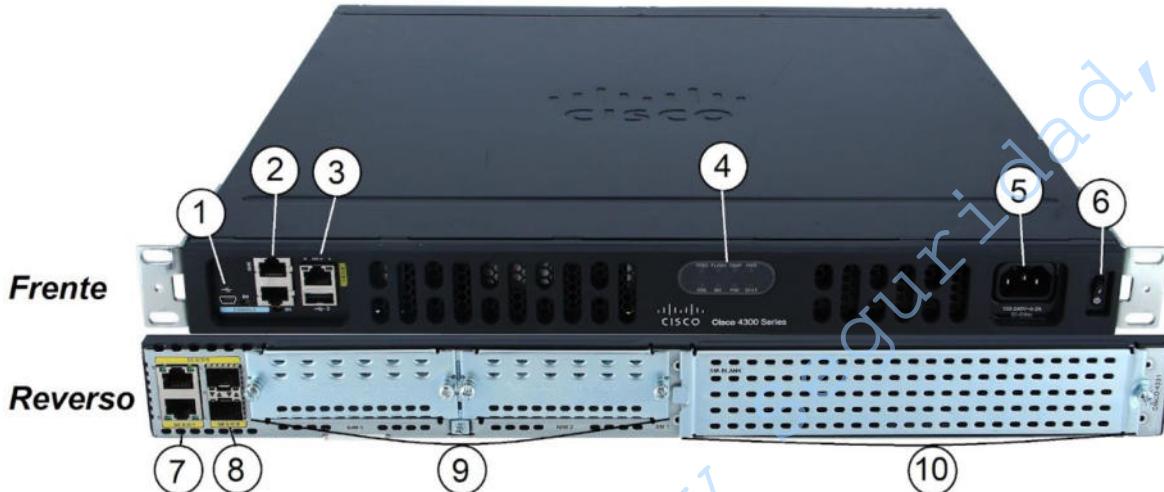


Figura No. 3. Modelo ISR4331.

Donde:

1. Mini puerto USB tipo B.
2. Puerto Auxiliar (arriba) y Puerto de Consola (abajo).
3. Puerto de Gestión (arriba) y Puerto USB tipo A (abajo).
4. Indicadores LED.
5. Entrada de corriente.
6. Botón Encendido/Apagado.
7. Puertos RJ45.
8. Puertos SFP.
9. Slots o ranuras de instalación de módulos adicionales.
10. Slot o ranura de instalación de módulos adicionales (No disponible en Packet Tracer).

Los switches son dispositivos de red utilizados para conectar dispositivos en una red local (LAN) y facilitar la comunicación entre ellos. Los switches Cisco utilizan el protocolo de comunicación Ethernet para enviar y recibir datos en la red (Figura No. 4).

Los switches operan en la capa 2 (capa de enlace de datos) y algunos en la capa 3 (capa de red) del modelo OSI (Open Systems Interconnection), conocidos como switches de capa 3. En la capa 2, los switches utilizan la dirección MAC de cada dispositivo conectado para enviar y recibir paquetes de datos en la red. En la capa 3, los switches utilizan la dirección IP para enrutar los paquetes de datos a través de la red.

Los switches Cisco ofrecen diversas funciones, como la segmentación de la red en VLANs (Virtual Local Area Networks), la agregación de enlaces (Link Aggregation Control Protocol - LACP), la detección y prevención de bucles de red (Spanning Tree Protocol - STP), y la calidad de servicio (Quality of Service - QoS), que permite priorizar el tráfico en la red.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	215/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				



Figura 4. Switches Cisco.

3.- Equipo y material necesario

Equipo del laboratorio:

- Software de simulación de redes Cisco Packet Tracer.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Identificación de módulos de routers.

- 4.1.1 Encienda el sistema y elija la opción de cargar Windows.
- 4.1.2 Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3 Ejecute la aplicación Cisco Packet Tracer (Ver Figura No. 5)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 216/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura 5. Simulador de CISCO Packet Tracer.

- 4.1.4** Dé clic en la sección de Dispositivos de red, después seleccione el apartado de Router y ahí ubique los modelos 1841, 2811 IOS15 y ISR 4331 (Figura No. 6). Una vez ubicados, arrastre una instancia de cada modelo al área de trabajo.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 217/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

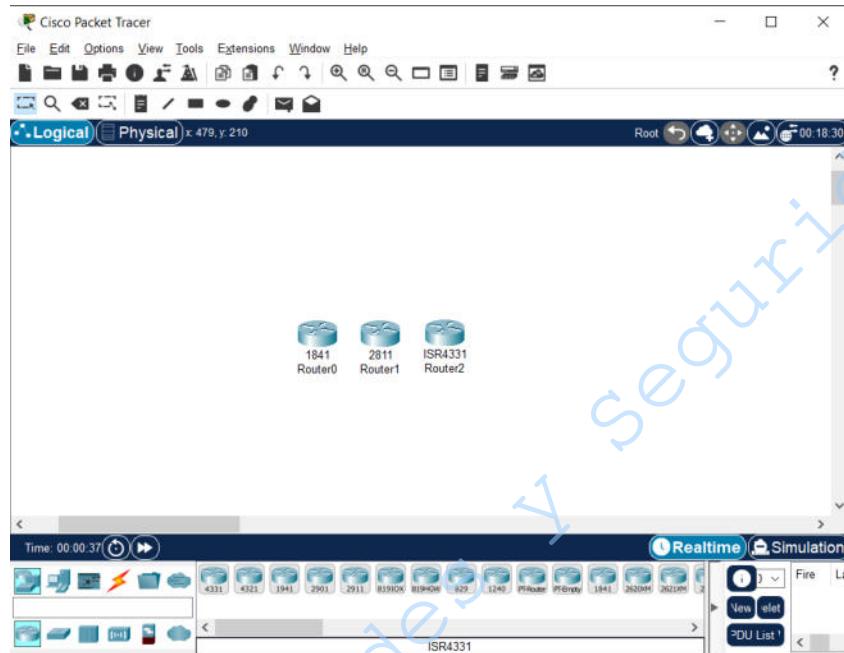


Figura 6. Routers modelo 1841, 2811 IOS15 y ISR 4331.

- 4.1.5** Dé clic sobre el Router0, posteriormente se abrirá una ventana nueva, la cual tiene varias pestañas. A la izquierda de la pestaña *Physical* se pueden visualizar a los módulos disponibles que se le pueden agregar al router 1841. Nótese que cuando hace clic en algún módulo, aparecerá en la esquina inferior derecha una representación de la vista física de ese módulo (Figura No. 7).
Por otro lado, en el espacio principal de la ventana se encuentra una imagen de cómo luce ese router físicamente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 218/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

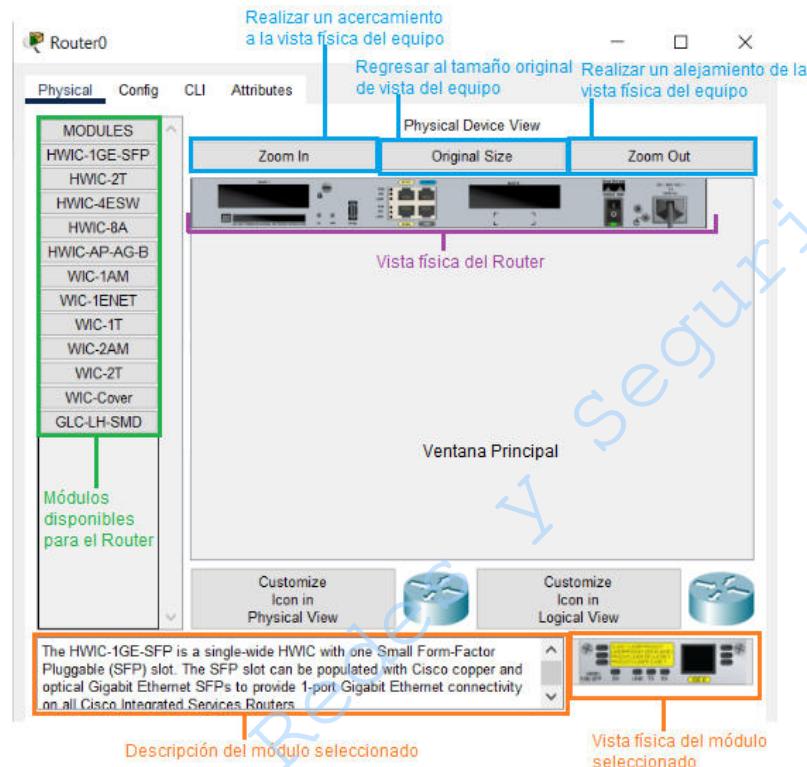


Figura No. 7. Módulos disponibles para el modelo 1841.

4.1.6 Seleccione el módulo que deseé y observe que cambian tanto la vista física del módulo, así como su descripción. Estas corresponden al módulo seleccionado (Figura No. 8).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 219/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

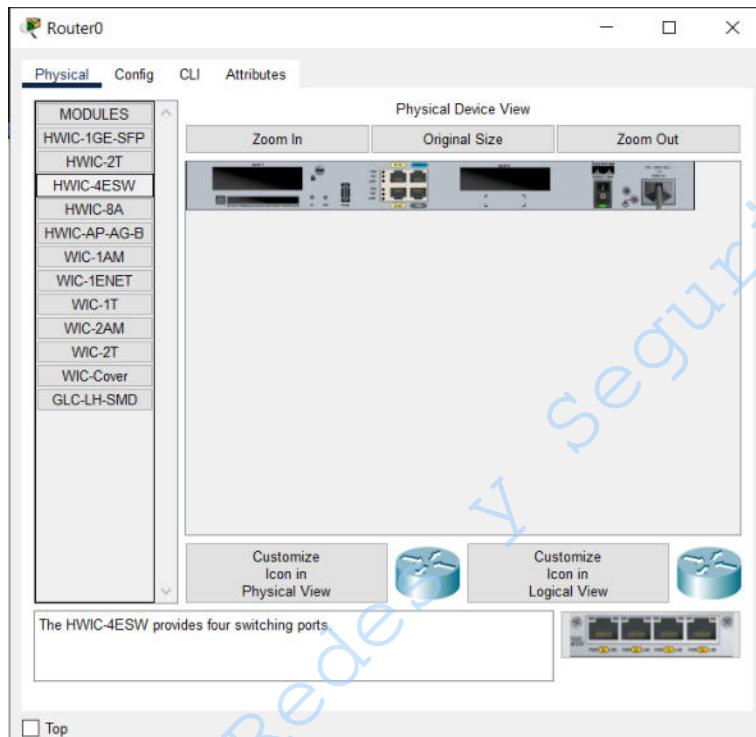


Figura No. 8. Descripción e imagen del módulo HWIC-4ESW.

- 4.1.7 Realice la acción del punto 4.1.6 con diferentes módulos.
- 4.1.8 Cierre la ventana del Router0 y seleccione el Router1. Podrá observar que se abrió la ventana correspondiente e igual se mostrarán ciertos módulos disponibles para el modelo 2811 IOS15, así como imágenes correspondientes al frente y reverso de ese modelo de router (Figura No. 9).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 220/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

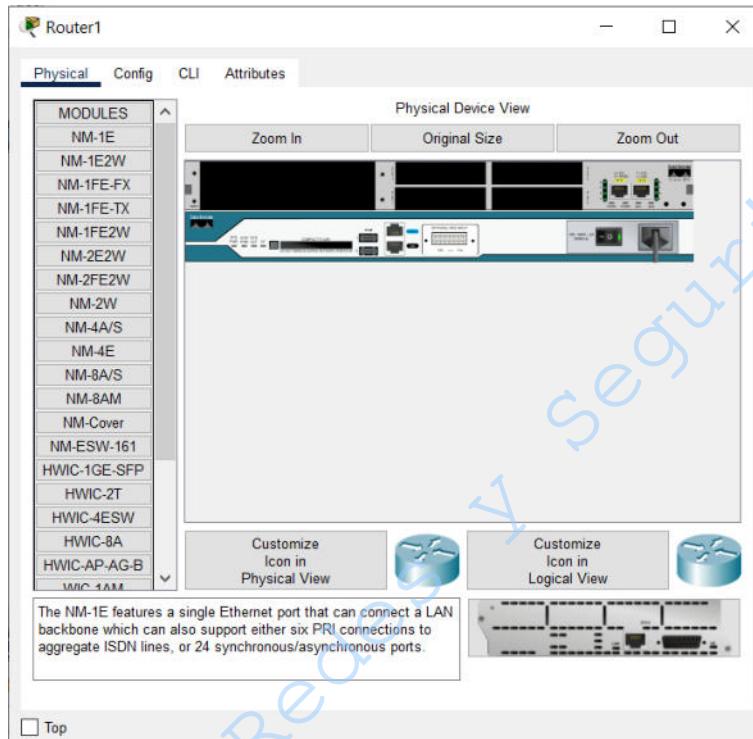


Figura No. 9. Módulos disponibles para el modelo 2811 IOS15.

- 4.1.9 Repita el paso 4.1.7 pero ahora con los módulos mostrados en la ventana del modelo 2811 IOS15.
- 4.1.10 Cierre la ventana del Router1 y seleccione el Router2. Verá que se abrió la ventana correspondiente e igual aparecen ciertos módulos disponibles para el modelo ISR4331. Observe los módulos disponibles y las imágenes presentadas de ese router.

4.2 Inserción de módulos a un router

- 4.2.1 Seleccione el Router0 del área de trabajo.
- 4.2.2 Dé clic en el botón *Zoom In*, ubicado encima de la vista física del router, de tal manera que pueda acercar más la imagen del router. La ubicación de dicho botón se menciona en el punto 4.1.5.
- 4.2.3 Para poder agregar o quitar módulos de un router, es necesario apagarlo antes. Identifique la ubicación del botón de Encendido/Apagado. Si el led que se encuentra al lado del botón está prendido, significa que está encendido el router y será necesario que

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	221/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

dé clic en el botón Encendido/Apagado. La ubicación de dicho botón se menciona en los Conceptos Básicos de la presente práctica.

- 4.2.4** Del modelo del Router 1841, indique cuántos slots disponibles se tienen y escriba a continuación cuántos módulos pueden instalarse en este modelo.

- 4.2.5** Agregue los módulos HWIC-2T y HWIC-4ESW. Para ello, dé clic sobre el módulo y manténgalo presionado, después arrastre el módulo hasta el slot deseado y suelte el clic (Figuras No. 10 y 11).



Figura No. 10. Módulo HWIC-2T



Figura No. 11. Módulo HWIC-4ESW

NOTA: Podría darse el caso de que un módulo tenga cierto tamaño y no pueda caber en cualquier slot, verifique el tamaño del módulo antes de arrastrarlo hacia el slot.

De los módulos que agregó, indique a continuación el tipo de cable que puede conectar a los puertos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 222/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

-
- 4.2.6** Una vez agregados los módulos en los slots, se debe de volver a prender el equipo. Identifique nuevamente la ubicación del botón de Encendido/Apagado y encienda el router.
- 4.2.7** Del modelo del Router 2811 IOS 15 (Figura No. 12), indique cuántos slots disponibles se tienen y escriba a continuación cuántos módulos pueden instalarse en este modelo.
-

NOTA: Para este modelo, hay dos tipos de módulo, los NM-**** que son módulos más grandes que caben en el slot A; mientras que los módulos HWIC-*** y WIC-*** son módulos más pequeños y caben en los slots B, C, D y E.

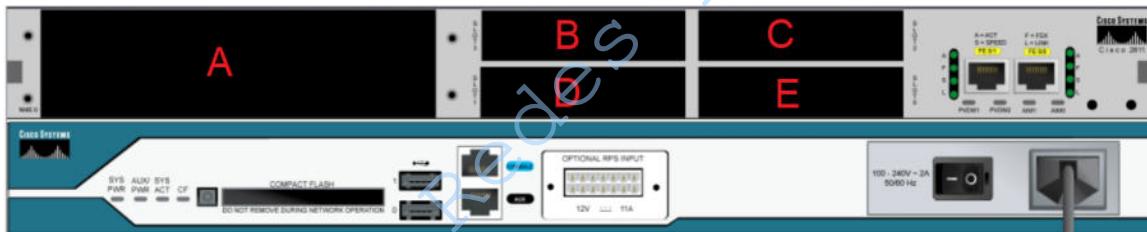


Figura No. 12. Slots del router 2811 IOS15

- 4.2.8** Escoja el módulo NM-8A/S para el slot A (Figura No. 13), mientras que para los demás slots, agregue los módulos HWIC-1GE-SFP, HWIC-2T, HWIC-4ESW y WIC-Cover. Recuerde que para agregarlos, el router debe estar apagado (Figuras No. 14 y 15).

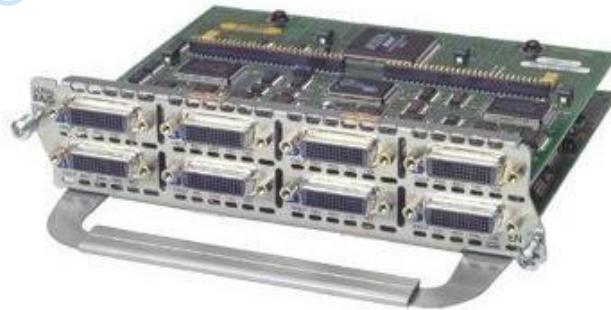


Figura No. 13. Módulo NM-8A/S

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	223/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura 14. Módulo HWIC-1GE-SFP



Figura 15. Módulo WIC-Cover

Escriba en la Tabla No. 1 el módulo que colocó en cada uno de los slots, cuántos puertos por módulo se tienen e indique el tipo de cable que puede conectar a los puertos.

Tabla 1. Designación de Puertos en los Slots e información sobre ellos.

Slot o ranura	Módulo añadido	Puertos por módulo	Tipo de cable
A	NM-8A/S		
B			
C			
D			
E			

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 224/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.9** Una vez agregados los módulos en los slots, debe de volver a prender el equipo. Identifique nuevamente la ubicación del botón de Encendido/Apagado y encienda el router.
- 4.2.10** Del modelo del Router ISR4331 (Figura No. 16), indique cuántos slots disponibles tiene y escriba a continuación cuántos módulos pueden instalarse en este modelo.

NOTA: Para este modelo, hay dos tipos de módulo, los NIM-**** que son módulos grandes que caben en los slots A y B; mientras que **los módulos GLC-**** son módulos pequeños** que se insertan en los puertos señalados con la letra C.



Figura 16. Slots del router ISR4331

- 4.2.11** Para este ejercicio se deben escoger los módulos NIM-2T, NIM-ES2-4, GLC-LH-SMD y GLC-TE (Figuras No. 17 a 20).

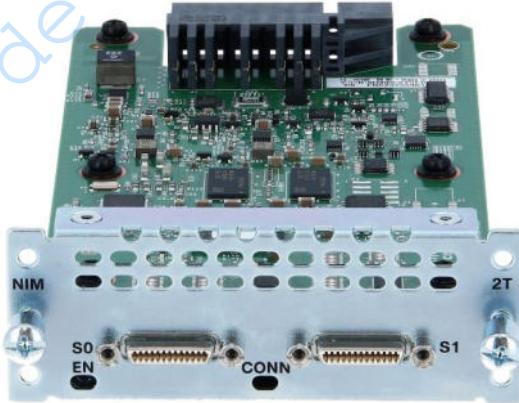


Figura 17. Módulo NIM-2T

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	225/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura 18. Módulo NIM-ES2-4



Figura 19. Módulo GLC-LH-SMD

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	226/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



Figura 20. Módulo GLC-TE

Escriba en la Tabla No. 2 el módulo que colocó en cada uno de los slots, cuántos puertos por módulo se tienen e indique el tipo de cable que puede conectar a los puertos.

Tabla 2. Designación de Puertos en los Slots e información sobre ellos.

Slot o ranura	Módulo(s) añadidos	Puertos por módulo	Tipo de cable
A			
B			
C			

4.3 Eliminación de módulos de un router

- 4.3.1 Para quitar los módulos de un router, primero debe dar clic en el router del que desee quitar el módulo y se abrirá la ventana de Detalles.
- 4.3.2 Ubique el botón de encendido/apagado, apague el router.
- 4.3.3 Dé clic en el módulo que desee quitar, sin soltar el clic, arrastre el módulo al área de módulos y suéltelo, de esta forma se quitan los módulos de un router en Packet tracer.
- 4.3.4 Identifique nuevamente la ubicación del botón de Encendido/Apagado y encienda el router para poder dejar en operación al equipo.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	227/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

4.4 Armado de una topología

- 4.4.1** Con lo aprendido en los ejercicios anteriores, se requiere que arme la topología, mostrada en la figura 21, en Cisco Packet Tracer, agregando y/o quitando los módulos necesarios para cada dispositivo.

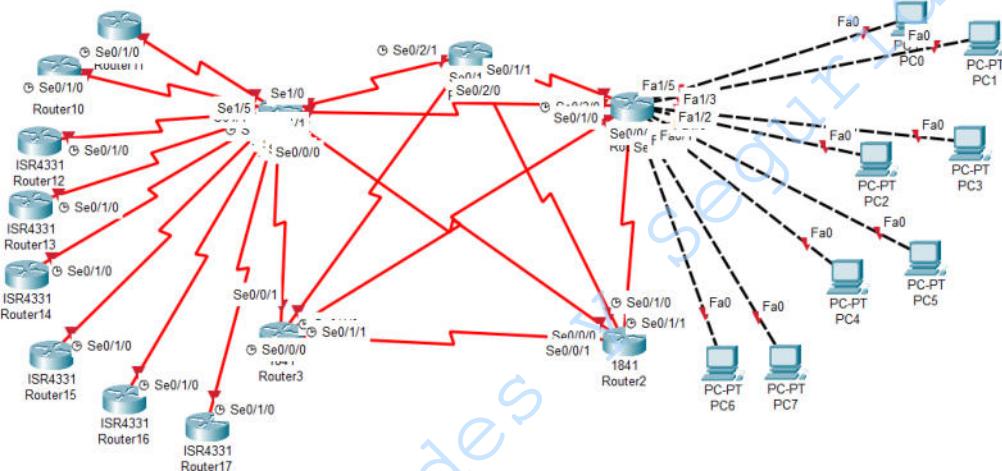


Figura 21. Topología 1 para armar.

- 4.4.2** Indique los módulos usados en los Routers 0, 1, 2, 3, 4 e identifique el o los tipos de topologías de red usados (malla, estrella, árbol, bus, etcétera.).

- 4.4.3** Se requiere que arme la topología, mostrada en la figura 22, en Cisco Packet Tracer, agregando y/o quitando los módulos necesarios para cada dispositivo.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	228/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

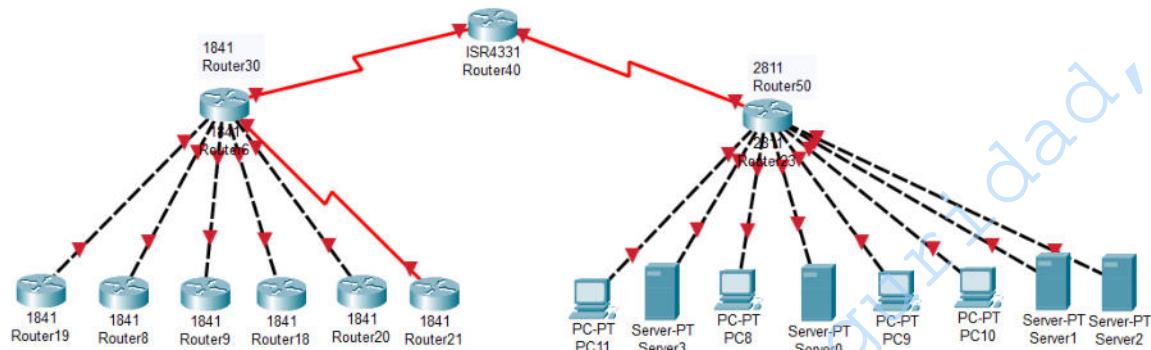


Figura 22. Topología 2 para armar

- 4.4.4 Indique los módulos usados en los Routers 30, 40, 50, 21, e identifique el o los tipos de topologías de red usados (malla, estrella, árbol, bus, etcétera.).

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	229/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	230/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 2

Instalación y cambio de módulos en routers

Cuestionario Previo

1. ¿Qué es un router?
2. Mencione los diferentes tipos de entradas (conectores) que puede tener un router, cuál es su función y los tipos de cables que pueden conectarse a dichas entradas.
3. Del router modelo ISR4331, ¿Para qué sirven los módulos GLC-LH-SMD y GLC-TE?
4. Mencione las características del cable serial DCE
5. Mencione las características de cable serial DTE
6. ¿Cuál es la diferencia entre el cable serial DCE y DTE?
7. Mencione los principales tipos de topología de red que existen.
8. Mencione cuáles son los diferentes cables de conexión que se pueden utilizar en Cisco Packet Tracer, investigue las características de cada uno y mencione al menos un ejemplo de un dispositivo al que se puede conectar.
9. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	231/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 3

Cableado estructurado

Capa 1 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 232/479 8.3 11 de agosto de 2023
Facultad de Ingeniería			Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

1.- Objetivos de aprendizaje

- El alumno o la alumna aplicará los estándares ANSI/EIA/TIA 568 y 569 para el diseño de una red de datos con cableado estructurado.

2.- Conceptos teóricos

El cableado estructurado es una topología física de red, con un tiempo de vida útil de diez a quince años. Es flexible y capaz de soportar cambios y crecimientos futuros.

La implementación de este sistema reduce costos en la instalación y el mantenimiento así como la facilidad de incorporar nuevos sistemas.

El diseño del sistema de cableado es independiente de la información que se transmite a través de él, de este modo es posible disponer de servicio de datos, voz, video, audio, seguridad, control y monitoreo.

La norma ANSI/EIA/TIA 568-A contiene los siguientes subsistemas para el cableado estructurado (Ver Figura No. 1):

1. Subsistema de cableado horizontal.
2. Subsistema de cableado vertical (backbone).
3. Subsistema de área de trabajo.
4. Subsistema de cuarto de telecomunicaciones.
5. Subsistema de cuarto de equipos.
6. Subsistema de entrada de servicios.

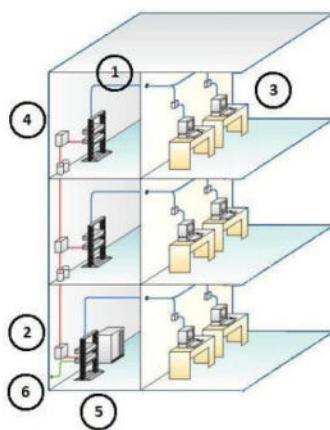


Figura No.1. Subsistemas del cableado estructurado.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 233/479 8.3 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Las redes también se pueden clasificar de acuerdo con su topología física; ésta define la representación geométrica de todos los enlaces de una red y los dispositivos físicos enlazados entre sí. Las principales son (Ver Figura No. 2):

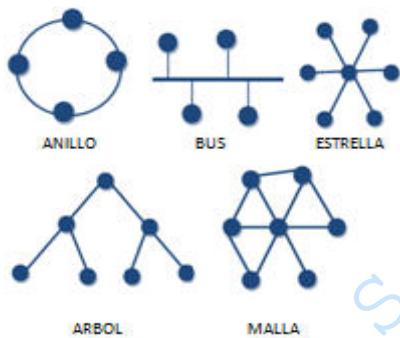


Figura No.2. Topologías de red.

- a) Topología de bus
- b) Topología de estrella
- c) Topología de anillo
- d) Topología jerárquica
- e) Topología de malla

3.- Equipo y material necesario

Material del alumno o de la alumna:

- Planos del proyecto indicados por la profesora o el profesor.
- Colores (bolígrafos, lápices, marcadores).
- Hojas blancas

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 234/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1 Ejercicio

Con base en los planos del proyecto, determine la ubicación de los subsistemas del cableado estructurado, tomando en cuenta las siguientes consideraciones:

Nota para la profesora o el profesor: Los planos deberán ser de un edificio de dos pisos como máximo. Se anexa la imagen de una sugerencia (Ver Figura No. 3).



Figura No.3. Sugerencia de planos.

1. Los cuartos de equipos deben ser accedidos únicamente por personal autorizado.
2. El equipo de contingencias (barreras contra fuego, extintores, entre otros) debe ser visible y de fácil aspecto.
3. La red eléctrica debe de estar aislada de la red de datos.
4. Alguna otra restricción propuesta por la profesora o el profesor.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	235/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Las siguientes áreas se deben de representar en los planos proporcionados:

- a) Área de vigilancia.
- b) Recepción o módulo de información.
- c) Servicio de Wi Fi en áreas comunes.
- d) Área de trabajo con un número de equipos proporcionados por la profesora o el profesor.

EJERCICIOS OPCIONALES

4.5 Costo de la propuesta del cableado estructurado.

- 4.5.1** Con base en su investigación previa, en hojas blancas realice la cotización de su propuesta de cableado estructurado, tome en cuenta también los aspectos: mantenimiento y garantía.
- 4.5.2** Indique qué consideraciones de seguridad debe tomar en cuenta para su propuesta y por qué.
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

- 4.5.3** Exponga ante el grupo su propuesta y justifíquela.

- 4.5.4** Analice las propuestas que expusieron sus compañeros e indique qué tan factible fue su propuesta. Justifique su respuesta.
-
-



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	236/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

4.3 Ventajas y Desventajas de los medios de transmisión a utilizar

Anexe en hojas blancas un cuadro donde mencione las ventajas y desventajas de usar fibra óptica o cable de par trenzado en su proyecto. Considere las normas internacionales para realizar este punto.

FIBRA ÓPTICA		CABLE PAR TRENZADO	
VENTAJAS	DESVENTAJAS	VENTAJAS	DESVENTAJAS



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	237/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

5.- Cuestionario

1. ¿Qué consideró para la creación de su propuesta? Argumente su respuesta.

2. ¿Cuáles son las ventajas y desventajas de la topología utilizada en la pregunta anterior?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	238/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	239/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 3

Cableado estructurado

Cuestionario Previo

1. Investigue el material necesario para realizar un cableado estructurado.
2. Investigue los costos de la lista del material que obtuvo en el punto anterior con proveedores autorizados en México (Algunos ejemplos de proveedores: eCore Networks, Adder, Nettowak Solutions)
3. Investigue costos de mantenimiento a una red de datos con proveedores autorizados en México.
4. Investigue las normas que se emplean en el cableado estructurado.
5. Mencione las normas de seguridad para el cableado estructurado en edificios comerciales.
6. Investigue las normas ANSI/EIA/TIA 568 y 569.
7. ¿Qué es una topología de red?
8. Investigue las características de las siguientes topologías:
 - a) Topología de bus.
 - b) Topología de estrella.
 - c) Topología de anillo.
 - d) Topología jerárquica.
 - e) Topología de malla.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 240/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 4

Compartición de archivos por Hub y Switch en Linux

Capa 2 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	241/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de aprendizaje

- El alumno o la alumna compartirá archivos por medio del hub y el switch.

2.- Conceptos teóricos

Para un administrador de red, es necesario e indispensable conocer los equipos, mecanismos y técnicas para extender las capacidades de las redes que están bajo su cargo. En algunas ocasiones es necesario extender físicamente una red para añadir nuevas estaciones así como para interconectarlas a una LAN con localización geográfica distinta. De igual forma, es conveniente planear el crecimiento de una LAN en términos de ancho de banda para hacer frente a necesidades de comunicación actuales.

La extensión de las capacidades de una red, se logra mediante dispositivos hardware definidos para cada uno de los tipos de redes, en el caso de las LAN se encuentran los *hubs*, *switches*, repetidores, puentes, *access point*; para las redes *MAN*, se tienen repetidores, canalizadores, módems analógicos, módems cable; en el caso de las redes *WAN*, hay routers, multicanalizadores, módems satelitales, etcétera.

Hub

Dispositivo que opera en la capa 1 del modelo OSI que tiene la finalidad de interconectar a los dispositivos finales en una red de datos mediante la transmisión de paquetes a todos y cada uno de los hosts conectados no importándole cuál sea el destinatario.

El *hub* es un dispositivo activo que actúa como elemento central. Cada estación se conecta al *hub* mediante dos enlaces: transmisión y recepción. El *hub* actúa como un repetidor: cuando transmite una única estación, el *hub* replica la señal en la línea de salida hacia cada host conectado. Regularmente el enlace consiste en dos pares trenzados no apantallados. Dada la alta velocidad y baja calidad de transmisión del par trenzado no apantallado, la longitud de un enlace está limitada a un entorno de 100m. Como alternativa se puede usar un enlace de fibra óptica en cuyo caso la longitud máxima dependerá si es multimodo (2 km) o monomodo (300 km) aproximadamente.

Varios niveles de hub se pueden colocar en cascada formando una configuración jerárquica, teniendo un hub raíz denominado HUB. Encabezado Hub (Header Hub) y uno o más hubs intermedios denominados IHUB, Hub Intermedios (Intermediate Hub). Esta estructura se adecúa bien a edificios cableados donde regularmente existe un armario de interconexiones en cada planta del edificio.

Existen hubs pasivos y activos, los primeros sólo interconectan dispositivos, mientras que los segundos además regeneran la señal recibida, como si fuera un repetidor, de ahí la denominación de repetidor multipuerto.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	242/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Switch

Dispositivo que opera en la capa 2 del modelo OSI que tiene el fin de integrar a los equipos finales en una red de datos, empleando la transmisión de paquetes únicamente al destinatario seleccionado para transmitir.

Un switch es un dispositivo hardware que incluye componentes similares a una computadora personal: CPU, RAM y un IOS, Sistema Operativo de Red (Internetworking Operating System). Puede ser administrado de la misma forma que un router o bien mediante una consola conectada a un puerto ya sea por Telnet o bien vía FTP.

Estos dispositivos de interconexión corresponden con la capa de enlace de datos, regularmente son implementados para preservar el ancho de banda de la red al utilizar la segmentación, ya que reenvían paquetes a un segmento en particular, utilizando el direccionamiento de hardware MAC.

Los switches pueden ser clasificados de acuerdo con la técnica que emplean, para el reenvío de los paquetes al segmento apropiado en:

- a) *Store-and-forward*, en esta técnica los switches procesan completamente el paquete incluyendo el campo del algoritmo CRC y la determinación del direccionamiento del paquete. Esto requiere el almacenamiento temporal del paquete antes de ser enviado al segmento apropiado. Su principal ventaja es la eliminación del número de paquetes dañados que son enviados a la red.
- b) *Cut-through*, esta técnica implementada por los switches hace que sean más rápidos, debido a que envían los paquetes tan pronto la dirección MAC es leída.

El switch implementado en el Laboratorio utiliza la primera técnica: store and forward.

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows.
- Software de simulación de Cisco, Packet Tracer en su versión más reciente.
- 1 Switch FastEthernet.
- 1 Hub.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	243/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1 Compartición de archivos en Debian.

- 4.1.1 En este punto el laboratorio se dividirá en dos equipos según sea indicado por la profesora o el profesor, cada equipo realizará la siguiente actividad con el dispositivo que se le sea asignado.
- 4.1.2 Conecte el dispositivo asignado (hub o switch, según sea el caso) a una roseta.
- 4.1.3 Conecte las PC al dispositivo asignado (hub o switch, según sea el caso).
- 4.1.4 Abra la aplicación VirtualBox.

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 1).

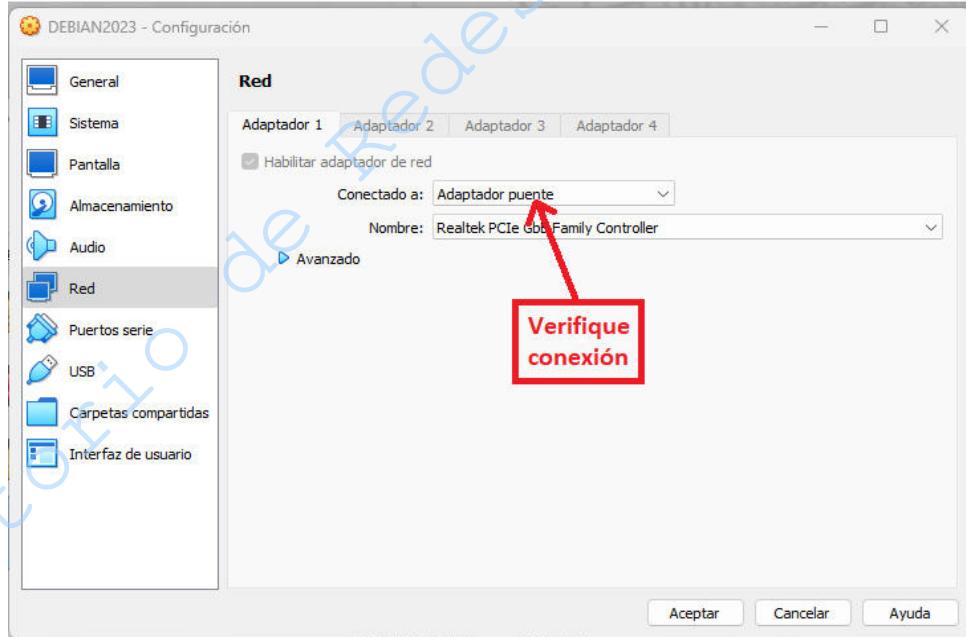


Figura No. 1. Conexión de red.

- 4.1.5 Encienda la máquina virtual
- 4.1.6 Elija la opción de cargar Linux, distribución Debian.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 244/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

- 4.1.7** Inicie sesión en la cuenta de redes.
- 4.1.8** Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación. (Ver Figura No. 2)

NOTA: *su* significa super usuario, por lo que se emplea la misma contraseña de root
redes@debian:~\$ su

```
redes@DEBIAN2023:~$ su
Password:
root@DEBIAN2023:/home/redes#
```

Figura No. 2. Terminal de comandos como root.

- 4.1.9** Emplee la ventana de comandos para verificar mediante el comando ifconfig que todas las PC conectadas a dicho dispositivo tengan una dirección IP con el mismo segmento de red, así como con la misma máscara de subred.

root@debian:/home/redes# ifconfig

Anote la dirección IP de su máquina _____

4.2 Configuración del servidor y del cliente

- 4.2.1** Designe una máquina como servidor.

Desde el paso 4.2.1.1 hasta el paso 4.2.1.7 se realizarán en el dispositivo designado como servidor

- 4.2.1.1** Mediante la siguiente instrucción cree una nueva carpeta para realizar la compartición de archivos:

root@debian:/home/redes# mkdir nombre_carpeta

NOTA: Donde *nombre_carpeta* será el nombre de la carpeta a crear.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 245/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

4.2.1.2 Teclee el siguiente comando para dar los permisos necesarios y poder compartir archivos:

```
root@debian:/home/redes# chown redes nombre_carpeta
```

NOTA: Donde **nombre_carpeta** será el **nombre de la carpeta creada**.

4.2.1.3 Para compartir archivos se requiere el uso de una contraseña (que será de su elección); con el siguiente comando se crea dicha contraseña y se solicita su confirmación (Ver Figura No. 3):

```
root@debian:/home/redes# smbpasswd redes -a
```

```
root@debian:/home/redes# smbpasswd redes -a
New SMB password:
Retype new SMB password:
Added user redes.
```

Figura No. 3. Creación de contraseña en Linux.

Anote la contraseña que utilizó _____

4.2.1.4 Indique para qué se usa el comando **smbpasswd** en este caso.

4.2.1.5 Al realizar la compartición de archivos, se le debe informar a samba el nombre de la carpeta, así como los permisos de lectura/escritura que se le están dando, para ello debe

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	246/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

acceder al archivo de configuración con el siguiente comando (Ver Figura No. 4) y escribir al final del archivo las siguientes líneas (Ver Figura No. 5):

root@debian:/home/redes# nano /etc/samba/smb.conf

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# nano /etc/samba/smb.conf
```

Figura No. 4. Acceso al archivo

```
[nombre_carpeta]
path = /home/redes/
writeable = yes
shares = yes
guest ok = yes
```

Figura No. 5. Permisos carpeta compartida

NOTA: Donde nombre_carpeta será el nombre de la carpeta creada.

Indique lo que significan cada uno de los parámetros que escribió en el archivo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	247/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.1.6 Reinicie el servicio de samba con el siguiente comando (Figura No. 6):

```
root@debian:/home/redes# /etc/init.d/samba restart
```

```
root@debian:/home/redes# /etc/init.d/samba restart
[ ok ] Restarting nmbd (via systemctl): nmbd.service.
[ ok ] Restarting smbd (via systemctl): smbd.service.
[ ok ] Restarting samba-ad-dc (via systemctl): samba-ad-dc.service.
root@debian:/home/redes#
```

Figura No. 6. Reinicio del servicio

4.2.1.7 Cree un documento de texto dentro de la carpeta para que pueda compartirlo, para ello teclee los siguientes comandos:

```
root@debian:/home/redes# cd nombre_carpeta
root@debian:/home/redes/nombre_carpeta# touch nombre_archivo
```

NOTA: Donde **nombre_carpeta** será el nombre de la carpeta creada en el punto 4.2.1.2 y **nombre_archivo** el nombre del archivo a compartir sin espacios ni caracteres especiales

4.2.2 Designe una máquina como cliente.

Desde el paso 4.2.2.1 hasta el paso 4.2.2.4 se realizarán en el dispositivo designado como cliente.

4.2.2.1 Instale samba cliente tecleando lo siguiente (Figura No. 7):

```
root@debian:/home/redes# apt-get install smbclient
```



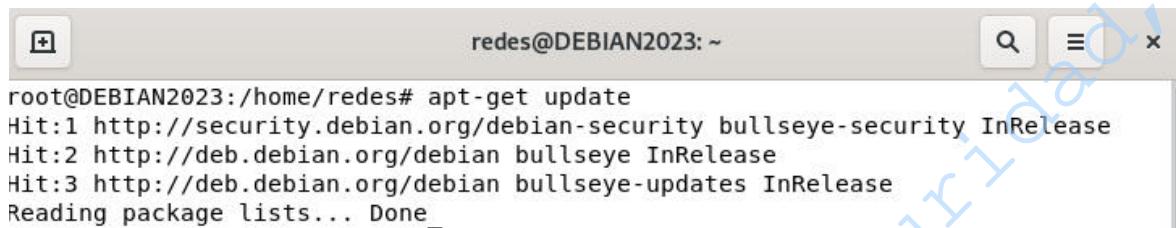
```
root@DEBIAN2023:/home/redes# apt-get install smbclient
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Figura No. 7. Instalando samba cliente

4.2.2.2 En caso de que no realice la instalación teclea el siguiente comando para actualizar los paquetes disponibles en el servidor de Debian (Figura No. 8)

```
root@debian:/home/redes# apt-get update
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	248/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



```
root@DEBIAN2023:/home/redes# apt-get update
Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists... Done
```

Figura No. 8. Actualizando paquetes

4.2.2.3 Una vez instalado samba cliente, verifique la conectividad del cliente al servidor, para ello envíe un ping desde la máquina cliente a la máquina servidor empleando la línea de comandos (Figura No. 9).

root@debian:/home/redes# ping 192.168.2.X



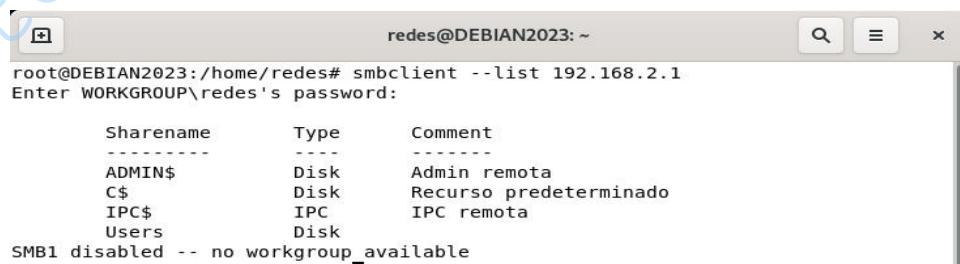
```
root@DEBIAN2023:/home/redes# ping 192.168.2.X
```

Figura No. 9. Ping de la máquina cliente al servidor

NOTA: Recuerde que la X debe sustituirse por la dirección de la máquina servidor.

4.2.2.4 Para observar las carpetas compartidas que se encuentran disponibles, debe teclear el siguiente comando (Figura No.10)

root@debian:/home/redes# smbclient --list 192.168.2.X



```
root@DEBIAN2023:/home/redes# smbclient --list 192.168.2.1
Enter WORKGROUP\redes's password:
Sharename      Type      Comment
-----        ----      -----
ADMIN$         Disk      Admin remota
C$             Disk      Recurso predeterminado
IPC$           IPC       IPC remota
Users          Disk      
```

SMB1 disabled -- no workgroup available

Figura No. 10. Solicitud de listado de carpetas compartidas

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	249/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA: Recuerde que la X debe sustituirse por la dirección de la máquina servidor.

4.3 Compartición de archivos entre Linux y Windows

La compartición de archivos entre un sistema operativo a otro se puede realizar a través de los servicios que ofrece samba.

- 4.3.1** Para acceder a la máquina designada como servidor vaya a la tecla de inicio en Windows y en la barra de búsqueda escriba lo siguiente (Figura No. 11):

\192.168.2.X

NOTA: La X debe sustituirse por la dirección IP de la máquina designada como servidor.

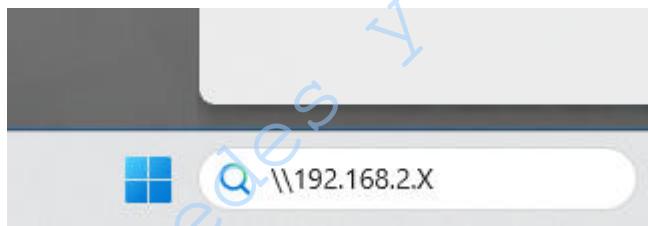


Figura No. 11. Acceso a la máquina designada como servidor

- 4.3.2** Cuando acceda a la máquina designada como servidor se mostrará la carpeta compartida (Figura 12), puede navegar dentro de ella para observar los documentos compartidos

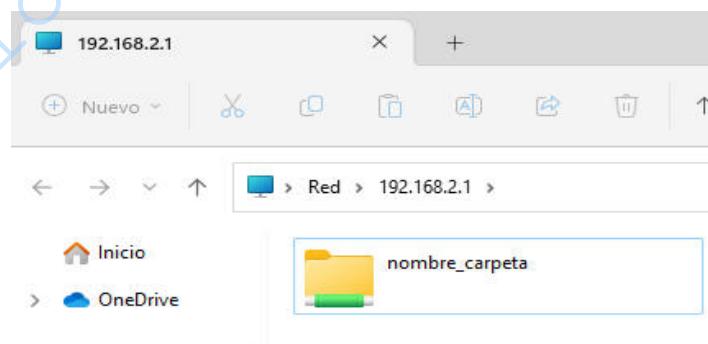


Figura No. 12. Acceso a la carpeta compartida en Windows

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	250/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.3.3 Mencione si tuvo algún problema para lograr acceder a la carpeta, de ser así ¿cuál fue su solución?

(Placeholder for answer to question 4.3.3)

4.3.4 Mencione ¿Qué pasaría si no se solicita contraseña para ingresar?

(Placeholder for answer to question 4.3.4)

4.3.5 Indique las diferencias que observó al compartir la misma carpeta en dos sistemas operativos diferentes.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 251/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.6** Indique en qué tipo de sistema operativo la compartición maneja mayor seguridad y por qué.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 252/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

- 4.3.7** ¿Por qué se puede realizar la compartición entre dos sistemas operativos?

EJERCICIO OPCIONAL

Con este ejercicio El alumno o la alumna visualizará la colisión de los dispositivos en forma simulada por medio del software Cisco Packet Tracer.

4.4 Construcción de la topología.

- 4.4.1** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 13).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 253/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

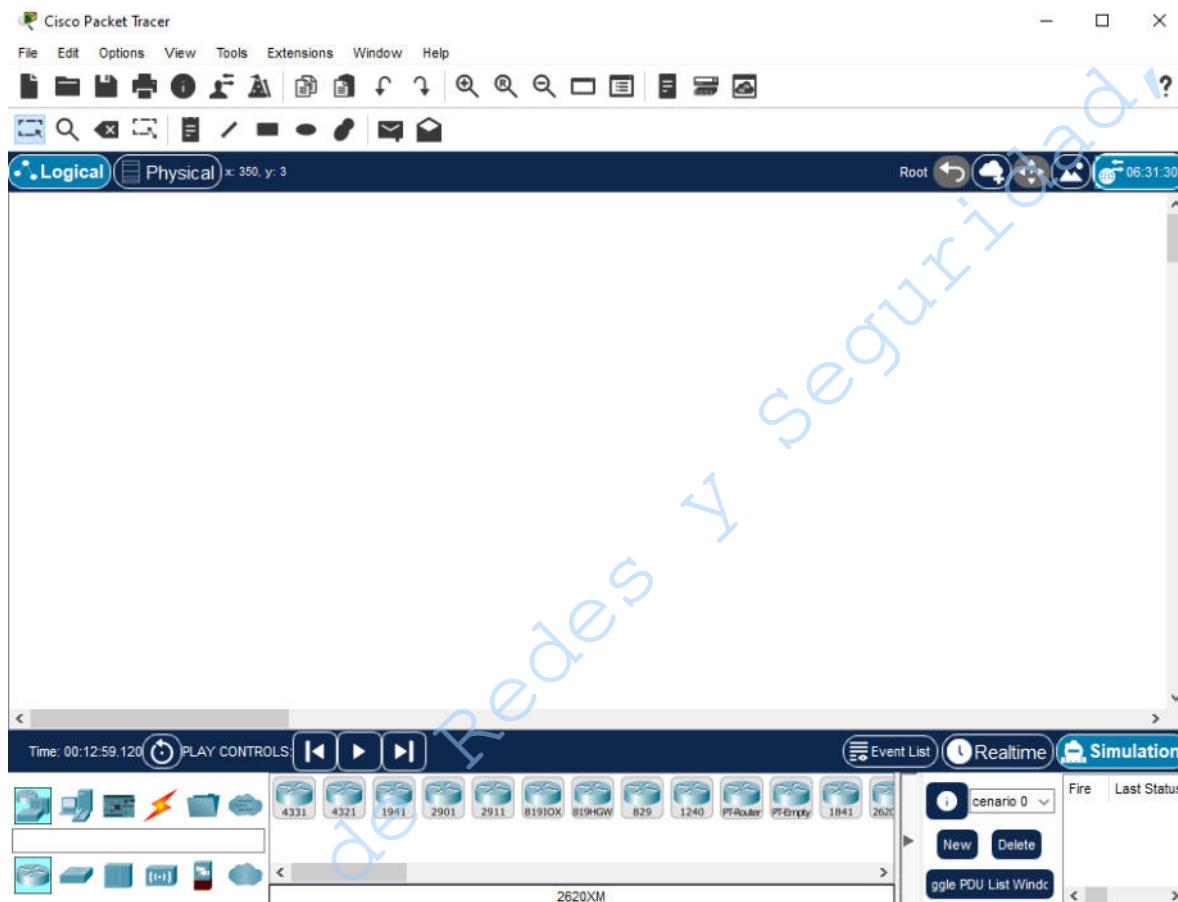


Figura No. 13. Interfaz gráfica de PT

- 4.4.2 Cuando Packet Tracer se inicia, muestra por default una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.
- 4.4.3 En la esquina inferior izquierda de la interfaz se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo (Ver figura No. 14).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 254/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 14. Secciones de dispositivos

- 4.4.4 La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos, en el cuadro de texto del centro aparece el nombre de este grupo.
- 4.4.5 La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán.
- 4.4.6 Con ayuda de su profesora o profesor realice la topología de red que se observa en la Figura No. 16 agregando al área de trabajo de Packet Tracer los dispositivos siguientes: 1 Switch 2950-24, 6 PC-PT y un Hub -PT (Figura 15).

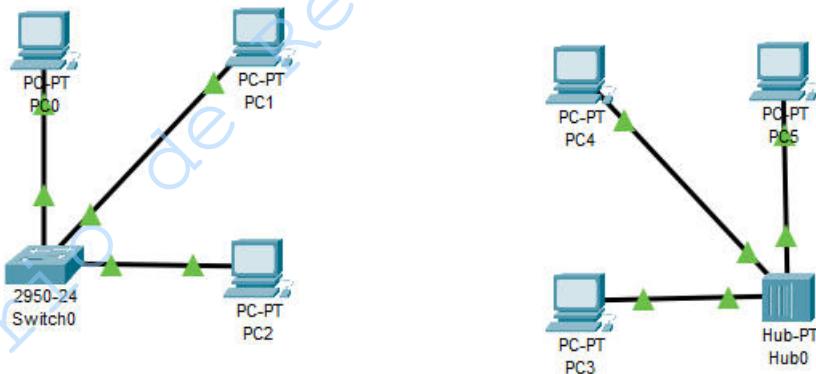


Figura No. 15. Topología de red.

- 4.4.7 Conecte la interfaz Port0 del Hub0 con la interfaz FastEthernet 0 de la PC3, la interfaz Port1 del Hub0 con la interfaz FastEthernet 0 de la PC4 y la interfaz Port2 del Hub0 con la interfaz FastEthernet 0 de la PC5.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 255/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.5 Configuración de los dispositivos

- 4.5.1 Dé clic sobre la PC0 conectada al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.5.2 Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.
- 4.5.3 Se abrirá una ventana solicitando la dirección IP, máscara de red y el Gateway (vea la figura No. 16). Ingrese los datos designados por su profesora o profesor.
- 4.5.4 Repita los pasos 4.4.1, 4.4.2 y 4.4.3 para las cinco PC restantes.

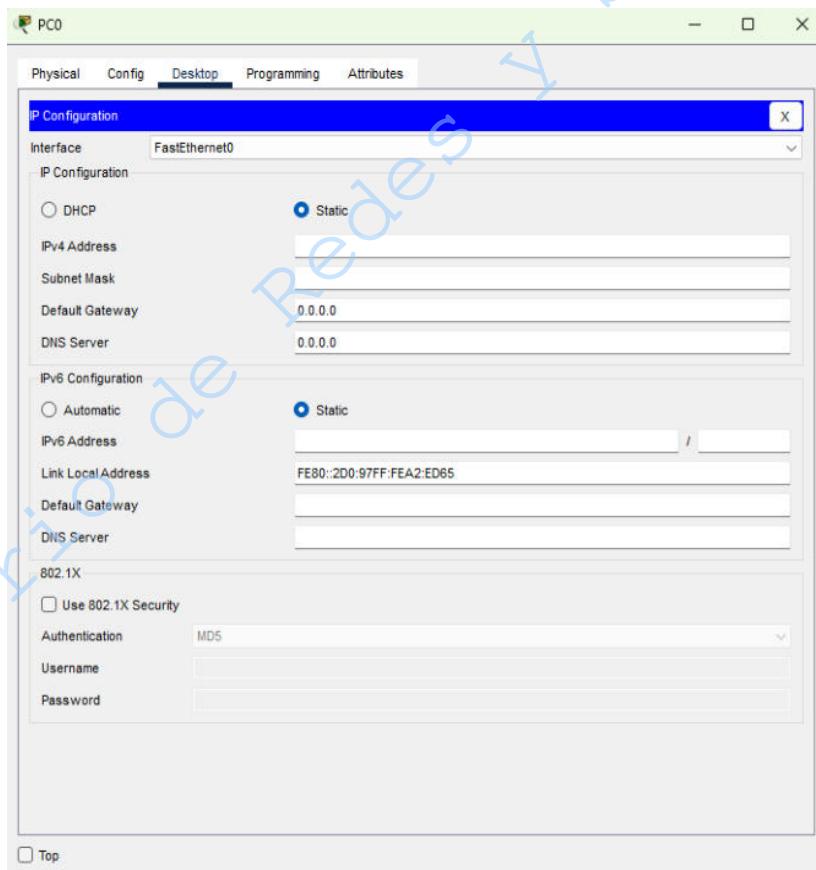


Figura No. 16. Configuración de la PC.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	256/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- 4.5.5** Una vez configurados los equipos de cómputo verifique que exista comunicación. Seleccione una PDU como se observa en la Figura No. 17 y dé clic sobre la PC1 y posteriormente sobre la PC2

- 4.5.6** Repita el procedimiento en cada PC del switch y cada PC del hub.

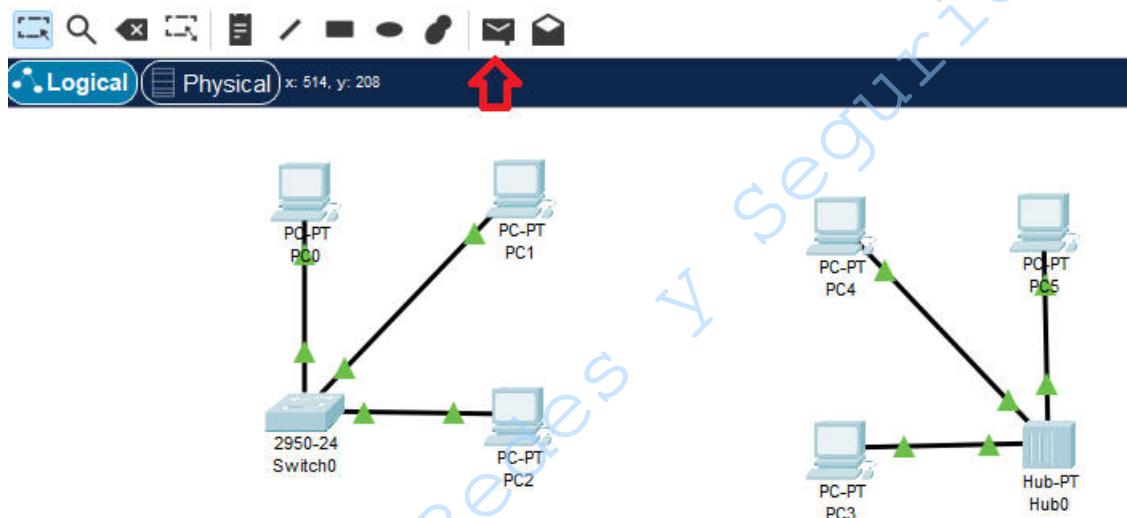


Figura No. 17. Pruebas.

- 4.5.7** ¿Se logró establecer la comunicación? Explique.

- 4.5.8** ¿Qué pasaría si no se asignan direcciones IP a las máquinas?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	257/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Cuestionario

1. ¿Cuál es la diferencia de descarga al compartir archivos entre ambos dispositivos?
Argumente su respuesta

2. Mencione algunas diferencias entre switch y hub para la transmisión de archivos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	258/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	259/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 4
Compartición de archivos por Hub y Swith en Linux
Cuestionario Previo

1. Investigue al menos un método que existe para compartir archivos, entre los sistemas operativos Linux, Windows, IOS.
2. Investigue los tipos de colisiones en la transmisión de datos existentes.
3. Investigue los métodos de seguridad que puede manejar el switch al compartir archivos.
4. ¿Qué es samba?
5. Mencione cuáles son los tipos de seguridad en samba.
6. ¿Qué contiene el archivo smb.conf?
7. Investigue qué significan los siguientes parámetros cuando se comparten recursos y se escriben en el archivo smb.conf.
 - a) comment
 - b) path
 - c) browsable
 - d) guest ok
 - e) writable
 - f) valid users
 - g) workgroup
8. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 260/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 5

Políticas de seguridad en las interfaces del switch

Capa 2 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	261/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno o la alumna implementará mecanismos adecuados de seguridad en los puertos del switch.
- El alumno o la alumna aprenderá los comandos para implementar distintos tipos de políticas de seguridad en los puertos de dispositivos de red tipo cisco.

2.- Conceptos teóricos

Los switches son dispositivos de uso generalizado en redes de área local. Al ser un elemento de red que requiere poca configuración es común que la seguridad en los mismos sea descartada por muchos administradores.

La capa de enlace de datos del modelo OSI ofrece servicio a todas las capas superiores, haciendo un encapsulamiento previo a la entrega de tramas a la capa física donde los paquetes son transferidos a través de un medio compartido. Es por ello que debemos prevenir que terceros no autorizados tengan acceso a este nivel en nuestra red local ya que podrían realizar escuchas no autorizadas (sniffers) o bien inyectar tráfico ilegítimo que comprometa el funcionamiento adecuado de la red.

Los switches CISCO cuentan con una característica conocida como seguridad de puerto (port security) con la que es posible limitar las estaciones de trabajo que pueden acceder a un puerto (por medio de su dirección MAC). Este límite puede definirse ya sea especificando un número máximo de direcciones o una lista de direcciones confiables que pueden acceder a cada uno de los puertos del switch.

3.- Equipo y material necesario

Equipo del Laboratorio:

- Software de simulación de redes Cisco Packet Tracer.

4.- Desarrollo

En esta práctica se presentan tres mecanismos para restringir el acceso a puertos en un switch cisco. Es importante mencionar que existen switches conocidos como no administrables que ciertos fabricantes ofrecen a precios reducidos, pero sin soporte a este tipo de configuración.

Modo de trabajar

La práctica se desarrollará en parejas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 262/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1 Construcción de la topología

- 4.1.1** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 1)

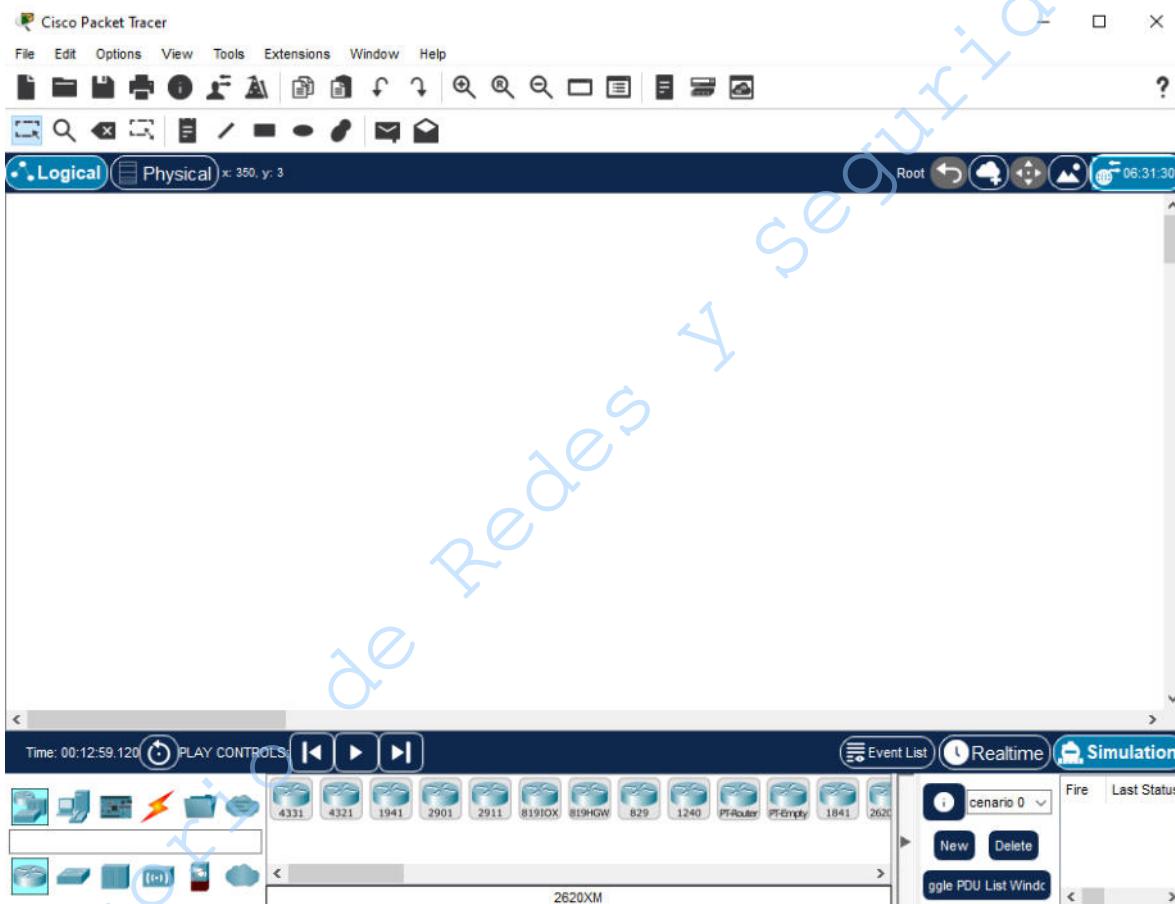


Figura No. 1. Interfaz gráfica de PT

- 4.1.2** Cuando Packet Tracer se inicia, muestra por default una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.
- 4.1.3** En la esquina inferior izquierda de la interfaz se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo (Ver figura No. 2.)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 263/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 2. Secciones de dispositivos

- 4.1.4** La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos, en el cuadro de texto del centro aparece el nombre de este grupo.
- 4.1.5** La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán.
- 4.1.6** Con ayuda de su profesora o profesor realice una topología básica de red agregando al área de trabajo de Packet Tracer un switch de 24 puertos (modelo 2950-24) y un par de dispositivos finales (PC y Laptop). Los dispositivos finales deberán conectarse desde la tarjeta de red Ethernet a alguno de los primeros dos puertos Fast Ethernet (Fa0/1 y Fa0/2) del switch empleando un cable directo (Ver figura No. 3.).

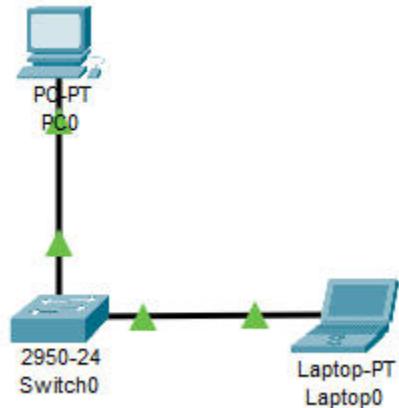


Figura No. 3. Topología básica

- 4.1.7** Asigne a cada uno de los dispositivos finales una dirección IP diferente que pertenezca al mismo segmento de red. El segmento de red será indicado por la profesora o el profesor.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	264/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.7.1 Dé clic sobre la PC0 conectada al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.1.7.2 Seleccione la pestaña Desktop y seleccione IP Configuration.

4.1.7.3 Se abrirá una ventana solicitando la dirección IP, máscara de red y el Gateway (vea la figura No. 4). Ingrese los datos designados por su profesora o profesor.

4.1.7.4 Repita los pasos 4.1.7.1, 4.1.7.2 y 4.1.7.3 para las laptop.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 265/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

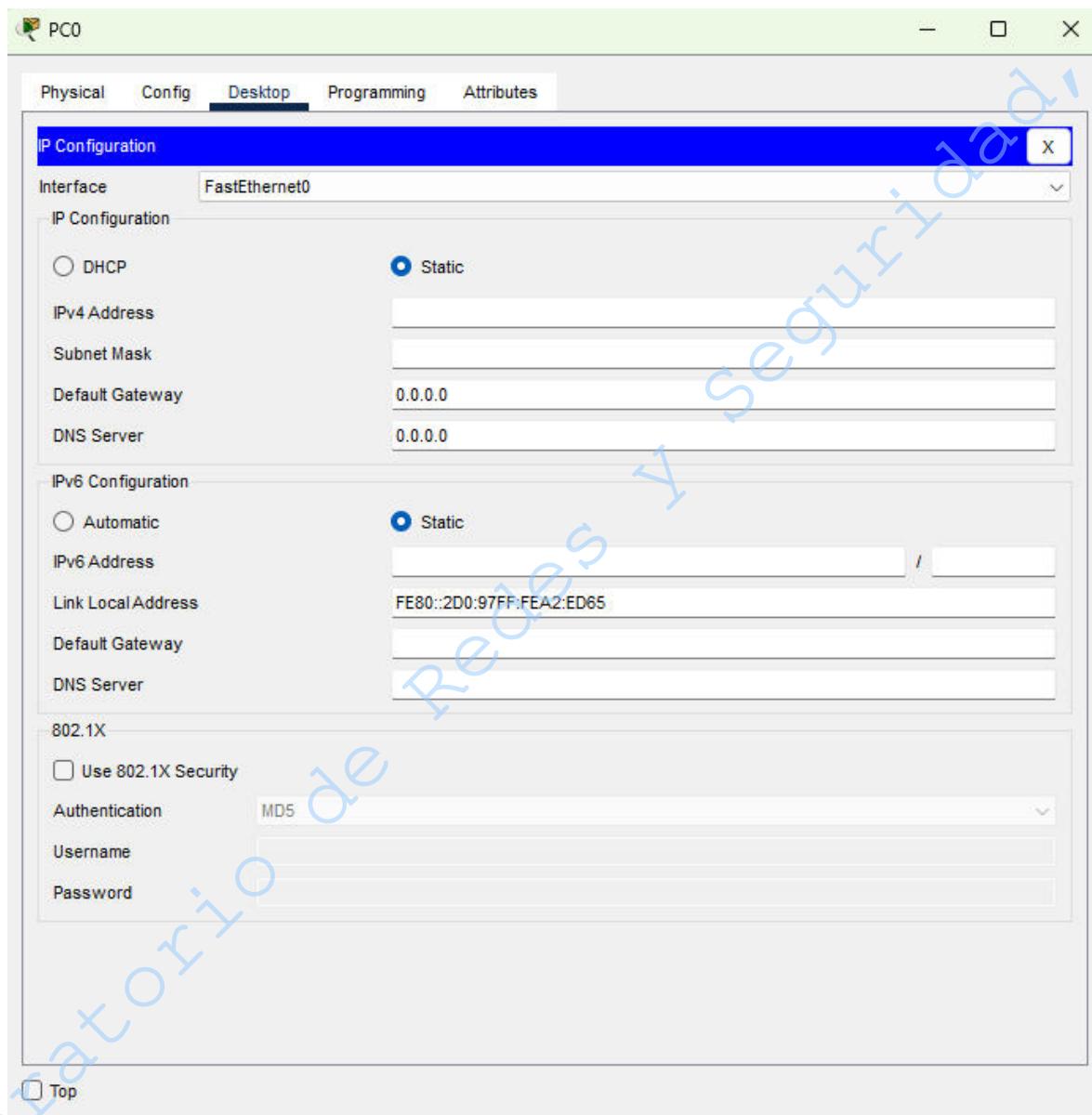


Figura No. 4. Configuración de la PC.

4.1.8 Tomando como base la topología construida se explicarán 2 técnicas para restringir el uso de puertos del switch a dispositivos no autorizados:

- Deshabilitar los puertos (interfaces) que no se utilicen.
- Implementar políticas de acceso a puertos con port security.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	266/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA: Para poder implementar políticas de acceso a puertos con port security es necesario primero deshabilitar los puertos (interfaces) que no se utilicen.

4.2 Deshabilitar los puertos sin utilizar

Con esta técnica se asegura que ningún dispositivo ajeno a la red local pueda conectarse sin la autorización correspondiente (inclusive un nodo no pueda ser cambiado de lugar). Con esta acción se garantiza que sólo estarán habilitados los nodos que realmente se necesitan y cuando se deban agregar más nodos, el administrador de red deberá habilitar solamente aquellos puertos requeridos.

- 4.2.1** Suponiendo que la red de la topología implementada únicamente funcionará con los primeros 10 nodos. Dé clic sobre el switch y seleccione la pestaña CLI. Ejecute los siguientes comandos para inhabilitar los puertos 11 a 24.

```

Switch>enable
Switch#config t
Switch(config)#interface range Fa0/11-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#end
Switch#

```

- 4.2.2** Explique qué sucede en la ventana CLI cuando se ejecuta el comando shutdown.

- 4.2.3** Agregue una nueva PC y conéctela al puerto Fa0/11 del switch. Describa el comportamiento que tiene la nueva conexión con respecto a las conexiones iniciales (Ver figura No. 5).



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	267/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

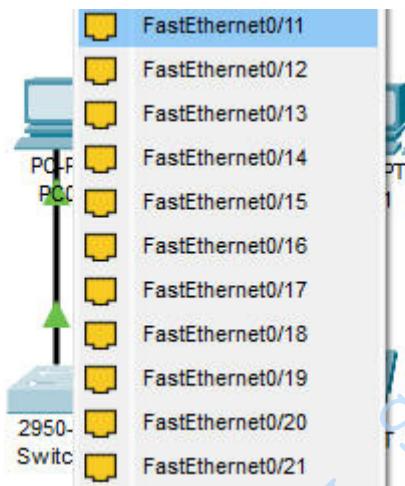


Figura No. 5. Añadiendo y conectando la nueva PC en el puerto 11

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	268/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.2.4** ¿Qué comandos deberían ejecutarse para que los puertos Fa0/11 a Fa0/15 se habiliten como parte una ampliación de la red? Pruebe los comandos en la ventana CLI y escríbalos en el siguiente cuadro:

4.3 Implementar políticas de acceso a puertos con port security.

Port security es una característica de Cisco en IOS (Command Line Interface) que permite restringir el tráfico que ingresa a la red limitando las direcciones MAC autorizadas a enviar tráfico a algún puerto. Al configurar direcciones MAC a un puerto, dicho puerto no reenviará ningún tráfico cuyo origen no provenga de alguna de las direcciones permitidas. En caso de que un puerto sólo acepte tráfico desde una única dirección MAC, el dispositivo conectado a éste puerto tendrá disponible el 100% de ancho de banda del puerto.

Una vez que se ha configurado port security, pueden ocurrir eventos que serán reportados como violaciones de seguridad cuando:

- a) Se alcanza el número máximo de direcciones MAC autorizadas para enviar paquetes a un puerto.
- b) Una dirección MAC intenta acceder a un puerto distinto al que se le configuró.

Una vez que ocurre una violación de seguridad (un nodo intenta enviar información por un puerto al que no se le ha dado autorización), el administrador puede configurar alguna de las siguientes acciones que deberá realizar el switch:

- 1) **protect**: el switch descartará los paquetes de dispositivos no permitidos sin dar alerta.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 269/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 2) **restrict**: mismo comportamiento que protect, pero aquí el dispositivo sí alertará en la consola sobre la violación de seguridad.
- 3) **shutdown**: el puerto pasará a estado apagado hasta que el administrador lo vuelva a habilitar manualmente.
- 4.3.1** Agregue una nueva PC al área de trabajo configúrela con una dirección IP perteneciente al mismo segmento que ha estado empleando y conéctela a la interfaz Fa0/12 del switch.
- 4.3.2** Para habilitar la opción de port security con una dirección MAC fija y un modo de violación shutdown en el puerto Fa0/12, ejecute los siguientes comandos en la ventana CLI del switch (Ver figura No. 6).

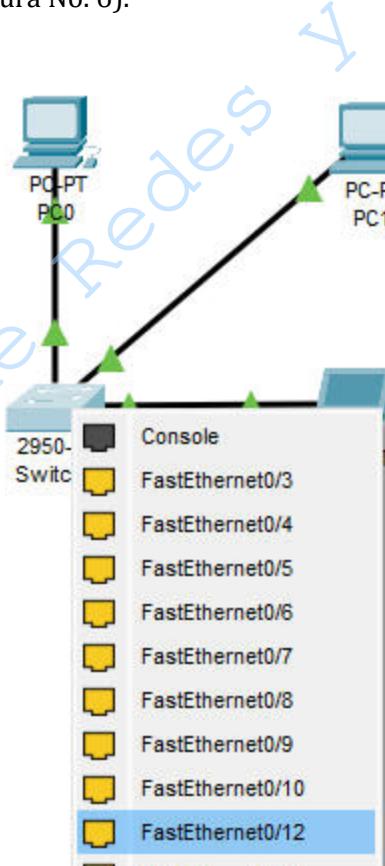


Figura No. 6. Añadiendo y conectando la nueva PC en el puerto 12

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 270/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

NOTA: Sustituya Dir_MAC por la dirección MAC de la nueva PC conectada en Fa0/12. Para obtener la Dir_MAC de la PC debe hacerse clic sobre la PC, seleccionar la pestaña Config y dar clic sobre el botón FastEthernet0 (Ver Figura No. 7)

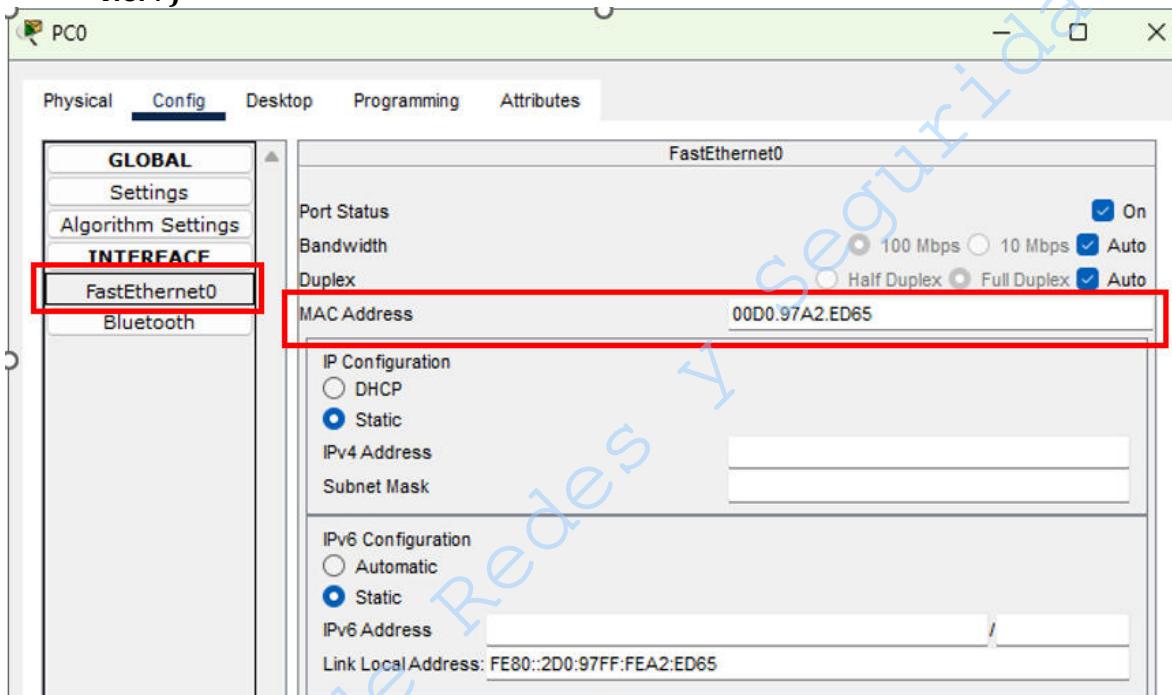


Figura No. 7. Obtener Dirección MAC

```

Switch>enable
Switch#config t
Switch(config)#interface Fa0/12
Switch(config)# switchport mode access
Switch(config)#switchport port-security
Switch(config)#switchport port-security mac-address Dir_MAC
Switch(config)#switchport port-security maximum 1
Switch(config)#switchport port-security violation shutdown
Switch(config)#end

```

- 4.3.3** Valide que la nueva PC tiene comunicación con las demás enviando mensajes Ping o con paquetes PDU simples. Hasta este punto la nueva PC deberá poder comunicarse con los otros nodos de la red. Para comprobar mediante mensajes ping que existe comunicación con el host, dé clic sobre la PC y seleccione la opción Command Prompt y teclee lo siguiente (Ver figuras No. 8 y 9):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	271/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PC> ping X.X.X.X

NOTA: X.X.X.X debe sustituirse por la dirección IP de otra PC.

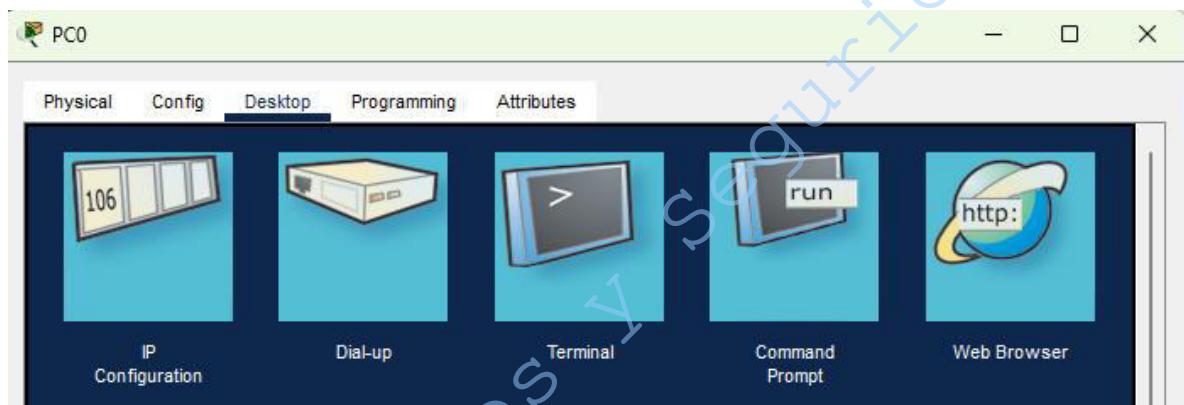


Figura No. 8. Command Prompt

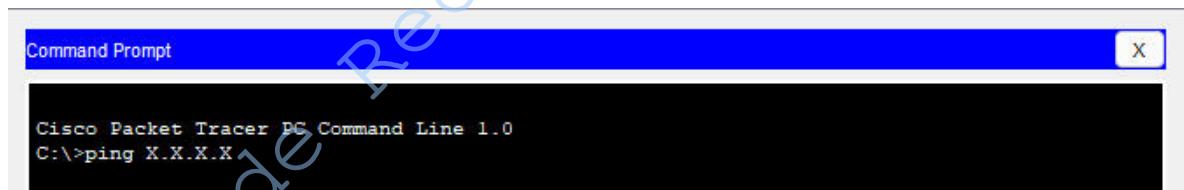


Figura No. 9. Ping

- 4.3.4 Para habilitar la opción sticky de port security ejecute los siguientes comandos en la ventana CLI del switch.

```

Switch>enable
Switch#config t
Switch(config)#interface Fa0/12
Switch(config)# switchport mode access
Switch(config)#switchport port-security
Switch(config)#switchport port-security mac-address sticky
Switch(config)#switchport port-security maximum 1
Switch(config)#switchport port-security violation shutdown
Switch(config)#end

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	272/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.5** Valide que la nueva PC tiene comunicación con las demás enviando mensajes Ping o con paquetes PDU simples.
- 4.3.6** Indique para qué sirve la opción sticky en este caso.

- 4.3.7** Para validar el funcionamiento de la política de seguridad implementada en el puerto Fa0/12 que apaga la interfaz cuando un cliente no autorizado intenta acceder al mismo debe eliminar el cable que conecta la PC en el puerto Fa0/12, posteriormente conecte un hub-PT con dos PC. El puerto 0 del hub se conecta con el puerto Fa0/12 del switch y los puertos 1 y 2 con las PC como se muestra en la figura No. 10.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	273/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

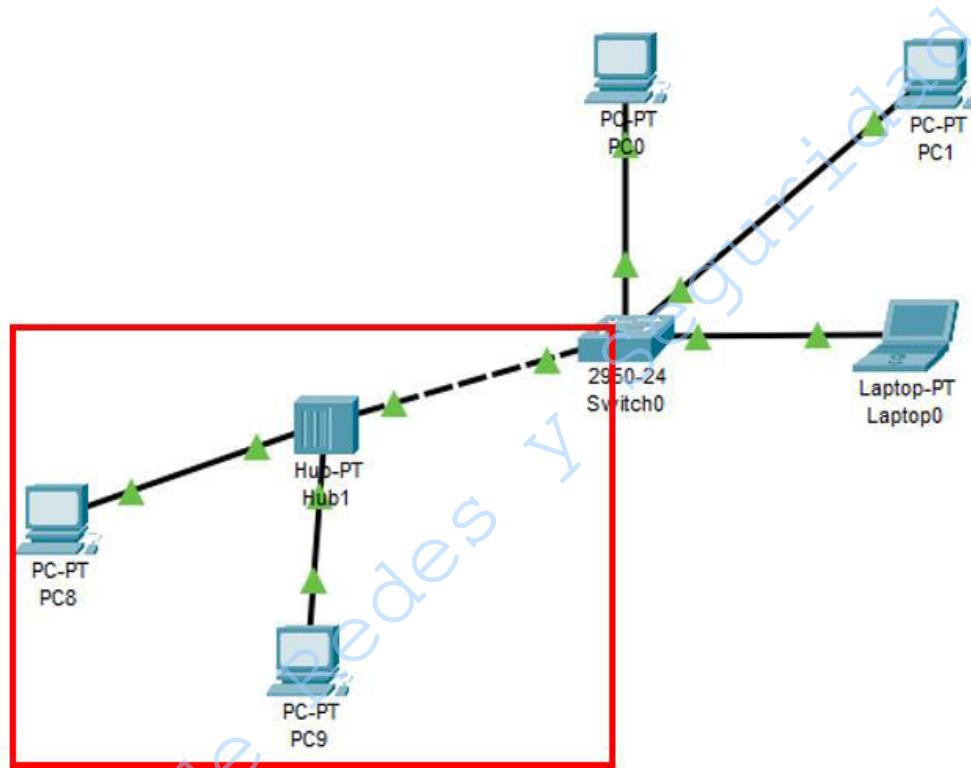
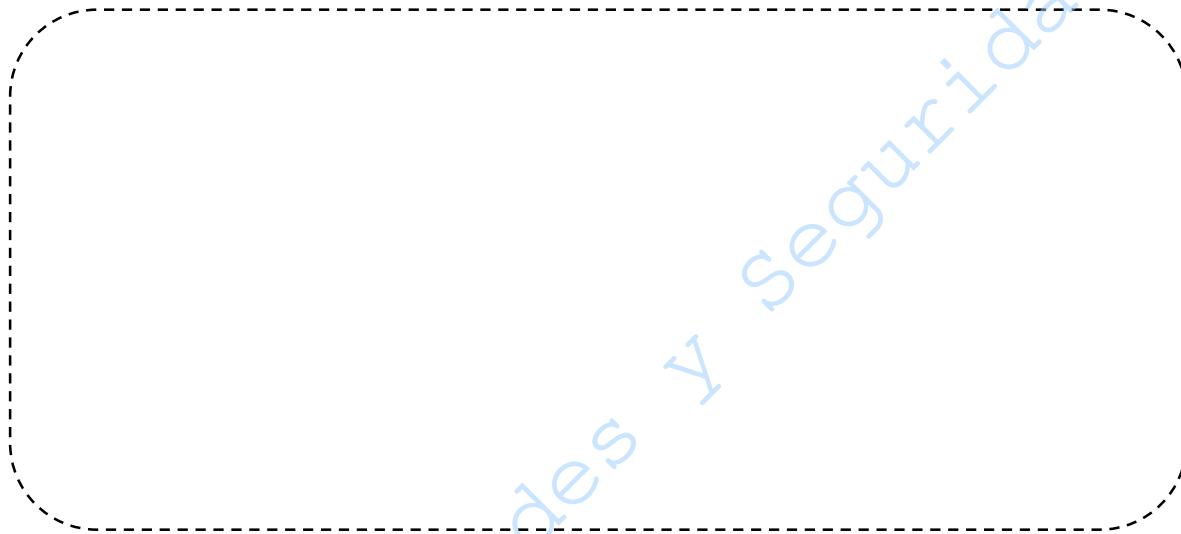


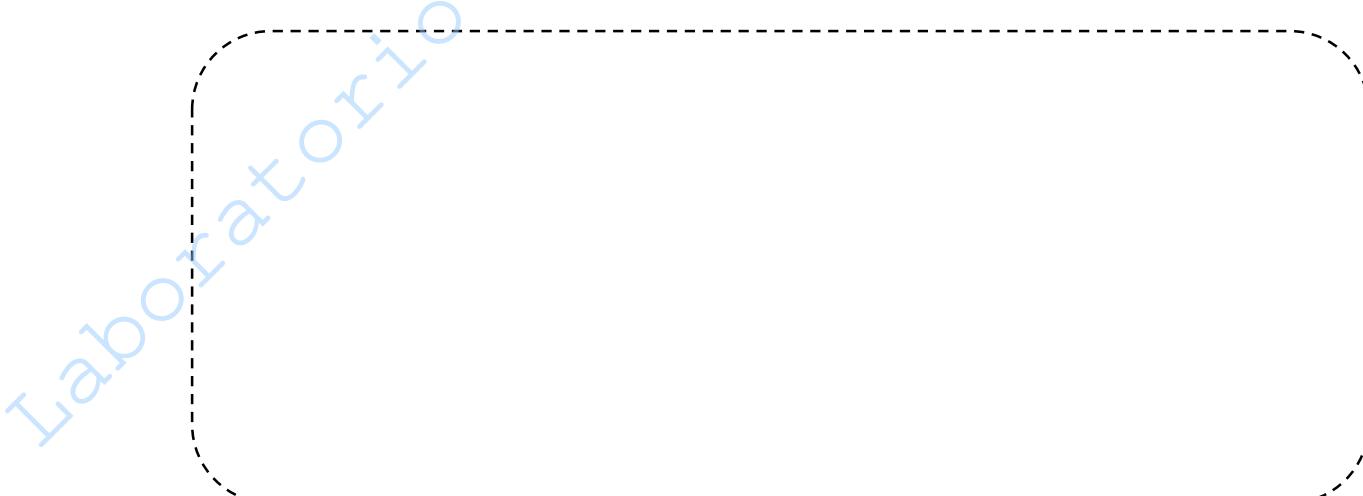
Figura No. 10. Añadiendo y conectando el hub en el puerto 12

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	274/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.8** Debe configurar una IP a estas nuevas máquinas y enviar mensajes Ping o PDU simples desde los nodos conectados al hub hacia todos los nodos conectados directamente al switch. Revise el simulador y la pestaña CLI del switch y explique lo que sucede.



- 4.3.9** La opción anterior para restringir los puertos a una sola dirección MAC puede ser muy restrictiva en ciertos escenarios. Además de que requiere que se conozcan las direcciones de todos los nodos y que éstas sean de nodos fijos. Ejemplifique el uso de la opción sticky de port security agregando 3 nuevas PC a los puertos Fa0/13, Fa0/14 y Fa0/15 y escriba los comandos necesarios a continuación.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 275/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4 Verificar configuración de port security

- 4.4.1** Existen diversos comandos que permiten revisar la configuración actual de la seguridad de puertos en IOS (Command Line Interface). Pruebe los siguientes comandos y explique la información que muestran:

Switch>enable
Switch#show port-security
Switch#show port-security interface PUERTO

NOTA: PUERTO debe sustituirse por la interfaz o puerto que desea revisar

- 4.4.2** Indique para qué se usa el comando show port-security address

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 276/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	277/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 5

Políticas de seguridad en los puertos del Switch

Cuestionario Previo

1. Realice una lista con al menos 3 ventajas y desventajas de adquirir un switch administrable en comparación con uno que no tenga dicha característica.
2. Investigue en qué consiste el ataque conocido como inundación de direcciones MAC (MAC Flooding Attack) y realice un diagrama donde se muestre su funcionamiento.
3. ¿Cómo se puede utilizar el ataque de inundación de direcciones MAC para hacer que un switch se comporte como HUB y realizar una escucha de todo el tráfico de los nodos conectados?
4. Investigue la sintaxis del comando port security para un switch Cisco.
5. Investigue qué permite realizar la opción sticky de port security.
6. Investigue cómo se podría utilizar la opción sticky de port security como una opción más flexible a MACs fijas.
7. ¿Para qué se utiliza la opción aging de port security?
8. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 278/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 6

EtherChannel y port security

Capa 2 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	279/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

1.- Objetivos de aprendizaje

- El alumno o la alumna comprenderá el concepto de EtherChannel.
- El alumno o la alumna configurará switches para establecer una conexión EtherChannel, utilizando el protocolo LACP en el simulador Packet Tracer.
- El alumno o la alumna aprenderá cuáles son los tipos de violaciones de un switch Cisco, así como la utilidad del comando port security y de sus diferentes parámetros.

2.- Conceptos teóricos

El EtherChannel es una tecnología de Cisco que permite una agrupación lógica de varios enlaces físicos Ethernet, de forma que la agrupación funcione como si se tratara de un único enlace Ethernet, lo que hace que se sume la velocidad de cada puerto físico utilizado y de esa forma se tenga solamente un enlace troncal de una alta velocidad.

Esta tecnología de agregación de enlaces permite hasta 8 puertos físicos FastEthernet, GigaEthernet o 10 GigabitEthernet que conforman a un EtherChannel. La finalidad de utilizar el EtherChannel es proporcionar tolerancia a fallos, uso compartido de carga, mayor ancho de banda y redundancia entre switches. Con el EtherChannel se pueden interconectar dispositivos como switches, routers, servidores o clientes.

Las ventajas de utilizar EtherChannel son varias, entre las que destacan:

- Permite enlaces full-duplex punto a punto.
- Es escalable.
- No se requiere actualización de hardware para aumentar la capacidad.
- Cuando un enlace falla, se redirige el tráfico a los otros enlaces.

Para configurar el EtherChannel, se tienen dos opciones: *Negociación* y *Manual*. En la opción *Manual*, todas las configuraciones se realizan una por una; mientras que en la *Negociación* se pueden identificar dos tipos:

- Port Aggregation Protocol (PAgP). Es un protocolo propietario de Cisco. En este, el dispositivo en cuestión negocia con el otro extremo cuáles son los protocolos que deben de activarse y es el propio protocolo el encargado de agrupar a los puertos que posean características similares.
- Link Aggregation Control Protocol (LACP). Es muy similar a su contraparte PAgP ya que también permite agrupar puertos con características similares. Define a los puertos como activos y pasivos, en donde los activos son capaces de iniciar negociaciones con otros puertos; mientras que los pasivos no pueden iniciar negociaciones.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	280/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Una desventaja que se tiene al usar EtherChannel es que para poder formar un grupo de agregación todos los puertos físicos deben de estar en el mismo conmutador.

Port Security es una característica de los switches Cisco, la cual permite tener una lista de cada una de las direcciones MAC conectadas a cada puerto de un switch de la red. Así, se permite agregar una capa de seguridad a la red, ya que sólo permite conectarse a la red mediante un puerto a la dirección definida en la lista y se evita que terceros puedan conectarse a la red ya sea por simple descuido o por intentar realizar un ataque de captura de tráfico.

Cuando se habilita el Port Security y se conecta a un puerto una dirección MAC que no está asignada ahí, el switch deshabilita dicho puerto; esto implica que cualquier dispositivo que se conecte a ese puerto, no se podrá conectar a la red, aunque el dispositivo tenga la MAC que sí esté definida para ese puerto. La manera en la que se puede volver a habilitar el puerto, sin perder la configuración de seguridad es a través de los comandos:

```
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

3.- Equipo y material necesario

Equipo del laboratorio:

- Software de simulación de redes Cisco Packet Tracer.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Creación de un port channel con protocolo LACP.

- 4.1.1 Encienda el sistema y elija la opción de cargar Windows.
- 4.1.2 Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3 Ejecute la aplicación Cisco Packet Tracer (Figura No. 1).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 281/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 1. Simulador de CISCO Packet Tracer.

- 4.1.4** Dé clic en la sección de Dispositivos de red, después seleccione el apartado de switches, ubique el modelo 2960 IOS15, arrastre dos instancias de los switches (Figura No. 2).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 282/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

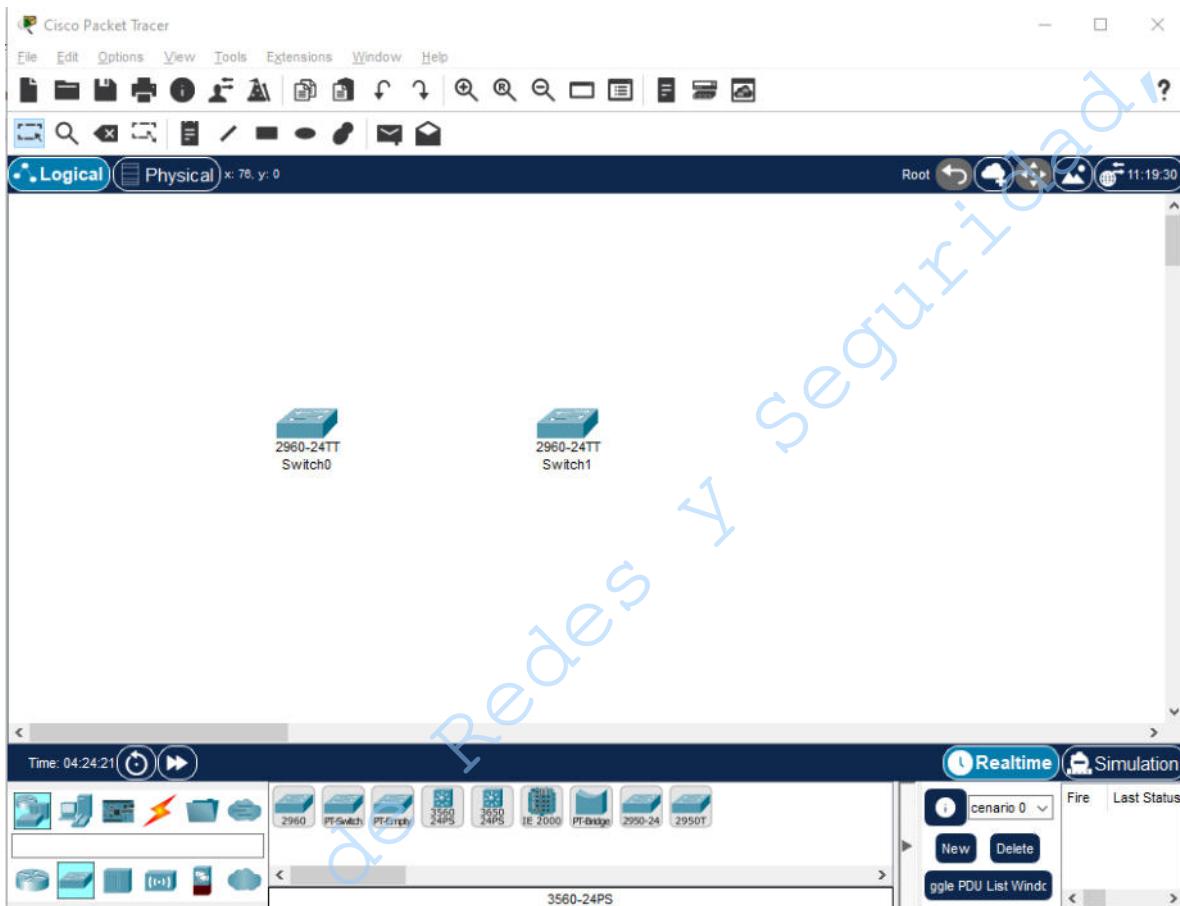


Figura No. 2. Switches modelo 2960

- 4.1.5 Dé clic en el apartado de *connections*, con 3 cables *copper cross over* conecte los dos switches, los puertos fa0/1, fa0/2 y fa0/3 del switch 0 deben estar conectados con los puertos fa0/1, fa0/2 y fa0/3 del switch 1, respectivamente (Figura No. 3).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 283/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

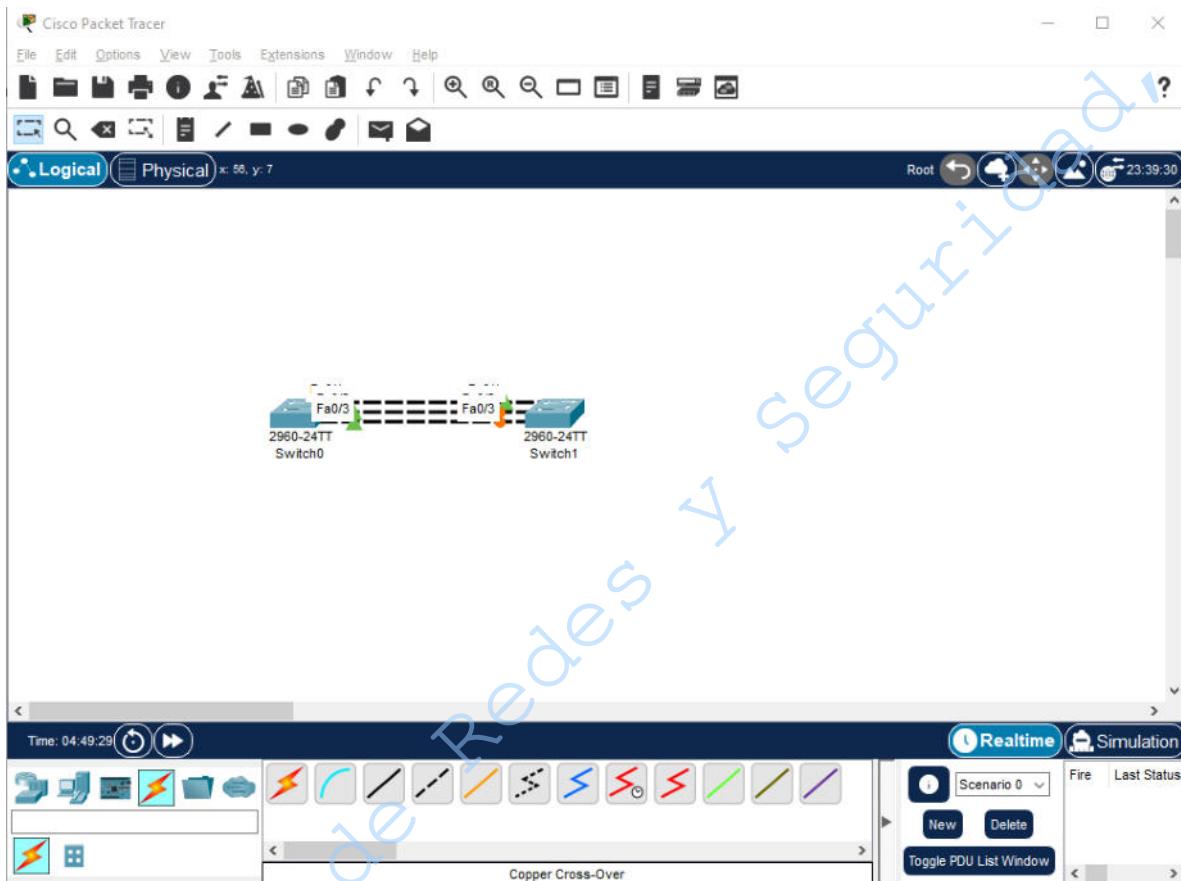


Figura No. 3. Switch 0 y 1 conectados

- 4.1.6 Acceda a la consola del switch 0 dando clic en el switch y después en la pestaña *CLI* (Figura No. 4), entre al modo *configuración global*, después cambie el nombre del switch por S0 mediante los siguientes comandos (Figura No. 5):

```

Switch>enable
Switch#configure terminal
Switch(config)#hostname S0

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	284/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

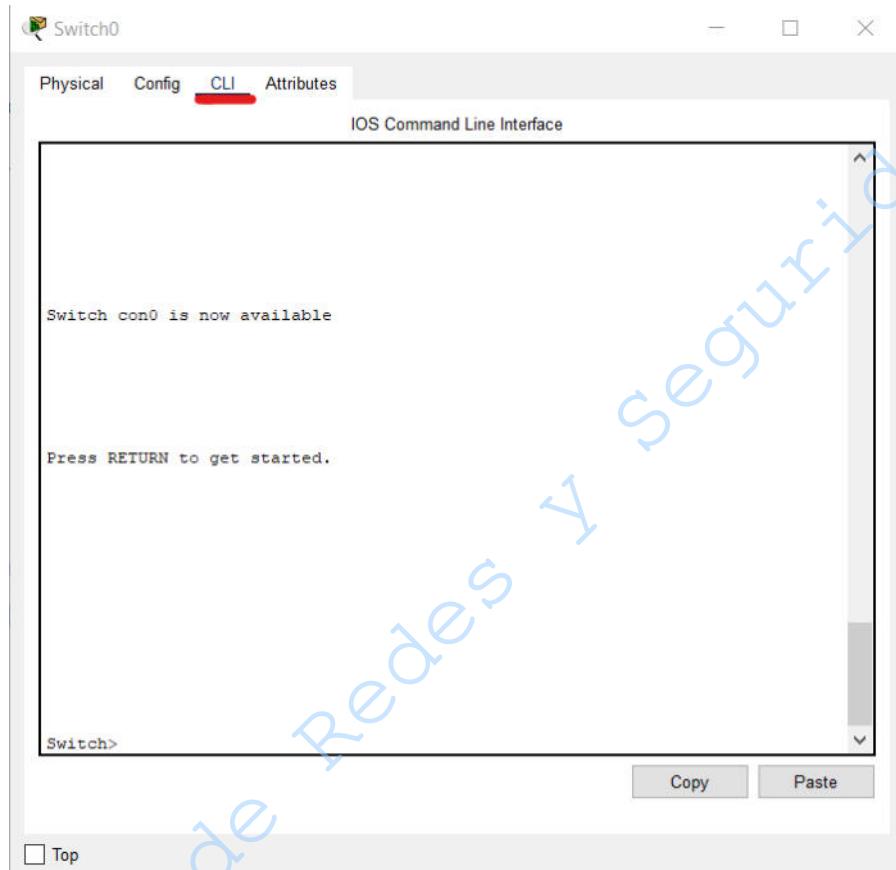


Figura No. 4. Terminal del switch

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S0
S0(config)#

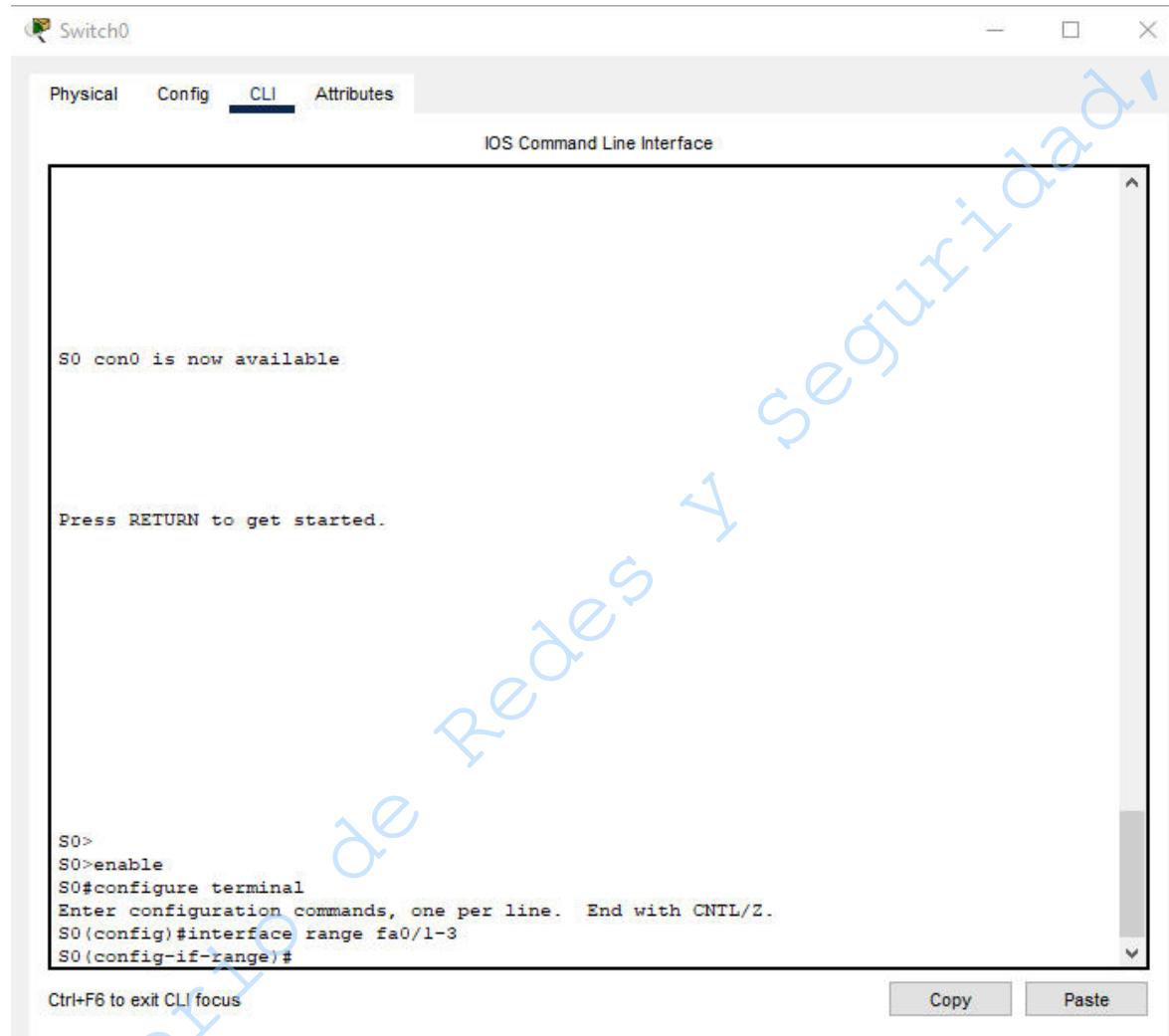
```

Figura No. 5. Cambio de nombre al S0

- 4.1.7** Desde el modo de configuración global, ingrese al grupo de interfaces fa0/1-3 mediante el siguiente comando (Figura No. 6):

S0(config)# interface range fa0/1-3

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	285/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



The screenshot shows a terminal window titled "Switch0" with the following content:

```

Physical Config CLI Attributes
IOS Command Line Interface

S0 con0 is now available

Press RETURN to get started.

S0>
S0>enable
S0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S0(config)#interface range fa0/1-3
S0(config-if-range)#
Ctrl+F6 to exit CLI focus

```

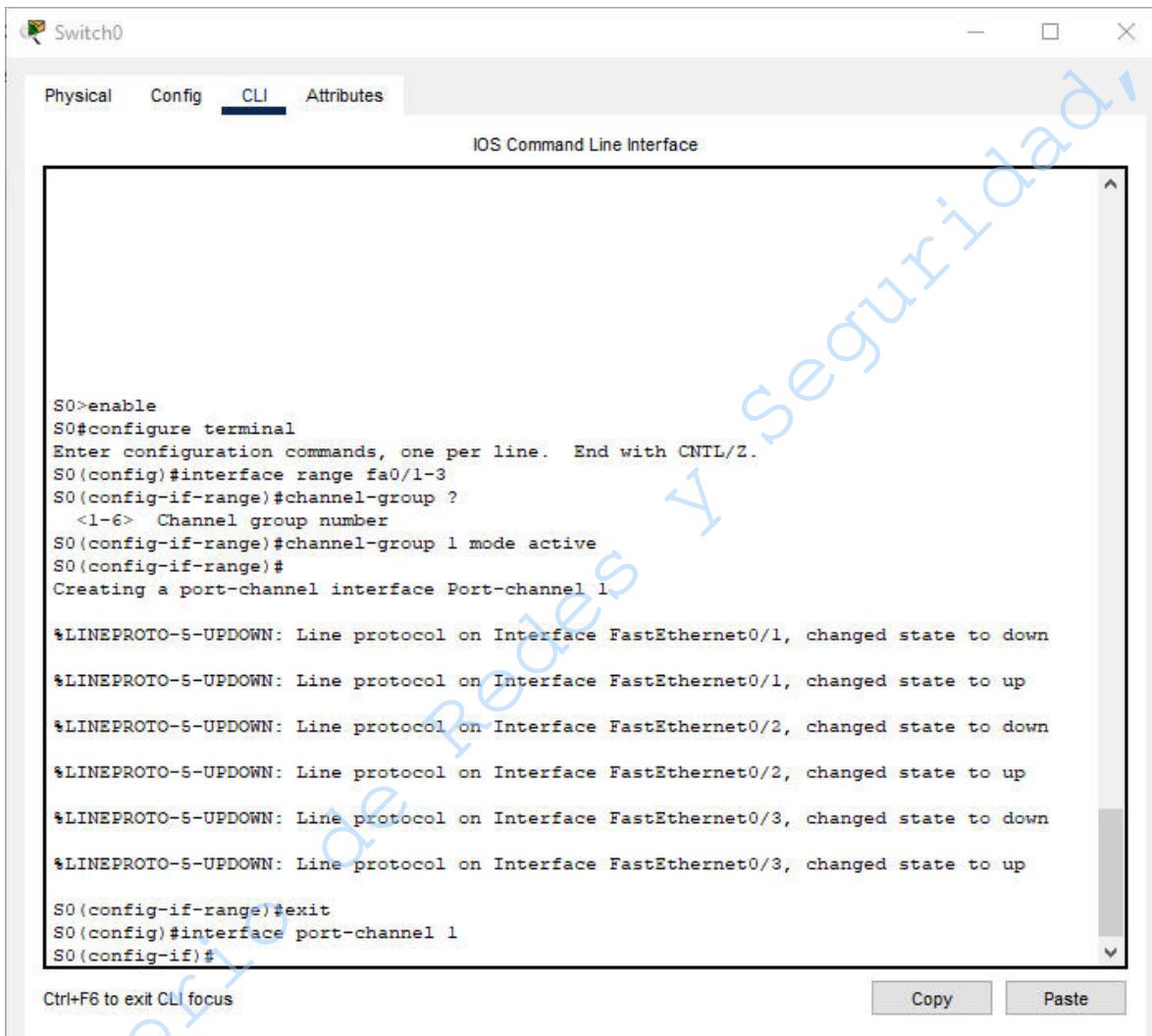
Copy Paste

Figura No. 6. Interface range switch 0

- 4.1.8 Dentro del interface range, cree un port channel con identificador 1, mediante el uso del siguiente comando (Figura No. 7):

S0(config-if-range)# channel-group 1 mode active

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 286/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



The screenshot shows a Windows application window titled "Switch0" with the "CLI" tab selected. The title bar also displays "IOS Command Line Interface". The main window contains the following CLI session output:

```

S0>enable
S0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S0(config)#interface range fa0/1-3
S0(config-if-range)#channel-group ?
<1-6> Channel group number
S0(config-if-range)#channel-group 1 mode active
S0(config-if-range)#
Creating a port-channel interface Port-channel 1

*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

S0(config-if-range)#exit
S0(config)#interface port-channel 1
S0(config-if)#

```

At the bottom left of the window, there is a note: "Ctrl+F6 to exit CLI focus". At the bottom right, there are "Copy" and "Paste" buttons.

Figura No. 7. Creación del channel group 1

4.1.9 Acceda al port channel creado, con el comando (Figura No. 8):

S0(config-if-range)# interface port-channel 1

Posteriormente, configure el port-channel en modo *trunk* con el siguiente comando:

S0(config-if)# switchport mode trunk

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 287/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```

S0>
S0>enable
S0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S0(config)#interface port-channel 1
S0(config-if)#switchport mode trunk
S0(config-if)#end
S0#
*SYS-5-CONFIG_I: Configured from console by console

S0#show etherchannel summary
Flags: D - down          P - 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
      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 (SD)       LACP    Fa0/1(I) Fa0/2(I) Fa0/3(I)
S0#
S0#
S0#
Ctrl+F6 to exit CLI focus

```

Copy Paste

Figura No. 8. Configuración del port channel

4.1.10 Para que pueda verificar que se haya creado y visualice qué interfaces componen el port channel 1 utilice los siguientes comandos (Figura No. 9):

```

S0(config-if)# exit
S0(config)# exit
S0# show etherchannel summary

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	288/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```

S0>
S0>enable
S0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S0(config)#interface port-channel 1
S0(config-if)#switchport mode trunk
S0(config-if)#end
S0#
*SYS-5-CONFIG_I: Configured from console by console

S0#show etherchannel summary
Flags: D - down          P - 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
      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 (SD)       LACP      Fa0/1(I) Fa0/2(I) Fa0/3(I)
S0#
S0#
S0#
Ctrl+F6 to exit CLI focus

```

Copy Paste

Figura No. 9. Etherchannel summary

Observe que en la columna de *port-channel* pueden aparecer las letras *SD* o *SU*, ¿Qué letras aparecen en este caso? Mencione su significado.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	289/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.1.11 Para el switch 1, repita los pasos desde el punto 4.1.6 hasta el 4.1.10, cambiando el nombre a S1.

Al realizar nuevamente el punto 4.1.10, en el apartado de *port-channel* observe que deberían de aparecer las letras *SU*. Regrese ahora a la terminal del Switch0 e ingrese otra vez el comando:

```
S0> enable  
S0# show etherchannel summary
```

Vea que cambió el apartado de Port-channel y ahora aparecen las letras *SU*, mencione su significado y dé una breve explicación de la razón por la que cree que cambiaron las letras mostradas en dicho apartado después de haber configurado el Switch1.

4.2 Topología con etherchannel.

4.2.1 A partir del ejercicio anterior, complete el armado de la topología mostrada en la Figura No. 10, los puertos fa0/4, fa0/6 y fa0/7 del switch 1 deben estar conectados con los puertos fa0/4, fa0/6 y fa0/7 del switch 2 respectivamente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 290/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

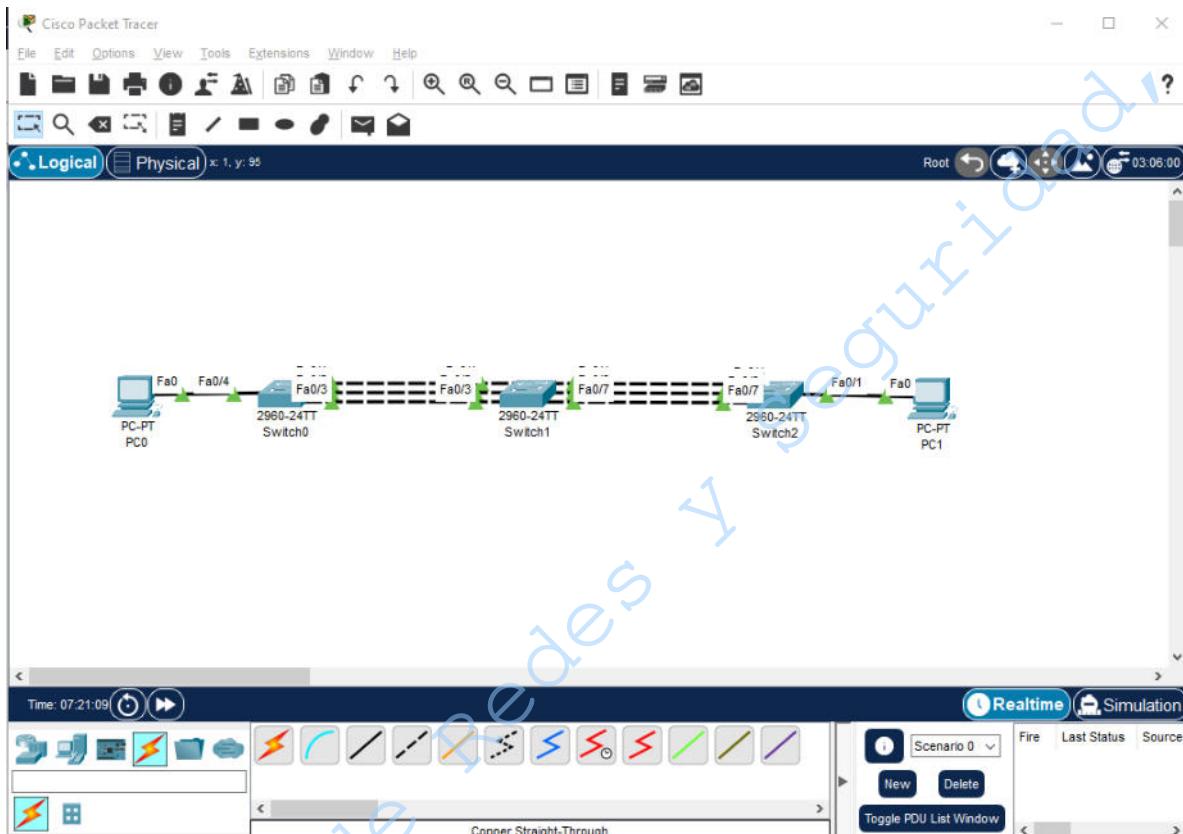


Figura No. 10. Topología para armar

4.2.2 Siguiendo las instrucciones desde el punto 4.1.6 hasta el 4.1.9 tanto en los Switches 1 y 2, cree un port channel entre estos, con identificador 2.

NOTA: Para usar el comando *interface range*, las interfaces deben estar consecutivas, por lo que para este ejercicio solamente puede usar *interface range* con las interfaces 6 y 7.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	291/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

4.2.3 Asigne las direcciones de las PC 0 y 1 de acuerdo a la información de la Tabla No. 1.

Tabla No. 1. Información de las tarjetas de red

	PC0	PC1
IPv4	192.168.1.1	192.168.1.2
Máscara de subred	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
DNS	0.0.0.0	0.0.0.0

4.2.4 Entre a la consola del switch 2 y ejecute el siguiente comando:

S2# show etherchannel summary

Observe que en el apartado de *port-channel* pueden aparecer las letras *SD* o *SU*, ¿Qué letras aparecen en este caso? Justifique su respuesta.

4.2.5 Envíe un paquete PDU simple desde la PC0 a la PC1, ¿el paquete fue enviado con éxito? Justifique su respuesta.

NOTA: En ocasiones, al mandar un paquete PDU simple, puede fallar en el primer intento; por lo que se recomienda que antes de verificar toda la configuración para encontrar el problema, se haga un segundo intento de envío.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	292/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

EJERCICIO OPCIONAL

4.3 Configuración de port security con MAC Address.

- 4.3.1** Abra un archivo nuevo en blanco. Dé clic en la sección de Dispositivos de red, después seleccione el apartado de switches, ubique el modelo 2960 IOS15, arrastre una instancia del switch. Dé clic en la sección de dispositivos finales y arrastre una instancia de una PC. Haga clic en el apartado de connections, ubique el cable directo y conecte la computadora al switch con este a través de la interfaz fa0/1 (Figura No. 11).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 293/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

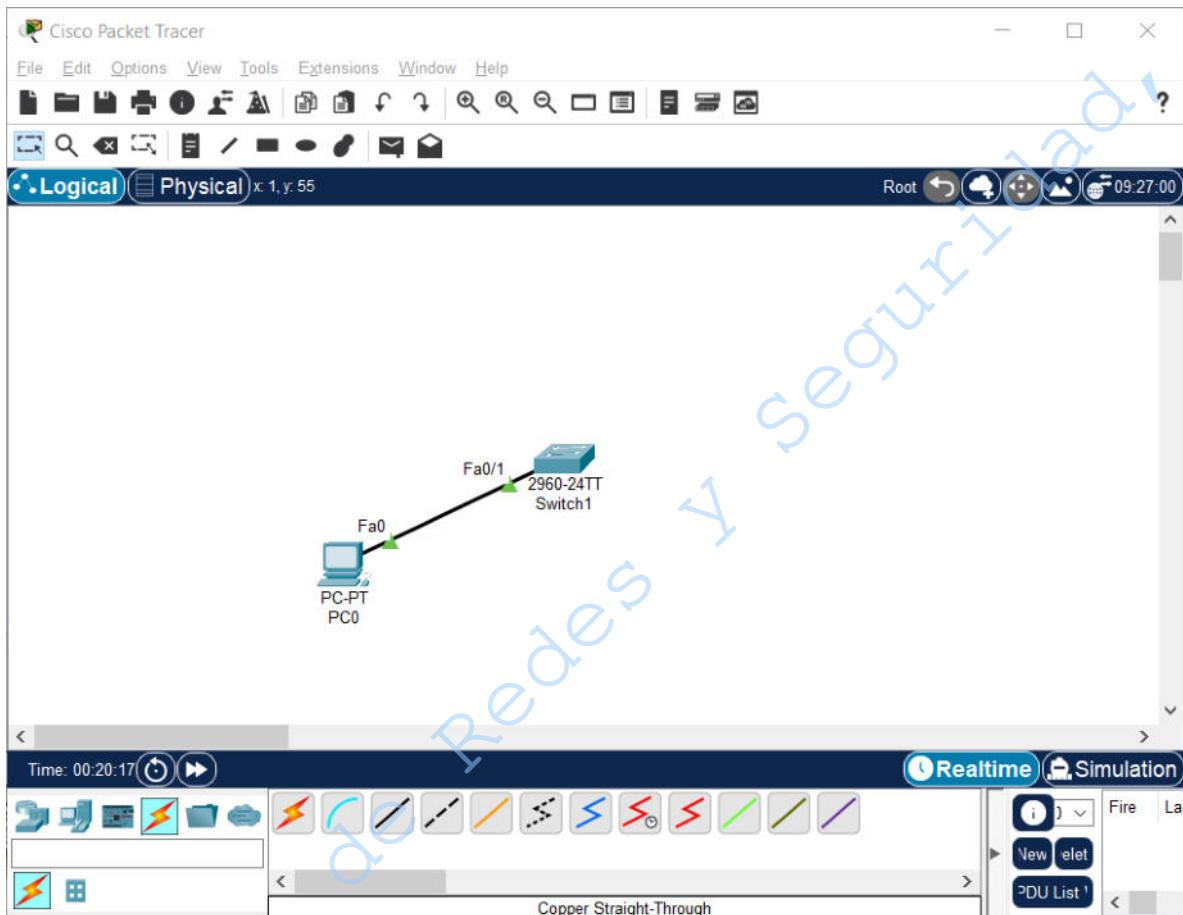


Figura No. 11. Topología configuración port security

- 4.3.2** Dé clic en la computadora PC0, ingrese a la pestaña Desktop y haga clic en el ícono que dice *Command Prompt* (Figura No. 12):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	294/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

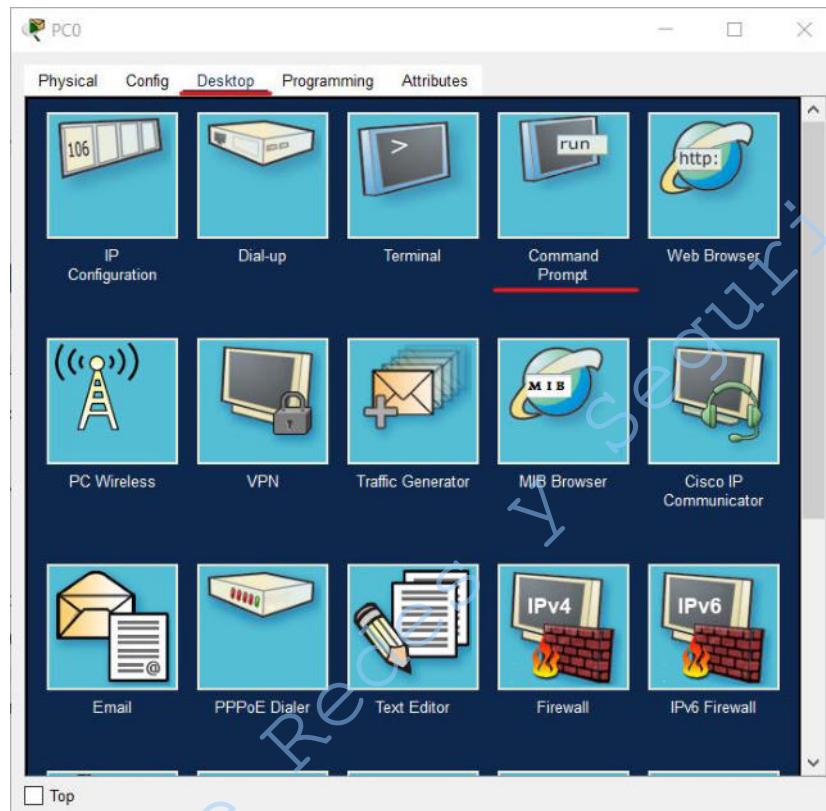


Figura No. 12. Íconos de la pestaña Desktop de la PC0.

4.3.3 Dentro del *Command Prompt*, ingrese el siguiente comando:

C:\> ipconfig /all

Una vez ejecutado el comando, identifique el apartado en el que aparece la dirección MAC de la PC0 (Figura No. 13).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	295/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0010.11B6.8D4A
Link-local IPv6 Address.....: FE80::210:11FF:FE86:8D4A
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
                           0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-A2-2B-33-22-00-10-11-
B6-8D-4A
DNS Servers.....: :::
                           0.0.0.0

```

Figura No. 13. Resultado del comando ipconfig

Anote a continuación la dirección física que arrojó el comando:

- 4.3.4** Dé clic en el switch, ingrese a la CLI, acceda al modo configuración global y cambie el nombre de switch por S1, con los siguientes comandos (Figura No. 14):

```

Switch>enable
Switch#configure terminal
Switch(config)# hostname S1

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	296/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Switch1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Switch con0 is now available

Press RETURN to get started.

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura No. 14. Cambio de nombre al S1

4.3.5 Acceda a la interfaz que esté conectada a la computadora con el siguiente comando (Figura No. 15):

S1(config)# interface fa0/1

```

S1(config)#interface fa0/1
S1(config-if)#

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	297/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Figura No. 15. Ingreso a la interfaz conectada a la computadora

- 4.3.6 Configure el port-security con modo de violación con los siguientes comandos (Figura No. 16):

```
S1(configconfig-if)#shutdown
S1(configconfig-if)#switchport mode access
S1(configconfig-if)#switchport port-security
S1(configconfig-if)#switchport port-security mac-address DIR_MAC
S1(configconfig-if)#switchport port-security maximum 1
```

NOTA: Sustituya DIR_MAC por la dirección MAC que anotó en el punto 4.3.3.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address 0010.11B6.8D4A
S1(config-if)#switchport port-security maximum 1
```

Figura No. 16. Configuración de port-security parte 1

Donde:

switchport mode access: Este comando configura el puerto en modo acceso.

switchport port-security: Este comando levanta la seguridad del puerto.

switchport port-security mac-address DIR_MAC: Este comando registra, como una dirección válida para este puerto, la MAC-ADDRESS que le demos.

switchport port-security maximum 1: Este comando registra el número máximo de MAC-ADDRESS que va a reconocer este puerto.

- 4.3.7 Existen 3 tipos de violación dentro de los switches Cisco; para poder conocer cuáles son, ingrese el siguiente comando:

```
S1(config-if)#switchport port-security violation ?
```

Escriba los tipos de violación que arroja el comando y describa cada uno de ellos:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	298/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.3.8** Configure el puerto con modo de violación shutdown de la siguiente forma (Figura No. 17):

```
S1(igconfig-if)#switchport port-security violation shutdown
S1(igconfig-if)#no shutdown
```

```
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#

```

Figura No. 17. Configuración del tipo de violación shutdown

- 4.3.9** Para confirmar que la configuración de seguridad quedó correcta, ingrese los siguientes comandos (Figura No. 18):

```
S1(configconfig-if)#end
S1#show port-security interface fa0/1
```

```
S1#show port-security interface fa0/1
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Figura No. 18. Confirmación de correcta configuración del port security

- 4.3.10** Dé clic en la sección de dispositivos finales y arrastre una instancia de una PC. Haga clic en el apartado de connections, ubique el cable directo y conecte la computadora al switch con este, a través de la interfaz fa0/1. Para conectar a esta interfaz, primero es necesario cambiar de puerto a la conexión ya existente y conectarla a la fa0/2.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	299/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

4.3.11 Asigne las direcciones de las PC 0 y 1 de acuerdo a la información de la Tabla No. 2.

Tabla No. 2. Información de las tarjetas de red

	PC0	PC1
IPv4	192.168.1.1	192.168.1.2
Máscara de subred	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0
DNS	0.0.0.0	0.0.0.0

4.3.12 Envíe un paquete PDU simple desde la PC0 a la PC1, ¿el paquete fue enviado con éxito?
Justifique su respuesta.

4.3.13 Entre a la terminal CLI del S1 e identifique si aparece un mensaje como el de la Figura No. 19:

```
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

Figura 19. Mensaje de bloqueo de puerto

Mencione a continuación qué es lo que indica el mensaje anterior:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	300/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

4.3.14 Vuelva a conectar la PC0 a la interfaz fa0/1 del Switch S1.

4.3.15 Para poder volver a habilitar el puerto fa0/1, debe hacerlo a través de los siguientes comandos (Figura No. 20):

```
S1#configure terminal
S1(config)#interface fa0/1
S1(config-if)#shutdown
S1(config-if)#no shutdown
```

```
S1(config)#interface fa0/1
S1(config-if)#shutdown
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#

```

Figura 20. Reinicio de puerto fa0/1

4.3.16 Conecte la PC1 a la interfaz fa0/2 del Switch S1, utilizando un cable directo y espere unos momentos a que el Switch detecte correctamente la conexión.

4.3.17 Envíe un paquete PDU simple desde la PC0 a la PC1, ¿el paquete fue enviado con éxito? Justifique su respuesta.

4.4 Configuración de port security con el parámetro “sticky”.

4.4.1 Continuando con el mismo archivo, arme la siguiente topología (Figura No. 21):



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	301/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

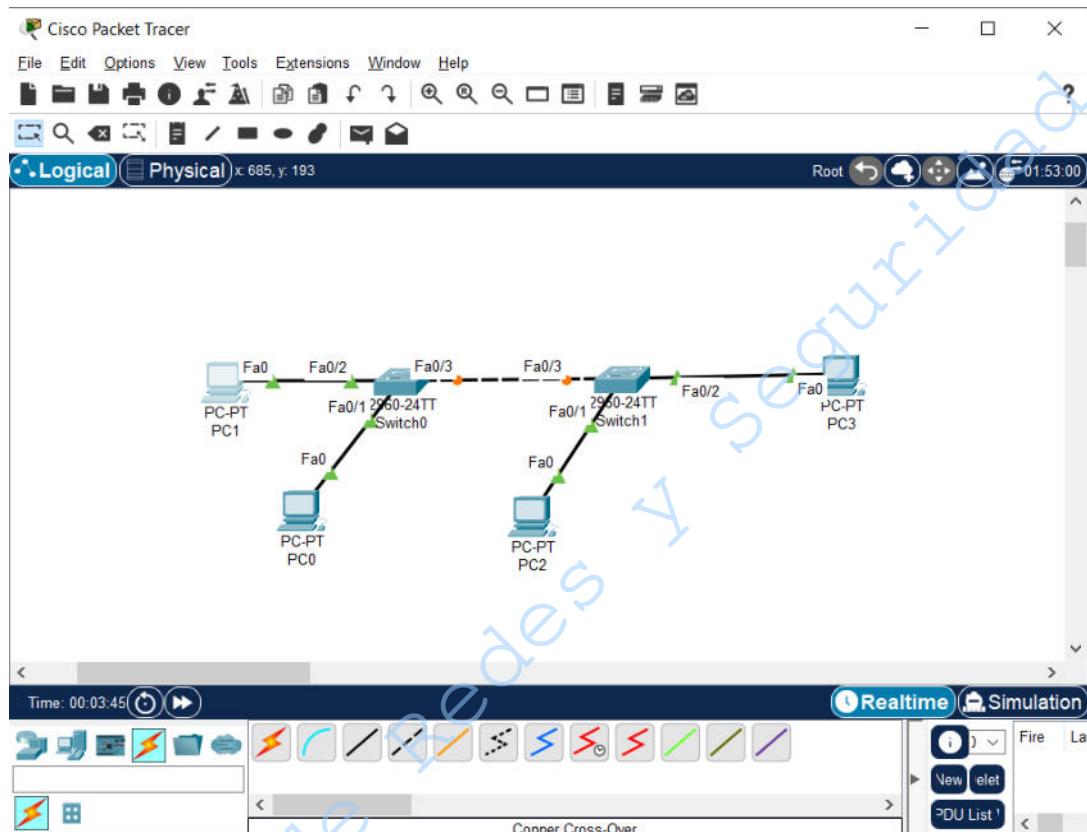


Figura No. 21. Topología de port-security con sticky

4.4.2 Asigne las direcciones de las PC 2 y 3 de acuerdo a la información de la Tabla No. 2.

Tabla No. 2. Información de las tarjetas de red

	PC2	PC3
IPv4	192.168.1.3	192.168.1.4
Máscara de subred	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	302/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

DNS	0.0.0.0	0.0.0.0
-----	---------	---------

- 4.4.3** Dé clic en el Switch1, ingrese a la CLI, acceda al modo configuración global y cambie el nombre de switch por S2, con los siguientes comandos:

```
Switch>enable
Switch#configure terminal
Switch(config)# hostname S2
```

- 4.4.4** Acceda a la interfaz que esté conectada a la computadora con el siguiente comando (Figura No. 22):

```
S2(config)# interface fa0/1
```

```
S1(config)#interface fa0/1
S1(config-if) #
```

Figura 22. Ingreso a la interfaz conectada a la computadora

- 4.4.5** Configure el port-security con modo de violación con los siguientes comandos (Figura No. 23):

```
S2(config-if)#shutdown
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#switchport port-security maximum 1
```

NOTA: Observe que en esta ocasión, en lugar de ocupar la dirección MAC del dispositivo, se ocupa el parámetro *sticky*, el cual detecta automáticamente la dirección MAC conectada a la interfaz.

```
S2(config-if)#switchport port-security mac-address sticky
S2(config-if) #
```

Figura 23. Configuración de MAC-ADDRESS con sticky.

- 4.4.6** Configure el puerto con modo de violación shutdown de la siguiente forma (Figura No. 24):

```
S2(configconfig-if)#switchport port-security violation shutdown
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	303/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

S2(configconfig-if)#no shutdown

```
S2 (config-if) #switchport port-security violation shutdown
S2 (config-if) #
```

Figura 24. Configuración del tipo de violación *shutdown*

- 4.4.7** Envíe un paquete PDU simple desde la PC2 a la PC3, el paquete debería de haber sido enviado con éxito. Este primer envío de paquete se realiza para que las tablas MAC del switch se actualicen y así el parámetro sticky pueda detectar la dirección física de la PC2.
- 4.4.8** Para confirmar que la configuración de seguridad quedó configurado correctamente, ingrese los siguientes comandos (Figura No. 25):

S2(configconfig-if)#end
S2#show port-security interface fa0/1

```
S2#show port-security interface fa0/1
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 00E0.A353.CBB3:1
Security Violation Count : 0
```

Figura 25. Confirmación de correcta configuración del port security

- 4.4.9** Conecte la PC2 a la interfaz fa0/4, mientras que la PC3 deberá conectarla a la interfaz fa0/1, de este modo se habrá conectado una dirección MAC distinta a la interfaz configurada anteriormente.
- 4.4.10** Espere unos momentos a que las conexiones sean detectadas y envíe un paquete PDU simple desde la PC2 a la PC3, ¿el paquete fue enviado con éxito? Justifique su respuesta.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	304/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.4.11** Entre a la terminal CLI del S2 e identifique si aparece un mensaje como el siguiente (Figura No. 26):

```
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

Figura 26. Mensaje de bloqueo de puerto

Mencione a continuación qué es lo que indica el mensaje anterior:

- 4.4.12** Ahora indique los pasos para que se pueda volver a mandar un paquete correctamente entre la PC2 y la PC3 ocupando las interfaces fa0/1 y fa0/2 del S2:
-
-
-
-

- 4.4.13** Realice en Cisco Packet Tracer los pasos que definió y compruebe la conexión con un paquete PDU simple.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	305/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad UNAM

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	306/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 6

EtherChannel y port security

Cuestionario Previo

1. Investigue el concepto de agregación de enlaces.
2. ¿Qué es el etherchannel?
3. Ventajas del etherchannel.
4. ¿Qué es un enlace troncal?
5. Investigue la sintaxis y el funcionamiento de los siguientes comando:
6. interface range
7. etherchannel summary
8. Investigue qué es el port security de un switch.
9. Investigue la utilidad del parámetro sticky en un switch Cisco.
10. Describa en qué consisten los tres tipos de violaciones de un switch Cisco (protect, restrict y shutdown), así como las diferencias entre cada uno.
11. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 307/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 7

Enrutamiento estático

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	308/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno o la alumna empleará el protocolo de enrutamiento estático y visualizará su funcionamiento dentro de una red de área local mediante el simulador de redes Cisco Packet Tracer en su versión más reciente.

2.- Conceptos teóricos

El administrador de redes requiere que los diferentes departamentos mantengan una comunicación fiable dentro de su red interna, para lo cual se necesitan utilizar los enrutamientos estáticos y dinámicos.

El enrutamiento es fundamental para cualquier red de datos, siendo el router el encargado de transmitir información de una red origen a una red destino.

El enrutamiento es el proceso que permite enviar paquetes entre diferentes redes, cuyo objetivo principal es buscar la mejor ruta. Para hallar la ruta más óptima debe considerarse la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa y el ancho de banda. Ningún paquete puede ser enviado sin seguir una ruta. La ruta es calculada con base en el protocolo de enrutamiento que se emplee. El dispositivo de red que realiza el proceso de enrutamiento es el router.

El encaminamiento estático funciona por medio de rutas estáticas definidas por el administrador de redes, obtenidas de las tablas de ruteo. Dicho encaminamiento es recomendado para redes pequeñas, por su bajo costo de mantenimiento y fiabilidad para transmitir paquetes, en cambio en redes grandes requiere de una configuración y mantenimiento constante por parte del administrador y es más vulnerable a errores por los cambios en la topología de red.

El protocolo de enrutamiento estático lo configura el propio administrador, todas las rutas estáticas que se le ingresen son las que el router contendrá en su tabla de ruteo y serán las únicas rutas que serán conocidas, por lo tanto sabrá enrutar paquetes hacia dichas redes.

Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que requieren los protocolos de enrutamiento dinámico. La creación de la tabla de rutas de forma manual, requiere que la topología de la red sea conocida previamente.

El encaminamiento dinámico es utilizado en redes más grandes, ya que tiene la capacidad de determinar rutas y priorizar la más óptima de acuerdo con la información de los routers en el envío de paquetes.

El Routing Information Protocol (RIP) es un protocolo vector-distancia y se especificó originalmente en el RFC 1058. Tiene por características principales las siguientes:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	309/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- Protocolo de enrutamiento con clase.
- Utiliza el conteo de saltos como métrica.
- Se emplea si el conteo de saltos de una red no es mayor a 15.
- Por defecto se envía un broadcast o multicast de las actualizaciones de enrutamiento cada 30 segundos.

RIP versión 2 (RIPv2) es un protocolo de enrutamiento sin clase, las máscaras de subred se incluyen en las actualizaciones de enrutamiento, lo que hace que RIP v2 sea compatible con los ambientes de enrutamiento modernos.

Este protocolo es una mejora de las funciones y extensiones de RIP versión 1, algunas de estas funciones mejoradas incluyen:

- Direcciones de siguiente salto incluidas en las actualizaciones de enrutamiento.
- Uso de direcciones multicast al enviar actualizaciones.
- Opción de autenticación disponible.

Los cables seriales se utilizan para interconexión de datos entre dispositivos digitales. La mayoría de estos cables seriales usan la entrada RS-232 que es la interfaz estándar para las comunicaciones entre este tipo de dispositivos.

El cable DTE y DCE se utilizan para comunicar un equipo terminal de datos y un equipo de comunicaciones de datos. DTE se refiere al punto de terminación para inicio de sesión y DCE se refiere a punto de una sesión de comunicación de reenvío.

3.- Equipo y material necesario

Equipo del Laboratorio:

- 1 Computadora con un sistema operativo Windows.
- Software de simulación de Cisco Packet Tracer en su versión más reciente.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 310/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1 Construcción de la topología

- 4.1.1** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 1)

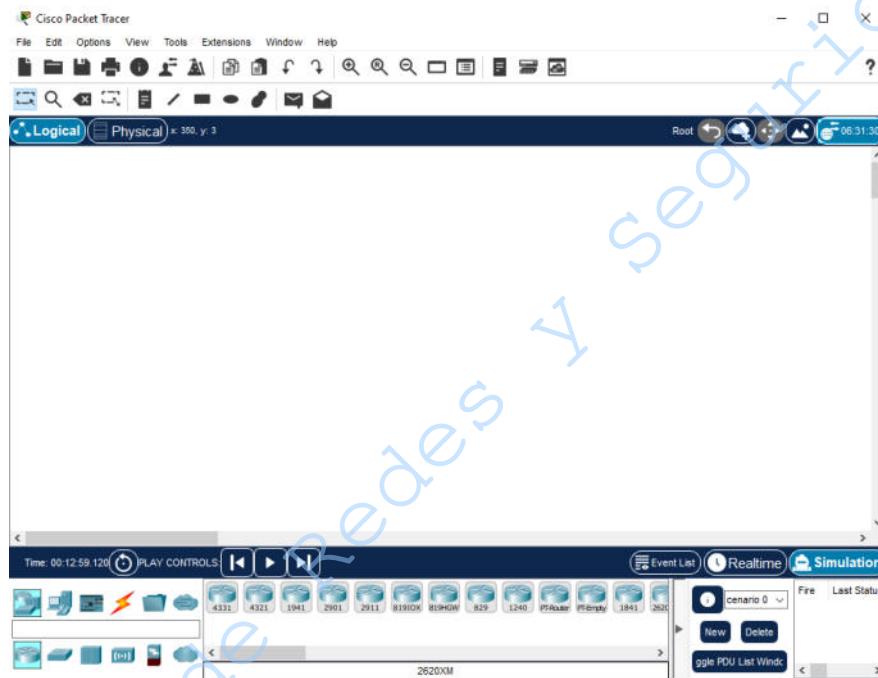


Figura No. 1. Interfaz gráfica de PT

- 4.1.2** Cuando Packet Tracer se inicia, muestra por default una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.
- 4.1.3** En la esquina inferior izquierda de la interfaz se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo (Ver figura No. 2.)



Figura No. 2. Secciones de dispositivos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 311/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.1.4** La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos, en el cuadro de texto del centro aparece el nombre de este grupo.
- 4.1.5** La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán.
- 4.1.6** Con ayuda de su profesora o profesor realice la topología de red que se observa en la Figura No. 3 agregando al área de trabajo de Packet Tracer los siguientes dispositivos: 3 routers 1841, 3 switches 2950-24 y 3 PC-PT.
- 4.1.7** Conecte la interfaz FastEthernet 0/0 del Router0 con la interfaz FastEthernet 0/1 del Switch0 y la interfaz FastEthernet 0/2 del Switch0 con la interfaz FastEthernet 0 de la PC.
- 4.1.8** Conecte la interfaz FastEthernet 0/0 del Router1 con la interfaz FastEthernet 0/1 del Switch1 y la interfaz FastEthernet 0/2 del Switch1 con la interfaz FastEthernet 0 de la PC.
- 4.1.9** Conecte la interfaz FastEthernet 0/0 del Router2 con la interfaz FastEthernet 0/1 del Switch2 y la interfaz FastEthernet 0/2 del Switch2 con la interfaz FastEthernet 0 de la PC.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	312/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

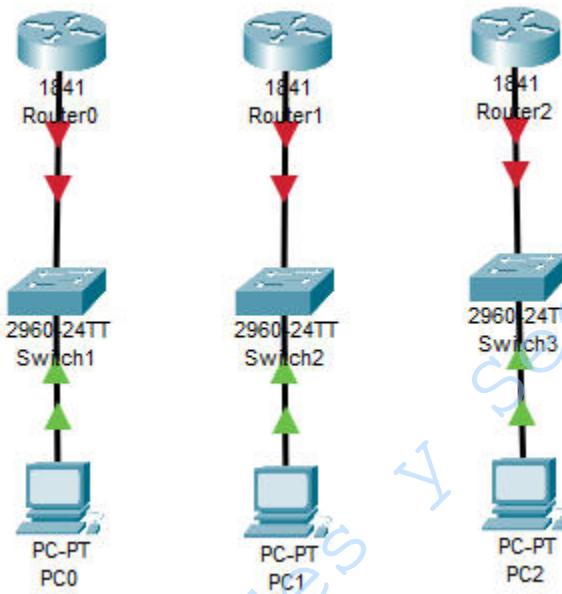


Figura No. 3. Topología de dispositivos.

4.2 Conexión de los routers

- 4.2.1** Dé clic sobre el Router0, seleccione la pestaña Physical, apáguelo y conecte el slot WIC-2T, que sirve para permitir la comunicación serial entre dos dispositivos digitales. Posteriormente vuelva a encenderlo y realice el mismo procedimiento en cada router (Ver Figura No. 4).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 313/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

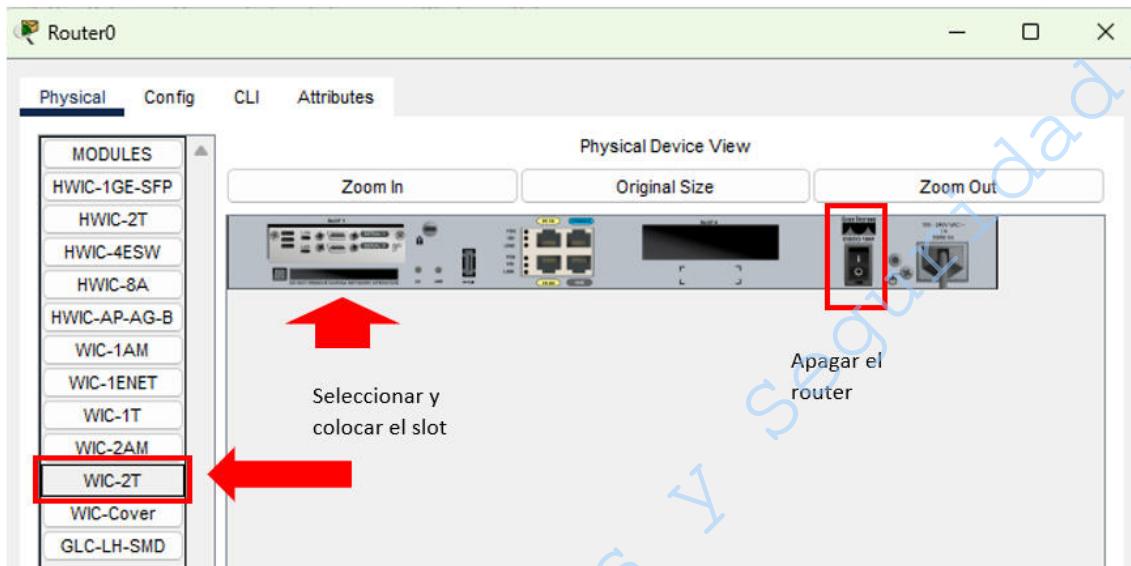


Figura No. 4. Agregar tarjetas seriales al router.

4.2.2 Realice la conexión de los routers para que obtenga la topología que se observa en la Figura No. 5

Consideré:

- a) Conectar la interfaz Serial0/1/0 del Router0 con la interfaz Serial0/1/0 del Router1
- b) Conectar la interfaz Serial0/1/1 del Router1 con la interfaz Serial0/1/0 del Router2

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	314/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

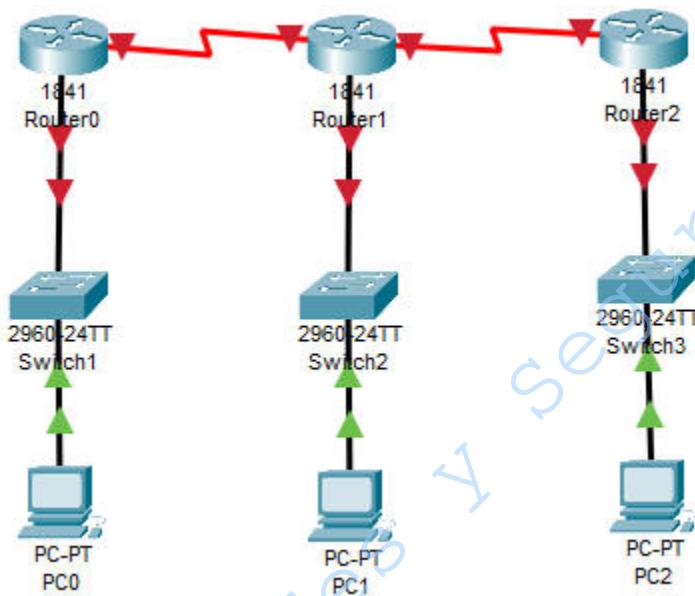


Figura No. 5. Conexión de los routers

4.3 Configuración de las interfaces de los routers

4.3.1 Seleccione el Router0 y d^eclic sobre la pestaña CLI, Cuando aparezca la pregunta **Continue with configuration dialog? [yes/no]:** escriba **no**.

4.3.2 Para configurar la interfaz FastEthernet 0/0 deben teclearse los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
    
```

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la subred GERENCIA

Ante la DIR_IP empleada en este caso _____

4.3.3 Para configurar la interfaz Serial0/1/0 deben teclearse los siguientes comandos:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	315/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

Router(config)#int Serial 0/1/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

```

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la subred Conexión 1

Anote la DIR_IP empleada en este caso_____

4.3.4 Seleccione el Router1 y dé clic sobre la pestaña CLI

4.3.5 Para configurar la interfaz FastEthernet 0/0 deben teclearse los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

```

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la subred SISTEMAS

Anote la DIR_IP empleada en este caso_____

4.3.6 Para configurar la interfaz Serial0/1/0 deben teclearse los siguientes comandos:

```

Router(config)#interface Serial 0/1/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown
Router(config-if)#exit

```

NOTA: DIR_IP se sustituye por la última dirección IP utilizable de la subred Conexión 1

Anote la DIR_IP empleada en este caso_____

4.3.7 Para configurar la interfaz Serial0/1/1 deben teclearse los siguientes comandos:

```

Router(config)#interface Serial 0/1/1
Router(config-if)#ip address DIR_IP 255.255.255.0

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	316/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la subred Conexión 2

Anote la DIR_IP empleada en este caso_____

4.3.8 Seleccione el Router2 y dé clic sobre la pestaña CLI.

4.3.9 Para configurar la interfaz FastEthernet 0/0 deben teclearse los siguientes comandos:

Router>enable
Router#configure t
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la subred ATENCIÓN A CLIENTES

Anote la DIR_IP empleada en este caso_____

4.3.10 Para configurar la interfaz Serial0/1/0 deben teclearse los siguientes comandos:

Router(config)#interface Serial 0/1/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown
Router(config-if)#exit

NOTA: DIR_IP se sustituye por la última dirección IP utilizable de la subred Conexión 2

Anote la DIR_IP empleada en este caso_____

4.4 Configuración de las computadoras

4.4.1 Dé clic sobre la PC conectada al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.4.2 Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	317/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- 4.4.3** Se abrirá una ventana solicitando la dirección IP, máscara de red, el gateway y DNS. Ingrese los datos que se muestran en la Tabla No.1.

Tabla No.1. Datos para la configuración del host.

IP Address	Cualquier dirección utilizable de la subred GERENCIA excepto la primera y la última Anote la dirección IP que emplee _____
Subnet Mask	255.255.255.0
Default Gateway	Dirección IP asignada a la interfaz Fa0/0 del Router0

- 4.4.4** Dé clic sobre la PC conectada al Switch1, en el área de trabajo, con lo que aparecerá la ventana de configuración.

- 4.4.5** Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.

- 4.4.6** Se abrirá una ventana solicitando la dirección IP, máscara de red, el gateway y DNS. Ingrese los datos que se muestran en la Tabla No. 2.

Tabla No.2. Datos para la configuración del host.

IP Address	Cualquier dirección utilizable de la subred SISTEMAS excepto la primera y la última Anote la dirección IP que emplee _____
Subnet Mask	255.255.255.0
Default Gateway	Dirección IP asignada a la interfaz Fa0/0 del Router1

- 4.4.7** Dé clic sobre la PC conectada al Switch3, en el área de trabajo, con lo que aparecerá la ventana de configuración.

- 4.4.8** Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	318/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- 4.4.9** Se abrirá una ventana solicitando la dirección IP, máscara de red, el gateway y DNS. Ingrese los datos que se muestran en la Tabla No.3.

Tabla No.3. Datos para la configuración del host.

IP Address	Cualquier dirección utilizable de la subred ATENCIÓN A CLIENTES excepto la primera y la última Añote la dirección IP que emplee _____
Subnet Mask	255.255.255.0
Default Gateway	Dirección IP asignada a la interfaz Fa0/0 del Router2

4.5 Configuración del enrutamiento estático.

- 4.5.1** Complete la información que se le solicita en la tabla de ruteo con ayuda de su profesora o profesor para realizar el encaminamiento estático (Tabla No. 4).

Tabla No. 4. Encaminamiento Estático

Subred	Dirección IP que representa al segmento de la subred (NETWORK)	Máscara de la subred (NETMASK)	Gateway
GERENCIA			
SISTEMAS			
ATENCIÓN A CLIENTES			

- 4.5.2** Es necesario configurar las rutas estáticas entre el Router0 y el Router1.

- 4.5.3** Seleccione el Router0 y dé clic sobre la pestaña CLI y teclee lo siguiente:

Router>enable

Router#configure terminal

Router(config)# ip route NETWORK NET_MASK NEXT_HOP_ADDRESS

Router(config)#exit

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	319/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Router#copy run start

NOTA 1: Reemplace el parámetro **NETWORK** con el segmento de red con el cual desea tener comunicación (red remota), el parámetro **NET_MASK** corresponde a la máscara de subred de la red remota. El parámetro **NEXT_HOP_ADDRESS** corresponde a la dirección de red de la interfaz del router remoto que está conectado directamente con el router que se está configurando, es decir, la siguiente interfaz con la que se requiere tener comunicación y que no está en el router que se está configurando.

NOTA 2: Cuando parezca la leyenda **Destination filename [startup-config]**? Solamente oprima enter

4.5.4 Seleccione el Router1 y dé clic sobre la pestaña CLI y teclee lo siguiente:

```
Router#configure terminal
Router(config)# ip route NETWORK NET_MASK NEXT_HOP_ADDRESS
Router(config)#exit
Router#copy run start
```

NOTA 1: Reemplace el parámetro **NETWORK** con el segmento de red con el cual desea tener comunicación (red remota), el parámetro **NET_MASK** corresponde a la máscara de subred de la red remota. El parámetro **NEXT_HOP_ADDRESS** corresponde a la dirección de red de la interfaz del router remoto que está conectado directamente con el router que se está configurando, es decir, la siguiente interfaz con la que se requiere tener comunicación y que no está en el router que se está configurando.

NOTA 2: Cuando parezca la leyenda **Destination filename [startup-config]**? Solamente oprima enter

4.5.5 Deberá repetir los pasos 4.5.3 y 4.5.4 para configurar las rutas estáticas entre el Router1 y el Router2 y entre el Router0 y el Router2, recuerde seleccionar el router correspondiente que va a configurar.

Escriba los comandos que tecleó en cada caso:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	320/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.5.6** Explique para qué sirve el comando copy run start y desde el punto de vista de seguridad qué beneficios trae ejecutarlo.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	321/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.6 Pruebas y aplicaciones

4.6.1 Seleccione una PDU como se observa en la Figura No. 6



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	322/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

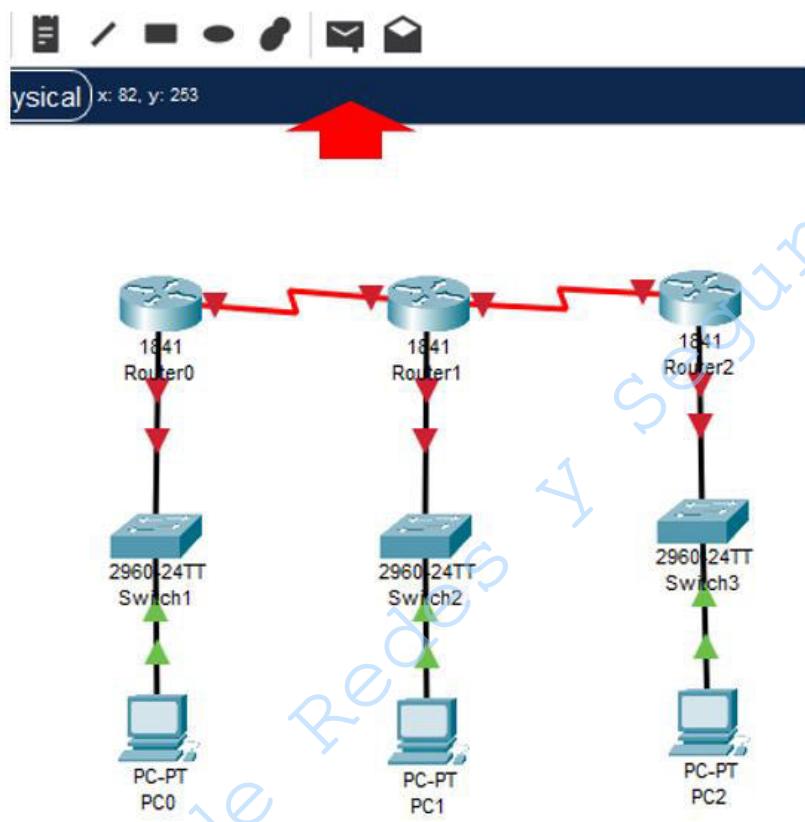


Figura No. 6. Pruebas

4.6.2 Dé clic sobre la PC1 y posteriormente sobre la PC2

4.6.3 ¿Se logró establecer la comunicación? Explique.

4.6.4 Dé clic sobre la PC2 y posteriormente sobre la PC3

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	323/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

4.6.5 ¿Se logró establecer la comunicación? Explique.

4.6.6 Dé clic sobre la PC1 y posteriormente sobre la PC3

4.6.7 ¿Se logró establecer la comunicación? Explique.

4.6.8 ¿Cómo se realizarían las pruebas haciendo uso del comando ping?

5.- Cuestionario

1. ¿Por qué es importante prestar atención al momento de establecer las direcciones IP en las interfaces del router?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	324/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

2. Para que la configuración de cada router sea más segura, indique qué consideraciones deben hacerse.

3. De los tipos de contraseñas que existen en el router, explique para qué sirve cada una e indique con base en su criterio cuál proporciona mayor seguridad. Justifique su respuesta.

4. En caso de que algún router pierda conexión con el resto de la topología ¿cómo lo resolvería?

5. Investigue los métodos de seguridad que serían convenientes utilizar en la topología de red que está empleando

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	325/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	326/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 7

Enrutamiento estático

Cuestionario Previo

1. Defina dirección IP.
2. Defina qué es una subred.
3. Investigue qué es un segmento de red.
4. Investigue qué es una máscara de red.
5. ¿Qué es un rango de direcciones IP y qué es un rango de direcciones IP utilizables?
6. Investigue cómo se configuran las tablas de ruteo de manera estática.
7. Investigue el parámetro ***NEXT_HOP_ADDRESS*** y cómo se utiliza.
8. Para qué sirve el comando ***show ip route***.
9. Investigue cuáles son los comandos que se utilizan para poner contraseñas en el router.
10. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	327/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 8

HSRP – Hot Standby Router Protocol

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 328/479 8.3 11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivos de aprendizaje

- El alumno o la alumna comprenderá qué es y cómo se aplica el protocolo HSRP (Hot Standby Router Protocol).

2.- Conceptos teóricos

HSRP (Hot Standby Router Protocol) es un protocolo exclusivo de Cisco que está diseñado para permitir la conmutación por falla de un dispositivo. HSRP se utiliza en un grupo de routers para seleccionar un dispositivo activo y uno de reserva. El dispositivo activo es aquel que encamina los paquetes, mientras que el dispositivo de reserva o en Standby, es el cual entra en acción y toma el control cuando el dispositivo activo llega a fallar.

La función principal del router de reserva en HSRP, es supervisar el estado operativo del grupo y en cuanto detecte que el router activo falla, asumir de forma rápida la responsabilidad del reenvío de paquetes.

El rol de router activo se asigna de manera determinada al router que posea la dirección IP numéricamente más alta. Sin embargo, lo correcto es asignarle una prioridad a cada uno de los dispositivos y así, el router activo se elegirá a partir de dicha prioridad. Los rangos de prioridades van desde 0 hasta 255, siendo 100 la prioridad determinada para cada dispositivo.

Una vez que un router activo falla y lo reemplaza el router de reserva, este último será el nuevo router activo y seguirá siéndolo incluso si otro router con una prioridad HSRP más alta está disponible. Para poder forzar que el router activo cambie al estar disponible uno de mayor prioridad, se debe hacer uso del comando *standby preempt*.

Para entender mejor el funcionamiento de HSRP, se presenta un ejemplo a partir de la siguiente topología (Figura No. 1):



Figura No. 1 Ejemplo de un grupo HSRP.

Se define un grupo que contiene dos routers: R1 y R2. El R1 se configuró con una prioridad de 150, mientras que el R2 se dejó con la prioridad por defecto (es decir, 100) y se habilitó el comando *standby preempt* en el R1. Por lo cual, como el R1 tiene la prioridad más alta del grupo, este será el router activo y el R2 será el de reserva.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	329/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Cuando ocurre un corte de energía, este solamente afecta al R1 y ya no está disponible, entonces el R2 asume el rol de router activo. Una vez que se restaura la energía, el R1 vuelve a estar en línea y, debido a que el R1 tiene prioridad más alta y fue activado el comando *standby preempt*, se cambiará el router activo para que el R1 cumpla con este rol.

3.- Equipo y material necesario

Equipo del laboratorio:

- Computadora con Cisco Packet Tracer.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Creación de topología para el uso del protocolo HSRP.

- 4.1.1 Encienda el sistema y elija la opción de cargar Windows.
- 4.1.2 Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3 Ejecute la aplicación Cisco Packet Tracer (Figura No. 2).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 330/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 2. Simulador de CISCO Packet Tracer.

- 4.1.4** Dé clic en la sección de Dispositivos de red, después seleccione el apartado de switches, ubique el modelo 2960 IOS15, arrastre una instancia del switch. Haga clic en la sección Carpeta Miscellaneous, ubique el modelo 1841 WIC-2T, arrastre tres instancias del router y conéctelos como se observa en la Figura No. 3.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 331/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

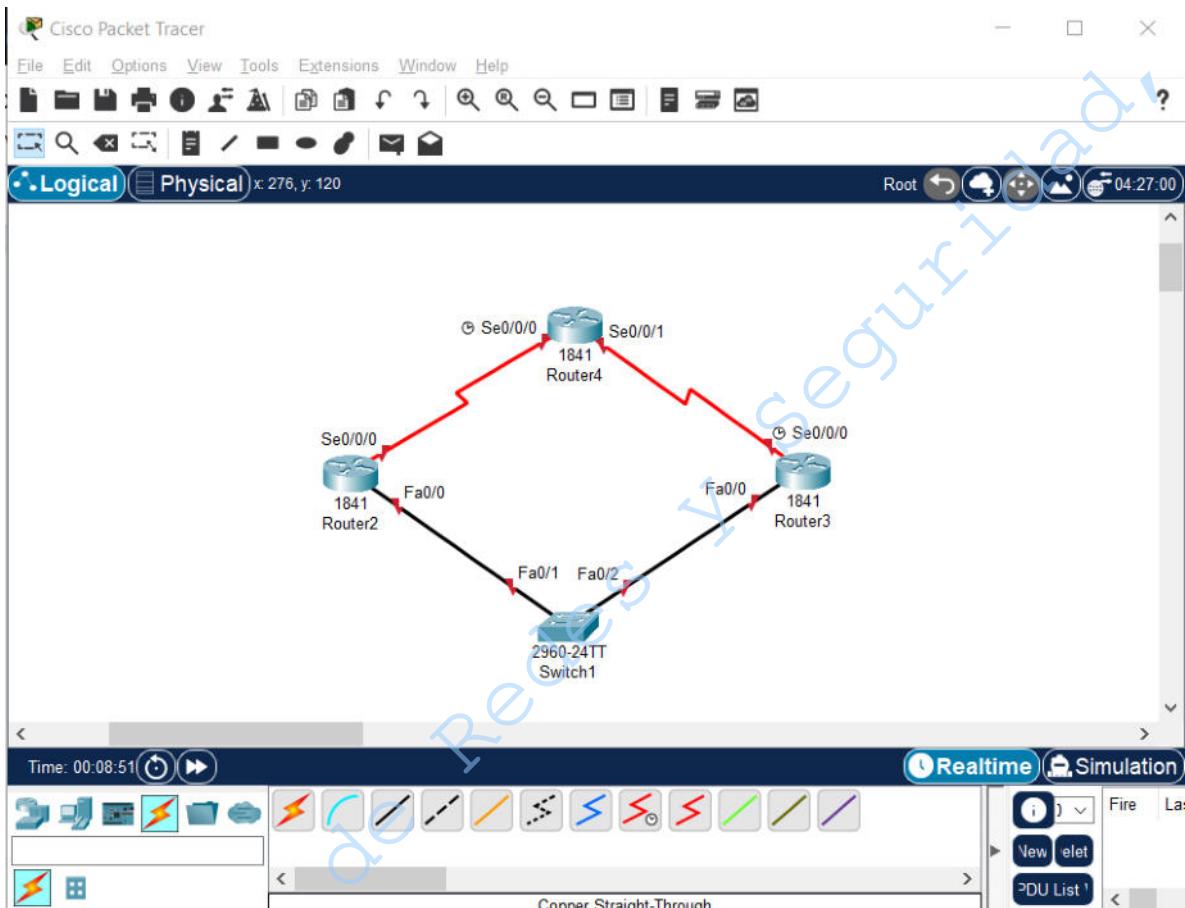


Figura No. 3. Topología para configurar HSRP

4.1.5 Para una mejor comprensión visual, cambie el nombre de los routers, de tal forma que queden como en la Figura No. 4.

NOTA: También se agregaron etiquetas con direcciones IP, estas direcciones serán las que tengan las interfaces de los routers.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 332/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

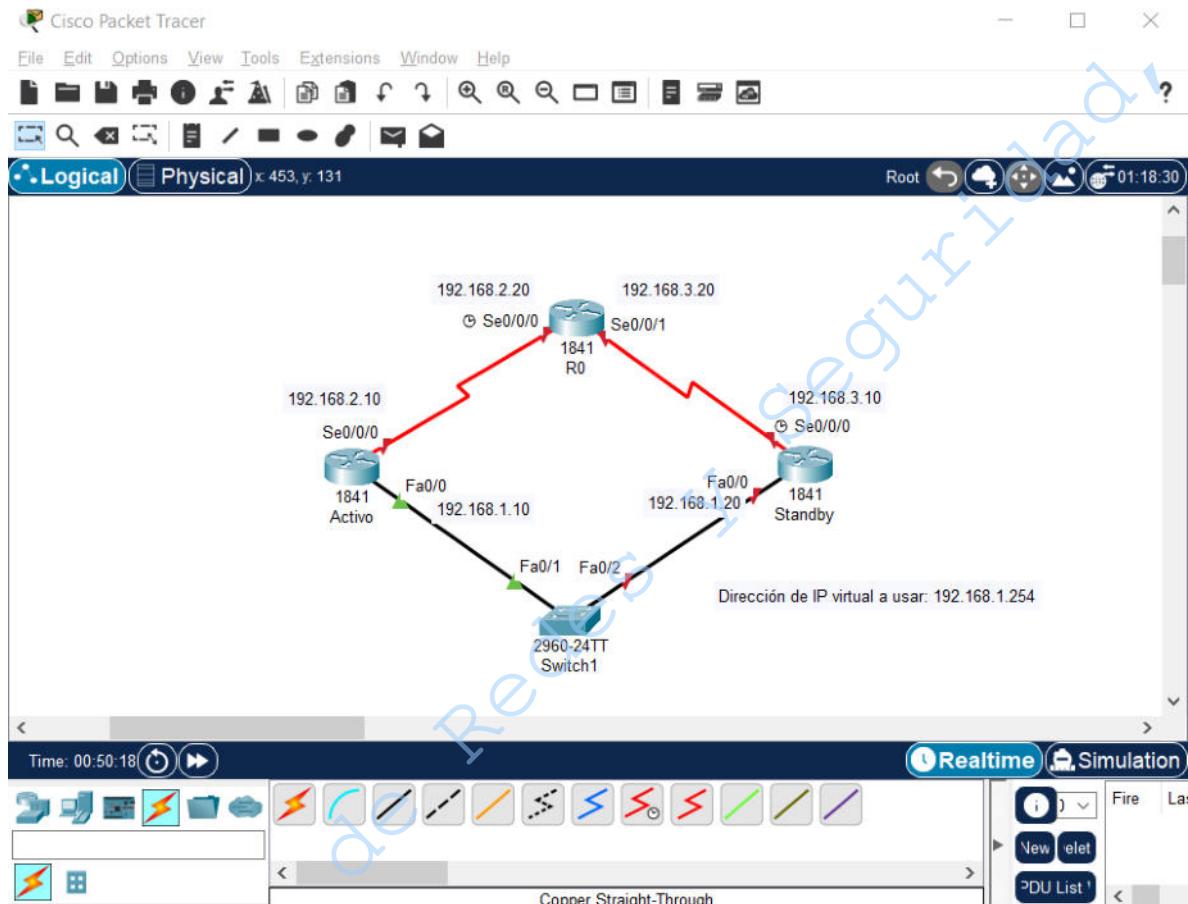


Figura No. 4. Topología para configurar HSRP con identificadores

4.2 Configuración de la topología

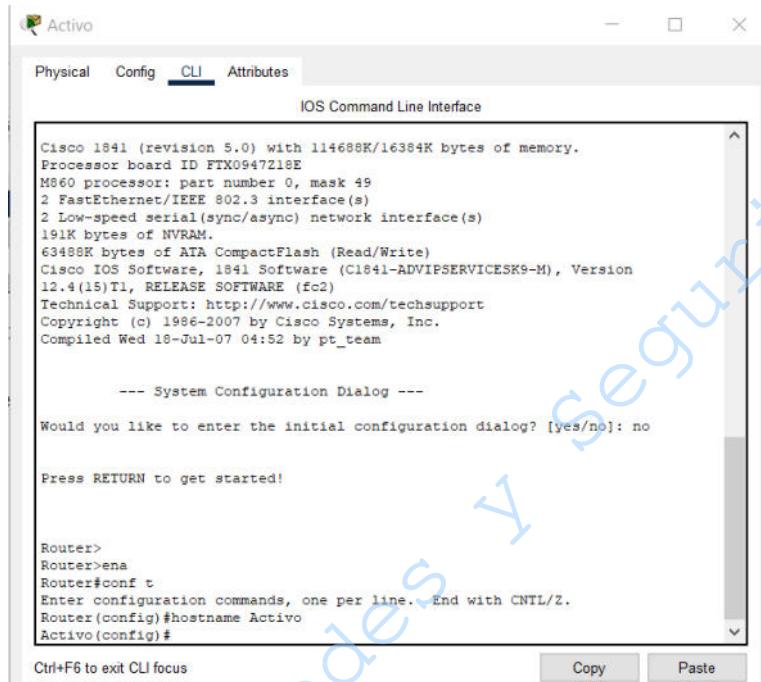
4.2.1 Ingrese a la consola CLI del router activo, cambie el hostname por el de **Activo** (Figura No. 5).

```

Router>enable
Router#configure terminal
Router(config)#hostname Activo

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 333/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
Router#ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Activo
Activo(config)#

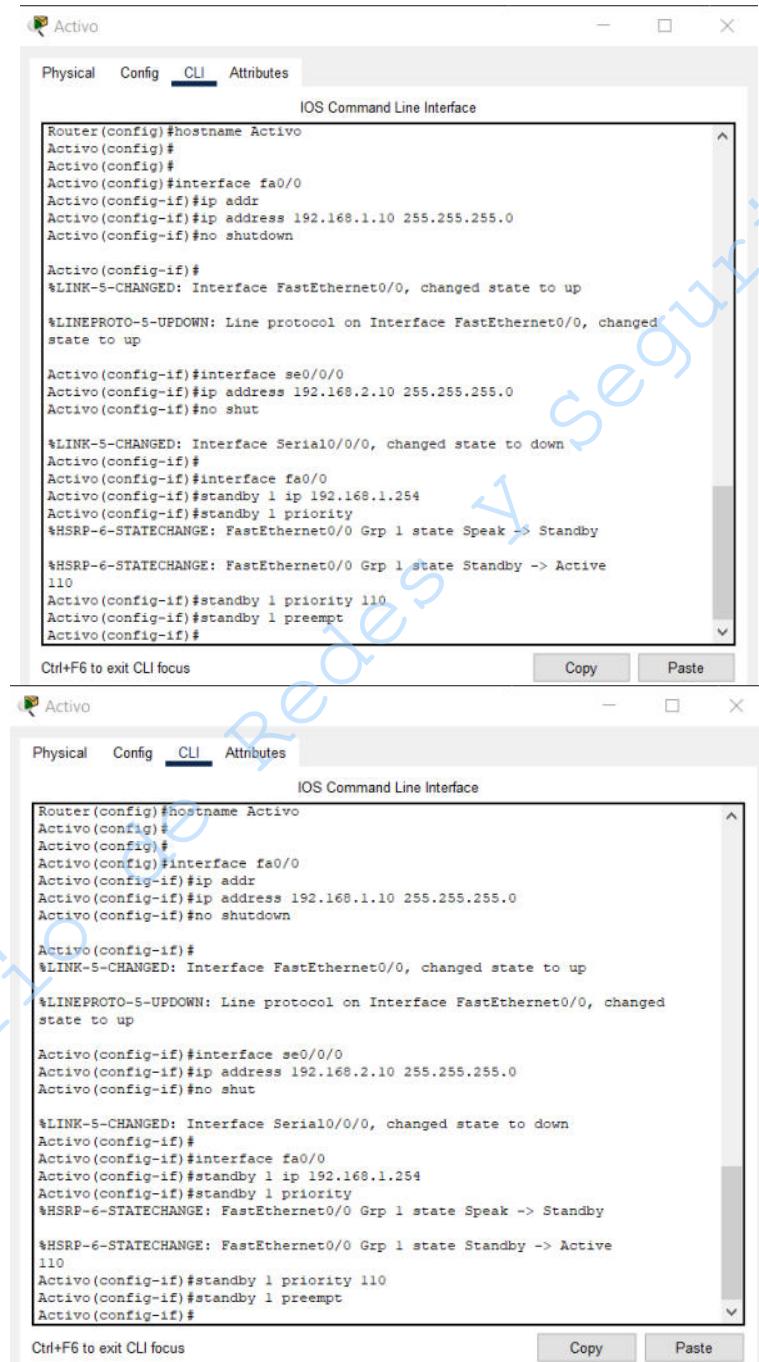
```

Figura No. 5. Cambio de hostname al router Activo

- 4.2.2** Configure las interfaces del router Activo, de forma que las direcciones IP de esas interfaces correspondan con la Figura No. 6.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 334/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

Laboratorio de Redes y Seguridad



```

Router(config)#hostname Activo
Activo(config)#
Activo(config)#
Activo(config)#interface fa0/0
Activo(config-if)#ip addr
Activo(config-if)#ip address 192.168.1.10 255.255.255.0
Activo(config-if)#no shutdown

Activo(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Activo(config-if)#interface se0/0/0
Activo(config-if)#ip address 192.168.2.10 255.255.255.0
Activo(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Activo(config-if)#
Activo(config-if)#interface fa0/0
Activo(config-if)#standby 1 ip 192.168.1.254
Activo(config-if)#standby 1 priority
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
110
Activo(config-if)#standby 1 priority 110
Activo(config-if)#standby 1 preempt
Activo(config-if)#

```

Ctrl+F6 to exit CLI focus Copy Paste


```

Router(config)#hostname Activo
Activo(config)#
Activo(config)#
Activo(config)#interface fa0/0
Activo(config-if)#ip addr
Activo(config-if)#ip address 192.168.1.10 255.255.255.0
Activo(config-if)#no shutdown

Activo(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Activo(config-if)#interface se0/0/0
Activo(config-if)#ip address 192.168.2.10 255.255.255.0
Activo(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Activo(config-if)#
Activo(config-if)#interface fa0/0
Activo(config-if)#standby 1 ip 192.168.1.254
Activo(config-if)#standby 1 priority
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
110
Activo(config-if)#standby 1 priority 110
Activo(config-if)#standby 1 preempt
Activo(config-if)#

```

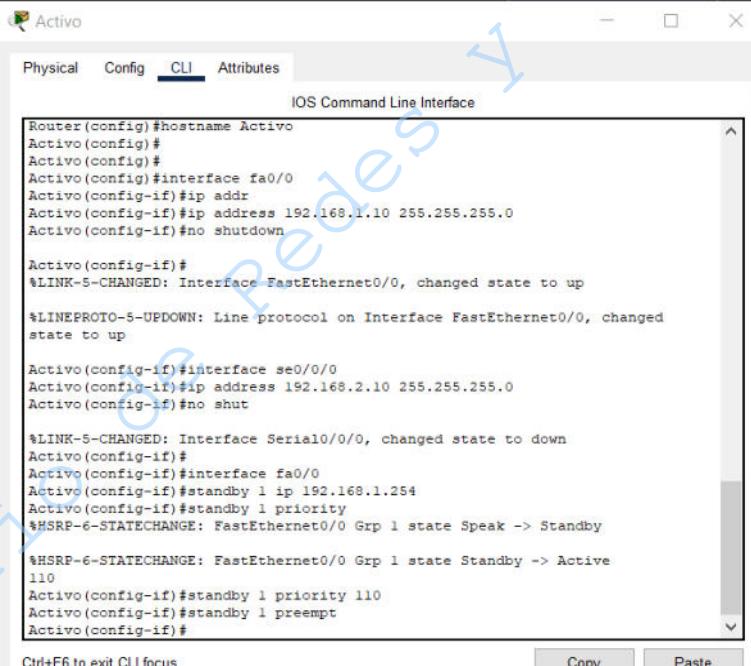
Ctrl+F6 to exit CLI focus Copy Paste

Figura No. 6. Configuración de los puertos del router Activo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 335/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.3 En la Figura No. 7 puede observar la configuración de los puertos del router Activo, así como también la configuración del protocolo HSRP:

- **standby 1 ip 192.168.1.254:** Este comando indica que el router Activo está en el grupo standby 1 y que la IP virtual que tendrá este puerto será la 192.168.1.254.
- **standby 1 priority 110:** Este comando indica la prioridad que tendrá el router, en este caso tiene una prioridad de 110. Al ser el router Activo, debe tener la prioridad más alta del grupo standby 1.
- **standby 1 preempt:** Este comando indica que este router tendrá la configuración Preempt.



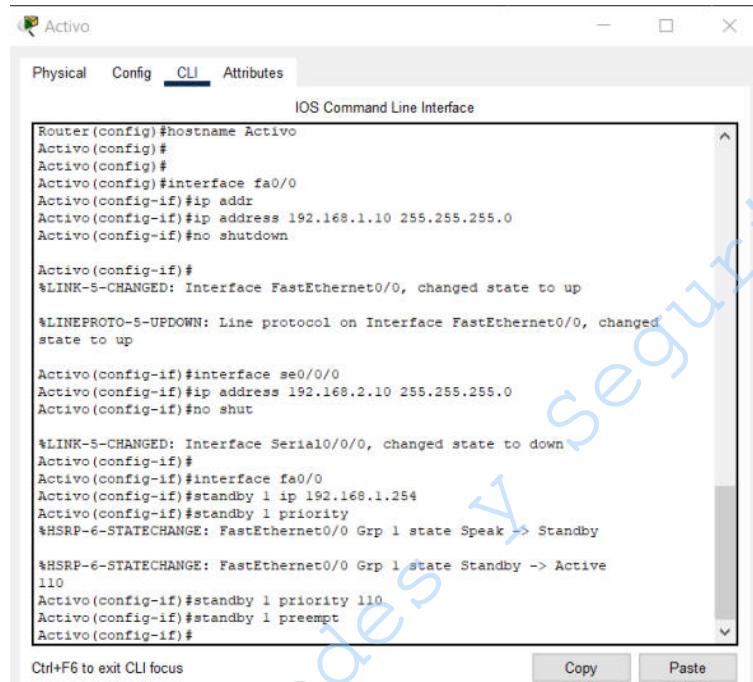
```

Activo
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#hostname Activo
Activo(config)#
Activo(config)#
Activo(config)#interface fa0/0
Activo(config-if)#ip addr
Activo(config-if)#ip address 192.168.1.10 255.255.255.0
Activo(config-if)#no shutdown
Activo(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Activo(config-if)#interface se0/0/0
Activo(config-if)#ip address 192.168.2.10 255.255.255.0
Activo(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Activo(config-if)#
Activo(config-if)#interface fa0/0
Activo(config-if)#standby 1 ip 192.168.1.254
Activo(config-if)#standby 1 priority
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
110
Activo(config-if)#standby 1 priority 110
Activo(config-if)#standby 1 preempt
Activo(config-if)#

```

Ctrl+F6 to exit CLI focus Copy Paste

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 336/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

Activo
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#hostname Activo
Activo(config)#
Activo(config)#
Activo(config)#interface fa0/0
Activo(config-if)#ip addr
Activo(config-if)#ip address 192.168.1.10 255.255.255.0
Activo(config-if)#no shutdown

Activo(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Activo(config-if)#interface se0/0/0
Activo(config-if)#ip address 192.168.2.10 255.255.255.0
Activo(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Activo(config-if)#
Activo(config-if)#interface fa0/0
Activo(config-if)#standby 1 ip 192.168.1.254
Activo(config-if)#standby 1 priority
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
110
Activo(config-if)#standby 1 priority 110
Activo(config-if)#standby 1 preempt
Activo(config-if)#
Ctrl+F6 to exit CLI focus
Copy Paste

```

Figura No. 7. Configuración del Standby

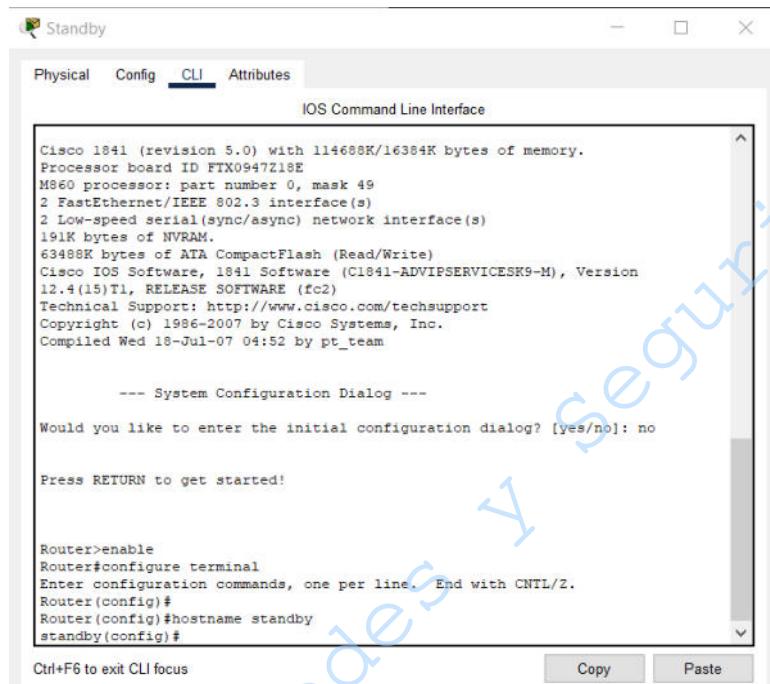
4.2.4 Ingrese a la consola del router Standby, cambie el hostname por el de **Standby**, mediante los siguientes comandos (Figura No. 8):

```

Router>enable
Router#configure terminal
Router(config)#hostname standby

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	337/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				



The screenshot shows a Windows command-line window titled "Standby". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the title "IOS Command Line Interface". The main area displays the following text:

```

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63408K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#hostname standby
standby(config)#

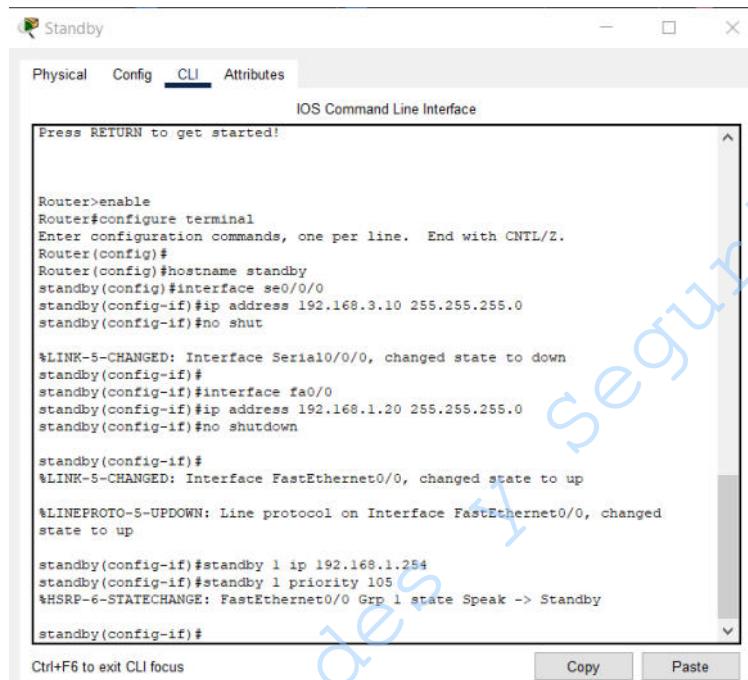
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

Figura No. 8. Cambio de hostname al router Standby

- 4.2.5 Configure las interfaces del router Standby, de forma que las direcciones IP de esas interfaces correspondan con la Figura No. 9.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 338/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

Standby

Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#hostname standby
standby(config)#interface se0/0/0
standby(config-if)#ip address 192.168.3.10 255.255.255.0
standby(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
standby(config-if)#
standby(config-if)#interface fa0/0
standby(config-if)#ip address 192.168.1.20 255.255.255.0
standby(config-if)#no shutdown

standby(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

standby(config-if)#standby 1 ip 192.168.1.254
standby(config-if)#standby 1 priority 105
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

standby(config-if)#

```

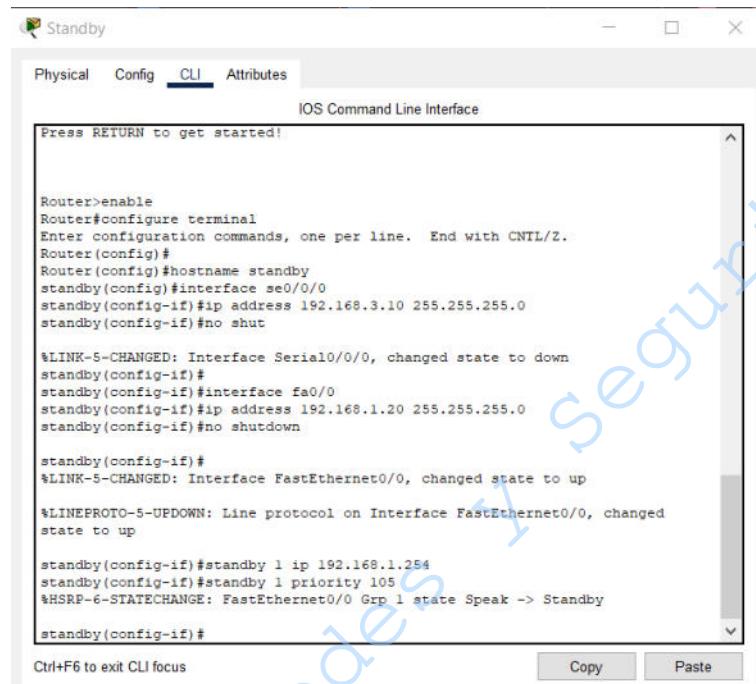
Ctrl+F6 to exit CLI focus Copy Paste

Figura No. 9. Configuración de los puertos del router Standby

4.2.6 En la Figura No. 10 puede observar la configuración de los puertos del router Standby, así como también la configuración del protocolo HSRP:

- **standby 1 ip 192.168.1.254:** Este comando indica que el router Standby está en el grupo standby 1 y que la IP virtual que tendrá este puerto será la 192.168.1.254.
- **standby 1 priority 105:** Este comando indica la prioridad que tendrá el router, en este caso tiene una prioridad de 105. Al ser un router Standby, debe tener una prioridad más baja a la del router Activo del grupo Standby 1.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 339/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



La captura de pantalla muestra la interfaz de línea de comandos (CLI) de Cisco IOS. La barra superior tiene pestañas para 'Physical', 'Config', 'CLI' (que está resaltada) y 'Attributes'. El título de la ventana es 'Standby'. El área central muestra el historial de comandos ejecutados:

```

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#hostname standby
standby(config)#interface se0/0/0
standby(config-if)#ip address 192.168.3.10 255.255.255.0
standby(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
standby(config-if)#
standby(config-if)#interface fa0/0
standby(config-if)#ip address 192.168.1.20 255.255.255.0
standby(config-if)#no shutdown

standby(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

standby(config-if)#standby 1 ip 192.168.1.254
standby(config-if)#standby 1 priority 105
%HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby

standby(config-if)#

```

En la parte inferior de la ventana, hay botones 'Copy' y 'Paste'.

Figura 10. Configuración del Standby

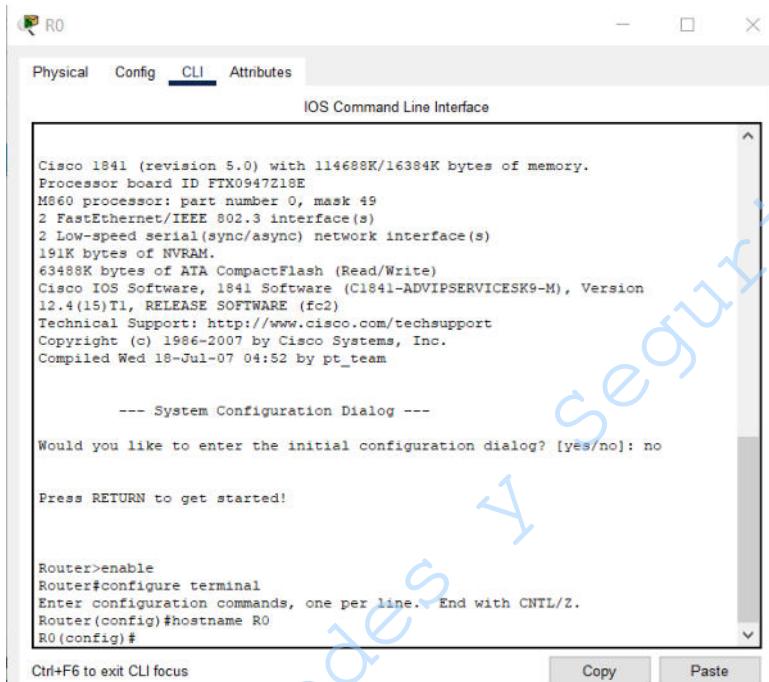
- 4.2.7** Ingrese a la consola del router R0, cambie el hostname por el de **R0**, mediante los siguientes comandos (Figura No. 11):

```

Router>enable
Router#configure terminal
Router(config)#hostname R0

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 340/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



IOS Command Line Interface

```

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947218E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

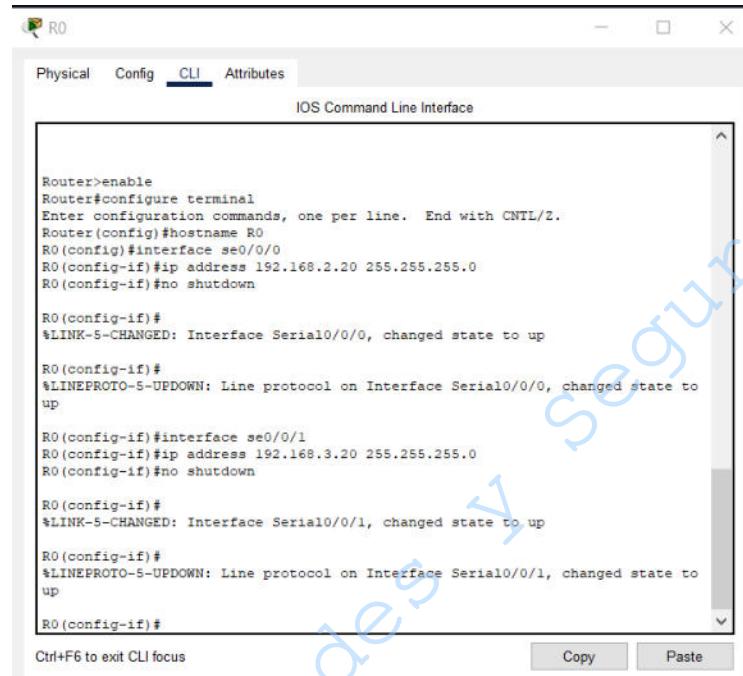
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R0
R0(config)#

```

Figura No. 11. Cambio de hostname al router R0

- 4.2.8** Configure las interfaces del router R0, de forma que las direcciones IP de esas interfaces correspondan con la Figura No. 12.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 341/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R0
R0(config)#interface se0/0/0
R0(config-if)#ip address 192.168.2.20 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#
\$LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R0(config-if)#
\$LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R0(config-if)#interface se0/0/1
R0(config-if)#ip address 192.168.3.20 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#
\$LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
R0(config-if)#
\$LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R0(config-if)#

Figura No. 12. Configuración de los puertos del router R0

- 4.2.9** Realice el proceso de enrutamiento de los tres routers de la topología (Activo, Standby y R0). Se recomienda utilizar el protocolo RIPv2, el cual, para el Router Activo, se configura utilizando los siguientes comandos en el modo de configuración global:

```

Activo(config-if)# exit
Activo(config)# router rip
Activo(config-router)# version 2
Activo(config-router)# network ID_SUBRED

```

NOTA: El parámetro ID_SUBRED se debe reemplazar por el ID de la subred correspondiente que se encuentre conectada al router que se está configurando. También es importante que indique todas y cada una de las subredes conectadas directamente empleando un comando *network* por cada subred.

Para esta práctica, los ID de subredes tienen el siguiente formato: 192.168.X.0. Donde X puede tomar el valor de 1, 2 o 3, según el caso.

- 4.2.10** Una vez que haya realizado el enrutamiento en cada uno de los routers de la topología, debe de realizar una prueba de conexión entre el router R0 y la IP virtual de gateway

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	342/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

del grupo HSRP (192.168.1.254), esta prueba de conexión se debe de realizar en la terminal CLI mediante el comando *ping* (Figura No. 13):

```
R0(config-router)#end
R0#ping 192.168.1.254
```

```
R0>enable
R0#ping 192.168.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/13/16 ms
```

Figura No. 13. Ping a la IP virtual

Si el resultado del *ping* es parecido al de la figura 13, significa que se realizó el enrutamiento de forma correcta y puede continuar.

4.2.11 Ejecute, en el router Activo los siguientes comandos (Figura No. 14):

```
Activo(config-router)#end
Activo#show standby

Activo#show standby
FastEthernet0/0 - Group 1
  State is Active
    5 state changes, last state change 00:45:55
    Virtual IP address is 192.168.1.254
    Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 1.261 secs
    Preemption enabled
    Active router is local
    Standby router is 192.168.1.20
    Priority 110 (configured 110)
    Group name is hsrp-Fa0/0-1 (default)
```

Figura No. 14. Comando show standby en el router Activo

4.2.12 Ahora, en el router Standby, ejecute los siguientes comandos (Figura No. 15):

```
standby(config-router)#end
standby#show standby
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	343/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

standby#show standby
FastEthernet0/0 - Group 1
  State is Standby
    6 state changes, last state change 01:28:56
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.681 secs
  Preemption disabled
  Active router is 192.168.1.10
  Standby router is local
  Priority 105 (configured 105)
  Group name is hsrp-Fa0/0-1 (default)

```

Figura No. 15. Comando show standby en el router Standby

- 4.2.13** Escriba las diferencias que encuentra entre lo mostrado al ejecutar el comando en el router Activo y el router Standby
-
-
-
-
-

4.3 Comando traceroute

- 4.3.1** Dé clic en la sección de dispositivos finales y arrastre una instancia de una PC. Haga clic en el apartado de connections, ubique el cable directo y conecte la computadora al switch 1 con este a través de la interfaz fa0/3 (Figura No. 16).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 344/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

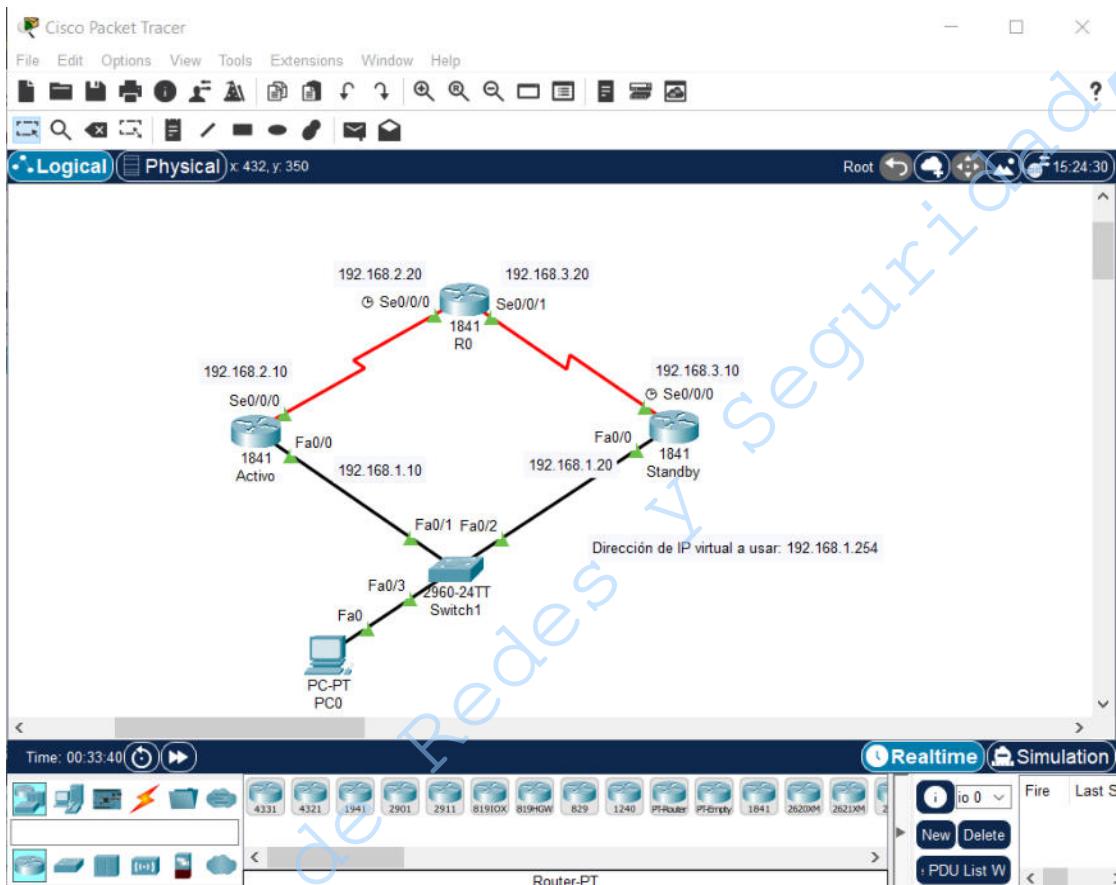


Figura 16. Topología para ocupar el comando tracert.

4.3.2 Asigne una dirección IP y Máscara de subred a la PC0, complete la Tabla No. 1 de acuerdo a la información ingresada. Ingrese todos los valores de la tabla en la configuración de IP de la PC0.

NOTA: La dirección IP debe de ser del segmento 192.168.1.0/24.

Tabla 1. Información de las tarjetas de red

	PC0
IPv4	
Máscara de subred	
Gateway	192.168.1.254

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	345/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

DNS	0.0.0.0
-----	---------

- 4.3.3** Dé clic en la computadora PC0, ingrese a la pestaña Desktop y haga clic en el ícono que dice *Command Prompt* (Figura No. 17):

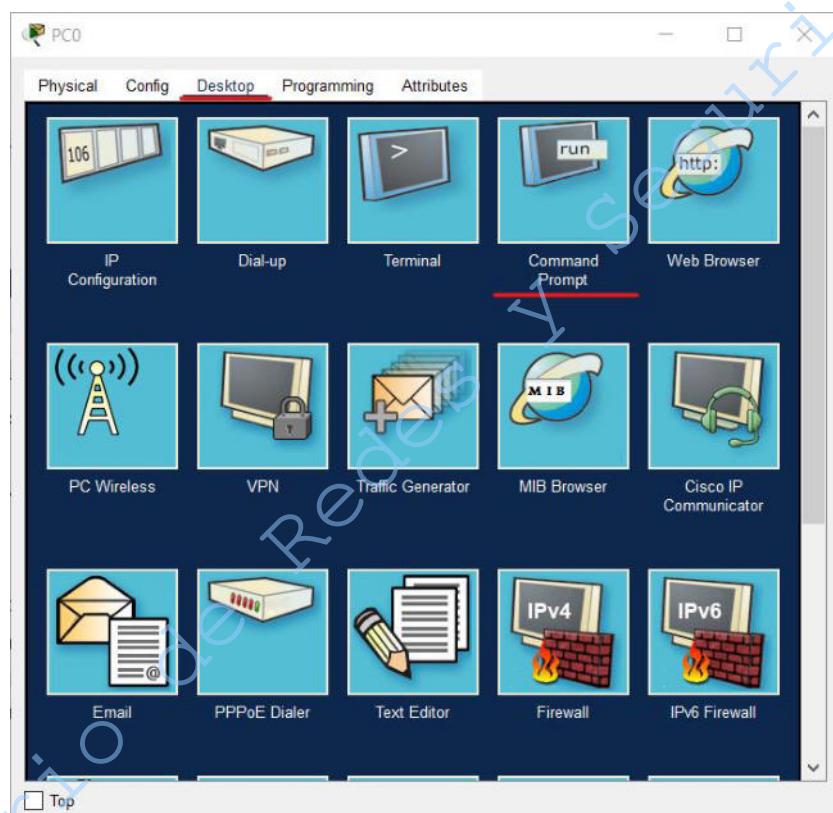


Figura No. 17. Íconos de la pestaña Desktop de la PC0.

- 4.3.4** Dentro del *Command Prompt*, ingrese el siguiente comando (Figura No. 18):

C:\> ping 192.168.1.254

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	346/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```
C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura No. 18. Comando ping a la IP virtual

4.3.5 Dentro del mismo *Command Prompt*, ingrese ahora el siguiente comando:

C:\> tracert 192.168.3.20

Escriba a continuación la ruta que toman los paquetes:

4.3.6 Abra el Router Activo, ingrese a la terminal CLI e ingrese los siguientes comandos para que al apagar el Router, quede guardada la configuración (Figura No. 19):

**Activo>enable
Activo#wr**

```
Activo>enable
Activo#wr
Building configuration...
[OK]
```

Figura No. 19. Guardado configuración

4.3.7 Diríjase al apartado físico del Router Activo, ubique el botón de Encendido/Apagado y proceda a apagar el equipo (Figura No. 20).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 347/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

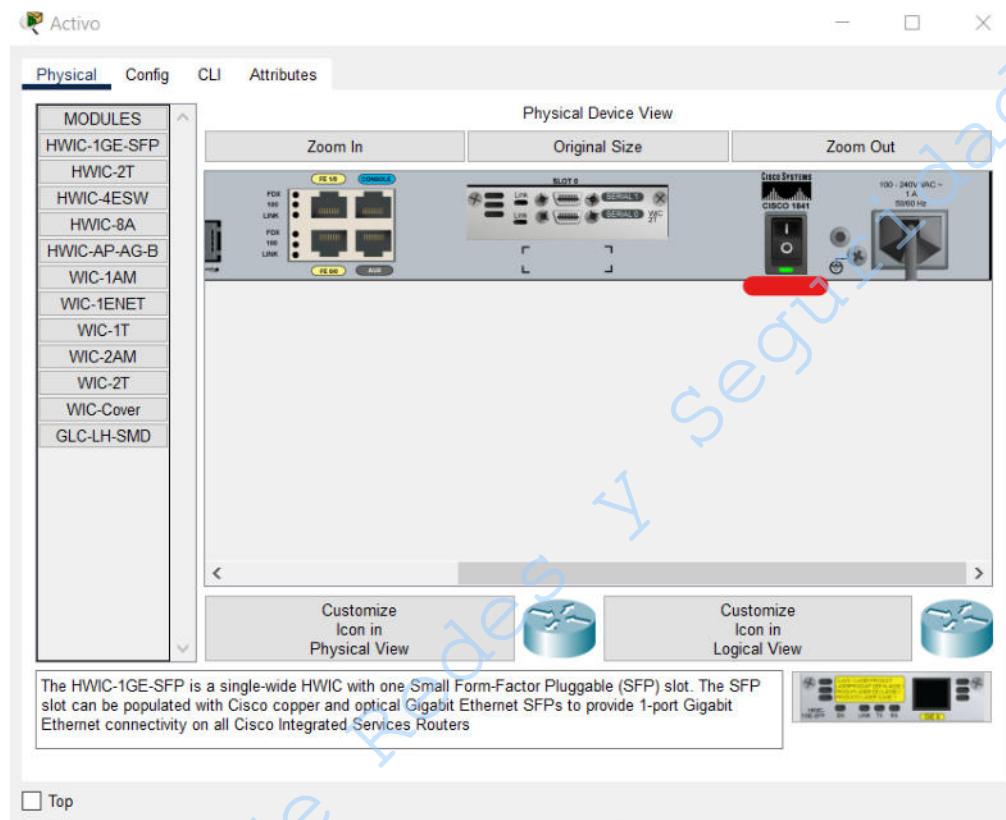


Figura No. 20. Botón de encendido/apagado

- 4.3.8** Una vez apagado el Router Activo, entre a la consola CLI del Router Standby y escriba a continuación qué mensaje aparece, así como su significado:

- 4.3.9** Dé clic en la computadora PC0, ingrese a la pestaña Desktop y haga clic en el ícono que dice *Command Prompt* (Figura No. 21).

- 4.3.10** Dentro del *Command Prompt*, ingrese el siguiente comando:

C:\> tracert 192.168.3.20

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	348/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

```
C:\>tracert 192.168.3.20
Tracing route to 192.168.3.20 over a maximum of 30 hops:
 1  0 ms      0 ms      0 ms      192.168.1.20
 2  3 ms      3 ms      3 ms      192.168.3.20
Trace complete.
```

Figura 21. Comando tracert

Escriba a continuación la ruta que toman los paquetes y justifique porqué sucede eso:

4.3.11 Diríjase al apartado físico del Router Activo, ubique el botón de Encendido/Apagado y proceda a prender el equipo.

4.3.12 Una vez prendido el Router Activo, entre a la consola CLI del mismo Router, espere unos segundos a que termine de encender el equipo y escriba a continuación qué mensaje aparece, así como su significado:

4.3.13 Dé clic en la computadora PC0, ingrese a la pestaña Desktop y haga clic en el ícono que dice *Command Prompt*.

4.3.14 Dentro del *Command Prompt*, ingrese el siguiente comando (Figura No. 22):

C:\> tracert 192.168.3.20

```
C:\>tracert 192.168.3.20
Tracing route to 192.168.3.20 over a maximum of 30 hops:
 1  0 ms      0 ms      0 ms      192.168.1.10
 2  *         *         0 ms      192.168.3.20
```

Figura 22. Comando tracert

Escriba a continuación la ruta que toman ahora los paquetes y justifique porqué sucede eso:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	349/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	350/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 8

HSRP – Hot Standby Router Protocol

Cuestionario Previo

1. ¿Qué es y para qué sirve el protocolo FHRP?
2. ¿Qué es y para qué sirve el protocolo HSRP?
3. ¿Cuál es la relación entre el protocolo FHRP y HSRP?
4. Explique para qué sirve el comando standby X preempt.
5. Explique para qué sirve el comando tracert ip.
6. ¿Cuál es la diferencia entre el comando tracert y el comando PING?
7. ¿Cuáles son las ventajas de implementar el protocolo HSRP?
8. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 351/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 9

Uso de protocolos TCP y UDP

Capa 4 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	352/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

1.- Objetivos de aprendizaje

- El alumno o la alumna aprenderá a hacer una conexión entre routers y switches, mediante los protocolos SSH y Telnet.
- El alumno o la alumna aprenderá cómo usar el protocolo FTP, Syslog y NTP.

2.- Conceptos teóricos

Las Telnet proviene del acrónimo Telecommunication Network y es básicamente un protocolo TCP/IP utilizado desde 1960 para poder establecer conexiones remotas con otras computadoras, servidores y dispositivos conectados a la red. Para lograr esta conexión remota se utiliza el puerto 23.

Actualmente, el uso de Telnet está limitado únicamente a redes internas aisladas de las redes exteriores, debido a que Telnet tiene el gran problema de que la información desde un extremo a otro viaja sin ningún tipo de cifrado; es decir, viaja como texto plano y esto corresponde a una brecha de seguridad enorme.

El protocolo SSH (Secure Shell) permite a los usuarios controlar y modificar dispositivos de forma remota a través de la red y un mecanismo de autenticación. Este protocolo se creó como un reemplazo seguro para Telnet de forma que se utilicen técnicas criptográficas para poder garantizar que todas las comunicaciones hacia y desde el dispositivo remoto no puedan ser vistas en claro fácilmente.

Por otro lado, el protocolo FTP (File Transfer Protocol - Protocolo de Transferencia de Archivos), se trata de un protocolo que permite transferir archivos desde un dispositivo a otro y ha estado vigente desde abril de 1971. Funciona conectando ambas computadoras a la misma red y así los archivos pueden compartirse de forma directa y sin intermediario. Sin embargo, al igual que en Telnet, la información no viaja cifrada y constituye una vulnerabilidad importante.

Ahora bien, existe el protocolo de Registro de Sistema (Syslog), el cual es una forma en la que los dispositivos de red pueden utilizar un mensaje estándar para poder comunicarse con un servidor de registro. Los mensajes de registro incluyen varios parámetros, dentro de los que destacan:

- Marca de tiempo.
- Clasificación de gravedad.
- ID de dispositivo.
- Dirección IP del dispositivo.
- Descripción breve de lo ocurrido.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	353/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Finalmente, el protocolo NTP significa Network Time Protocol (Protocolo de Tiempo de Red) y fue publicado en septiembre de 1985. Este protocolo se describe como un protocolo para poder sincronizar varios relojes de una red, a través del uso de un conjunto de clientes y servidores repartidos. Utiliza el puerto 123 para poder establecer la comunicación; es decir, ocupa el protocolo UDP.

NTP proporciona mecanismos para poder sincronizar los relojes de diferentes sistemas con una precisión incluso de nanosegundos y contiene también indicaciones para especificar la precisión y las posibles fuentes de error del reloj del sistema local.

3.- Equipo y material necesario

Equipo del laboratorio:

- Software de Simulación Cisco Packet Tracer.

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Creación de topología para el uso de los protocolos.

- 4.1.1 Encienda el sistema y elija la opción de cargar Windows.
- 4.1.2 Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3 Ejecute la aplicación Cisco Packet Tracer (Ver Figura No. 1).



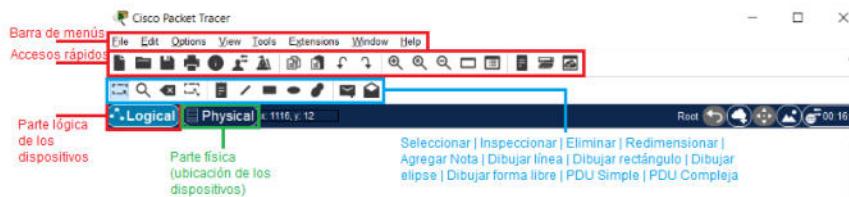
Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	354/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada



Área de trabajo



Figura No. 1. Simulador de CISCO Packet Tracer.

- 4.1.4** Dé clic en la sección de Dispositivos de red, después seleccione el apartado de switches, ubique el modelo 2960 IOS15, arrastre cuatro instancias del switch. Dé clic en la sección *Carpeta Miscellaneous*, ubique el modelo 1841 WIC-2T, arrastre dos instancias del router. Dé clic en la sección de dispositivos finales y arrastre una instancia de PC, tres de Server y conéctelos como se observa en la Figura No. 2.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página: 355/479 Sección ISO: 8.3 Fecha de emisión: 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

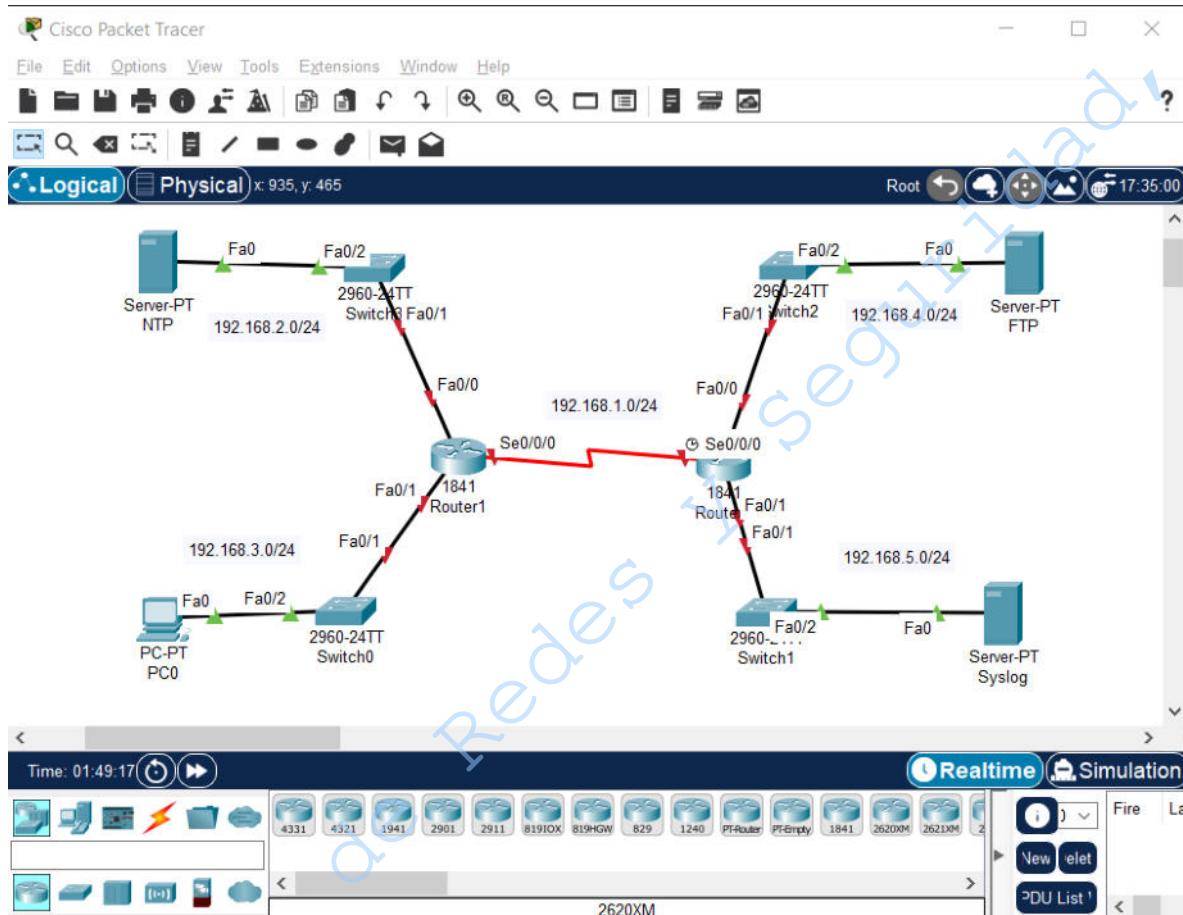


Figura No. 2. Topología para SSH, Telnet, FTP, Syslog y NTP

- 4.1.5 Dé clic en el nombre de los servidores y cambie el nombre del *Server0* por FTP, *Server1* por Syslog, *Server2* por NTP.

4.2 Configuración de topología

- 4.2.1 Asigne las direcciones de la PC 0, Servidor Syslog, Servidor NTP y Servidor FTP de acuerdo a la información de la Tabla No. 1.

Tabla No. 1. Información de las tarjetas de red

	PC0	Servidor Syslog	Servidor NTP	Servidor FTP
IPv4	192.168.3.1	192.168.5.1	192.168.2.1	192.168.4.1

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	356/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Máscara de subred	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.3.254	192.168.5.254	192.168.2.254	192.168.4.254
DNS	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

4.2.2 Configure las interfaces del Router 1 utilizando los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config)#interface se0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#interface fa0/0
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface fa0/1
Router(config-if)#ip address 192.168.3.254 255.255.255.0
Router(config-if)#no shutdown

```

4.2.3 Configure las interfaces del Router 2 utilizando los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config-if)#interface se0/0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#interface fa0/0
Router(config-if)#ip address 192.168.4.254 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#interface fa0/1
Router(config-if)#ip address 192.168.5.254 255.255.255.0
Router(config-if)#no shutdown

```

4.2.4 Realice el proceso de enrutamiento de los dos routers de la topología. Se recomienda utilizar el protocolo RIPv2, el cual, para el Router 1, se configura utilizando los siguientes comandos en el modo de configuración global:

```

Router(config-if)# exit
Router(config)# router rip

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	357/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
Router(config-router)# version 2
Router(config-router)# network ID_SUBRED
```

NOTA: El parámetro ID_SUBRED se debe reemplazar por el ID de la subred correspondiente que se encuentre conectada al router que se esté configurando. También es importante que indique todas y cada una de las subredes conectadas directamente empleando un comando *network* por cada subred.

Para esta práctica, los ID de subredes tienen el siguiente formato: 192.168.X.0.
Donde X puede tomar el valor de 1, 2, 3, 4 o 5 según el caso.

- 4.2.5** Ingrese a la consola del Switch S0, cambie el hostname por el de **S0**, mediante los siguientes comandos (Figura No. 3):

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S0
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch(config)#hostname S0
S0(config) #
```

Figura No. 3. Cambio de hostname al router S0

- 4.2.6** A continuación, debe poner IP a los switches, mediante la creación de la interfaz VLAN 1, utilizando los siguientes comandos (Figura No. 4).

```
S0(config)#interface vlan 1
S0(config-if)#ip address 192.168.X.10 255.255.255.0
S0(config-if)#no shutdown
S0(config-if)#exit
```

NOTA: La X debe de sustituirse por el segmento de red al que esté conectado el Switch. Para el caso del S0, se debe ingresar la IP 192.168.3.10

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	358/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.3.10 255.255.255.0
Switch(config-if)#no shutdown

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

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

Switch(config-if)#exit

```

Figura 4. Creación VLAN 1 en el S0.

- 4.2.7 Repetir para todos los switches los pasos 4.2.5 - 4.2.6, cambiando el nombre del Switch por el S1, S2 y S3.
- 4.2.8 Acceda a los routers y cambie el hostname con los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config)#hostname RX

```

NOTA: La X debe ser sustituida por el número de router que es.

4.3 Configuración de SSH y Telnet

- 4.3.1 Como se muestra en la figura 5, el Router 1, Switch 3 y Switch 0 se configurarán usando el protocolo SSH. Mientras que el Router 2, Switch 1 y Switch 2 se configurarán usando el protocolo TELNET (Figura No. 5).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	359/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

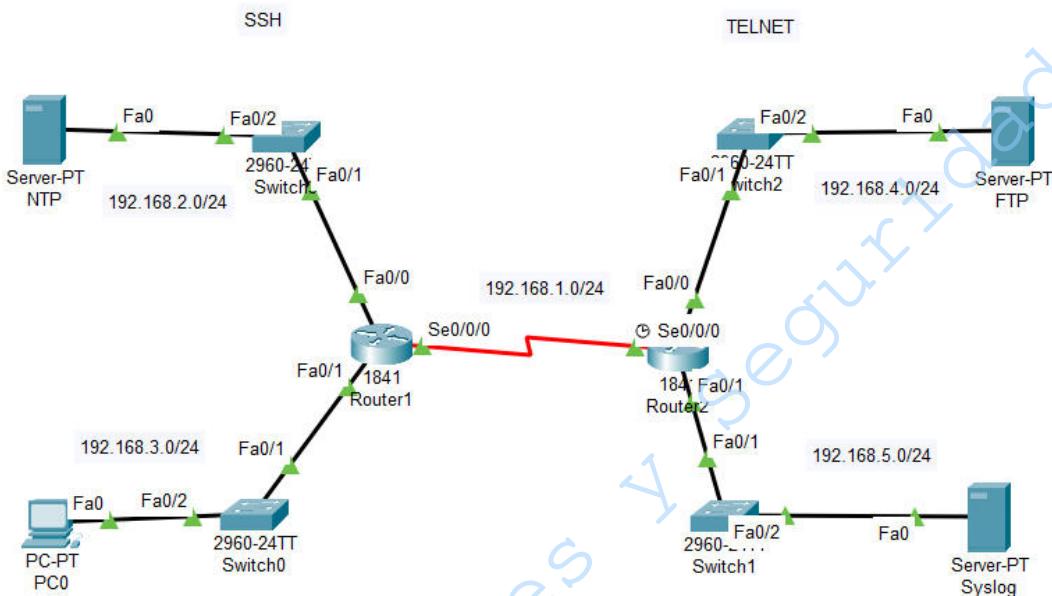


Figura 5. Topología para el protocolo SSH y TELNET.

- 4.3.2** Elija un nombre de usuario del Switch 3, una contraseña para dicho usuario, así como una contraseña para acceder a la configuración del Switch. Escriba los parámetros elegidos a continuación:

Nombre de usuario Switch 3: _____

Contraseña usuario Switch 3: _____

Contraseña Switch 3: _____

- 4.3.3** Acceda a la consola del Switch 3 e ingrese los siguientes comandos para la configuración de SSH (Figura No. 6):

```

S3>enable
S3#configure terminal
S3(config)#username NOMBRE_USUARIO secret PASSWORD
S3(config)#enable secret CONTRASEÑA
S3(config)#ip domain-name LabRedes
S3(config)#crypto key generate rsa

```

How many bits in the modulus [512]: 1024

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	360/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

S3(config)#ip ssh authentication-retries 3
S3(config)#ip ssh time-out 60
S3(config)#aaa new-model
S3(config)#line vty 0 15
S3(config-line)#transport input ssh
S3(config-line)#exit

```

NOTA: Debe sustituir:

- **NOMBRE_USUARIO** por el nombre de usuario que eligió en el punto 4.3.2.
- **PASSWORD** por la contraseña para ingresar al usuario.
- **CONTRASEÑA** por la contraseña para entrar el modo enable del switch.

```

S3>enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#username Jisus secret Jisus
S3(config)#enable secret contral23
S3(config)#ip domain-name LabRedes
S3(config)#crypto key generate rsa
The name for the keys will be: S3.LabRedes
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S3(config)#ip ssh authentication-retries 3
*Mar 1 0:22:53.73: %SSH-5-ENABLED: SSH 1.99 has been enabled
S3(config)#ip ssh time-out 60
S3(config)#aaa new-model
S3(config)#line vty 0 15
S3(config-line)#transport input ssh
S3(config-line)#exit
S3(config)#
S3(config)#ip default-gateway 192.168.2.254

```

Figura No. 6. Ejemplo de configuración de SSH

4.3.4 Repetir el paso 4.3.3 tanto en el router 1, como en el switch 0. Debe definir nuevas credenciales para cada dispositivo. Escríbalas a continuación:

Nombre de usuario Router 1: _____

Contraseña usuario Router 1: _____

Contraseña Router 1: _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	361/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Nombre de usuario Switch 0: _____

Contraseña usuario Switch 0: _____

Contraseña Switch 0: _____

- 4.3.5** Ahora, para configurar los dispositivos con Telnet, elija un nombre de usuario para el Switch 2 y una contraseña para este usuario. Escriba los parámetros elegidos a continuación:

Nombre de usuario Switch 2: _____

Contraseña usuario Switch 2: _____

- 4.3.6** Acceda a la consola del Switch 2 e ingrese los siguientes comandos para configurar el protocolo Telnet (Figura No. 7):

```
S2>enable
S2#configure terminal
S2(config)#username NOMBRE_USUARIO secret CONTRASEÑA
S2(config)#line vty 0 9
S2(config-line)#login local
S2(config-line)#exit
```

NOTA: Debe sustituir:

- **NOMBRE_USUARIO** por el nombre de usuario que eligió en el punto 4.3.5.
- **CONTRASEÑA** por la contraseña para ingresar al usuario.

```
S2>enable
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#username Jisus secret Jisus
S2(config)#line vty 0 9
S2(config-line)#login local
S2(config-line)#exit
```

Figura No. 7. Ejemplo de configuración de Telnet

- 4.3.7** Repetir el paso 4.3.6 en el router 2 y switch 1. Debe definir nuevas credenciales para cada dispositivo. Escríbalas a continuación:

Nombre de usuario Router 2: _____

Contraseña usuario Router 2: _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	362/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Nombre de usuario Switch 1: _____

Contraseña usuario Switch 1: _____

- 4.3.8** Adicionalmente, ingrese el siguiente comando para todos los switches (No routers) (Figura No. 8):

S3(config)# ip default-gateway <ip_gateway>

NOTA: El comando anterior define cuál será el gateway de cada switch, por lo que, según cada caso, se deberá sustituir *ip_gateway* por la dirección IP de gateway de cada segmento de red.

S3 (config) #ip default-gateway 192.168.2.254

Figura No. 8. Ejemplo de uso del comando default gateway en el switch 3.

4.4 Configuración de FTP, Syslog y NTP

- 4.4.1** Acceda al servidor que se nombró como FTP, dé clic en la pestaña superior nombrada *services*, luego en el apartado de *FTP*. En caso de que el servicio esté apagado, dé clic en la opción *On* (Figura No. 9).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 363/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

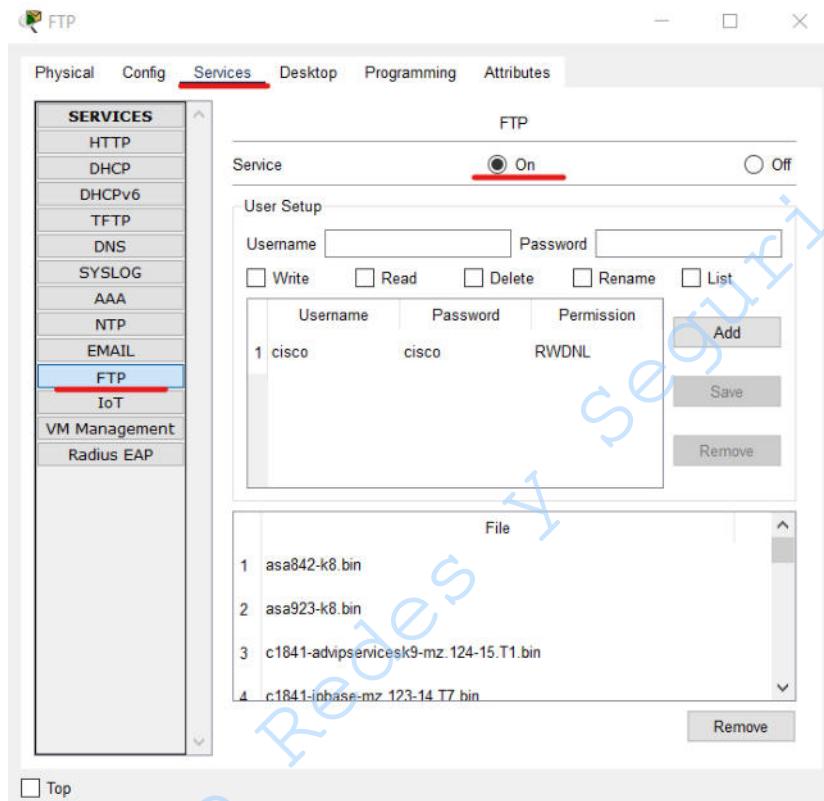


Figura No. 9. Servicio de FTP encendido

- 4.4.2** Elija un nombre de usuario y una contraseña para el usuario de FTP. Escriba los parámetros elegidos a continuación:

Nombre de usuario: _____

Contraseña usuario: _____

- 4.4.3** Dentro del servicio FTP, agregue el usuario con la contraseña definida en el punto 4.4.2, dé clic en las casillas *Write*, *Read*, *Delete*, *Rename* y *List*; estos son los permisos que se le otorgarán al usuario que se va a crear. Posteriormente, dé clic en el botón *Add*. (Tome la Figura No. 10 como referencia).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 364/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

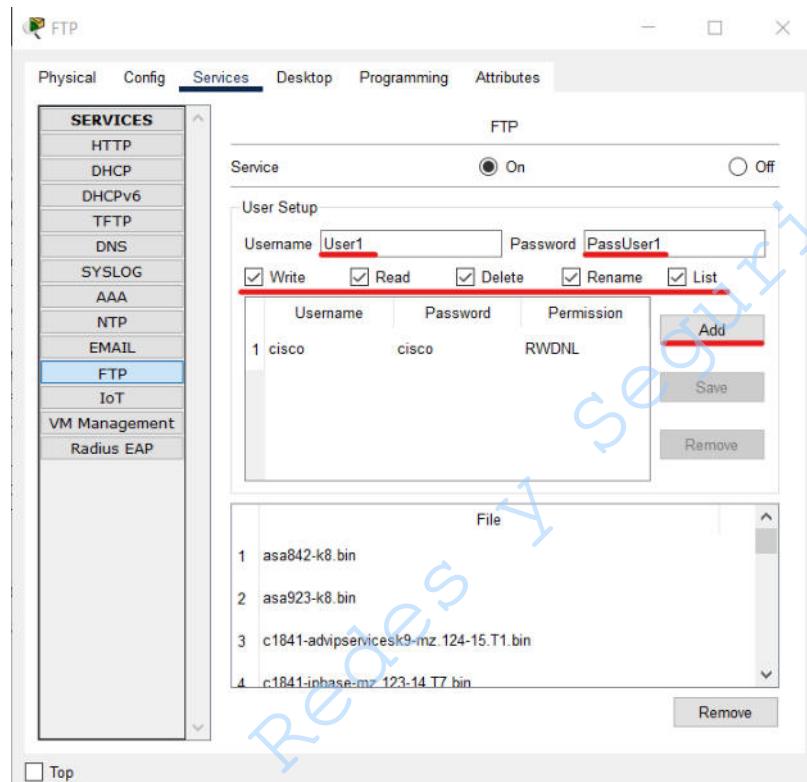


Figura No. 10. Creación de usuario para servicio FTP

- 4.4.4** Dentro del servicio FTP, en el apartado de *File*, seleccione archivo por archivo y presione el botón *Remove*, de tal forma que no quede ningún archivo en el servidor (Figura No. 11).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	365/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

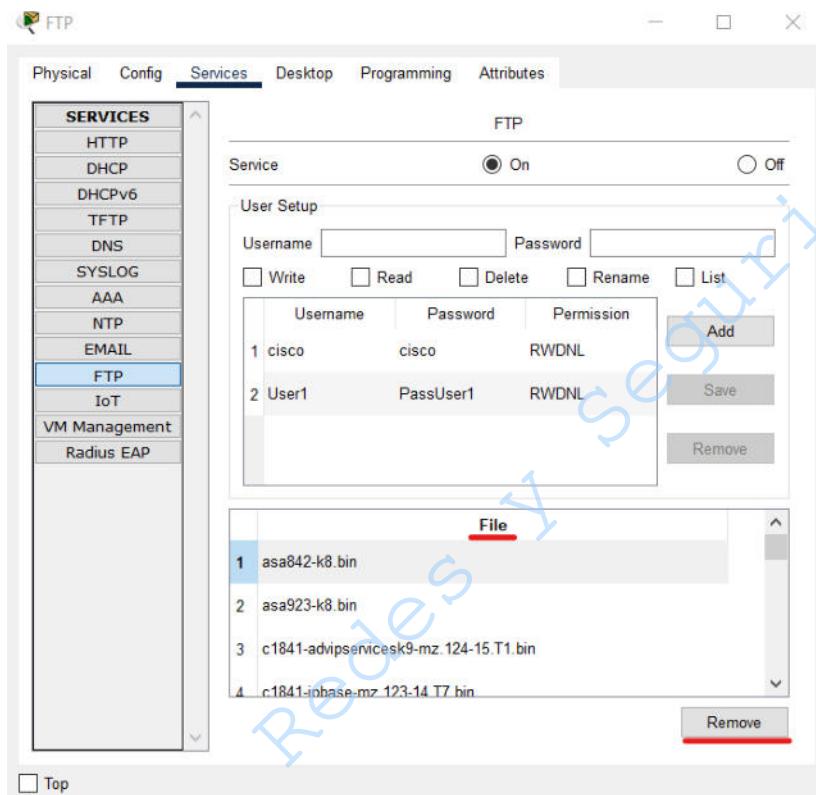


Figura No. 11. Eliminación de archivos del servidor FTP

4.4.5 Acceda al router 1 e introduzca los siguientes comandos para que configure el protocolo NTP (Figura No. 12):

NOTA: Al momento de acceder al modo enable se pedirá la contraseña que se configuró en el paso 4.3.3.

```
R1>enable
Password:
R1#configure terminal
R1(config)#ntp server 192.168.2.1
```

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 192.168.2.1
R1(config)#exit
```

Figura No. 12. Configuración de NTP

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 366/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.4.6 Repita el paso 4.4.5 para el switch 0, 1, 2, 3 y el router 2.

4.4.7 Acceda al servidor que se nombró como NTP, dé clic en la pestaña *services* y posteriormente dé clic en NTP. En caso de estar apagado el servicio, de clic en la opción *On* (Figura No. 13) .

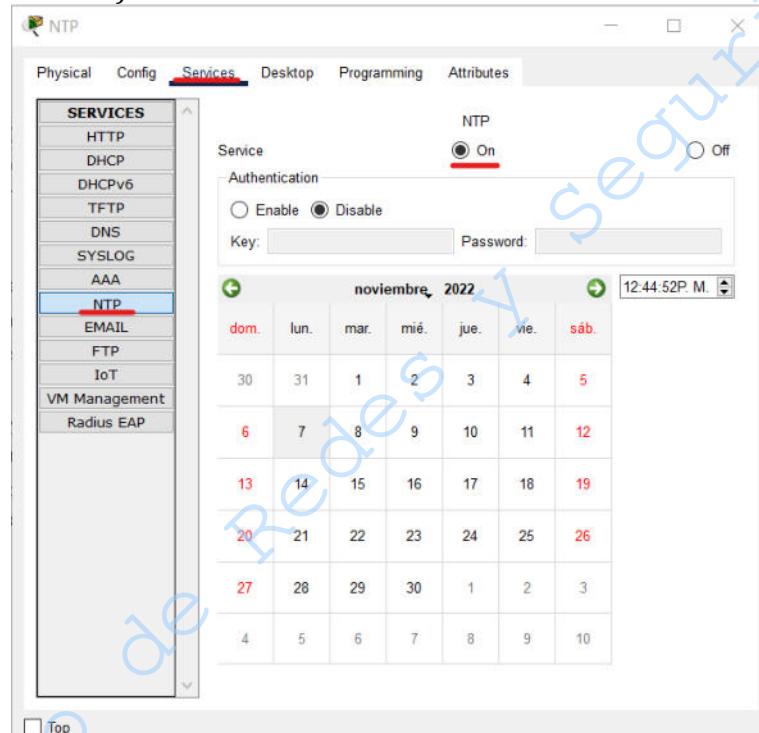


Figura No. 13. Servicio de NTP encendido

4.4.8 En el calendario que se muestra en la ventana de la Figura No. 14, haga clic en el día en el que esté realizando la práctica e ingrese la hora actual a la que está realizando el ejercicio.



Manual de prácticas del Laboratorio de Redes de Datos Seguras		Código:	MADO-31
		Versión:	06
		Página	367/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	

La impresión de este documento es una copia no controlada

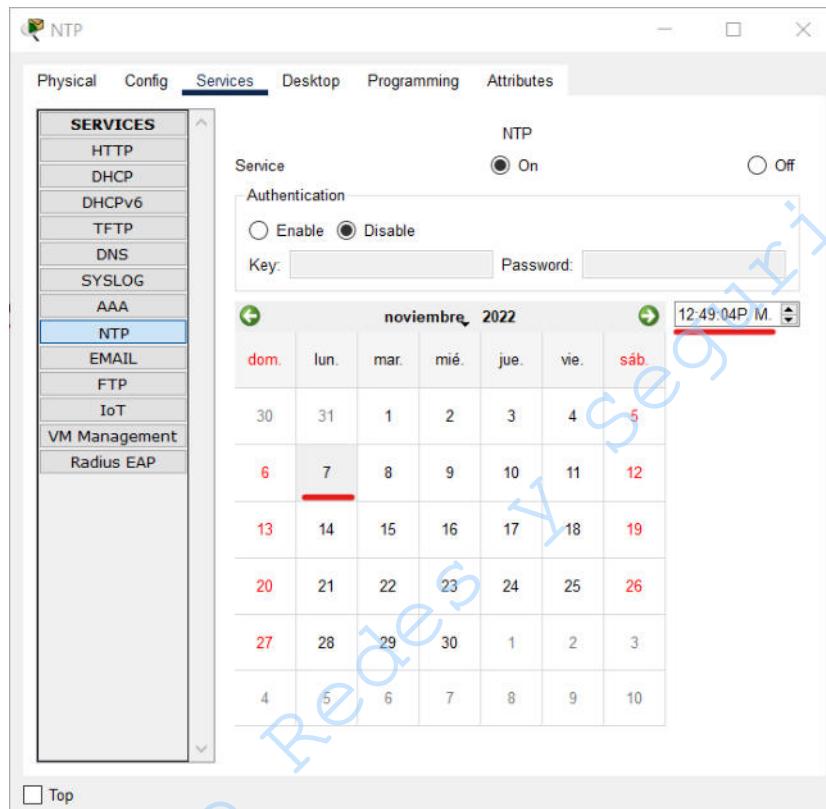


Figura No. 14. Configuración del día y hora del servidor NTP

- 4.4.9** Dé clic 3 veces en la opción *Fast forward time* y después introduzca el siguiente comando en cualquier dispositivo para mostrar la fecha y hora que tiene el servidor NTP (Figura No. 15):

R1#show clock

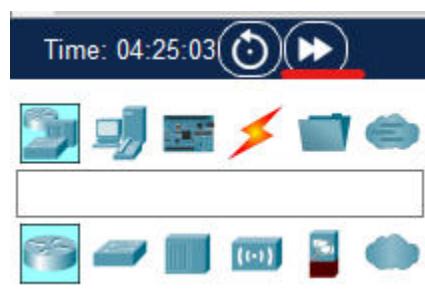


Figura 15. Opción Fast forward time

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 368/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.4.10** Acceda al servidor nombrado como *syslog*, dé clic en la pestaña *Services* y luego en el apartado *Syslog*. En caso de estar apagado el servicio, dé clic en la opción *On* (Figura No. 16).

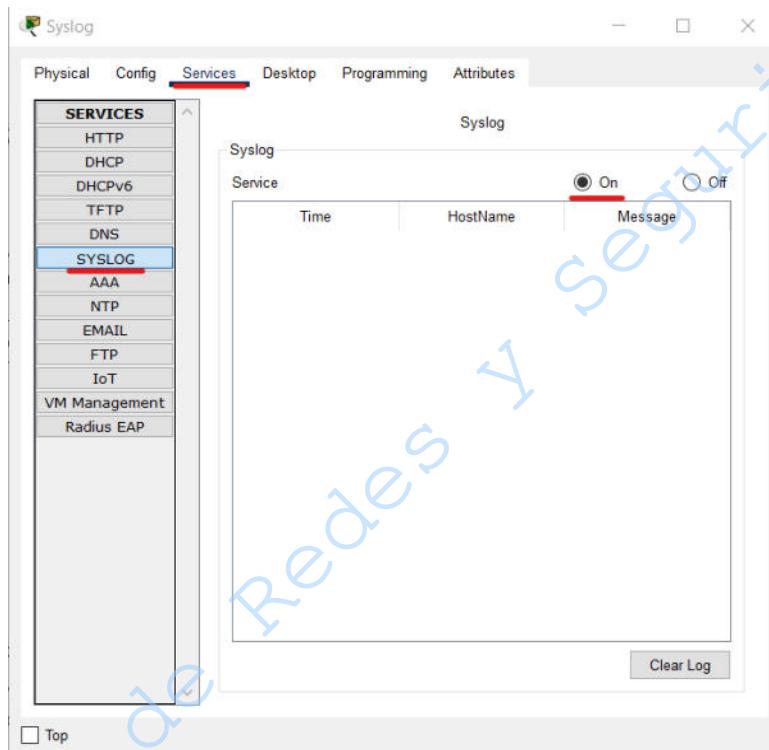


Figura No. 16. Servicio de syslog encendido

- 4.4.11** Acceda al router 1 e introduzca los siguientes comandos para configurar el syslog.

NOTA: Al momento de acceder al modo enable se pedirá la contraseña que se configuró en el paso 4.3.3 (Figura No. 17).

```
R1>enable
Password:
R1#configure terminal
R1(config)#logging host 192.168.5.1
R1(config)#service timestamps log datetime msec
R1(config)#exit
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	369/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#logging host 192.168.5.1
R1(config)#service timestamps log datetime msec
R1(config)#exit
R1#
*Nov 07, 13:05:34.055: SYS-5-CONFIG_I: Configured from console by console
*Nov 07, 13:05:34.055: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.5.1 port 514 started - CLI initiated
```

Figura No. 17. Configuración de syslog en el router 1

- 4.4.12 En la topología, haga clic sobre alguno de los triángulos verdes de la conexión cableada entre el Switch 0 y el Router 1. De esta forma se desconecta el cable del dispositivo.
- 4.4.13 A continuación vuelva a conectar el mismo cable en la misma interfaz de donde se desconectó. Lo anterior se realizó para poder activar una notificación en la red y que el servidor *syslog* pueda guardarla.
- 4.4.14 Acceda de nueva cuenta al servidor *syslog*, dé clic en la pestaña *Services* y luego en el apartado *Syslog* y llene la tabla de acuerdo con lo mostrado en pantalla:

Tabla No. 1. Mensajes en el servidor syslog

-			
1			
2			
3			

4.5 Pruebas de conexión Telnet y SSH.

- 4.5.1 Dé clic en la computadora PC0, ingrese a la pestaña Desktop y haga clic en el ícono que dice *Command Prompt* (Figura No. 18):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 370/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

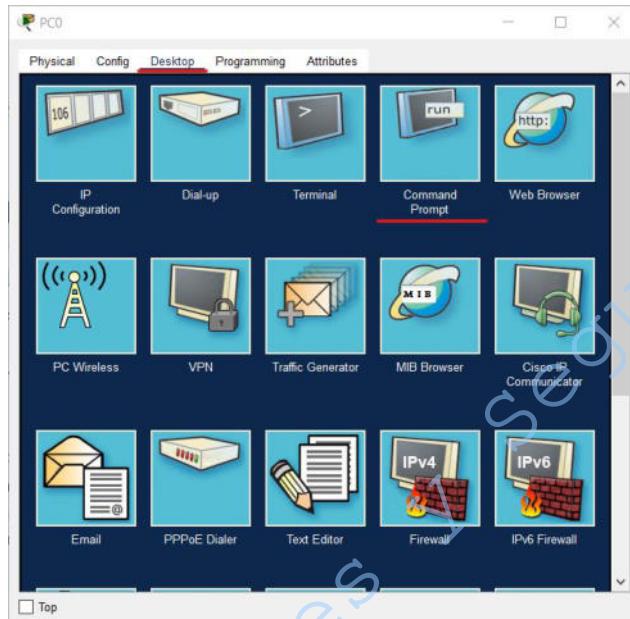


Figura 18. Íconos de la pestaña Desktop de la PC0.

4.5.2 Dentro del *Command Prompt*, ingrese el siguiente comando:

```
C:\> ssh -l <USERNAME> 192.168.3.10
```

El comando anterior realiza una conexión remota al Switch 0 desde la PC0.

NOTA: <USERNAME> debe ser sustituido por el nombre de usuario que haya definido en el punto 4.3.4. Después de dar enter al comando, se le pedirá la contraseña del usuario del Switch, dicha contraseña es la definida en el punto 4.3.4.

4.5.3 Escriba a continuación el cambio que ocurrió en la terminal cuando se realizó correctamente el punto 4.5.2:

4.5.4 Dentro del mismo *Command Prompt* de la PC0, ingrese el siguiente comando:

```
S0> en
S0# ssh -l <USERNAME> 192.168.2.10
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	371/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

El comando anterior realiza una conexión remota al Switch 3 desde el Switch 0, a través de la PC0.

NOTA: <USERNAME> debe ser sustituido por el nombre de usuario que haya definido en el punto 4.3.2. Después de dar enter al comando, se le pedirá la contraseña del usuario del Switch, dicha contraseña es la definida en el punto 4.3.2.

- 4.5.5** Escriba a continuación el cambio que ocurrió en la terminal cuando se realizó correctamente el punto 4.5.4:
-
-

- 4.5.6** Siguiendo en el *Command Prompt* de la PC0, ingrese el siguiente comando:

S3> telnet 192.168.4.10

NOTA: Despues de dar enter al comando, se le pedirá que ingrese el nombre de usuario y la contraseña del usuario del Switch 2, dichas credenciales son las definidas en el punto 4.3.5.

- 4.5.7** Describa a continuación a dónde se conectó, desde dónde y a través de qué dispositivo cuando realizó correctamente el punto 4.5.6:
-
-

- 4.5.8** Dentro del *Command Prompt* de la PC0, ingrese el siguiente comando:

S2> telnet 192.168.5.254

NOTA: Despues de dar enter al comando, se le pedirá que ingrese el nombre de usuario y la contraseña del usuario del Router 2, dichas credenciales son las definidas en el punto 4.3.7.

- 4.5.9** Describa a continuación a dónde se conectó, desde dónde y a través de qué dispositivo cuando realizó correctamente el punto 4.5.8:
-
-

- 4.5.10** En el *Command Prompt* de la PC0, ingrese el siguiente comando:

R2> telnet 192.168.5.10

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	372/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

NOTA: Después de dar enter al comando, se le pedirá que ingrese el nombre de usuario y la contraseña del usuario del Switch 1, dichas credenciales son las definidas en el punto 4.3.7.

- 4.5.11** Describa a continuación a dónde se conectó, desde dónde y a través de qué dispositivo cuando realizó el punto 4.5.10:
-
-

- 4.5.12** Aún en el *Command Prompt* de la PC0, ingrese el siguiente comando:

```
S1> en
S1# ssh -l <USERNAME> 192.168.2.254
```

NOTA: <USERNAME> debe ser sustituido por el nombre de usuario que haya definido en el punto 4.3.4. Después de dar enter al comando, se le pedirá la contraseña del usuario del Router, dicha contraseña es la definida en el punto 4.3.4.

- 4.5.13** Describa a continuación a dónde se conectó, desde dónde y a través de qué dispositivo cuando realizó el punto 4.5.12:
-
-

4.6 Conexión al servidor FTP.

- 4.6.1** Dé clic en la computadora PC0, ingrese a la pestaña Desktop y haga clic en el ícono que dice *Text Editor* (Figura No. 19):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 373/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

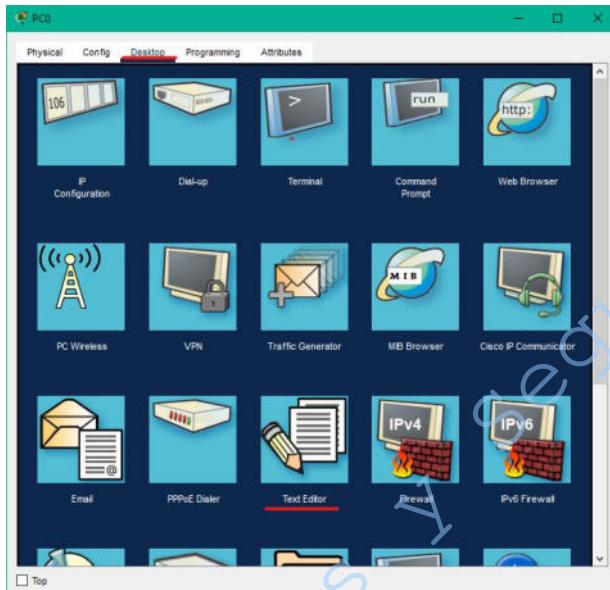


Figura No. 19. Íconos de la pestaña Desktop de la PC0

- 4.6.2** Cree un archivo como se muestra en la Figura No. 20 y guárdelo con el nombre LabRedes.txt.

NOTA: Para guardar el archivo, debe hacer clic en la X como si fuera a cerrar el Text Editor, después aparecerá una ventana preguntando si desea guardar el archivo y finalmente pedirá que ingrese el nombre.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 374/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

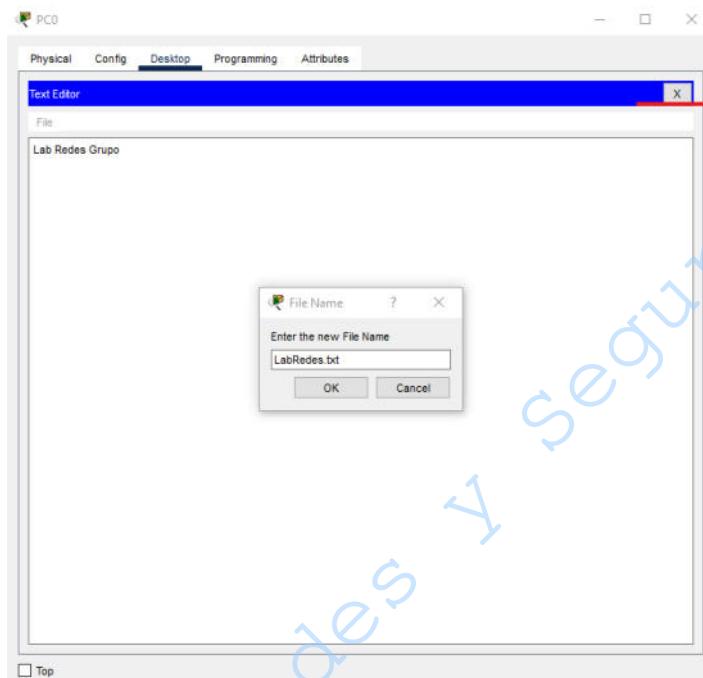


Figura No. 20. Creación del archivo LabRedes.txt

- 4.6.3** Ahora abra el *Command Prompt* de la PC0 e ingrese el siguiente comando para poder conectarse al servidor *ftp* (Figura No. 21):

```
R1>exit
C:\>ftp 192.168.4.1
```

NOTA: Después de dar enter al comando, se le pedirá que ingrese el nombre de usuario y la contraseña del usuario del servidor *ftp*, dichas credenciales son las definidas en el punto 4.4.2.

```
C:\>ftp 192.168.4.1
Trying to connect...192.168.4.1
Connected to 192.168.4.1
220- Welcome to PT Ftp server
Username:User1
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Figura No. 21. Conexión al servidor FTP



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	375/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- 4.6.4** Una vez que accedió remotamente al servidor ftp, copie el archivo LabRedes.txt de la PC0 al servidor ftp y verifique que se encuentre en el servidor, utilizando los siguientes comandos:

```
ftp>put LabRedes.txt  
ftp>dir
```

- #### 4.6.5 Mencione a continuación qué aparece en pantalla y porqué:

segno

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	376/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 9

Uso de protocolos TCP y UDP

Cuestionario Previo

1. Defina Investigue y describa: ¿Qué es y cómo se configura el protocolo NTP en un router?
2. Investigue y mencione las diferencias entre Telnet y SSH.
3. ¿Cuál es la dirección ip denominada como gateway?
4. ¿Cuál es la función de un servidor syslog?
5. Investigue los comandos que se necesitan para poder configurar un servidor FTP.
6. Investigue cuáles son las notificaciones soportadas por el protocolo Syslog.
7. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 377/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 10

Sistema Operativo de Switch y Router

Capa 5 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	378/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

1.- Objetivos de aprendizaje

- El alumno o la alumna aprenderá cómo hacer un respaldo del sistema operativo de un switch y un router.
- El alumno o la alumna aprenderá a borrar un sistema operativo de un switch y un router.
- El alumno o la alumna aprenderá a cargar un sistema operativo de un switch y un router utilizando el protocolo TFTP.

2.- Conceptos teóricos

El sistema operativo es el software primordial de un dispositivo electrónico, debido a que permite interactuar con él y darle órdenes. También realiza la administración de los recursos del equipo.

El SO ya viene instalado por default en la computadora y normalmente no se le hace ningún tipo de modificaciones; sin embargo, existe la posibilidad de actualizarlo, cambiarlo o respaldarlo periódicamente. Todos los sistemas operativos utilizan una interfaz gráfica o de comandos para interactuar con el usuario.

Ahora, el protocolo TFTP (Trivial File Transfer Protocol) es un protocolo cliente-servidor bastante simple que regula la transferencia de archivos en las redes informáticas. Por defecto TFTP se basa en el protocolo UDP, el cual ofrece la posibilidad de transmitir datos sin la necesidad de una conexión fija entre los miembros de la comunicación, haciendo que TFTP sea muy usado para realizar transferencias de datos de forma remota.

TFTP funciona mediante paquetes de datos y forma parte de la familia de protocolos TCP/IP, originalmente la implementación fue pensada en ser lo más sencilla y ligera posible.

Un servidor TFTP puede ayudar a administrar el almacenamiento y las revisiones de las imágenes del sistema operativo de los dispositivos de red. Para cualquier red, es aconsejable tener una copia de seguridad de la imagen del software IOS de Cisco, en caso de que la imagen de sistema en el router se dañe o se elimine accidentalmente. Un servidor TFTP también se puede utilizar para almacenar nuevas actualizaciones del IOS y, luego, se puede implementar en la red donde sea necesario.

Un router Cisco tiene cinco diferentes modos, los cuales son los siguientes:

- Modo de ejecución del usuario. Este es el primer modo en el que inicia el router y está limitado únicamente a unos comandos de monitorización.
- Modo privilegiado. En este modo se puede ver y cambiar la configuración del router. Se accede escribiendo "enable" en el modo de ejecución del usuario.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	379/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- **Modo de configuración global.** Los comandos que se pueden ejecutar en ese modo se llaman comandos globales y afectan a la configuración de la ejecución del router. Para acceder a él se debe escribir “configure terminal” en el modo privilegiado.
- **Modo de configuración de interfaz.** Aquí sólo se realiza la configuración de las interfaces, como asignar dirección IP o abrir una interfaz.
- **Modo ROMMON.** Normalmente se accede a este modo durante el proceso de recuperación de la contraseña del router o cuando se recupera la copia de seguridad del sistema operativo. A este modo se puede acceder cuando se interrumpe el proceso de arranque del router.

3.- Equipo y material necesario

Equipo del laboratorio:

- Software de Simulación Cisco Packet Tracer

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Creación de topología para el uso del protocolo TFTP.

- 4.1.1 Encienda el sistema y elija la opción de cargar Windows.
- 4.1.2 Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3 Ejecute la aplicación Cisco Packet Tracer (Figura No. 1).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 380/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 1. Simulador de CISCO Packet Tracer.

- 4.1.4** Dé clic en la sección de Dispositivos de red, después seleccione el apartado de switches, ubique el modelo 2960 IOS15, arrastre una instancia del switch. Dé clic en el apartado routers, ubique el modelo ISR4331, arrastre una instancia del router. Dé clic en la sección de dispositivos finales, arrastre una instancia de PC y una de Server, conéctelos como se observa en la Figura No. 2.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 381/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

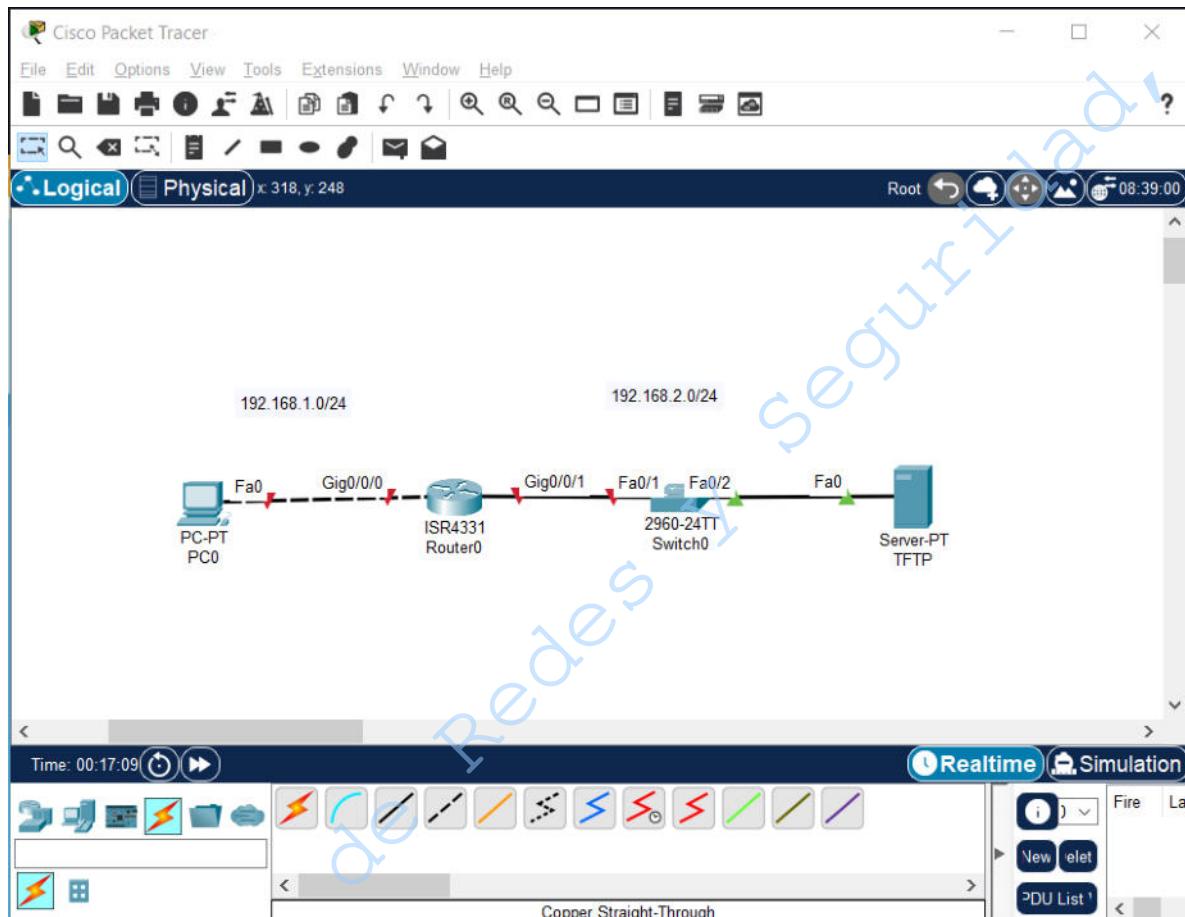


Figura No. 2. Topología para TFTP

- 4.1.5 Cambie el nombre del *server0* por TFTP.
- 4.1.6 Acceda al router 0, cambie el nombre a R0 y configure las interfaces GigabitEthernet 0/0/0 y GigabitEthernet 0/0/1, asignándoles direcciones IP y encendiendo dichas interfaces, todo a partir de los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config)#hostname R0
R0(config)#interface gi0/0/0
R0(config-if)#ip address 192.168.X.Y 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	382/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

```
R0(config)#interface gi0/0/1
R0(config-if)#ip address 192.168.X.Y 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#exit
```

NOTA: Debe intercambiar X por el segmento de red correspondiente, Y por el valor del último octeto que, en este caso, pertenece al host.

- 4.1.7** Acceda al switch 0, configure la interfaz Vlan 1, así como el default-gateway y cambie el nombre a S0, utilizando los siguientes comandos:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.2.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.2.254
Switch(config)#hostname S0
S0(config)#exit
```

- 4.1.8** Dé clic en la computadora PC0, ingrese a la pestaña Desktop, haga clic en el ícono que dice *IP Configuration* y asígnele una dirección IP de acuerdo al segmento de red en el que se encuentra el dispositivo (Figura No. 3).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 383/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

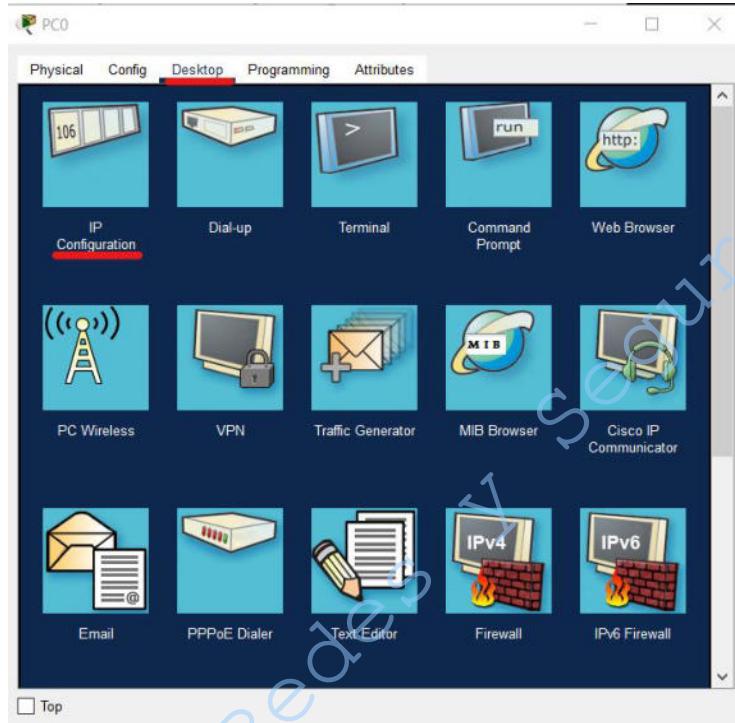


Figura No. 3. Ip configuration de PC0.

4.1.9 Repita el paso 4.1.8, pero configurando ahora la IP del Servidor TFTP.

4.1.10 Apunte en la Tabla No. 1 las direcciones IP que le asignó a las interfaces gigabitethernet 0/0 y gigabitethernet 0/1.

Tabla No. 1. Parámetros de red de los dispositivos

	Dirección IPv4	Máscara	Gateway
Router gi0/0/0			N/A
Router gi0/0/1			N/A
Switch Vlan 1			
Servidor TFTP			
PC0			

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	384/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 4.1.11** Realice el proceso de enrutamiento del router de la topología. Se recomienda utilizar el protocolo RIPv2, el cual, para el Router 0, se configura utilizando los siguientes comandos en el modo de configuración global:

```
R0(config-if)# exit
R0(config)# router rip
R0(config-router)# version 2
R0(config-router)# network ID_SEGMENTO
```

NOTA: El parámetro ID_SEGMENTO se debe reemplazar por el ID de la subred correspondiente que se encuentre conectada al router que se está configurando. También es importante que indique todas y cada una de las subredes conectadas directamente empleando un comando *network* por cada subred.

- 4.1.12** Acceda al router y ejecute el siguiente comando ping, enviándolo a la dirección IP que tiene el servidor (Figura No. 4).

```
R0>enable
R0#ping 192.168.2.X
```

NOTA: Debe intercambiar X por el número de host que le corresponde al servidor.

El resultado esperado es que se envíen la mayoría de los paquetes.

```
R0>enable
R0#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

Figura No. 4. Comando ping de router 0 - servidor tftp

4.2 Respaldo del sistema operativo de un router y un switch

- 4.2.1** Acceda al router 0 e identifique el nombre del archivo del sistema operativo del router, con el siguiente comando (Figura No. 5):

```
R0>enable
R0#dir flash:
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	385/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```
R0>enable
R0#dir flash:
Directory of flash:/

 3  -rw-    486899872      <no date>  isr4300-universalk9.16.06.04.SPA.bin
 2  -rw-     28282        <no date>  sigdef-category.xml
 1  -rw-     227537       <no date>  sigdef-default.xml

3249049600 bytes total (2761893909 bytes free)
```

Figura No. 5. Archivos del directorio *flash*

NOTA: El archivo que es el sistema operativo es el que tiene extensión “.bin”.

4.2.2 Escriba a continuación el nombre completo del archivo del sistema operativo del router.

4.2.3 Copie el sistema operativo del router al servidor TFTP con los siguientes comandos: (Figura No. 6)

```
R0#copy flash: tftp:
Source filename []? <Nombre_Archivo_SO.bin>
Address or name of remote host []? <IP servidor TFTP>
Destination filename [isr4300-universalk9.16.06.04.SPA.bin]?
```

NOTA: <Nombre_Archivo_SO.bin> debe sustituirse por el nombre escrito en el punto 4.2.2. Mientras que <IP servidor TFTP> debe ser sustituido por la IP del servidor TFTP definida en la tabla 1 del punto 4.1.10.

Cabe mencionar que, después de ejecutar este comando, empezarán a aparecer muchos signos de exclamación.

```
R0#copy flash: tftp:
Source filename []? isr4300-universalk9.16.06.04.SPA.bin
Address or name of remote host []? 192.168.2.1
Destination filename [isr4300-universalk9.16.06.04.SPA.bin]?

Writing isr4300-
universalk9.16.06.04.SPA.bin....!!!!!!!!!!!!!!
```

Figura No. 6. Generando copia del SO en el servidor TFTP

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 386/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.4** Repetir los pasos 4.2.1 al 4.2.3 con el switch 0, ingresando a continuación el nombre completo del archivo del sistema operativo del switch.

- 4.2.5** Acceda al servidor TFTP, dé clic en la pestaña *Services*, dé clic en la opción TFTP y verifique que los archivos de los dos sistemas operativos se encuentren en el servidor (Figura No. 7):

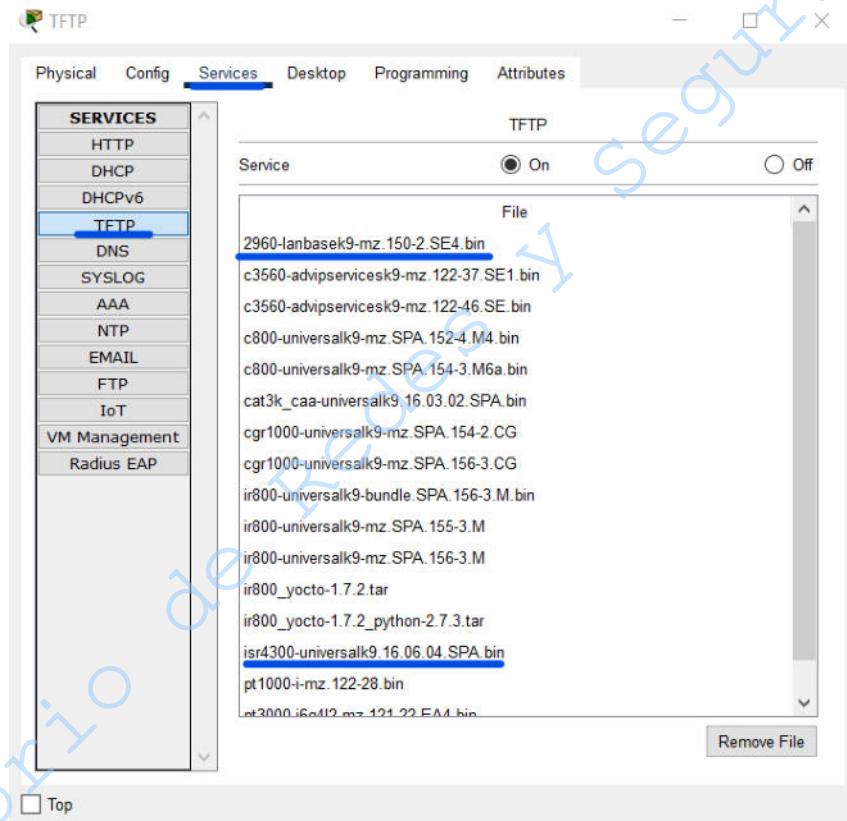


Figura No. 7. Archivos .bin en el servidor TFTP

- 4.2.6** A continuación escriba de forma breve por qué es importante realizar respaldos del sistema operativo de un dispositivo de la red y con qué periodicidad debería de realizarse.
-
-
-

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	387/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

- 4.2.7** Mencione algunas medidas de seguridad adicionales para garantizar un respaldo adecuado de los sistemas operativos.

- 4.2.8** Investigue y escriba a continuación, ¿qué buenas prácticas existen para poder brindar una buena seguridad en los sistemas operativos?

- 4.2.9** ¿Considera adecuado el uso de la nube para realizar respaldos del sistema operativo de un router o un switch? Justifique su respuesta.

4.3 Eliminación de un sistema operativo de switch y router

- 4.3.1** Antes de eliminar el sistema operativo del R0, cambie la conexión de forma que quede ahora como se muestra en la Figura No. 8:

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 388/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

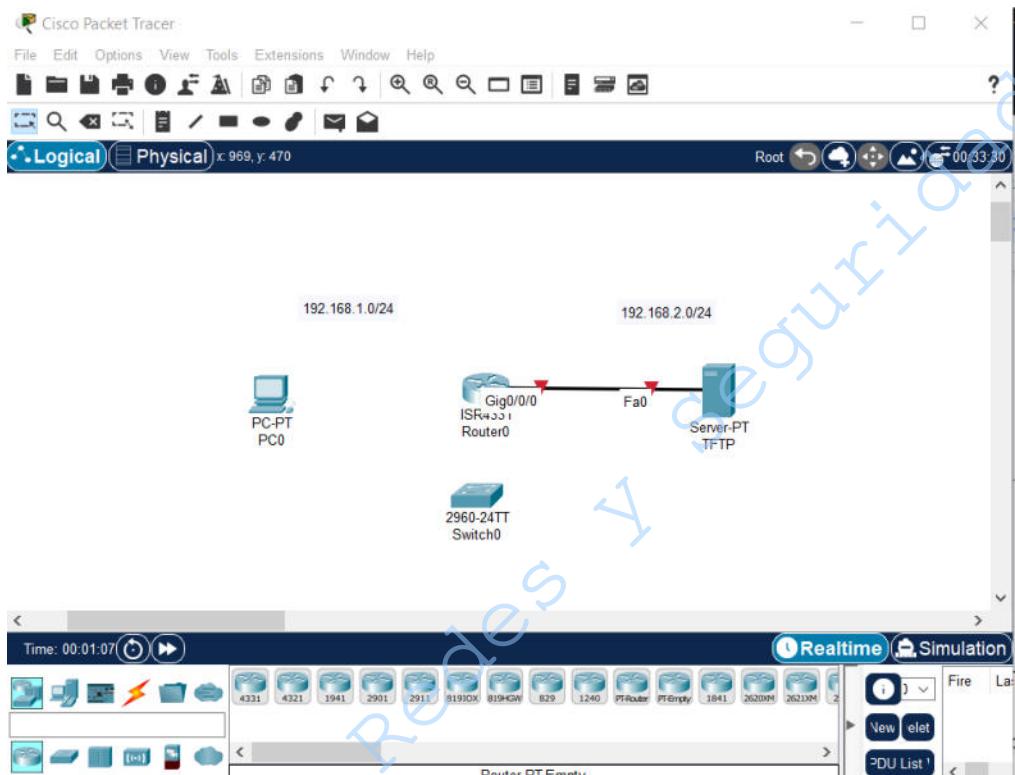


Figura No. 8. Conexión necesaria para eliminación y recuperación del SO de un Router

4.3.2 Acceda al router 0 y borre el sistema operativo del dispositivo, con el siguiente comando:

```
R0>enable
R0#delete flash:
Delete filename []?isr4300-universalk9.16.06.04.SPA.bin
Delete flash:/isr4300-universalk9.16.06.04.SPA.bin? [confirm]
```

```
R0>enable
R0#delete flash:
Delete filename []?isr4300-universalk9.16.06.04.SPA.bin
Delete flash:/isr4300-universalk9.16.06.04.SPA.bin? [confirm]

R0#
```

Figura No. 9. Eliminación del sistema operativo de un router

4.3.3 Reinicie el router con el siguiente comando y observe los efectos de eliminar el sistema operativo (Figura No. 10):

```
R0#reload
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	389/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```

R0#reload
Proceed with reload? [confirm]
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Boot process failed...

The system is unable to boot automatically. The BOOT
environment variable needs to be set to a bootable
image.
rommon 1 >

```

Figura No. 10. Reinicio del router sin sistema operativo

4.3.4 ¿En qué modo entró el router? Explique ¿por qué entró a este modo?

4.3.5 Explique, ¿qué acciones se pueden realizar en este modo?

4.4 Recuperación del sistema operativo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	390/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 4.4.1** Dentro del router en modo rommon, ingrese los siguientes comandos para recuperar el sistema operativo a partir de la copia de seguridad realizada en el servidor TFTP (Figura No. 11):

```
rommon 1 > IP_ADDRESS=<IP a asignar al router>
rommon 2 > IP_SUBNET_MASK=<Máscara de subred>
rommon 3 > DEFAULT_GATEWAY=<IP de gateway de ese segmento>
rommon 4 > TFTP_SERVER=<IP asignada al servidor TFTP>
rommon 5 > TFTP_FILE=<Nombre del archivo de sistema operativo>
rommon 6 > tftpdnld
```

```
rommon 1 > IP_ADDRESS=192.168.2.10
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.2.254
rommon 4 > TFTP_SERVER=192.168.2.1
rommon 5 > TFTP_FILE=isr4300-universalk9.16.06.04.SPA.bin
rommon 6 > tftpdnld
```

```
IP_ADDRESS: 192.168.2.10
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.2.254
TFTP_SERVER: 192.168.2.1
TFTP_FILE: isr4300-universalk9.16.06.04.SPA.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
```

Do you wish to continue? y/n: [n]: y

```
.
Receiving isr4300-universalk9.16.06.04.SPA.bin from 192.168.2.1
!!!!!!!!!!!!!!
```

Figura No. 11. Ejemplo de comandos para recuperar sistema operativo

- 4.4.2** Reinicie el router para que guarde los cambios hechos, con el siguiente comando (Figura No. 12):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	391/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

rommon 7 > reset

```

program flash location 0x7d030000
program flash location 0x7d040000
program flash location 0x7d050000

rommon 7 > reset
Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####

```

Figura No. 12. Reinicio del router con la copia de seguridad del SO.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	392/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	393/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 10

Sistema Operativo de Switch y Router

Cuestionario Previo

1. ¿Qué es un servidor TFTP y cuáles son las funciones de incorporarlo a una red?
2. Investigue cuál es el sistema operativo presente en los Routers y Switches Cisco, así como sus características principales.
3. ¿Qué es el modo ROMmon en un dispositivo Cisco y cuáles son sus características?
4. ¿Cuáles son las opciones que se tienen para volver a cargar el sistema operativo de un dispositivo Cisco?
5. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 06 394/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 11

VPN

Capa 6 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	395/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

1.- Objetivos de aprendizaje

- El alumno o la alumna realizará la creación y configuración de un servidor de red VPN a través del protocolo PPTP en una distribución Linux.
- El alumno o la alumna establecerá conexión desde el sistema operativo Windows con el servidor VPN creado.

2.- Conceptos teóricos

VPN son las siglas en inglés de Virtual Private Network (Red Privada Virtual) y pretende brindar una red privada a través de internet. La VPN crea una conexión punto a punto virtual mediante el uso de distintas técnicas como protocolos virtuales de *tunnelling* o cifrado de tráfico.

Una VPN brinda protección al cifrar y ocultar el tráfico de red. También redirige los paquetes de datos a través de los servidores VPN. Al hacerlo, una VPN cambia la dirección IP visible del usuario, adicionalmente, una VPN hace que parezca que el usuario está navegando desde la ubicación del servidor VPN en lugar desde el dispositivo original desde donde el usuario navega. Es por esta razón que una VPN permite que un usuario pueda *aparecer* prácticamente en cualquier parte del mundo mediante la red.

Cuando un usuario se conecta a Internet a través de una VPN, esta establece un túnel virtual seguro entre el dispositivo y uno de sus servidores. Este túnel se utiliza para transferir todo el tráfico de Internet procedente de las aplicaciones y los sitios web que el usuario visite.

Aunque la conexión VPN va un paso más allá y para garantizar la seguridad del proceso de tunelización, el cliente VPN y el servidor VPN cifran los datos utilizando una clave compartida. El cliente VPN y el servidor VPN hacen este proceso de cifrado cada vez que los datos viajan a través del túnel cifrado. De este modo, nadie podrá husmear en el tráfico que pasa por el túnel. De este modo, una VPN garantiza que la dirección IP, ubicación e identidad del usuario permanezcan ocultas al proveedor de servicios de Internet y a los sitios web de terceros.

Existen algunos servicios que permiten la creación de una red VPN, una de ellas es PPTP, el cual es el que será usado en la realización de esta práctica. El PPTP (Point-to-Point Tunneling Protocol o Protocolo de Túnel Punto a Punto) es un protocolo de red creado por Microsoft y utilizado para crear túneles VPN entre redes públicas. Los servidores PPTP también se conocen como servidores de Virtual Private Dialup Network (VPDN). PPTP es preferible a otros protocolos VPN porque es más rápido y tiene la capacidad de trabajar con dispositivos móviles. Se puede configurar un total de diez túneles PPTP en un servidor PPTP. Es un protocolo muy estable, rápido y es nativo en la mayoría de los Sistemas Operativos de muchos dispositivos.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 396/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

acuerdo al protocolo de red transmitido. En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RSA RC4 a partir del password del usuario. La longitud de dicha clave puede ser de 128 o 40 bits.

3.- Equipo y material necesario

Equipo del laboratorio:

- PC con sistema operativo Linux, Debian.

4.- Desarrollo

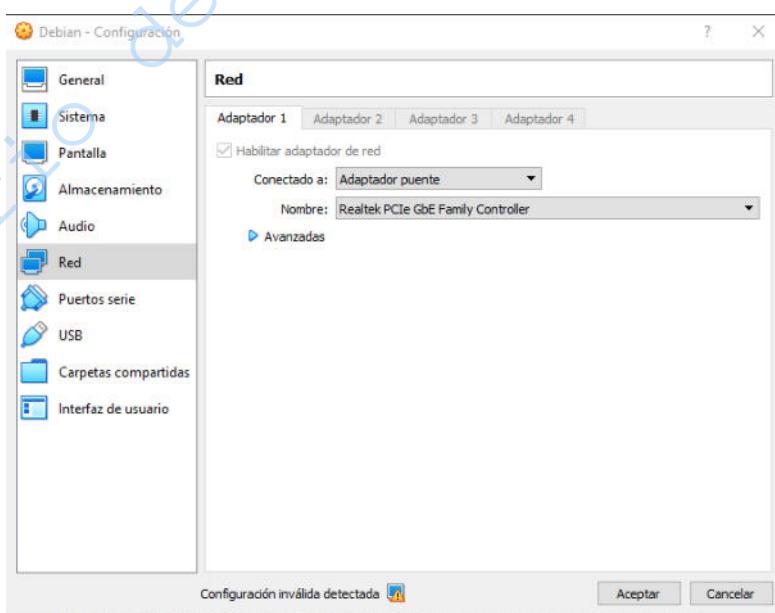
Modo de trabajar

La práctica se desarrollará por mesa de dos parejas.

4.1 Creación de VPN.

4.1.1 Elija una de las dos computadoras de la mesa y en ella abra la aplicación VirtualBox.

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 1).



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	397/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Figura No. 1. Conexión de red en la máquina virtual.

- 4.1.2 Encienda la máquina virtual.
- 4.1.3 Elija la opción de cargar Linux, distribución Debian.
- 4.1.4 Inicie sesión en la cuenta de redes.
- 4.1.5 Abra una terminal e ingrese como super usuario, para ello teclee el comando que se muestra a continuación.

```
redes@debian:~$ su
Contraseña:
```

NOTA: Despues de ejecutar el primer comando, le pedirá ingresar la contraseña del usuario root.

- 4.1.6 Instale la herramienta del servidor PPTPD, mediante el siguiente comando:

```
redes@debian:/home/redes# apt-get install pptpd
```

- 4.1.7 Una vez que se instaló la herramienta, ingrese el comando siguiente para conocer la IP asignada a la máquina virtual (Figura No. 2).

```
redes@debian:/home/redes# ifconfig
```

```
root@debian:/home/redes# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:47:2d:34
          inet addr:192.168.2.40 Bcast:192.168.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe47:2d34/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:158506 (154.7 KiB) TX bytes:19933 (19.4 KiB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3779 (3.6 KiB) TX bytes:3779 (3.6 KiB)
```

Figura No. 2. Direcciones IP.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	398/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Anote la dirección IP de la máquina virtual.

- 4.1.8** Ejecute ahora el siguiente comando para comenzar con la configuración del servidor PPTPD (Figura No. 3).

```
redes@debian:/home/redes# nano /etc/pptpd.conf
```

Al entrar en la edición de este archivo, vaya hasta el final del archivo y ubique las siguientes líneas:

```
# (Recommended)
#localip 192.168.0.1
#remoteip 192.168.0.234-238,192.168.0.245
# or
#localip 192.168.0.234-238,192.168.0.245
#remoteip 192.168.1.234-238,192.168.1.245
```

Figura No. 3. Líneas a modificar en el archivo pptpd.conf.

Elimine los hash (#) de las líneas *localip* y *remoteip* y cambie el parámetro de la línea *localip* por la dirección IP anotada en el punto 4.1.7. Lo demás puede dejarlo sin modificaciones.

Guarde los cambios y salga del editor.

- 4.1.9** Ingrese el siguiente comando en la consola para poder editar ciertas configuraciones del servidor VPN.

```
redes@debian:/home/redes# nano /etc/ppp/pptpd-options
```

Al entrar en la edición de este archivo, ubique la sección mostrada en la Figura No. 4 y cambie el nombre del servidor al que usted decida, dejando la palabra *name* y escribiendo después el nombre elegido.

```
# Name of the local system for authentication purposes
# (must match the second field in /etc/ppp/chap-secrets entries)
name pptpd
```

Figura No. 4. Nombre del servidor VPN.

Escriba a continuación el nombre que le dio al servidor:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	399/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Dentro de ese mismo archivo, baje y encuentre la sección mostrada en la Figura No. 5.

```
# If pppd is acting as a server for Microsoft Windows clients, this
# option allows pppd to supply one or two DNS (Domain Name Server)
# addresses to the clients. The first instance of this option
# specifies the primary DNS address; the second instance (if given)
# specifies the secondary DNS address.
# Attention! This information may not be taken into account by a Windows
# client. See KB311218 in Microsoft's knowledge base for more information.
#ms-dns 10.0.0.1
#ms-dns 10.0.0.2
```

Figura No. 5. DNS.

Ahí deberá eliminar los hash (#) de las líneas de *ms-dns* y agregar lo siguiente:

**ms-dns 8.8.8.8
ms-dns 8.8.4.4**

Guarde los cambios y salga del editor.

4.1.10 Ingrese el siguiente comando en la consola para poder agregar usuarios del servidor VPN.

redes@debian:/home/redes# nano /etc/ppp/chap-secrets

Dentro de ese archivo, deberá agregar:

- Un cliente.
- El nombre del servidor VPN (escrito en el punto 4.1.9).
- La contraseña del usuario
- Las direcciones IP que podrá tomar para usar ese usuario. Para este caso se escribirá un * para que cualquier IP pueda usar ese usuario.

Escriba a continuación el usuario y la contraseña que definió para el nuevo cliente.

Verifique que el archivo quede similar a la Figura No. 6.

# Secrets for authentication using CHAP	IP addresses
# client server secret	*
LabRedesVPN RedVPN D1oSe520	

Figura No. 6. Creación de un nuevo cliente.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	400/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Guarde los cambios y salga del editor.

- 4.1.11** Ejecute el siguiente comando para poder reiniciar el servicio de PPTPD y que se apliquen los cambios hechos:

```
redes@debian:/home/redes# service pptpd restart
```

- 4.1.12** Ingrese el siguiente comando en la consola para poder habilitar el reenvío de paquetes a través de IPv4.

```
redes@debian:/home/redes# nano /etc/sysctl.conf
```

Dentro de ese archivo, encuentre la sección mostrada en la Figura No. 7.

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```

Figura No. 7. Reenvío de paquetes a través de IPv4.

Ahí deberá eliminar el hash (#) de la línea de *net.ipv4.ip_forward=1*.

Guarde los cambios y salga del editor. En seguida, ejecute el siguiente comando:

```
redes@debian:/home/redes# sysctl -p
```

- 4.1.13** En esa terminal ejecute uno a uno los siguientes cuatro comandos:

```
redes@debian:/home/redes# iptables -I INPUT -p tcp --dport 1723 -m state --state NEW -j ACCEPT
```

```
redes@debian:/home/redes# iptables -I INPUT -p gre -j ACCEPT
```

```
redes@debian:/home/redes# iptables -t nat -I POSTROUTING -o enp0s3 -j MASQUERADE
```

```
redes@debian:/home/redes# iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN -s [IPADDRESS]/24 -j TCPMSS --clamp-mss-to-pmtu
```

NOTA: El único parámetro de los comandos anteriores que debe cambiar es el de *[IPADDRESS]*, ahí deberá colocar la IP del servidor VPN definida en el punto 4.1.7.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 401/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2 Conexión a la VPN

- 4.2.1 En la otra computadora; es decir, en la que no creó la VPN, encienda el sistema y elija la opción de cargar Windows.
- 4.2.2 Inicie sesión en una cuenta con privilegios de administrador.
- 4.2.3 Una vez iniciada sesión, abra el panel de control y haga clic en el rubro de Redes e Internet (Figura No. 8).

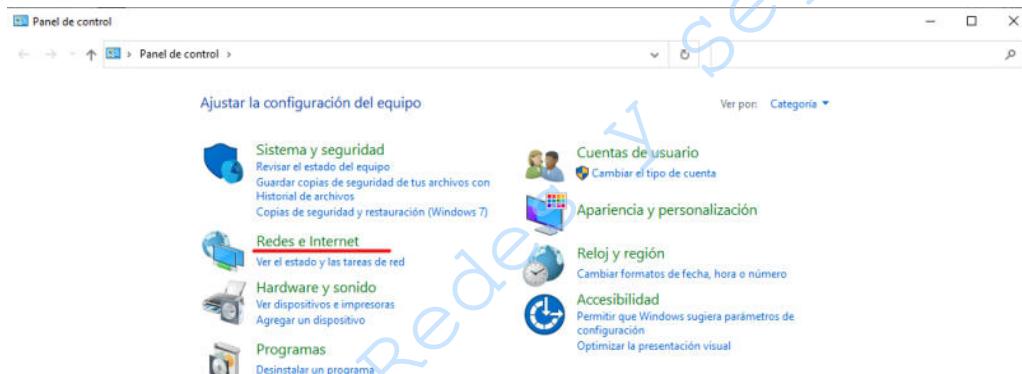


Figura No. 8. Panel de control.

- 4.2.4 Una vez dentro, haga clic en la sección de Centro de redes y recursos compartidos (Figura No. 9).

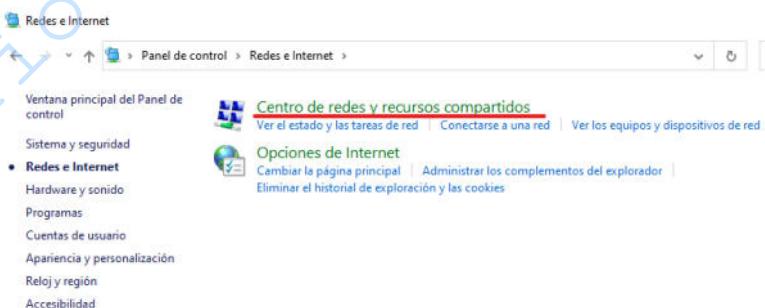


Figura No. 9. Redes e internet.

- 4.2.5 Ahora proceda a configurar una nueva conexión o red.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 402/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

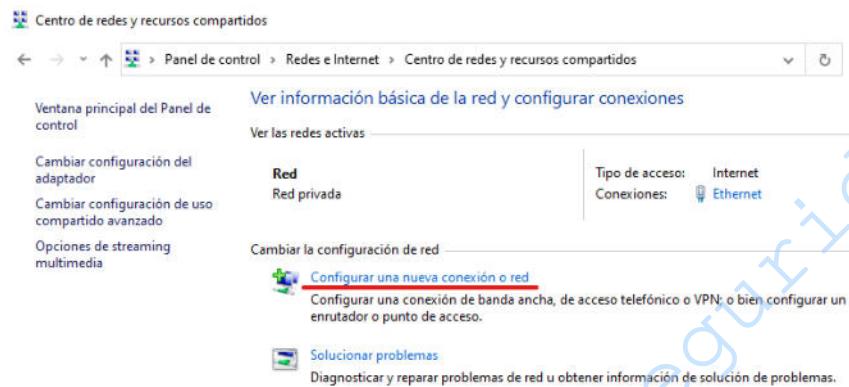


Figura No. 10. Centro de redes y recursos compartidos.

Aquí seleccione la opción de Conectarse a un área de trabajo (Figura No. 11).

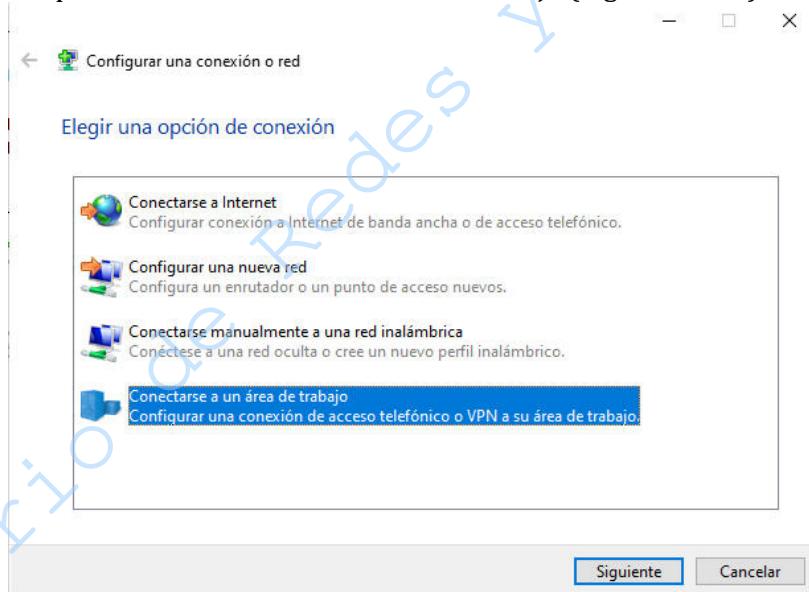


Figura No. 11. Configurar una conexión o red.

Le preguntará el sistema cómo es que desea conectarse, haga clic en la opción de Usar mi conexión a Internet (VPN).

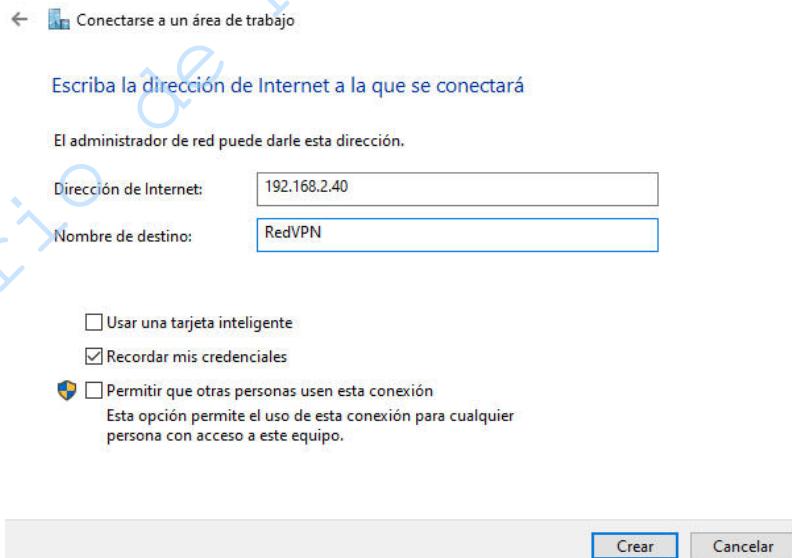
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 403/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 12. Conectarse a un área de trabajo.

Ahora deberá ingresar los siguientes parámetros (Figura No. 13):

- *Dirección de internet.* Es la investigada en el punto 4.1.7
- *Nombre de destino.* Es el definido en el punto 4.1.9



← Conectarse a un área de trabajo

Escriba la dirección de Internet a la que se conectará

El administrador de red puede darle esta dirección.

Dirección de Internet: 192.168.2.40

Nombre de destino: RedVPN

Usar una tarjeta inteligente
 Recordar mis credenciales
 Permitir que otras personas usen esta conexión
Esta opción permite el uso de esta conexión para cualquier persona con acceso a este equipo.

Crear Cancelar

Figura No. 13. Parámetros de VPN.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 404/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.6** Ya que fue creada la VPN, se deberá conectar a ella. Haga clic en el ícono de Red (💻) presente en la Barra de Tareas de Windows, ubique y seleccione la opción de Configuración de red e Internet (Figura No. 14).

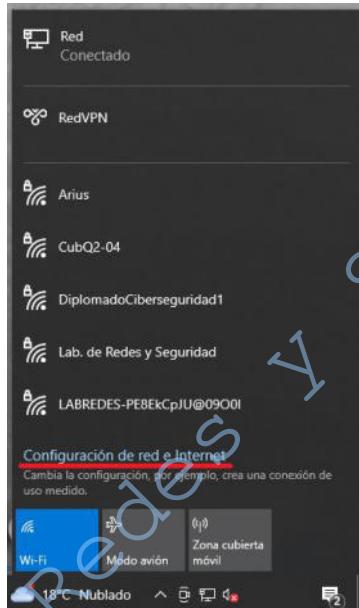


Figura 14. Redes disponibles.

Dentro de la configuración de red, ingrese a la sección de VPN (Figura No. 15).

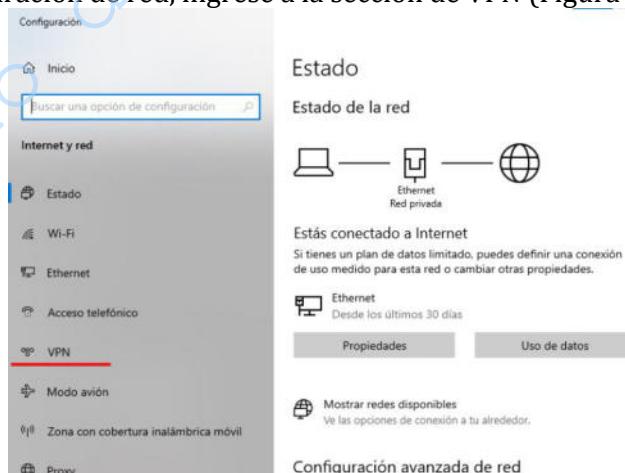


Figura No. 15. Configuración de red e internet.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 405/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

En la sección de VPN aparecerán las redes VPN disponibles, ahí deberá ver la que acaba de crear, haga clic sobre ella y conéctese (Figura No. 16).



Figura No. 16. Conexión a VPN.

Después de unos segundos, le pedirá iniciar sesión, aquí deberá ingresar las credenciales del usuario definido en el punto 4.1.10 (Figura No. 17).

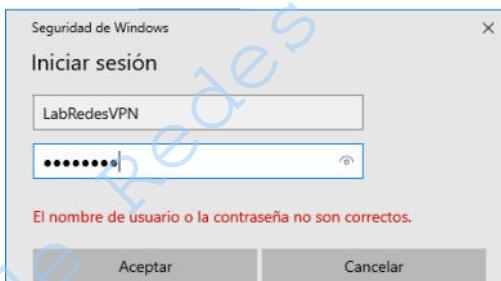


Figura No. 17. Inicio de sesión a la VPN.

Antes de dar clic en Aceptar, asegúrese que escribió correctamente el usuario y la contraseña. Al Aceptar, después de unos segundos, deberá aparecer que se ha conectado a la VPN (Figura No. 18).

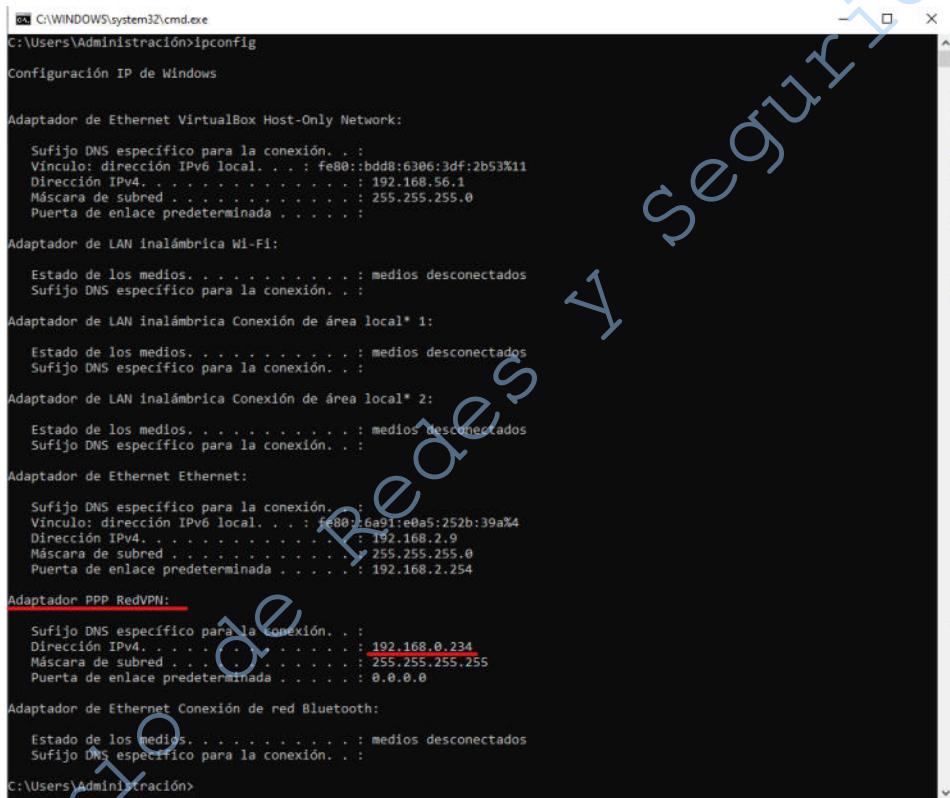


Figura No. 18. Conexión exitosa a la VPN.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 406/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.2.7** Para comprobar que la conexión fue realmente exitosa, acceda a la terminal CMD de Windows (WINDOWS+R -> cmd -> ENTER). Una vez ahí, escriba el siguiente comando (Figura No. 19):

C:\Users\Administración>ipconfig



```

C:\Windows\system32\cmd.exe
C:\Users\Administración>ipconfig

Configuración IP de Windows

Adaptador de Ethernet VirtualBox Host-Only Network:
  Sufijo DNS específico para la conexión. . .
  Vinculo: dirección IPv6 local. . . : fe80::bdd8:6306:3df:2b53%11
  Dirección IPv4. . . . . : 192.168.56.1
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . .

Adaptador de LAN inalámbrica Wi-Fi:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . .

Adaptador de LAN inalámbrica Conexión de área local* 1:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . .

Adaptador de LAN inalámbrica Conexión de área local* 2:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . .

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . .
  Vinculo: dirección IPv6 local. . . : fe80::6a91:e0a5:252b:39a%4
  Dirección IPv4. . . . . : 192.168.2.9
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . : 192.168.2.254

Adaptador PPP RedVPN:
  Sufijo DNS específico para la conexión. . .
  Dirección IPv4. . . . . : 192.168.0.234
  Máscara de subred . . . . . : 255.255.255.255
  Puerta de enlace predeterminada . . . . : 0.0.0.0

Adaptador de Ethernet Conexión de red Bluetooth:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . .

C:\Users\Administración>

```

Figura No. 19. Comando ipconfig.

Aquí busque la red VPN creada y verifique la dirección IP asignada, esta deberá coincidir con el rango especificado en el archivo /etc/pptpd.conf del punto 4.1.7.

- 4.2.8** Si la conexión fue exitosa, debería de poder conectarse sin inconveniente alguno a internet.

Abra un navegador y acceda a cualquier página web.

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	407/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 408/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 11

VPN

Cuestionario Previo

1. Mencione y describa 3 ejemplos del uso de una VPN.
2. Investigue al menos 5 nombres de proveedores de VPN.
3. Dibuje y describa un diagrama de cómo funciona un servicio de VPN.
4. ¿Qué características de seguridad provee una VPN?
5. Mencione y describa los distintos tipos de VPN que existen.
6. ¿Para qué se usa el comando apt-get install pptpd o apt install pptpd?
7. Investigue qué es el editor nano y cuáles son sus comandos principales.
8. ¿Para qué se usa el comando ipconfig en Windows?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO Fecha de emisión	MADO-31 06 409/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 12

Firewall básico

Capa 7 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	410/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

1.- Objetivos de Aprendizaje

- El alumno o la alumna analizará, investigará e implementará mecanismos adecuados de seguridad en los puertos lógicos de entrada de un servidor de red.
- El alumno o la alumna aprenderá las reglas básicas para implementar las distintas opciones de entrada de paquetes a través de un Firewall de seguridad en los puertos lógicos del servidor en red.

2.- Conceptos teóricos

Un servidor de red es un ordenador que ofrece el acceso a los recursos o servicios compartidos entre las estaciones de trabajo u otros servidores conectados en una red de datos. Los recursos o servicios compartidos pueden incluir acceso a hardware, como discos duros, impresoras, software, servicios de email o acceso a internet.

Un firewall, también conocido como cortafuegos, es un elemento informático (es decir, es un dispositivo de hardware o un software) que trata de bloquear el acceso, a una red privada conectada a Internet, a usuarios no autorizados. Por tanto, el cortafuegos se centra en examinar cada uno de los mensajes que entran y salen de la red para obstruir la llegada de aquellos que no cumplen con unos criterios de seguridad, al tiempo que da vía libre a las comunicaciones que sí están reglamentadas.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

- Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.
- Registrar todos los intentos de entrada y salida de una red. Los intentos de entrada y salida se almacenan en logs.
- Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones. Así por lo tanto con el filtro de direcciones se puede bloquear o aceptar el acceso a un equipo con cierta dirección IP a través del puerto 22. Recordar sólo que el puerto 22 acostumbra a ser el puerto de un servidor SSH.
- Filtrar determinados tipos de tráfico en la red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son http, https, Telnet, TCP, UDP, SSH, FTP, etcétera.
- Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.
- Controlar las aplicaciones que pueden acceder a Internet. Así por lo tanto se puede restringir el acceso a ciertas aplicaciones, como por ejemplo dropbox, a un determinado grupo de usuarios.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	411/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

- Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

3.- Equipo y material necesario

Equipo del Laboratorio:

- Software de simulación de redes Cisco Packet Tracer.

4.- Desarrollo

En esta práctica se realizarán y explicarán las reglas para restringir el acceso a la entrada de los puertos lógicos de un servidor en red. Es importante mencionar que existen distintos tipos de servidores de red con una gran variedad de sistemas operativos, pero en general las reglas de un firewall aplican a todos ellos.

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Construcción de la topología

- 4.1.1** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 1)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 412/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

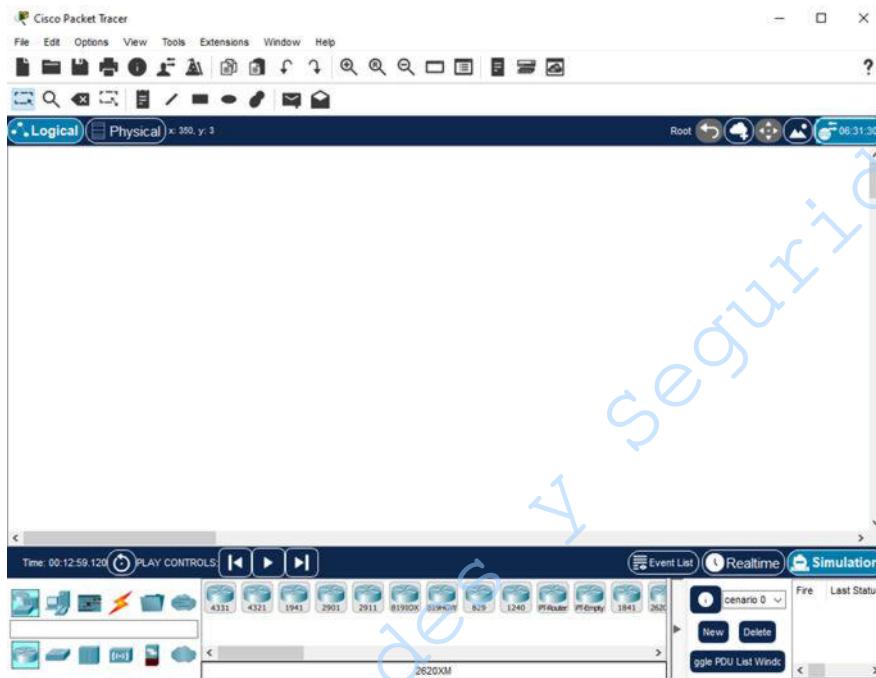


Figura No. 1. Interfaz gráfica de PT

- 4.1.2** Cuando Packet Tracer se inicia, muestra por default una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.
- 4.1.3** En la esquina inferior izquierda de la interfaz se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo (Ver figura No. 2.)



Figura No. 2. Secciones de dispositivos

- 4.1.4** La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos, en el cuadro de texto del centro aparece el nombre de este grupo.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 413/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1.5 La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán.

4.1.6 Con ayuda de su profesora o profesor realice una topología básica de red agregando al área de trabajo de Packet Tracer 2 switches de 24 puertos (modelo 2950-24), 1 router genérico (router-PT), un par de servidores (server-PT) y 3 dispositivos finales (2 PC y una laptop), como se muestra en la figura No. 3.

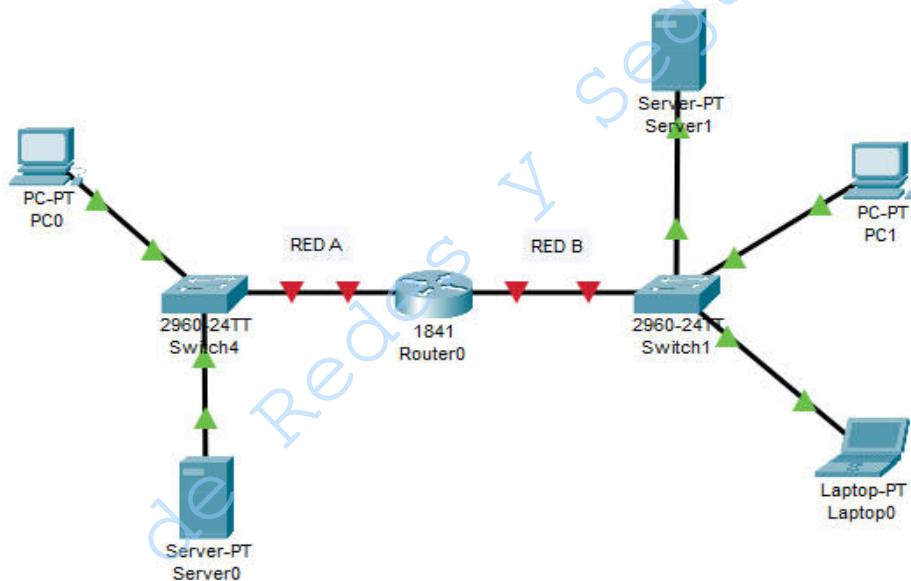


Figura No. 3. Topología básica

4.1.7 Conecte la interfaz FastEthernet 0/0 del Router0 con la interfaz FastEthernet 0/1 del Switch0 y la interfaz FastEthernet 1/0 del Router0 con la interfaz FastEthernet 0/1 del Switch1.

4.1.8 Conecte la interfaz FastEthernet 0/2 del Switch0 con la interfaz FastEthernet 0 del Server0 y la interfaz FastEthernet 0/3 del Switch0 con la interfaz FastEthernet 0 de la PC0.

4.1.9 Conecte la interfaz FastEthernet 0/2 del Switch1 con la interfaz FastEthernet 0 del Server1, la interfaz FastEthernet 0/3 del Switch1 con la interfaz FastEthernet 0 de la PC1 y la interfaz FastEthernet 0/4 del Switch1 con la interfaz FastEthernet 0 de la Laptop0.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	414/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2 Configuración de las interfaces del router

- 4.2.1** Seleccione el Router0 y dé clic sobre la pestaña CLI.
- 4.2.2** Para configurar la interfaz FastEthernet 0/0 deben teclearse los siguientes comandos:

```
Router>enable
Router#configure t
Router(config)#int FastEthernet 0/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

NOTA: DIR_IP se sustituye por la última dirección IP utilizable de clase C para la red A

- 4.2.3** Para configurar la interfaz FastEthernet 1/0 deben teclearse los siguientes comandos:

```
Router>enable
Router#configure t
Router(config)#int FastEthernet 1/0
Router(config-if)#ip address DIR_IP 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la clase A para la red B

- 4.2.4** Explique qué sucede en la ventana CLI cuando se ejecuta el comando show running-config.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 415/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

4.3 Configuración de los dispositivos

- 4.3.1 Dé clic sobre la PC conectada al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.3.2 Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.
- 4.3.3 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. Ingrese los datos que se muestran en la Tabla No.1.

Tabla No.1. Datos para la configuración de los dispositivos conectados al Switch0

IP Address	Cualquier dirección IP utilizable de la red A excepto la última Añote la dirección IP que empleó _____
Subnet Mask	255.255.255.0
Default Gateway	Dirección IP asignada a la interfaz Fa0/0 del Router0

- 4.3.4 Dé clic sobre el Server0 conectado al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.3.5 Seleccione la pestaña Desktop y seleccione IP Configuration.
- 4.3.6 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. utilice los datos de Subnet Mask y Default Gateway que se muestran en la Tabla No.1. y anote la dirección IP (distinta a la que utilizó en la PC0) que empleó _____.
- 4.3.7 Dé clic sobre la PC conectada al Switch1 en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.3.8 Seleccione la pestaña Desktop y seleccione IP Configuration.
- 4.3.9 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. Ingrese los datos que se muestran en la Tabla No.2.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	416/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Tabla No.2. Datos para la configuración de los dispositivos conectados al Switch1

IP Address	Cualquier dirección IP utilizable de la red B excepto la primera Añote la dirección IP que empleó _____
Subnet Mask	255.0.0.0
Default Gateway	Dirección IP asignada a la interfaz Fa1/0 del Router0

4.3.10 Dé clic sobre el Server1 conectado al Switch1 en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.3.11 Seleccione la pestaña Desktop y seleccione IP Configuration.

4.3.12 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. utilice los datos de Subnet Mask y Default Gateway que se muestran en la Tabla No.2. y anote la dirección IP (distinta a la que utilizó en la PC1) que empleó_____.

4.3.13 Dé clic sobre la Laptop0 conectado al Switch1 en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.3.14 Seleccione la pestaña Desktop y seleccione IP Configuration.

4.3.15 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. utilice los datos de Subnet Mask y Default Gateway que se muestran en la Tabla No.2. y anote la dirección IP (distinta a la que utilizó en la PC1 y Server1) que empleó_____.

4.3.16 Para validar el funcionamiento de las comunicaciones entre los dispositivos de la red A y los de la red B, se debe dar clic en cualquier dispositivo de la red A (PC0 o Server0), seleccione la pestaña Desktop y posteriormente seleccione la opción de Command Prompt como se muestra en la Figura No. 4.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 417/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

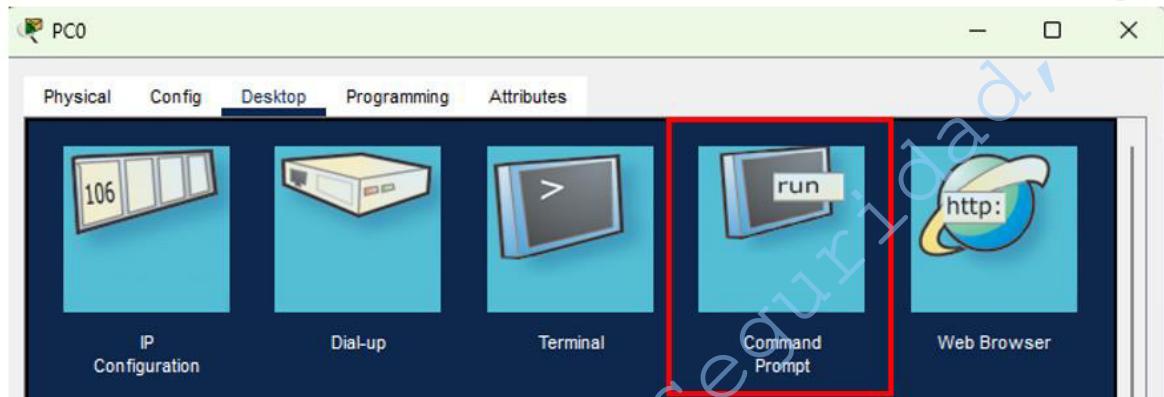


Figura No. 4. Seleccionando la Opción de Command Prompt

4.3.17 Usando el comando ping desde el dispositivo seleccionado de la red A pruebe la conexión con algún dispositivo de la red B. Anote los resultados obtenidos.

4.3.18 ¿Se logró establecer la comunicación? Explique

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 418/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.3.19** Seleccione nuevamente la pestaña Desktop y posteriormente seleccione la opción de Web Browser como se muestra en la Figura No. 5.

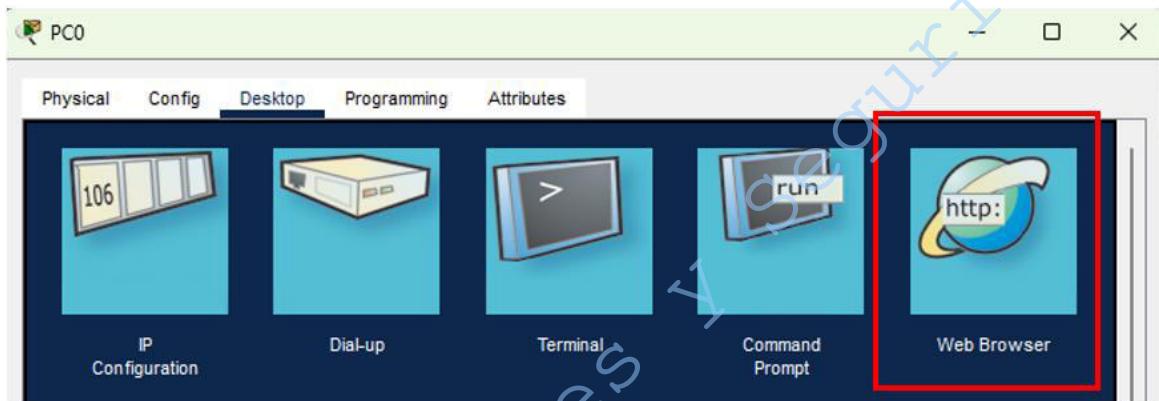


Figura No. 5. Seleccionando la Opción de Web Browser

- 4.3.20** Coloque en el URL del Web Browser del dispositivo seleccionado de la red A, la dirección IP del Server1 de la red B y pruebe la conexión. Anote los resultados obtenidos.

- 4.3.21** ¿Se logró establecer la comunicación? Explique
-
-
-

- 4.3.22** También puede probar la conectividad en el sentido inverso desde la red B hacia la red A. Indique el resultado obtenido.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 419/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.4 Configuración del Firewall a través del Router

- 4.4.1** Seleccione el Router0 y dé clic sobre la pestaña CLI y teclee lo siguiente:

```
Router>enable
Router#configure t
Router(config)# access-list 101 deny icmp any any host-unreachable
Router(config)# access-list 101 permit tcp any any eq www
Router(config)# interface FastEthernet1/0
Router(config-if)# ip access-group 101 in
```

- 4.4.2** Para validar el funcionamiento de las comunicaciones entre los dispositivos de la red A y los de la red B, se debe dar clic en cualquier dispositivo de la red B (PC1 o Laptop1) seleccione la pestaña Desktop y posteriormente seleccione la opción de Command Prompt como se muestra en la Figura No. 6.

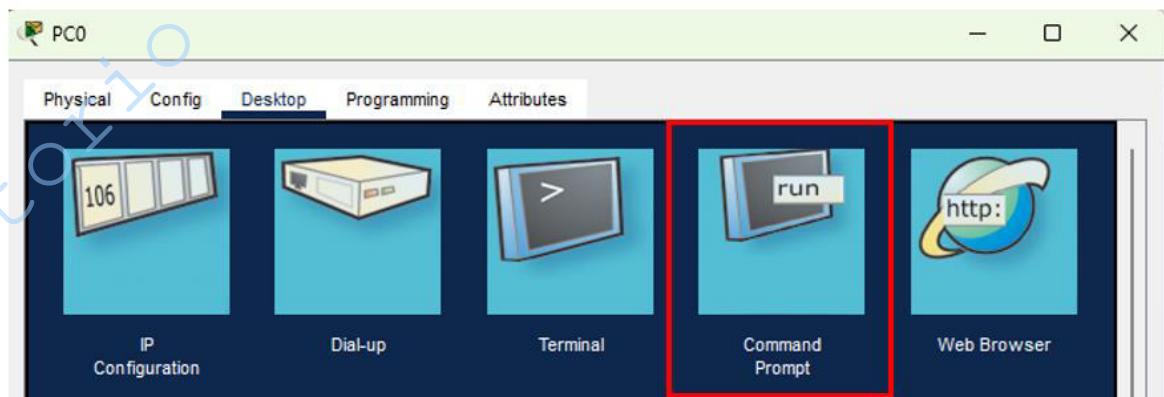


Figura No. 6. Seleccionando la Opción de Command Prompt

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	420/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.4.3** Usando el comando ping desde el dispositivo seleccionado de la red B pruebe la conexión con el Server0 de la red A. Anote los resultados obtenidos.

()

- 4.4.4** De acuerdo con las reglas de entrada puestas en el Router0 ¿Se logró el bloqueo de los paquetes de entrada en la interfaz Ethernet 1/0 del router? Explique
-
-
-

- 4.4.5** Seleccione nuevamente la pestaña Desktop y posteriormente seleccione la opción de Web Browser como se muestra en la Figura No. 7.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 421/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

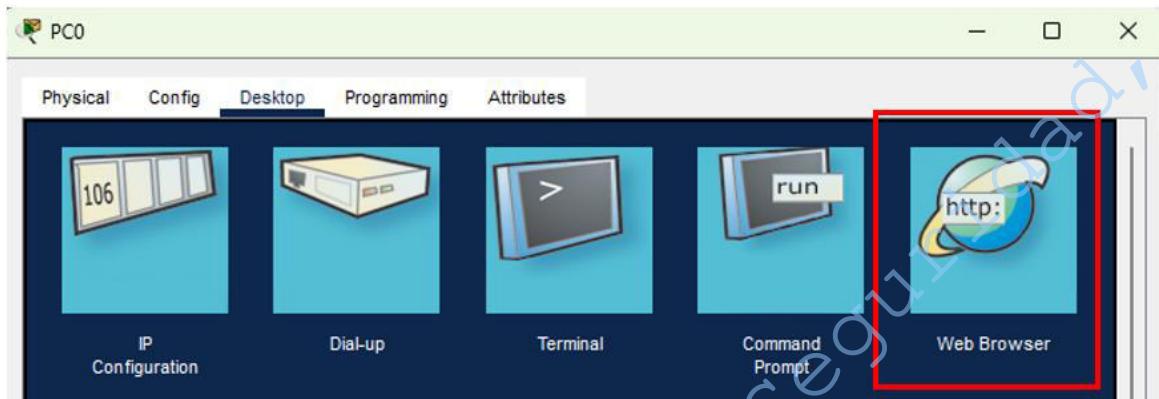


Figura No. 7. Seleccionando la Opción de Web Browser

- 4.4.6** Coloque en el URL del Web Browser del dispositivo seleccionado de la red B la dirección IP del Server0 de la red A y pruebe la conexión. Anote los resultados obtenidos.

- 4.4.7** De acuerdo con las reglas de entrada puestas en el Router0 verificar si se permite la entrada de los paquetes http en la interfaz Ethernet 1/0 del router. Anote los resultados obtenidos.

- 4.4.8** También es importante probar la conectividad en el sentido inverso desde la red A hacia la red B. Tomando un dispositivo de la red A y repitiendo los pasos desde el 4.4.2 hasta

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	422/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

el 4.4.7. Ya que la respuesta que se obtiene no es host-unreachable, indique los resultados obtenidos haciendo uso del comando ping.

4.4.9 Indique los resultados obtenidos haciendo uso del Web browser.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	423/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

EJERCICIO OPCIONAL

4.5 Implementar políticas de acceso al puerto de entrada del Router en la Interfaz Fast Ethernet 0/0 para permitir el acceso al Ping

Las instrucciones para implementar las reglas del firewall que permitan la entrada de los paquetes Ping dentro de la red B, las puede deducir del apartado **Configuración del Firewall a través del Router**.

4.5.1 Proceda a realizar el escenario para definir las reglas de configuración del firewall y así usted podrá definir cuáles servicios se pueden acceder desde una red externa e incluso de alguna que pertenezca a Internet y que sea capaz de acceder a su red local.

4.5.2 Indique los comandos tecleados.

4.5.3 Valide el funcionamiento de las comunicaciones entre los dispositivos de la red A y los de la red B, tomando un dispositivo de la red A y repitiendo los pasos del 4.4.2 al 4.4.7. Indique los resultados obtenidos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	424/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	425/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 12

Firewall básico

Cuestionario Previo

1. Mencione la definición de red local y red externa.
2. ¿Qué es un Firewall?
3. Mencione las características de un Firewall con reglas de entrada.
4. ¿Qué es un servidor de red?
5. ¿Para qué sirve el servicio ICMP?
6. ¿Para qué sirve el comando access-list 101 deny icmp any any host-unreachable?
7. ¿Para qué sirve el comando access-list 101 permit tcp any any eq www?
8. ¿Para qué sirve el comando ip access-group 101 in?
9. ¿Cuál es la diferencia entre un Firewall perimetral y uno local?
10. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	426/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 13

Configuración básica de una comunicación de Voz IP

Capa 7 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	427/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

1.- Objetivos de Aprendizaje

- El alumno o la alumna realizará la configuración básica de una VLAN de voz y de datos.
- El alumno o la alumna manipulará de manera lógica equipos de interconexión como son routers y switches mediante el uso de la herramienta de simulación de redes Cisco Packet Tracer.

2.- Conceptos teóricos

Una VLAN (Virtual LAN) funciona igual que una LAN, pero con la diferencia de que los equipos o estaciones de trabajo no necesariamente deben estar ubicados en un mismo segmento físico, es decir, agrupa a un conjunto de dispositivos de red de manera lógica.

Enlace troncal

Los enlaces troncales son capaces de transportar el tráfico de más de una VLAN y se suele utilizar para interconectar dos switches, un switch y un router, un switch y un servidor, al cual se le ha instalado una tarjeta de red, capaz de soportar trunking. Los enlaces troncales permiten transportar de manera lógica las VLAN utilizando un enlace físico. (ver Figura No. 1)



Figura No. 1 Enlace troncal

IEEE 802.1Q

El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE que se utilizó para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

Características:

- Las VLAN permiten dividir la red local en redes virtuales.
- Los equipos de la red que pertenecen a la misma VLAN pueden comunicarse entre ellos como si estuviesen conectados al mismo switch.
- Para que exista comunicación entre los diferentes hosts se requiere de un dispositivo de capa 3.
- A cada VLAN se le asigna un identificador (ID).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 428/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

Ventajas:

- Permiten reconfigurar si hay un cambio sin tocar cables ni switches.
- Aumenta la seguridad.
- Aumenta el rendimiento de la red al separar dominios de difusión.
- La organización de la red se basa en las tareas de los usuarios y no en su localización física.

Tipos de VLAN:

- a) **VLAN DE DATOS:** Es una VLAN configurada para enviar solamente tráfico de datos que es generado por el usuario.
- b) **VLAN PREDETERMINADA:** La VLAN predeterminada para los switches de Cisco es la VLAN 1 y tiene todas las características de cualquier VLAN, excepto que no se puede volver a denominar ni se puede eliminar.
- c) **VLAN NATIVA:** Una VLAN nativa está asignada a un puerto troncal 802.1Q y admite el tráfico que llega de muchas VLAN. Sirve como un identificador común en extremos opuestos de un enlace troncal.
- d) **VLAN DE ADMINISTRACIÓN:** Es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. Se asigna una dirección IP y una máscara de subred. Se puede manejar un switch mediante HTTP, telnet, SSH o SNMP.
- e) **VLAN DE VOZ:** Es recomendable separar el tráfico de la VLAN de DATOS y de la VLAN de VOZ ya que si no se separa se puede perder la calidad de transmisión en una llamada y no será posible comprender lo que la persona que la está utilizando quiere decir.

El tráfico de VoIP requiere:

- Ancho de banda para asegurar la calidad de la voz.
- Prioridad de la transmisión sobre los tipos de tráfico de la red.
- Capacidad para ser enrutado en áreas congestionadas de la red.

La función de la VLAN de voz permite que los puertos de switch envíen tráfico de voz IP desde un teléfono IP. Cuando se conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado que envíe el tráfico de voz etiquetado con un ID de VLAN de voz.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	429/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada	

3.- Equipo y material necesario

Equipo del Laboratorio

- Software de Simulación Cisco Packet Tracer

4.- Desarrollo

La práctica tiene por objetivo conocer los comandos básicos para configurar una comunicación de VozIP en los routers y switches mediante el uso de VLAN.

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Configuración de las VLAN

- 4.1.1** Encienda el sistema y elija la opción de cargar Windows.
- 4.1.2** Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.3** Ejecute la aplicación Cisco Packet Tracer (Ver Figura No. 2).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	430/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

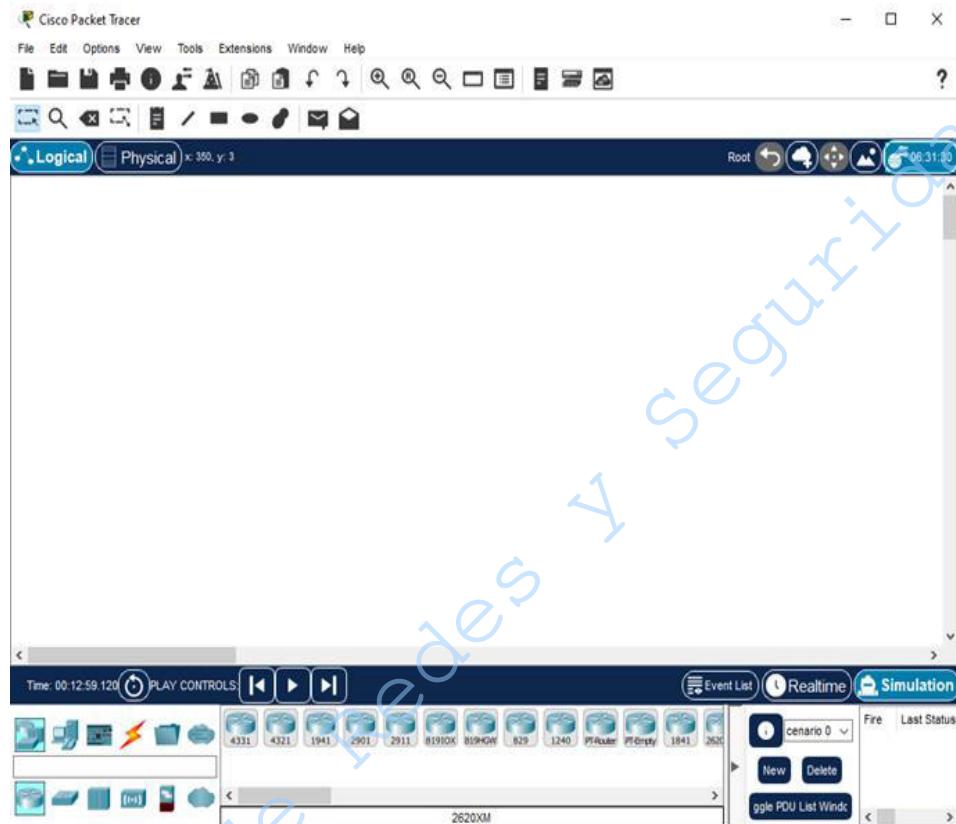


Figura No. 2. Simulador de Cisco Packet Tracer

El objetivo de la Figura No. 3 será conocer la aplicación y los elementos importantes:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 431/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

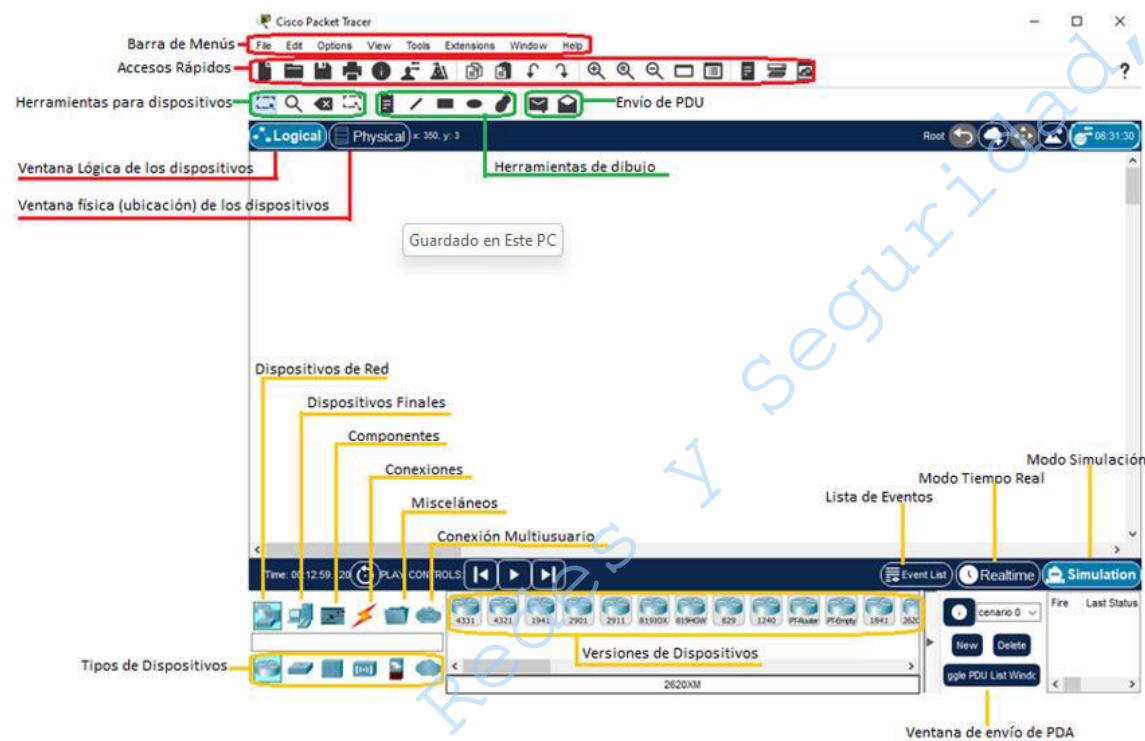


Figura No. 3. Área de Trabajo del simulador de Cisco Packet Tracer



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	432/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- 4.1.4** Agregue al área de trabajo los siguientes componentes así como se muestra en la figura No. 4.

2 routers 2811
2 switches 2960-24
2 laptop-PT
2 IP Phone 7960

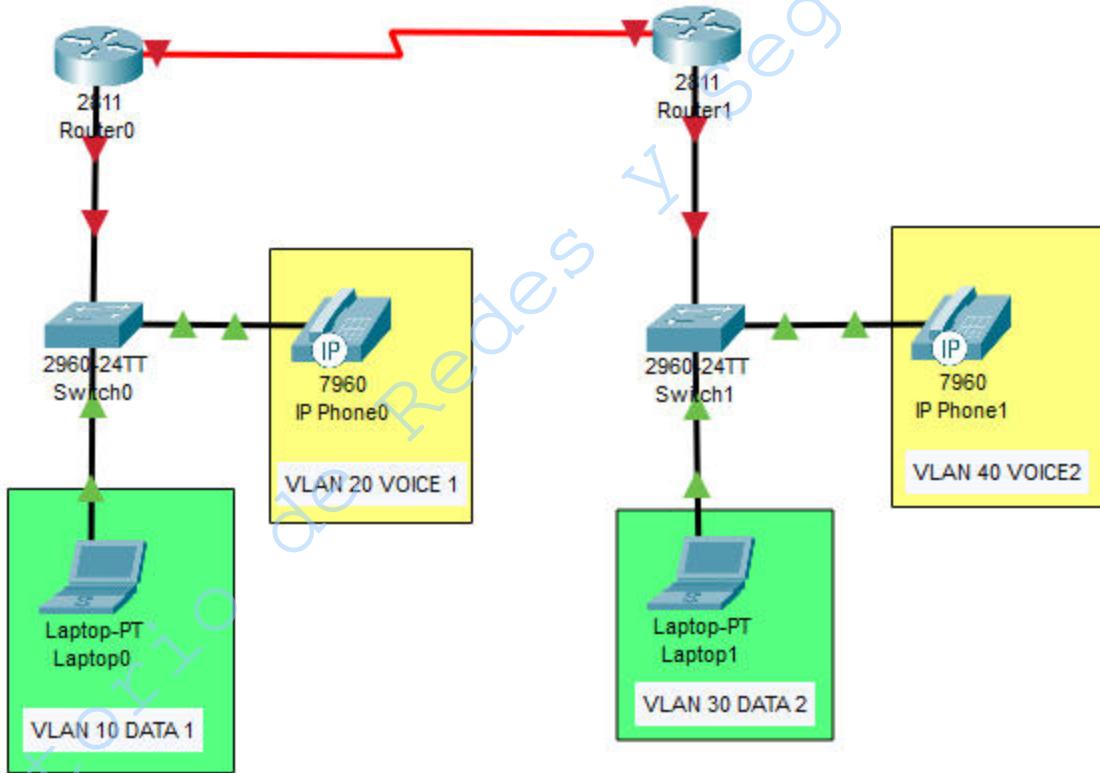


Figura No. 4 Topología de Red.

- 4.1.5** Las conexiones deben realizarse con base en la tabla No. 1.

NOTA: Con ayuda de su profesora o profesor agregue la interfaz Serial WIC-2T en el Router 2811 ya que es necesaria.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 433/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

Tabla 1. Conexiones entre dispositivos

RED	Dispositivo Inicial e Interfaz	Dispositivo Final e Interfaz
	Router0 Se0/0/0	Router1 Se0/0/0
	Router0 Fa0/0	Switch0 Fa0/1
	Router1 Fa0/0	Switch1 Fa0/1
VLAN 10	Laptop0 Fa0	Switch0 Fa0/2
VLAN 20	Switch	Switch0 Fa0/24
VLAN 30	Laptop1 Fa0	Switch1 Fa0/2
VLAN 40	Switch	Switch1 Fa0/24

- 4.1.6** Para conectar el teléfono dé clic sobre éste y diríjase a la pestaña Physical, arrastre el cable de corriente y conéctelo al dispositivo tal y como se muestra en la Figura No. 5. Realice ese mismo paso para el IP Phone 2.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 434/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

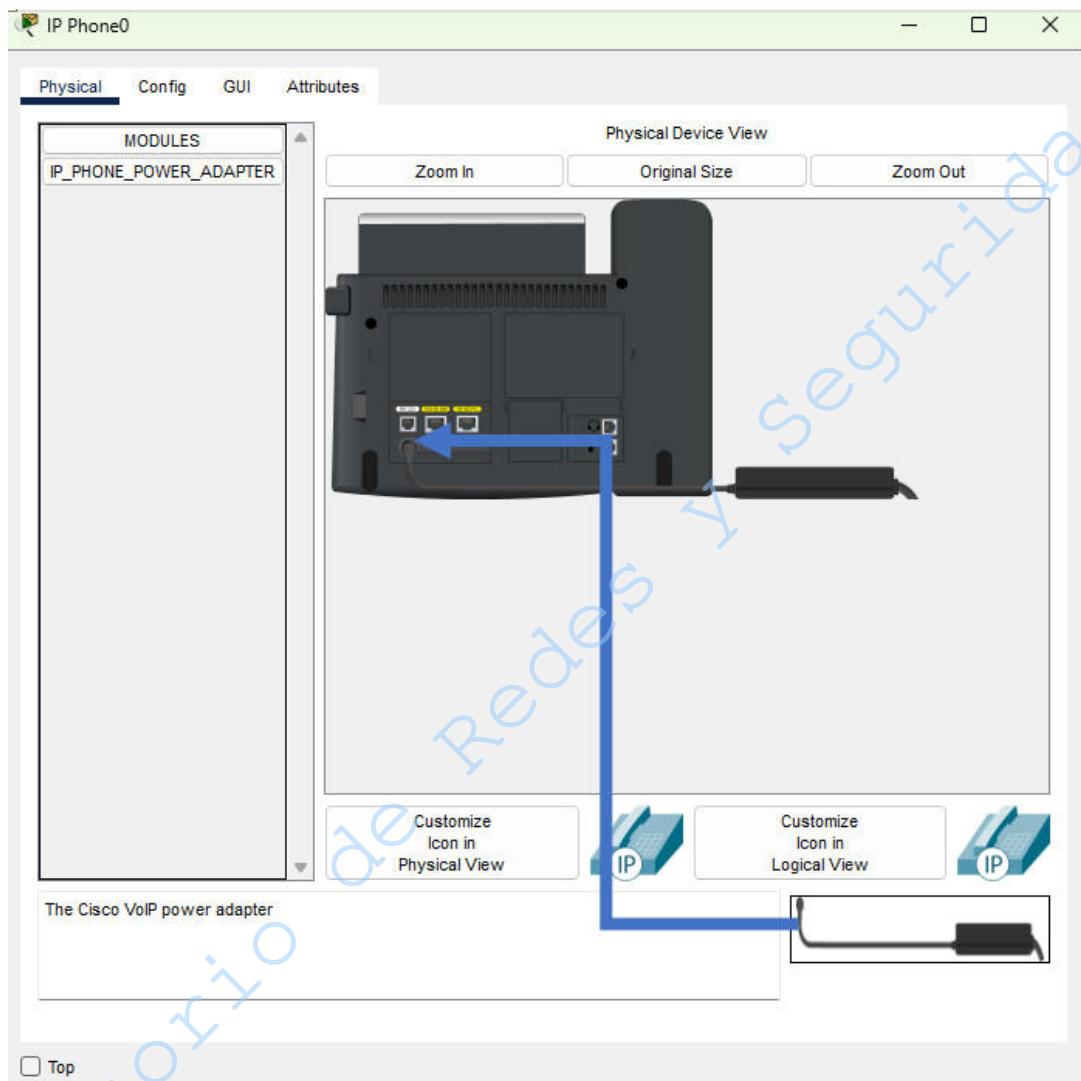


Figura No. 5. Conexión del cable de corriente

4.2 Configuración de contraseñas de acceso a los dispositivos Switch y Router.

Cuando se implementa una red, es necesario que los dispositivos que se desean configurar tengan como medida básica el establecimiento de contraseñas de acceso a las configuraciones de los equipos, ya que en caso de no contar con este nivel de protección, cualquier usuario mal intencionado puede tener el control y hacer un uso indebido del equipo.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	435/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Existe la configuración de contraseñas en modo privilegiado y la configuración de terminal virtual y consola, los cuales deberá configurar en al menos 1 solo equipo (router o switch).

- 4.2.1** Para la contraseña de acceso en modo privilegiado, introduzca los siguientes comandos:

Ejemplo para el switch0:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch0
Switch0(config)#enable secret PALABRA_CLAVE
Switch0(config)#end
Switch0>
```

NOTA: **PALABRA_CLAVE** se sustituye por una palabra que el usuario quiera establecer como contraseña.

Anote la **PALABRA_CLAVE** empleada _____

Hasta este punto solamente ha configurado la contraseña de acceso a modo privilegiado, para verificarlo introduzca nuevamente el siguiente comando. Si la configuración fue realizada de manera correcta le solicitará como password la palabra clave que previamente introdujo.

```
Switch0>enable
Password:
Switch0#config t
```

- 4.2.2** Para configurar la contraseña de acceso de terminal virtual y de consola, introduzca los siguientes comandos:

```
Switch0(config)#line console 0
Switch0(config-line)#password CONTRASEÑA
Switch0(config-line)#login
Switch0(config-line)#line vty 0 15
Switch0(config-line)#password CONTRASEÑA
Switch0(config-line)#login
Switch0(config-line)#exit
Switch0(config)# exit
Switch0# exit
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	436/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Switch0>

NOTA: CONTRASEÑA se sustituye por una palabra que el usuario quiera establecer como contraseña.

Anote la CONTRASEÑA empleada_____

Si la configuración se realizó correctamente verifique ingresando nuevamente al dispositivo y le deberá solicitar las contraseñas que previamente configuró.

NOTA: Para fines prácticos solamente se configurará un solo dispositivo.

4.3 Configuración de las VLAN

4.3.1 Para agregar una VLAN es necesario configurar su identificador y su nombre en cada switch. Dé clic sobre el Switch0 y diríjase a la pestaña CLI, en donde debe introducir los siguientes comandos:

```
Switch0>enable
Switch0#configure terminal
Switch0(config)#vlan vlan-id
Switch0(config-vlan)#name nombre_vlan
Switch0(config-vlan)#exit
```

Donde:

vlan-id: Se sustituye por el número que identifica a cada VLAN. (Ejemplo para la VLAN 10 su número identificador es el 10).

nombre-de-vlan: Se sustituye por el nombre asignado a cada VLAN (ejemplo: para la VLAN 10 corresponde al nombre DATA1). Este proceso debe realizarse en todos los switches para todas las VLAN.

4.3.2 Realice el procedimiento del paso 4.3.1 para configurar las VLAN de VOZ y DATOS respectivamente, con los nombres e identificadores que se muestran en la tabla No. 2.

Tabla No. 2. Nombres, ID de cada VLAN

Dispositivo	VLAN	NOMBRE	ID
Switch0	VLAN 10	DATA1	10
	VLAN 20	VOICE1	20
Switch1	VLAN 30	DATA2	30

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	437/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

	VLAN 40	VOICE2	40
--	---------	--------	----

- 4.3.3** Es necesario configurar las interfaces de un switch que fueron asignados a una VLAN específica, en este caso se comenzará con la VLAN DE DATOS. Para ello, debe ingresar al modo de configuración de la interfaz del Switch0 (dé clic sobre el Switch0 y diríjase a la pestaña CLI) y seleccione la interfaz correspondiente a la VLAN que va a configurar, introduciendo los siguientes comandos:

Ejemplo para la VLAN de datos:

```

Switch0>enable
Switch0#configure terminal
Switch0(config)#interface interface_id
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan vlan-id
Switch0(config-if)#exit

```

Nota: La interfaz Fa0/2 del switch0 está conectada a la PC0 y se encuentra asociada a la VLAN 10.

Donde:

interface: Es el comando para entrar al modo de configuración de interfaz.

interface-id: Se sustituye por el puerto a configurar.

switchport mode access: Define el modo de asociación a la VLAN para el puerto.

switchport access vlan: Asigna un puerto a la VLAN.

vlan-id: Se sustituye por el número identificador de la VLAN (ejemplo: 10).

- 4.3.4** Realice el proceso de los pasos 4.3.2 y 4.3.3 para la VLAN de datos del Switch1.

- 4.3.5** Configure las interfaces en cada switch que fueron asignados a una VLAN de VOZ. Para ello debe ingresar al modo de configuración de la interfaz del Switch0 (dé clic sobre el switch0 y diríjase a la pestaña CLI) y seleccione la interfaz correspondiente a la VLAN que va a configurar, introduciendo los siguientes comandos:

```

Switch0>enable
Switch0#configure terminal
Switch0(config)#interface interface_id
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport voice vlan id-vlan
Switch0(config-if)#exit

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	438/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

Donde:

interface: Es el comando para entrar al modo de configuración de interfaz.

interface-id: Se sustituye por el puerto a configurar.

switchport mode access: Define el modo de asociación a la VLAN para el puerto.

switchport access vlan: Asigna un puerto a la VLAN.

vlan-id: Se sustituye por el número identificador de la VLAN (ejemplo: 30).

4.3.6 Realice el proceso del paso 4.3.5 para la VLAN de voz del Switch1.

4.3.7 Defina con su profesora o profesor y escriba en la tabla No. 3 qué dirección IP, máscara de subred y gateway utilizará en cada VLAN, de acuerdo con cada segmento de red proporcionado.

Tabla No. 3. Direcciones de Red

VLAN	Segmento de Red	Rango de Direcciones IP	Máscara	Gateway
10				
20				
30				
40				

4.3.8 Para el enlace WAN defina con su profesora o profesor qué segmento utilizará.

WAN1	Segmento de Red	Rango de Direcciones IP	Máscara

4.4 Configuración de un enlace troncal 802.1Q

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva el tráfico de varias VLAN. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre dispositivos de red intermedios.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	439/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Existen diferentes modos de enlaces troncales como el 802-1Q y el ISL. En la actualidad se utiliza el 802.1Q dado que el ISL es empleado por las redes antiguas. Un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, éste administra la negociación del enlace sólo si el puerto en el otro switch se configura en modo de enlace troncal que admite DTP.

- 4.4.1** Mencione cuáles son los enlaces (interfaces) troncales de acuerdo con la topología que ha construido. (Ver Figura No. 4)
-
-

- 4.4.2** Para configurar un enlace troncal el switch entre en modo privilegiado al Switch0 (dé clic sobre el switch y diríjase a la pestaña CLI) y teclee los siguientes comandos.

```
Switch0>enable
Switch0#configure terminal
Switch0(config)#interface interface-id
Switch0(config-if)#switchport mode trunk
Switch0(config-if)#exit
```

Donde:

interface-id: se sustituye por el puerto del enlace troncal (ejemplo para el switch0: fa0/1).
switchport mode trunk: Define que el enlace que conecta a los switches sea un enlace troncal.

- 4.4.3** Realice el proceso del paso 4.4.2 para el enlace troncal del Switch1.

4.5 Configuración del DHCP de Datos

Para que se asignen las direcciones IP mediante DHCP es necesario realizar las configuraciones necesarias en cada router, por lo que es necesario excluir la dirección de Gateway, para que no se asigne en los hosts que se conecten a éste.

- 4.5.1** Dé clic sobre el Router0 y diríjase a la pestaña CLI, en donde debe introducir los siguientes comandos:

```
Router0>enable
Router0#configure terminal
Router0(config)#ip dhcp excluded-address gateway
Router0(config)#ip dhcp pool nombre_servidor_dhcp
Router0(dhcp-config)#default-router gateway
Router0(dhcp-config)#network segmento_de_red máscara
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	440/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Router0(dhcp-config)#exit

Donde:

gateway: Se sustituye por la dirección del gateway que pertenece al segmento de red de la VLAN de DATOS.

nombre_servidor_dhcp: Es el nombre que se le va a asignar al servidor dhcp de datos.

segmento_de_red: Se coloca el segmento de red al que pertenece esa subred.

máscara: se escribe la máscara que pertenece al segmento de red.

4.5.2 Realice el proceso del paso 4.5.1 y ahora configure el DHCP de datos en el Router1.

4.6 Configuración del DHCP de VOZ.

Para que se asiganen direcciones IP en cada uno de los teléfonos conectados a las subredes que pertenecen a una VLAN, es necesario realizar la configuración de direcciones mediante DHCP. Se recomienda excluir la dirección del gateway para evitar que se asigne a los teléfonos.

4.6.1 Dé clic sobre el Router0 y diríjase a la pestaña CLI, en donde debe introducir los siguientes comandos:

```
Router0>enable
Router0#configure terminal
Router0(config)#ip dhcp excluded-address gateway
Router0(config)#ip dhcp pool nombre_servidor_dhcp
Router0(dhcp-config)# network segmento_de_red máscara
Router0(dhcp-config)# default-router gateway
Router0(dhcp-config)#option 150 ip gateway
Router0(dhcp-config)#exit
```

Donde:

gateway: Se sustituye por la dirección del gateway que pertenece al segmento de red de la VLAN de VOZ.

nombre_servidor_dhcp: Es el nombre que se le va a asignar al servidor dhcp de datos.

segmento_de_red: Se coloca el segmento de red al que pertenece esa subred.

máscara: se escribe la máscara que pertenece al segmento de red.

4.6.2 Realice el proceso del paso 4.6.1 y ahora configure el DHCP de voz en el Router1.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	441/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.7 Configuración de las subinterfaces de las VLAN en el router.

Un router sólo puede tener una dirección IP por interface. Puesto que el enlace troncal entre el switch y router es único y cada VLAN requiere su propia puerta de enlace, es necesario crear subinterfaces.

Una subinterfaz es una interfaz lógica dada de alta en una interfaz física del router. Se crearán 2 subinterfaces en cada router y cada una será designada para cada VLAN (VOZ y DATOS respectivamente).

4.7.1 Dé clic sobre el Router0 y diríjase a la pestaña CLI. Introduzca los siguientes comandos:

```
Router0>enable
Router0#configure terminal
Router0(config)#interface fastethernet interface-id.vlan-id
Router0(config-subif)#encapsulation dot1q vlan-id
Router0(config-subif)#ip address gateway máscara
Router0(config-subif)#description nombre_servidor_dhcp
Router0(config-subif)#exit
```

Donde:

interface-id.vlan-id: Se sustituye para crear una subinterfaz para una VLAN, (ejemplo para la VLAN 10; fa0/0.10).

Encapsulation dot1Q: Configura la subinterfaz para que funcione en una VLAN específica.

vlan-id: Se sustituye por el identificador de la VLAN que se va a configurar.

gateway: Se sustituye por la dirección del gateway que pertenece al segmento de red de la VLAN que se está configurando.

máscara: se escribe la máscara de subred de la puerta de enlace.

nombre_servidor_dhcp: Es el nombre que se le va a asignar al servidor dhcp de datos.

4.7.2 Repita el paso 4.7.1 para realizar todas las configuraciones para las VLAN de VOZ y DATOS en cada router

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 442/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

- 4.7.3** Asigne direcciones IP en la Interfaz Serial de cada router. Para ello teclee los siguientes comandos para el router0:

```
Router0>enable
Router0#configure terminal
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown
Router(config-if)#exit
```

- 4.7.4** Levante las interfaces Físicas Ethernet y Serial en los routers, dé clic sobre el Router0 y diríjase a la pestaña CLI. Introduzca los siguientes comandos:

```
Router0>enable
Router0#configure terminal
Router0(config)#interface fastethernet id-interface
Router0(config-subif)# no shutdown
Router0(config-subif)# exit
Router0(config)#interface serial id-interface
Router0(config-subif)# no shutdown
Router0(config-subif)# exit
```

Donde:

id-interface: se sustituye por la interfaz que se está levantando.

- 4.7.5** Repita el paso 4.7.3 para levantar las interfaces Físicas Ethernet y Serial en el Router1.

- 4.7.6** Asigne direcciones IP de manera automática en los hosts dando clic sobre cada uno y seleccionando la pestaña Desktop y habilitando la opción DHCP para que se le asigne una dirección IP de manera automática, verifique que se le haya asignado una. De esta manera se puede corroborar que el servidor DHCP de datos funciona correctamente. (ver Figura No. 6)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 443/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

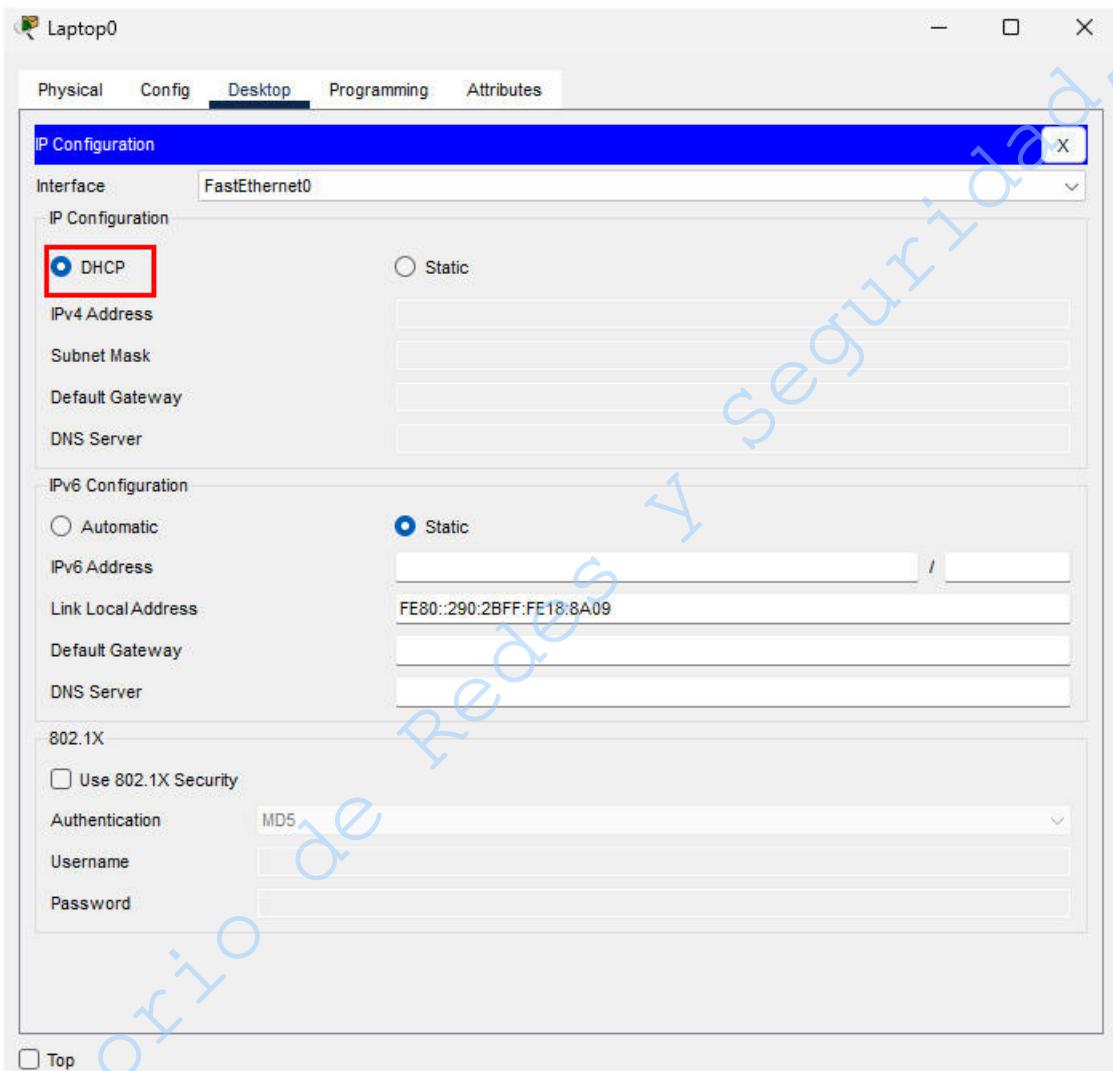


Figura No. 6. Asignación por DHCP

4.7.7 Aplique el protocolo de encaminamiento dinámico RIPv2 en cada router.

Recuerde que los comandos para aplicar encaminamiento dinámico RIPv2 son:

```

Router0>enable
Router0#configure terminal
Router0(config)#router rip
Router0(config)#version 2

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	444/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

**Router0(config-router)#network NETWORK_ADDRESS
Router0(config-router)#exit**

Donde:

NETWORK_ADDRESS: se sustituye por el segmento de red que representa a la subred conectada directamente al router.

NOTA: Recuerde que se cuenta con 3 subredes conectadas a cada router, por lo que este paso deberá realizarse tres veces para el router que se está configurando

4.7.8 Indique cuáles son las tres subredes que se cuentan conectadas a cada router

4.8 Configuración del servicio de VoIP.

4.8.1 Para que las subredes que tienen una VLAN de voz configurada puedan establecer comunicación, es necesario configurar los routers correspondientes. Para ello, ingrese los siguientes comandos:

Ejemplo para el Router0:

```
Router0>enable
Router0#configure terminal
Router0(config)#telephony-service
Router0(config-telephony)#max-dn 5
Router0(config-telephony)#max-ephones 5
Router0(config-telephony)#auto assign 1 to 5
Router0(config-telephony)#ip source-address gateway port 2000
Router0(config-telephony)#exit
```

Donde:

max-dn y **max-ephone**: permiten asignar el número máximo de extensiones y teléfonos conectados.

auto assign: define el rango dinámico de números de teléfonos.

ip source-address: define la dirección y puerto que presta el servicio de telefonía.

4.8.2 Repita el paso 4.8.1 para configurar el Router1.

4.8.3 Creación de los números VoIP.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	445/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada	

Ejemplo para el router0:

```
Router0>enable
Router0#configure terminal
Router0(config)#telephony-service
Router0(config-telephony)#ephone-dn 1
Router0(config-ephone-dn)#number número_de_ext.
Router0(config-ephone-dn)#exit
```

Donde:

número_de_ext: es el número que se le va a asignar al teléfono que pertenece a la subred que se desea configurar. Ejemplo para el Router0 se podría asignar la extensión 1234.

Indique el número de extensión que le asignó al Router0_____

4.8.4 Repita el paso 4.8.3 para asignar el números de extensión al Router1-

Indique el número de extensión que le asignó al Router1_____

4.9 Configuración del router para el enrutamiento de comunicación de VoIP.

4.9.1 Para establecer comunicación entre teléfonos que pertenecen a diferentes subredes, es necesario configurar un encaminamiento o enrutamiento en cada router. Para ello es necesario que ejecute los siguientes comandos:

Ejemplo para Router0:

```
Router0>enable
Router0#configure terminal
Router0(config)#dial-peer voice Id voip
Router0(config-dial-peer)#destination-pattern xxxx
Router0(config-dial-peer)#session target ipv4:dir_ip
Router0(config)#exit
```

Donde:

Id: es el número identificador del enrutador, puede ser cualquier valor unitario 1, 2, 3....

xxxx: Es el número de extensión que pertenece a los teléfonos conectados a la subred destino, es decir, se trata de la extensión con la que se desea comunicar. Ejemplo para la subred conectada al router0, se quiere comunicar con la extensión 3333.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	446/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

dir_ip: Dirección que se utiliza para señalar un direccionamiento de red específico para recibir llamadas de voz sobre IP. (Ejemplo; para router0 la dirección IP que se requiere es la de la interfaz serial del Router 1)

4.9.2 Repita el paso 4.9.1 para configurar al Router1.

4.9.3 Con ayuda de su profesora o profesor, verifique el funcionamiento de los teléfonos, es necesario que dé clic sobre un teléfono y marque el número de extensión destino. Así como se muestra en la figura No.7.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	447/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada



Figura No. 7. Comunicación entre Teléfonos IP.

5. Cuestionario

1.- Mencione 3 ventajas de implementar una VLAN de VOZ.

2.- Indique cuál es la importancia de mantener separadas una VLAN de VOZ y una VLAN de DATOS.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	448/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

3.- Investigue cuáles son los comandos para eliminar una VLAN.

4.- Cuando se configuran VLAN, al router se le tiene que configurar el estándar 802.1Q. Indique la importancia de realizar esta configuración. ¿Qué sucedería si no se configura?

5.- Introduzca los siguientes comandos dentro del Switch0, analice el contenido e indique qué muestran:

a) show vlan

b) show vlan brief

c) show interface trunk

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	449/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

5.- Describa en qué consisten las VLAN de:

- a) Datos

- b) Predeterminada

- c) Nativa

- d) Administración

- e) Voz

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	450/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Laboratorio de Redes y Seguridad

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	451/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 13
Configuración básica de una comunicación de Voz IP
Cuestionario Previo

1. Investigue cuáles son los diferentes tipos de VLAN que se pueden implementar en una RED.
2. Escriba cuáles son los comandos para establecer la contraseña de administrador en los dispositivos switch y router en Cisco Packet Tracer.
3. ¿Cuál es la importancia de configurar un enlace troncal?
4. Analice los siguientes comandos que se utilizan en el router e indique a qué se hace referencia cada línea.
5. Router0>enable
6. Router0#configure terminal
7. Router0(config)#ip dhcp excluded-address **gateway**
8. Router0(config)#ip dhcp pool **nombre_servidor_dhcp**
9. Router0(dhcp-config)# network **segmento_de_red** máscara
10. Router0(dhcp-config)# default-router **gateway**
11. Router0(dhcp-config)#option 150 ip **gateway**
12. Router0(dhcp-config)#exit
13. Investigue qué comandos se deben utilizar para habilitar la seguridad de los puertos de un switch en cisco packet tracer, en modo dinámico.
14. Investigue cuáles son los comandos para configurar la contraseña en modo EXEC privilegiado.
15. Investigue para qué sirven los comandos **ephone-dn** y **telephony-service**
16. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 452/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 14

Web DNS e IP Helper

Capa 7 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 453/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

1.- Objetivos de aprendizaje

- El alumno o la alumna aprenderá a hacer una ruta estática por defecto para establecer una conexión entre un cliente y un servidor web con el uso del protocolo DNS.

2.- Conceptos teóricos

Un DNS (Domain Name System - Sistema de Nombres de Dominio) es un registro el cual contiene en su interior nombres de sitios web y de las direcciones IP asociadas. Así, la correlación de estas dos favorece la transferencia de datos entre las computadoras y también permite el acceso a Internet.

El DNS resulta de gran importancia debido a que este toma las direcciones IP (que es como se comunican las computadoras entre sí) y los traduce a nombres de dominios que sean entendibles para los seres humanos.

Existen dos tipos de servicios de DNS:

- DNS autoritativo. Este servicio responde como tal a las consultas DNS convirtiendo los nombres de dominio en la IP correspondiente al sitio para que pueda existir la comunicación.
- DNS recurrente. Al contrario, este servicio es a donde realmente llegan directamente las consultas de los clientes, pero no tiene acceso a los registros DNS. Lo que hace entonces es recibir la petición del cliente, la procesa y si es que el DNS recurrente tiene la referencia solicitada en caché o almacenada por algún motivo, responde en seguida la consulta suministrando la información de la IP o de la fuente. Pero si es que no tiene guardada esa consulta, delega la consulta a uno o más servidores DNS autoritativos para poder completar la petición.

Por otro lado, IP helper-address permite implementar un proxy, el cual recibirá la solicitud en formato de broadcast y la convertirá en un paquete unicast, cuya dirección destino será la del servidor. De esta manera, la solicitud de conectarse al servidor DHCP puede llegar más allá de una sola subred. Es muy útil utilizarlo en redes complejas o extensas donde hay múltiples subredes y en el que se encuentran uno o más servidores en un área de red específica, de forma que puedan ser utilizados o accedidos en cualquier otro segmento de red.

3.- Equipo y material necesario

Equipo del laboratorio:

- Software de Simulación Cisco Packet Tracer.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	454/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Creación de topología para el uso de los protocolos.

- 4.1.1** Encienda el sistema y elija la opción de cargar Windows.
 - 4.1.2** Inicie sesión en una cuenta con privilegios de administrador.
 - 4.1.3** Ejecute la aplicación Cisco Packet Tracer (Figura No. 1).

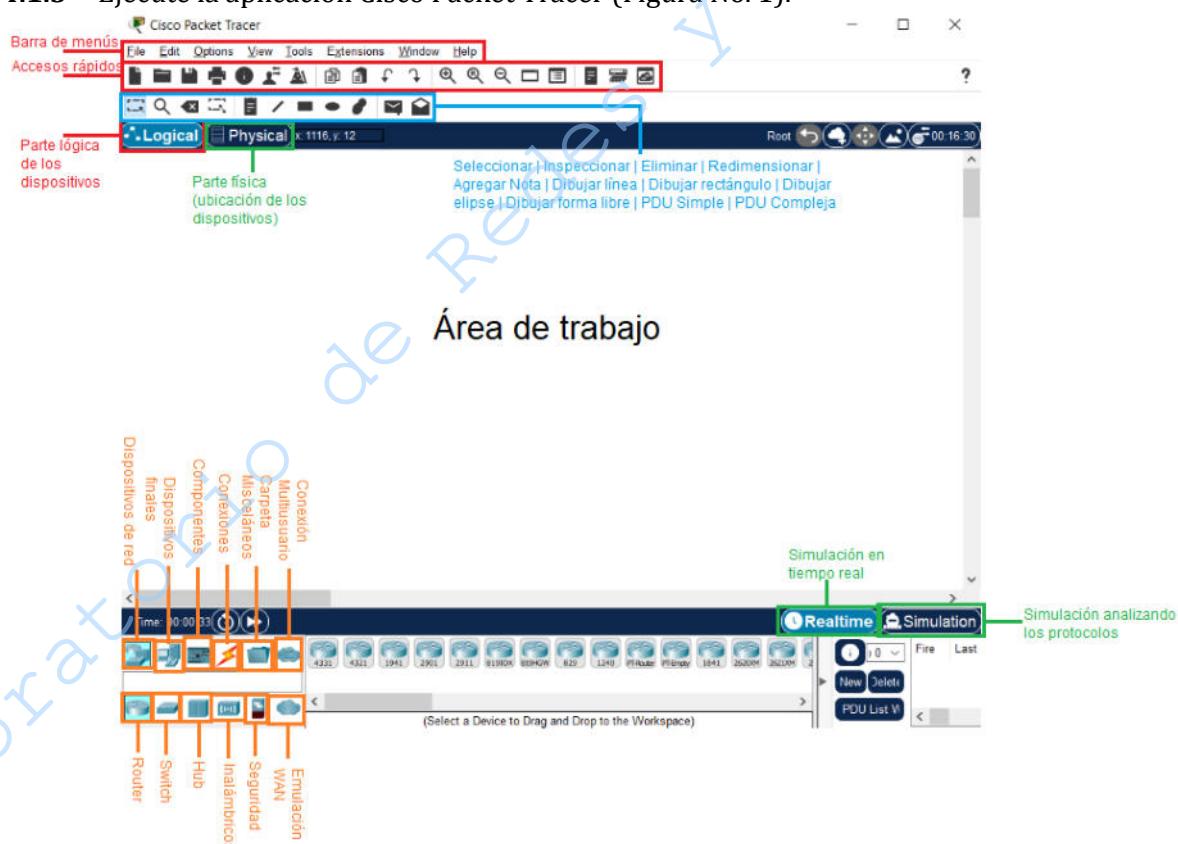


Figura 1. Simulador de CISCO Packet Tracer.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 455/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.1.4** Dé clic en la sección de Dispositivos de red, después seleccione el apartado de switches, ubique el modelo 2960 IOS15, arrastre dos instancias del switch. Dé clic en la sección *Carpeta Miscellaneous*, ubique el modelo ISR4331, arrastre tres instancias del router. Dé clic en la sección de dispositivos finales y arrastre una instancia de PC, dos de Server y conéctelos como se observa en la Figura No. 2.

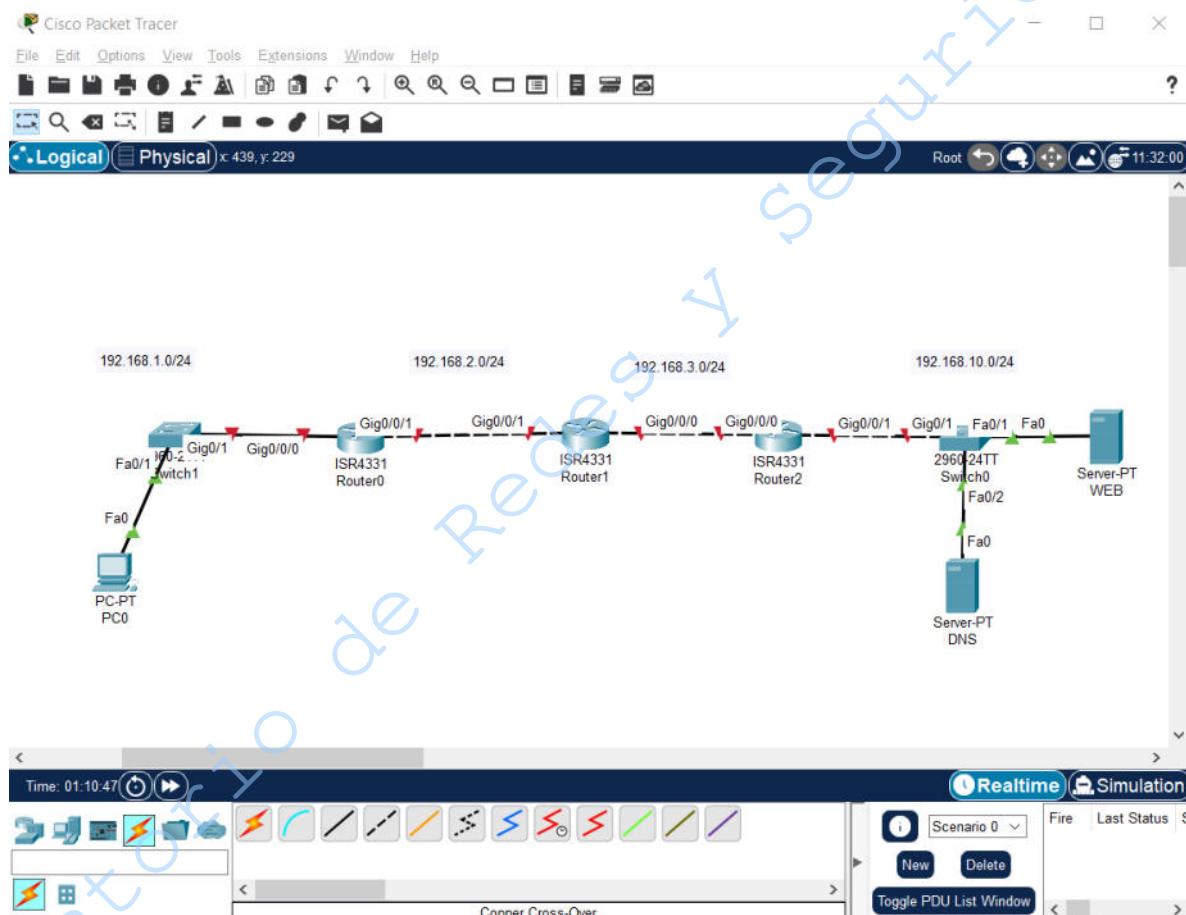


Figura 2. Topología para IP Helper y Web DNS.

- 4.1.5** Dé clic en el nombre de los servidores y cambie el nombre del *Server0* por *WEB*, *Server1* por *DNS*.

4.2 Configuración de topología.

- 4.2.1** Asigne las direcciones del Servidor WEB y Servidor DNS de acuerdo con la información de la Tabla No. 1.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	456/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

	Servidor WEB	Servidor DNS
IPv4	192.168.10.10	192.168.10.20
Máscara de subred	255.255.255.0	255.255.255.0
Gateway	192.168.10.254	192.168.10.254
DNS	192.168.10.20	192.168.10.20

Tabla No. 1. Información de las tarjetas de red

4.2.2 Configure las interfaces del Router 0 utilizando los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config)#interface gi0/0/0
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#interface gi0/0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

```

4.2.3 Configure las interfaces del Router 1 utilizando los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config-if)#interface gi0/0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#interface gi0/0/1
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown

```

4.2.4 Configure las interfaces del Router 2 utilizando los siguientes comandos:

```

Router>enable
Router#configure terminal
Router(config-if)#interface gi0/0/0

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31
		Versión: 06
		Página 457/479
		Sección ISO 8.3
		Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
		La impresión de este documento es una copia no controlada

**Router(config-if)#ip address 192.168.3.254 255.255.255.0
Router(config-if)#no shutdown**

**Router(config-if)#interface gi0/0/1
Router(config-if)#ip address 192.168.10.254 255.255.255.0
Router(config-if)#no shutdown**

- 4.2.5** Realice el proceso de enrutamiento del Router 0 y 1 de la topología. Se recomienda utilizar el protocolo RIPv2, el cual, para el Router 0, se configura utilizando los siguientes comandos en el modo de configuración global:

**Router(config-if)# exit
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network DIRECCION_IP**

NOTA: El parámetro DIRECCION_IP se debe reemplazar por el ID de la subred correspondiente que se encuentre conectada al router que se esté configurando. También es importante que indique todas y cada una de las subredes conectadas directamente empleando un comando *network* por cada subred.

Para esta práctica, los ID de subredes tienen el siguiente formato: 192.168.X.0.

- 4.2.6** Acceda a los routers y cambie el hostname con los siguientes comandos:

**Router>enable
Router#configure terminal
Router(config)#hostname RX**

NOTA: La X debe ser sustituida por el número de router que es.

- 4.2.7** Repetir el paso anterior para todos los switches, cambiando el nombre del Switch por el S1 y S2, según corresponda. La topología debe de lucir como en la Figura No. 3.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 458/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

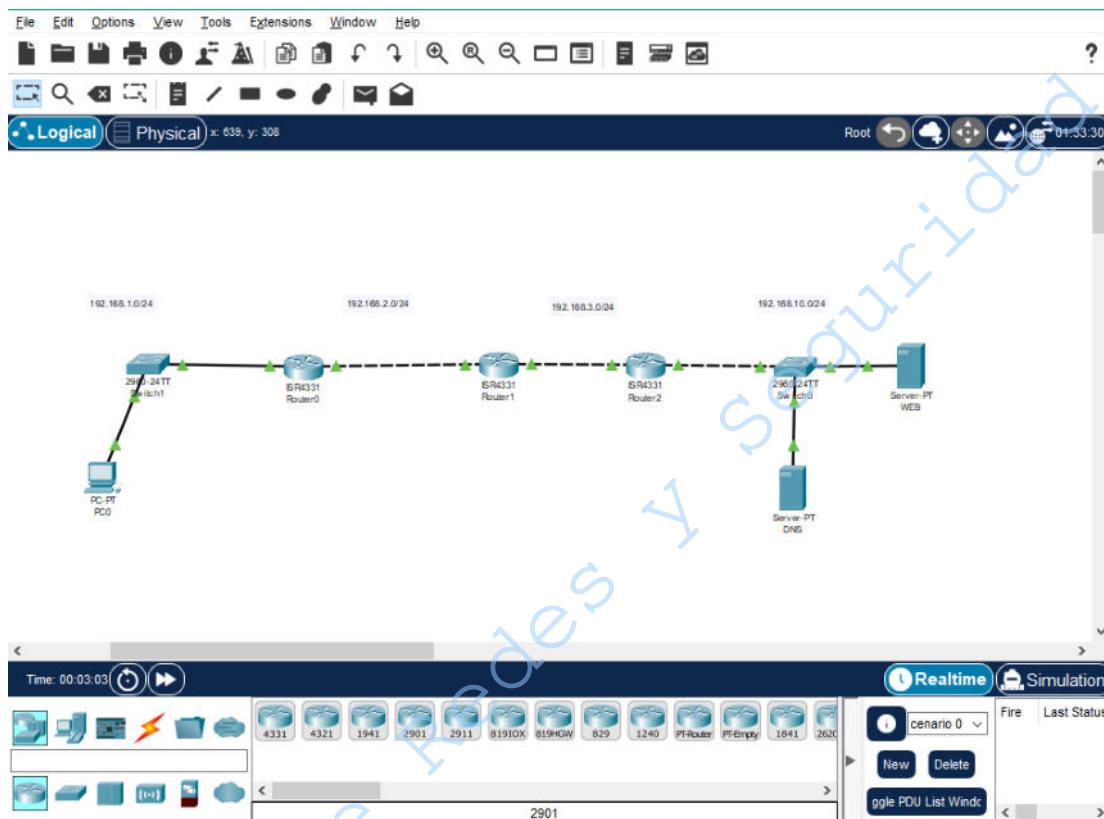


Figura No. 3. Topología.

- 4.2.8** A continuación, seleccione el Router2, el Switch0, el Servidor Web y el Servidor DNS. Una vez seleccionados haga clic en el botón de *Create New Cluster* o bien teclee Shift+U. El botón de *Create New Cluster* tiene forma de una nube y se ubica en la parte superior derecha del Área de Trabajo (Figura No. 4).



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	459/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

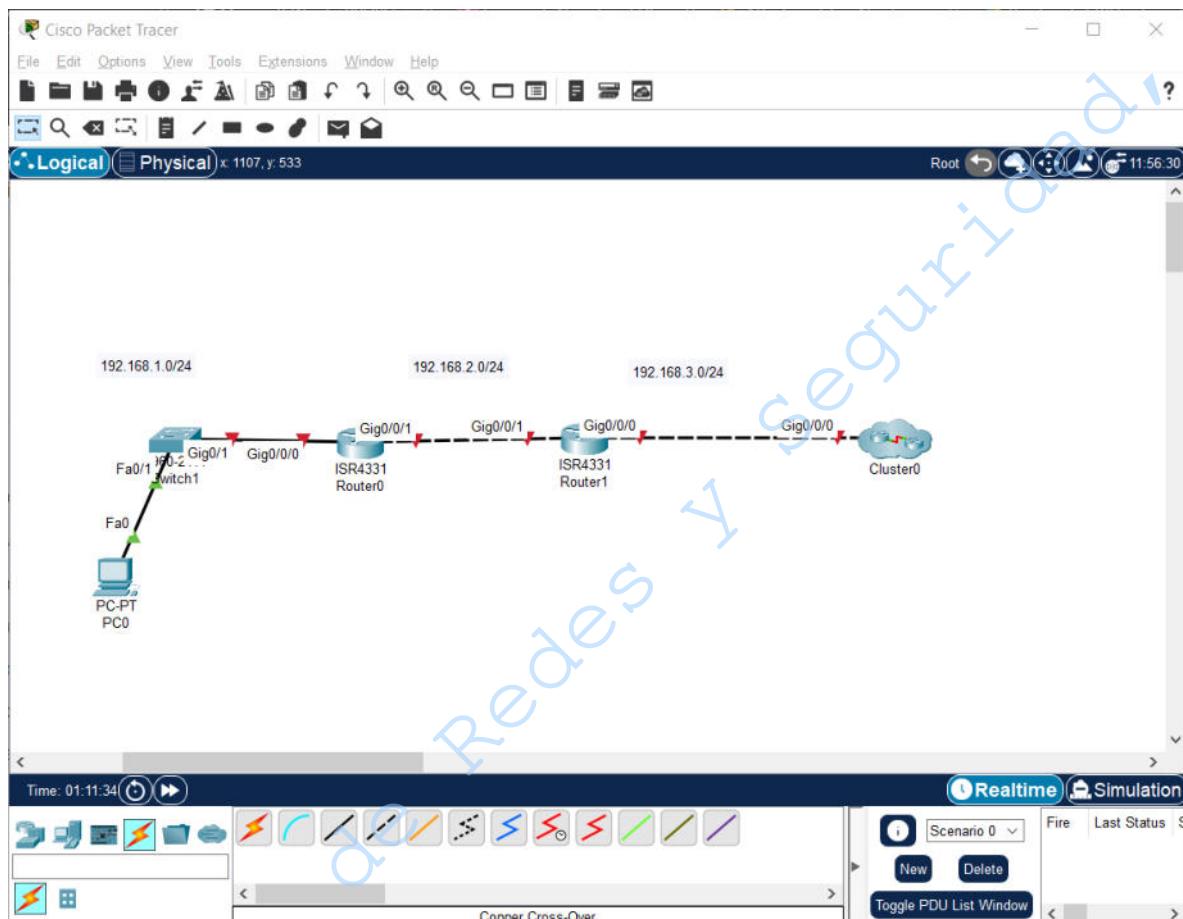


Figura No. 4. Topología con el clúster hecho.

- 4.2.9** Ejecute los siguientes comandos para poder realizar el ruteo de la red de forma estática por defecto.

R1>enable

R1#configure terminal

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.254
```

R1(config)#router rip

R1(config-router)#default-information originate

R1(config-router)#end

- 4.2.10** Una vez que se realizó el ruteo, haga doble clic en el Clúster para ver su interior (Figura No. 5).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 460/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

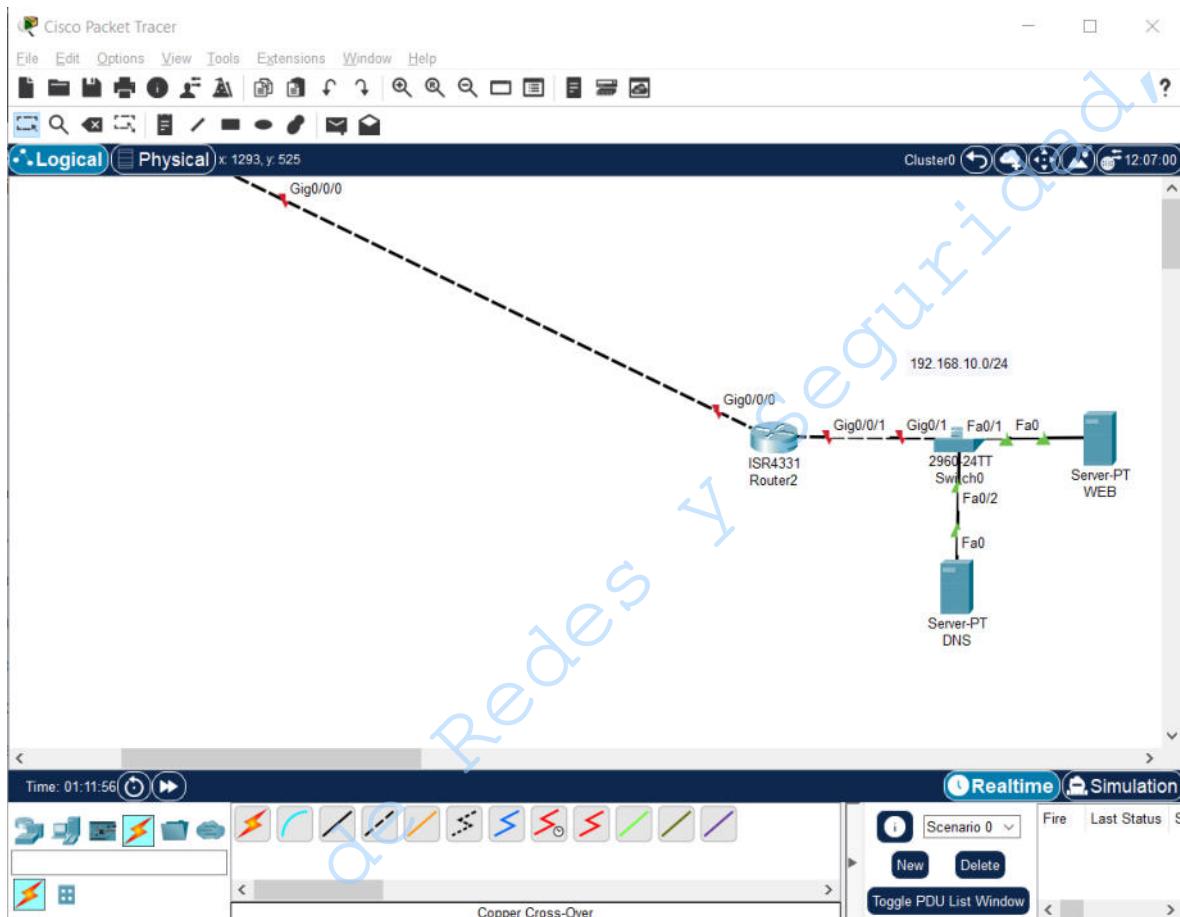


Figura No. 5. Topología del interior del Clúster.

4.2.11 Ahora haga clic en el servidor Web, después en la pestaña de *Services*, luego en el apartado *HTTP* y verifique que se encuentre encendido. Posteriormente haga clic donde se indica para editar el archivo *index.html* (Figura No. 6).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 461/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

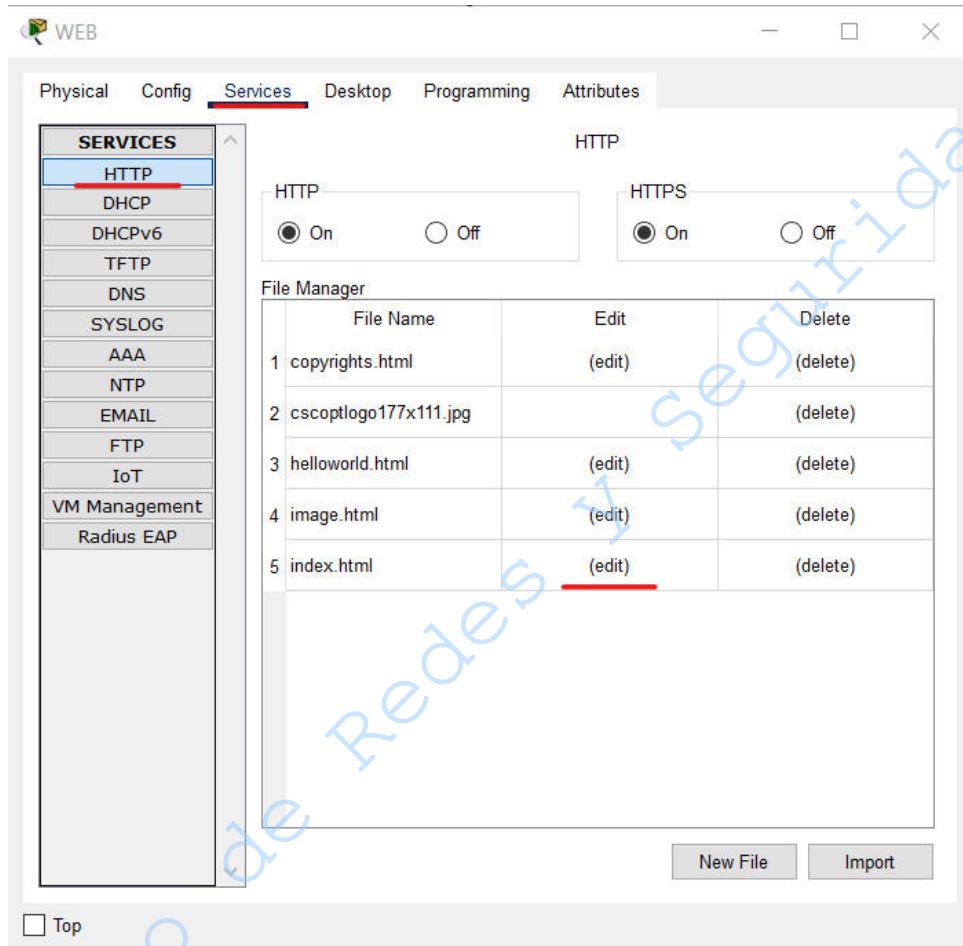


Figura No. 6. Pestaña Services del Servidor Web.

4.2.12 Una vez dentro del archivo, ubique la línea de código que define el título de la página web (Figura No. 7).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 462/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

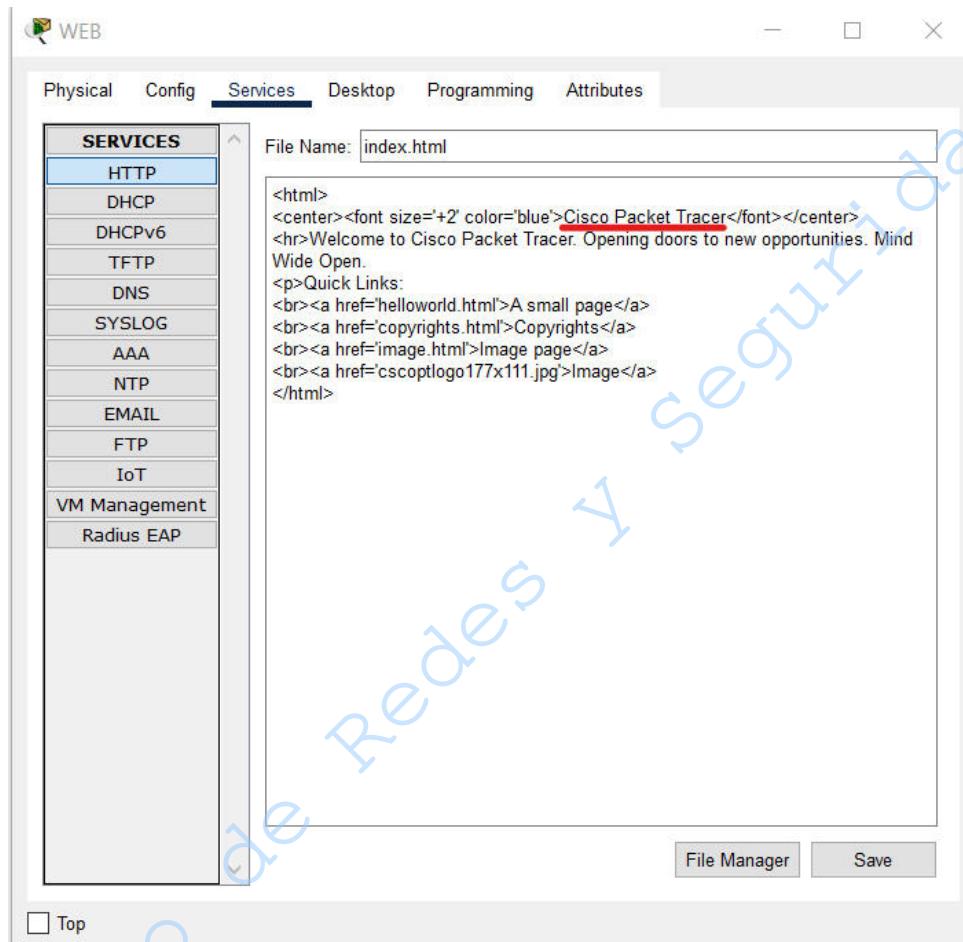


Figura No. 7. Edición del archivo index.html.

- 4.2.13 Cambie la leyenda *Cisco Packet Tracer* por el nombre con apellidos de uno de los integrantes del equipo. Finalmente haga clic en *Save* para guardar los cambios (Figura No. 8).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 463/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

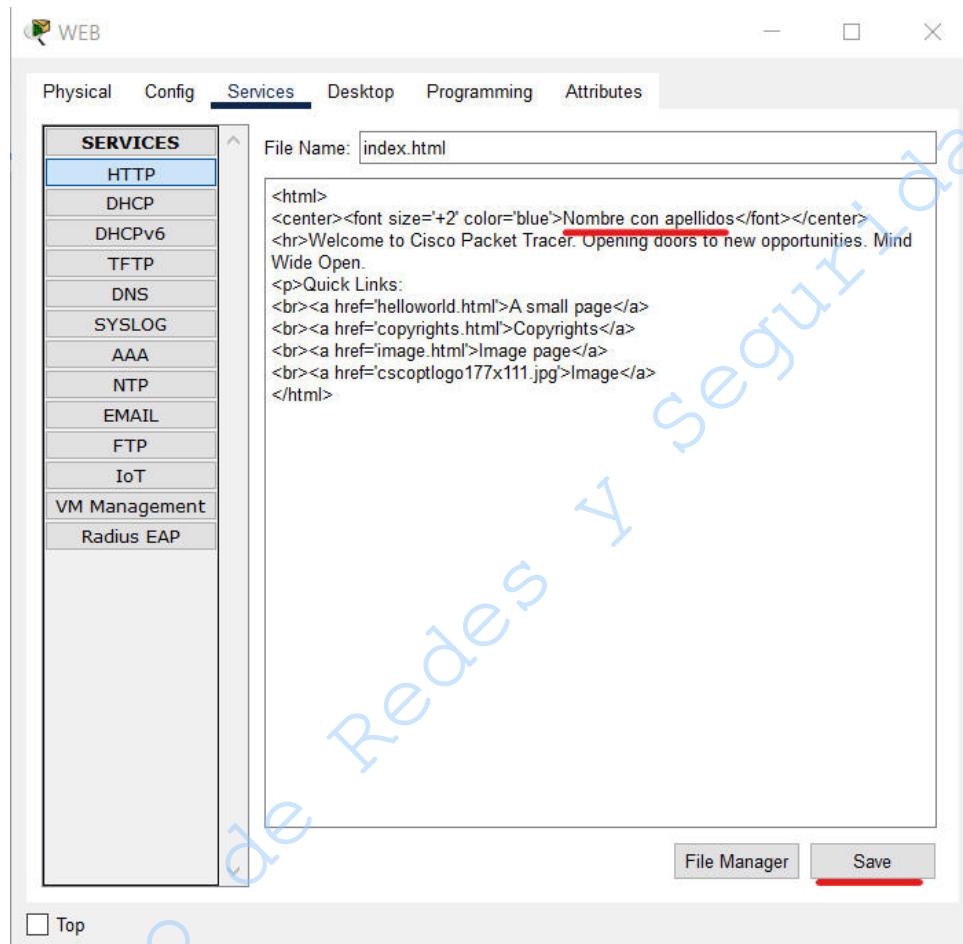


Figura No. 8. Archivo index.html editado.

- 4.2.14** Cierre la ventana del Servidor Web y ahora haga clic sobre el Servidor DNS. En él diríjase a la pestaña *Services* y entre al apartado *DNS*. Asegúrese que esté encendido, nombre a la página web como usted desee, ingrese la dirección IP del Servidor Web en el cuadro de *Address* y finalmente dé clic en *Add* (Figura No. 9).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 464/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

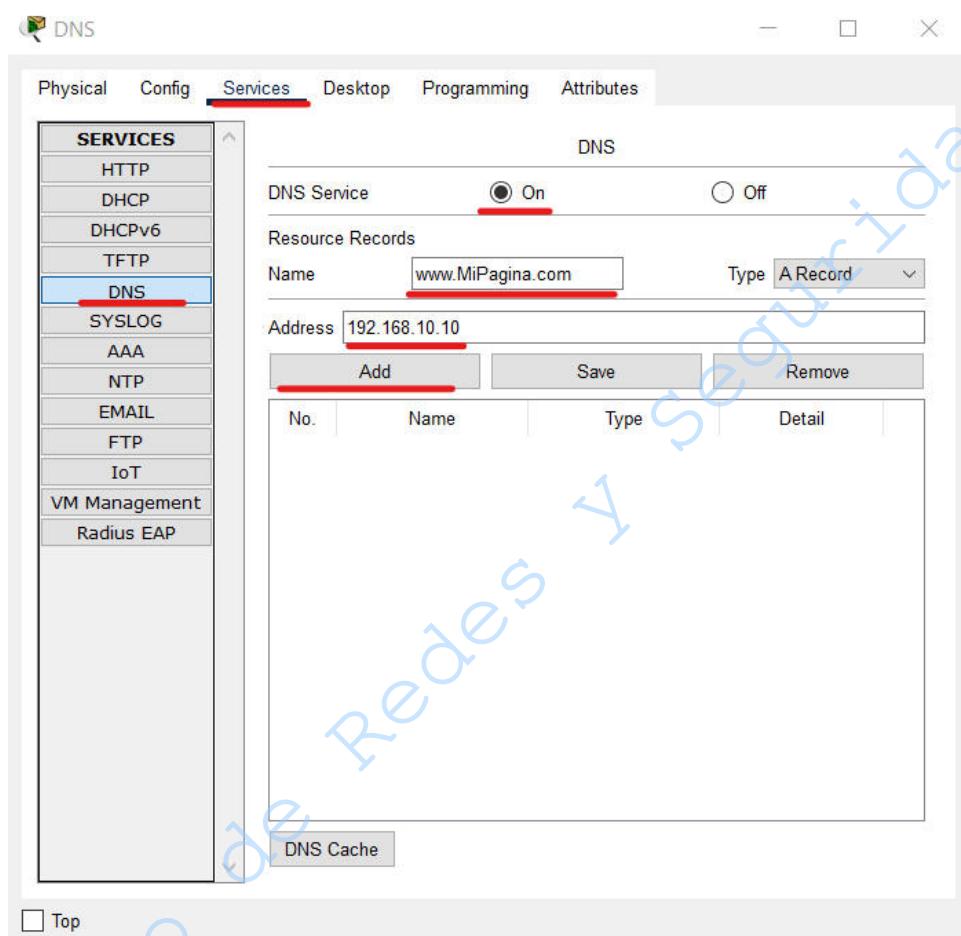


Figura No. 9. Configuración del Servidor DNS.

Escriba a continuación el nombre que le dio a la página web.

- 4.2.15 Cierre la ventana anterior y cierre también el Clúster, quedando así en la topología principal. Ahí, haga clic en la PC0, y después en *Web Browser* (Figura No. 10).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	465/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

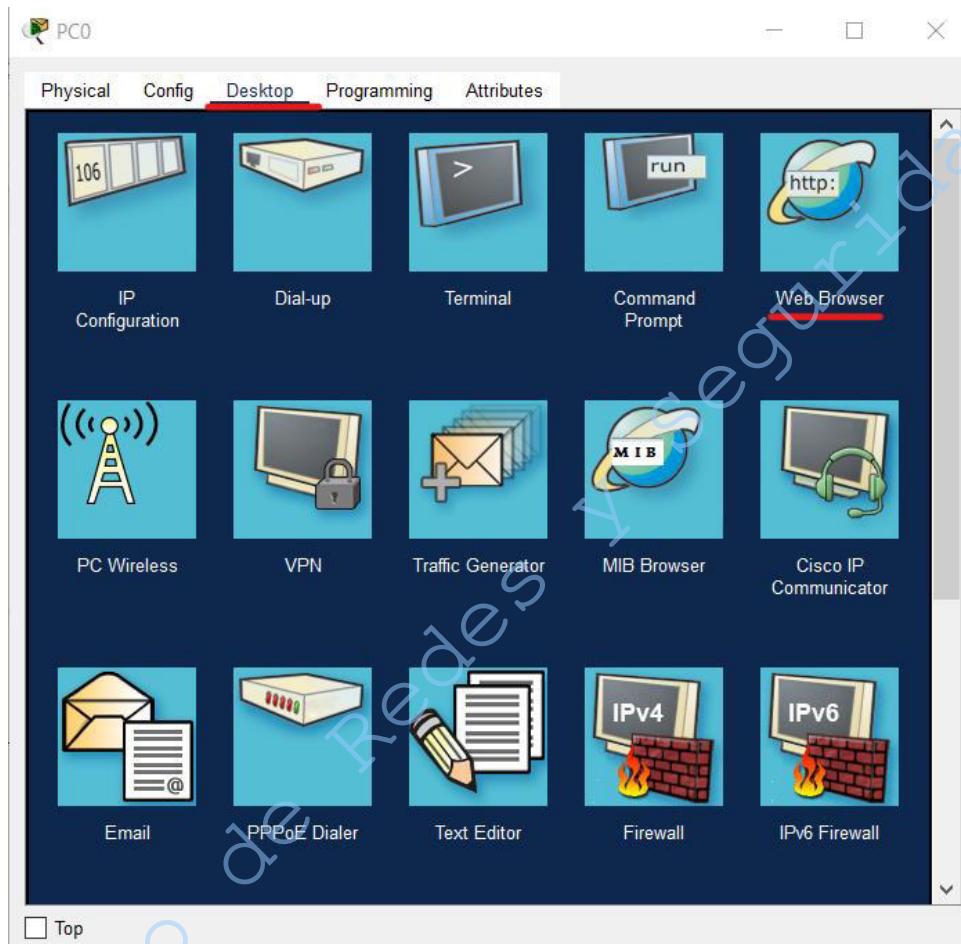


Figura No. 10. Pestaña Desktop de la PC0.

- 4.2.16** Una vez dentro, haga clic en la pestaña *Desktop* e introduzca el nombre que le dio a la página web en el punto 4.2.13 (Figura No. 11).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	466/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

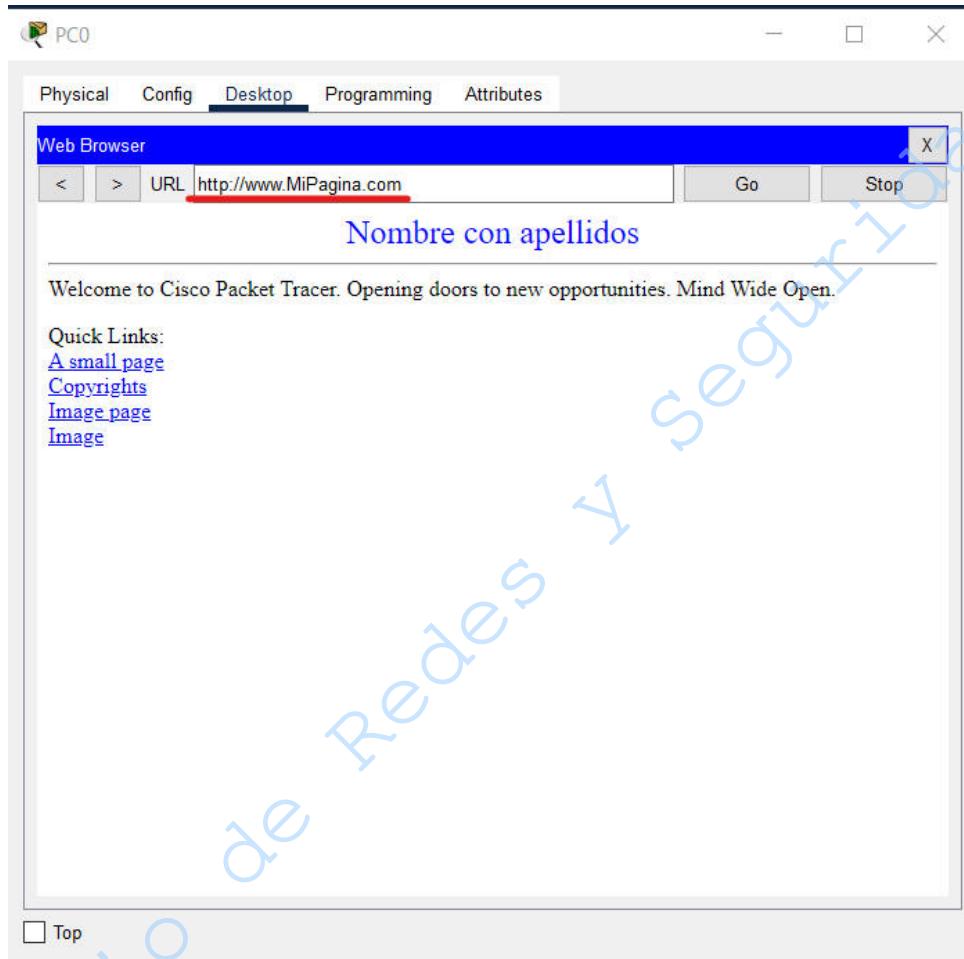


Figura No. 11. Página web creada.

- 4.2.17** Si se muestra una página web similar a la de la imagen 11 y esta contiene sus apellidos en el título, realizó todo correctamente.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	06
Página	467/479
Sección ISO	8.3
Fecha de emisión	11 de agosto de 2023

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	468/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 14

Web DNS e IP Helper

Cuestionario Previo

1. Investigue, ¿para qué se utiliza el ruteo estático por default? y ¿Cómo se aplica en Cisco Packet Tracer?
2. Investigue, ¿en qué consiste un Clúster y su funcionalidad en Cisco Packet Tracer?
3. En una red estática por default qué significan los 8 ceros que se introducen en el comando.
4. ¿Cuál es el contenido del archivo index.html en un Servidor Web?
5. Para emplear el software Cisco Packet Tracer debe contar con una cuenta en Skills for All, consulte el Anexo de este manual para crearla, si ya tiene una cuenta, puede consultar el mismo anexo para utilizar el software.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión	MADO-31 06 469/479 8.3 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Anexo

Manual para la creación de una cuenta en Skills for All para descargar y emplear Cisco Packet Tracer

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	470/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1. Objetivo

El alumno o la alumna realizará el proceso correspondiente para la creación de una cuenta personal en el software Cisco Packet Tracer.

2. Instrucciones

Lea detenidamente y siga cada uno de los pasos que se describen a continuación para obtener su cuenta personal.

Es importante que cada estudiante obtenga su cuenta para emplear Cisco Packet Tracer, en caso contrario NO podrá realizar las prácticas de la asignatura.

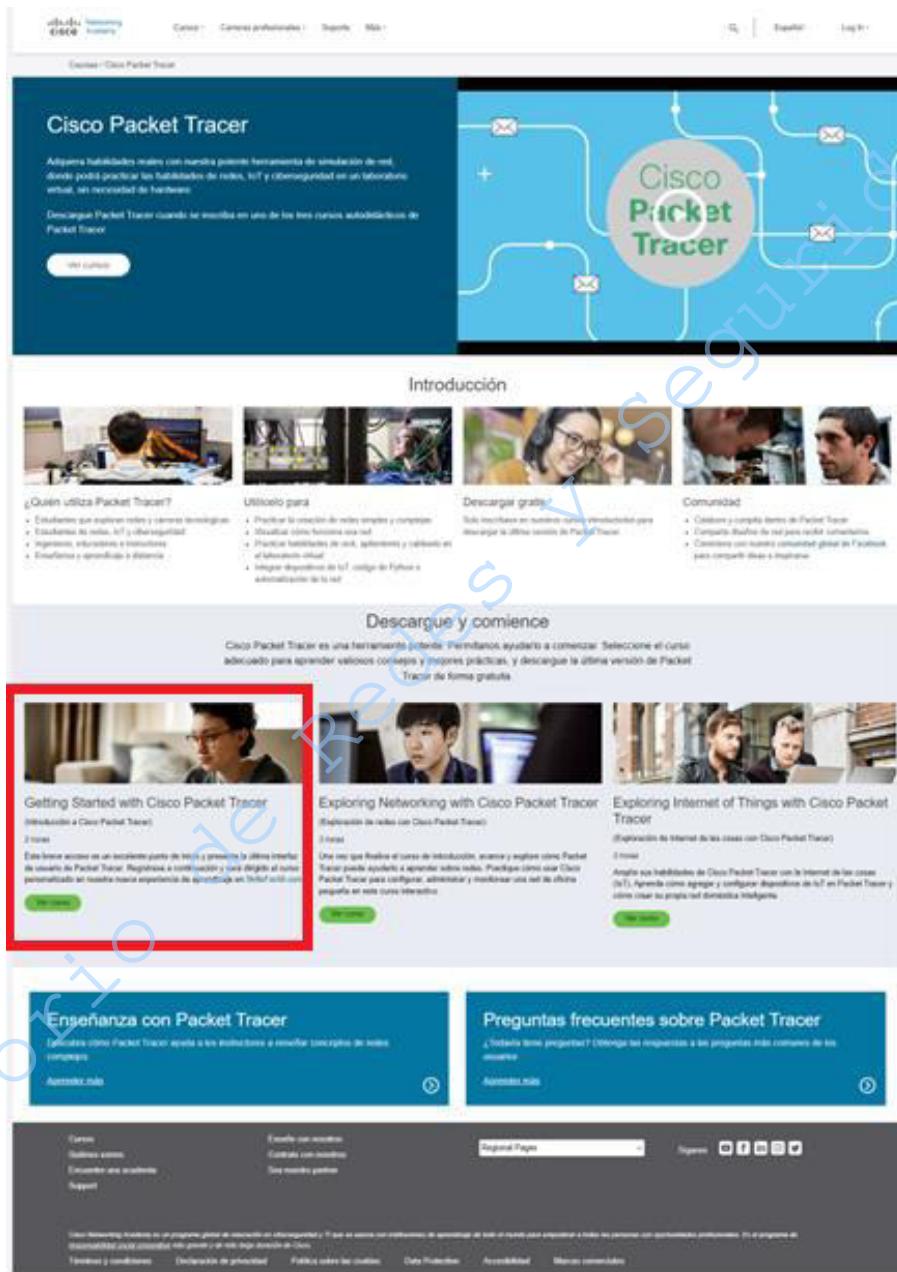
a) Proceso para la obtención de cuenta personal.

2.1 Para realizar la instalación de Cisco Packet Tracer, ingrese al siguiente sitio:

<https://prelogin-authoring.netacad.com/es/courses/packet-tracer>

El sitio debe de tener una vista similar a la de la Figura No. 1, busque y dé clic en el curso *Getting Started with Cisco Packet Tracer*.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 471/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



The screenshot shows the Cisco Packet Tracer landing page. At the top, there's a navigation bar with links like 'Inicio', 'Cursos', 'Cámaras profesionales', 'Sobre mí', and 'Míos'. Below the header, the main title 'Cisco Packet Tracer' is displayed with a subtext: 'Adquiere habilidades reales con nuestra potente herramienta de simulación de red, donde podrás practicar las habilidades de redes, IoT y ciberseguridad en un entorno virtual, sin necesidad de hardware'. A large button labeled 'Obtener ahora' is present. To the right, there's a graphic showing a network diagram with nodes and arrows, and a prominent 'Cisco Packet Tracer' logo.

Introducción

This section contains several images of people working on computers, followed by four columns of text:

- ¿Quién utiliza Packet Tracer?**
 - Estudiantes que estudian redes e ingeniería de telecomunicaciones
 - Estudiantes de redes, IoT y ciberseguridad
 - Ingenieros, informáticos e investigadores
 - Educación y aprendizaje a distancia
- Utilizado para**
 - Practicar la creación de redes simples o complejas
 - Visualizar cómo funciona una red
 - Practicar habilidades de red, implementar y configurar en el laboratorio virtual
 - Integrar dispositivos de IoT, como de Arduino e interfaz de programación de la red
- Descargar gratis**

Solo inscríbete en nuestro curso interactivo para descargar la última versión de Packet Tracer.
- Comunidad**
 - Cámbiate y comparte temas de Packet Tracer
 - Comparte tu diseño de red para recibir comentarios
 - Comparte con nuestro comunidad global en Facebook para compartir ideas e inspiración

Descarga y comienza

This section highlights three free courses:

- Getting Started with Cisco Packet Tracer** (Introducción a Cisco Packet Tracer) - 2 horas: A brief overview of what Packet Tracer is and how to download the latest version. It includes a video thumbnail of a person using the software.
- Exploring Networking with Cisco Packet Tracer** (Exploración de redes con Cisco Packet Tracer) - 3 horas: Describes the introductory course, which covers basic networking concepts and how to use Packet Tracer to practice them. It includes a video thumbnail of two people working on a computer.
- Exploring Internet of Things with Cisco Packet Tracer** (Exploración del Internet de las cosas con Cisco Packet Tracer) - 3 horas: Describes the course on IoT, which teaches how to configure, administer, and monitor IoT devices in Packet Tracer. It includes a video thumbnail of two people looking at a computer screen.

Enseñanza con Packet Tracer

This section provides information on how Packet Tracer can be used in the classroom to teach concepts related to networking. It includes a 'Aprende más' button.

Preguntas frecuentes sobre Packet Tracer

This section answers common questions about Packet Tracer. It includes a 'Aprende más' button.

At the bottom of the page, there are footer links for 'Cursos', 'Sistemas operativos', 'Encuentra una academia', 'Soporte', 'Encuentra un mentor', 'Contacta con mentores', 'Soy mentor premium', 'Aprende más', and 'Aprende más'. There's also a 'Aprende Pages' dropdown and social media icons for LinkedIn, Facebook, Twitter, YouTube, and Instagram.

Figura No. 1. Sitio NETACAD

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31	
		Versión:	06	
		Página	472/479	
		Sección ISO	8.3	
		Fecha de emisión	11 de agosto de 2023	
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada				

2.2 Al dar clic aparecerá una ventana emergente indicando que se le redireccionará a un nuevo sitio (Figura No. 2).

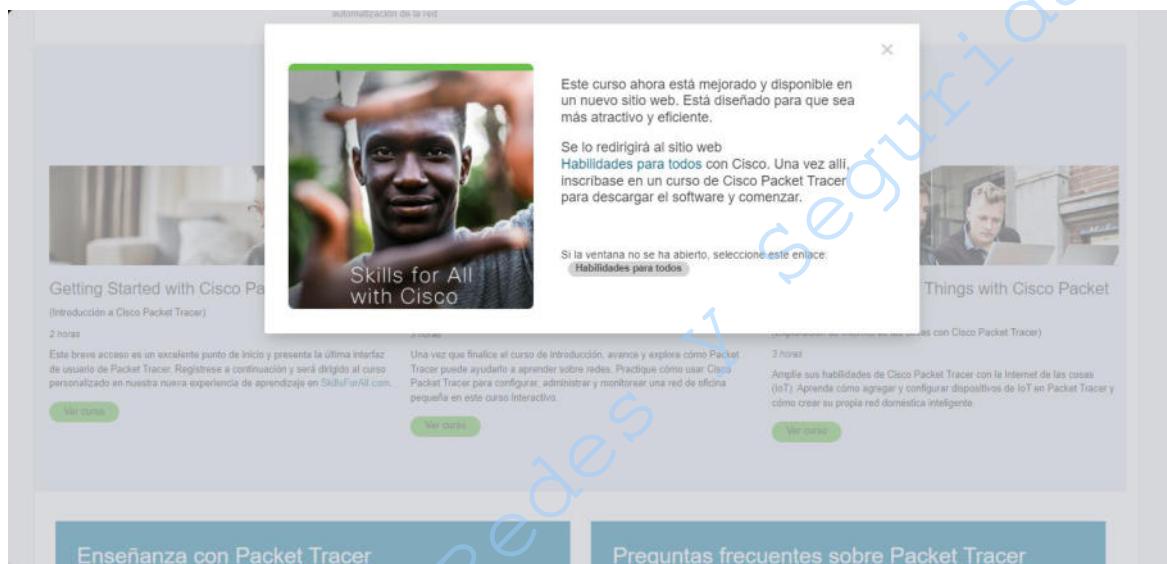
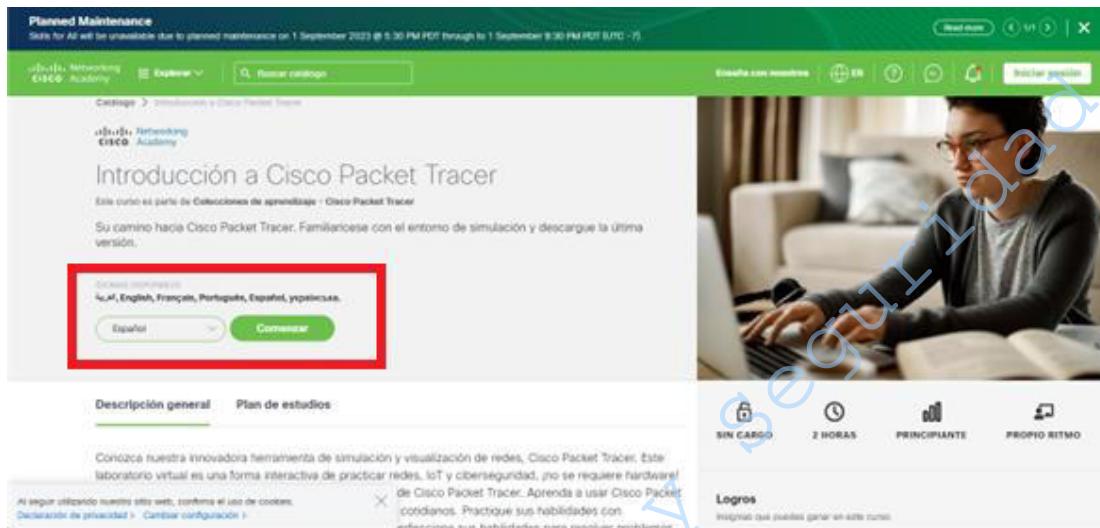


Figura No. 2. Ventana emergente

2.3 Una vez dentro del sitio *Skills for All*, seleccione el idioma de su preferencia y dé clic en *Comenzar* (Figura No. 3).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 473/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Planned Maintenance
Site will be unavailable due to planned maintenance on 1 September 2023 @ 5:00 PM PDT through to 1 September 9:00 PM PDT (UTC -7)

Cursos > Introducción a Cisco Packet Tracer

Introducción a Cisco Packet Tracer

Este curso es parte de Colecciones de aprendizaje - Cisco Packet Tracer

Su camino hacia Cisco Packet Tracer. Famíliense con el entorno de simulación y descargue la última versión.

Idiomas disponibles: Español, English, Français, Português, Español, y portugués.

Comenzar

Descripción general Plan de estudios

SIN CARGO 2 HORAS PRINCIPIANTE PROPIO RITMO

Logros

Al seguir utilizando nuestro sitio web, confirma el uso de cookies. [Declaración de privacidad](#) | [Cambiar configuración](#)

Figura No. 3. Selección de idioma

2.4 Si tiene una cuenta inicie sesión, de lo contrario dé clic en *Crear cuenta* (Figura No. 4).



Skills for All con Cisco

Cursos gratuitos en línea respaldados por la experiencia de Cisco y conectados con carreras profesionales reales.

Iniciar sesión

¡Le damos la bienvenida!

Inicie sesión en su cuenta

Correo electrónico:

Contraseña:

Recuérdeme

Olvidé mi contraseña?

Iniciar sesión

O continúe con:

G Google Síntesis

¿No tiene cuenta? [Iniciar base](#)

Figura No. 4. Creación de cuenta

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 474/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

2.5 Complete los campos con la información que se le pide, seleccionando la opción que mejor se adapte a su caso (Figura No. 5).

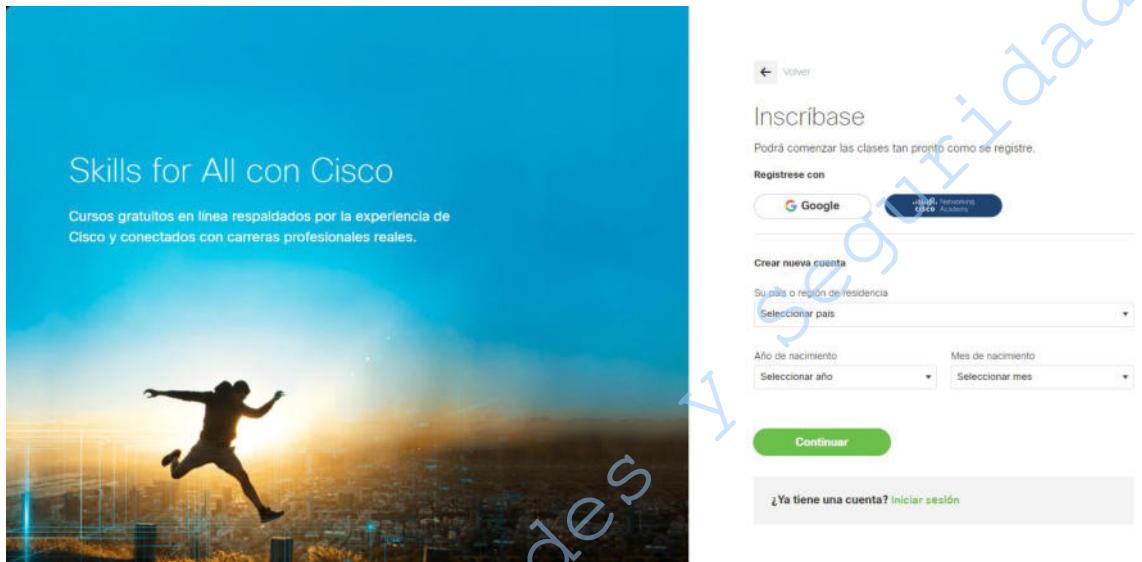


Figura No. 5. Datos del usuario

2.6 Una vez completado, se aceptan términos y condiciones (Figura No. 6).



Figura No. 6. Términos y condiciones

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	475/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

2.7 Al finalizar el procedimiento de registro se accede al sitio donde se encuentra el curso, en el primer módulo, en el apartado *1.0.3 Descargue Cisco Packet Tracer* se encuentra el enlace al sitio de descarga (Figura No. 7).

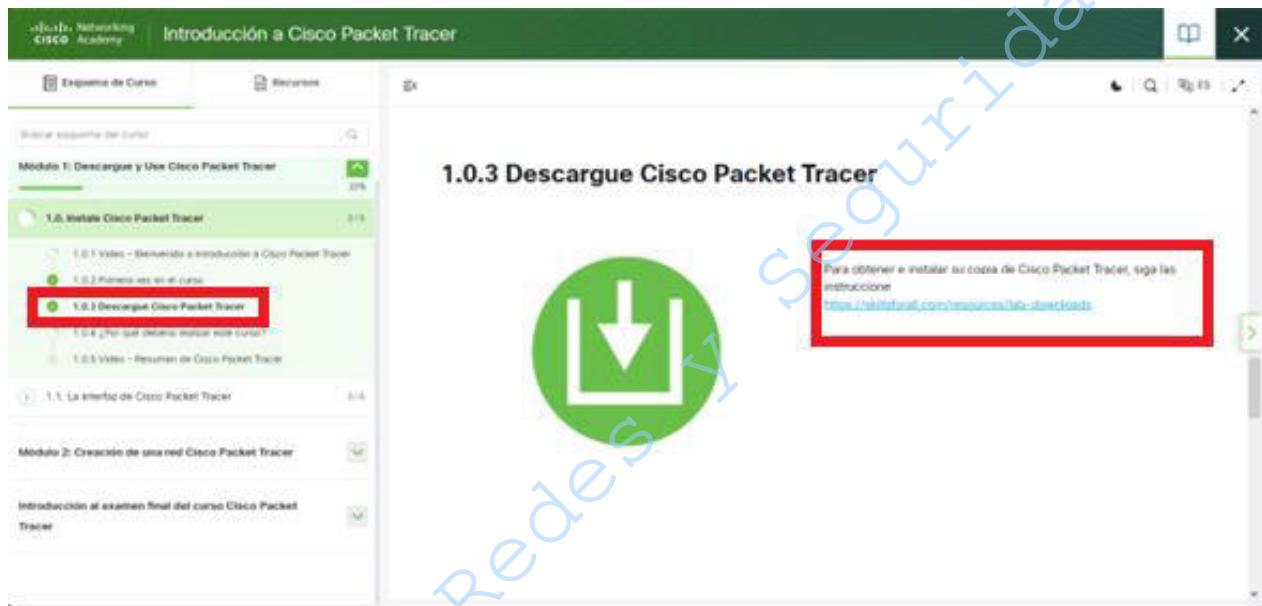


Figura No. 7. Enlace de descarga

2.8 Dé clic en el enlace y lo redireccionará a un nuevo sitio donde se encuentran los pasos a seguir para realizar la descarga e instalación del programa (Figura No. 8).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 476/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

Planned Maintenance

This site will be unavailable due to planned maintenance on 1 September 2023 @ 5:30 PM PDT through to 1 September 10:00 PM PDT (UTC -7).

Study Resources

Resource Hub

Skills for All is proud to offer a one stop for easy access to all resources that you may find useful. Stay updated and learn on!

The best way to learn is to do it.

To complete the hands-on activities in the courses, you might need to download and install on your computer some of the lab tools you can find twice on this page.

Learning Resources

Cisco Packet Tracer

To obtain and install your copy of Cisco Packet Tracer, please follow these simple steps:

Step 1. Download the version of Packet Tracer you require:

- [Packet Tracer 8.0.1 Mac/OS X64](#)
- [Packet Tracer 8.0.1 Ubuntu 64bit](#)
- [Packet Tracer 8.0.1 Windows X64](#)

Step 2. Launch the Packet Tracer install program

Step 3. Launch Cisco Packet Tracer by selecting the appropriate icon.

Step 4. When prompted, click on Select For All green button to authenticate.

Step 5. Cisco Packet Tracer will launch and you are ready to explore its features.

If you need more guidance, please follow the [Cisco Packet Tracer Download and Installation Instructions](#).

System Requirements:

Computer with either Windows (10, 11), Mac OS (10.14 or newer) or Ubuntu (20.04, 22.04) LTS operating system, amd64(64-bit) CPU, 4 GB of free RAM, 1.4 GB of free disk space.

Cybersecurity LabVM Workstation (CSE-LABVM, Security Workstation): Virtual Machine for the Cybersecurity courses

A Linux virtual machine that includes all the software tools you need to complete the labs and hands-on activities in the "Cybersecurity Essentials", "Enterprise Security", "Network Defense", "Cyber Threat Management", "Network Security", and "CyberOps Associate" courses.

Download the Virtual Machine file and follow the setup instructions from the course:

- [Cybersecurity Essentials Virtual Machine for Intel or AMD CPU](#)
- [Cybersecurity Essentials Virtual Machine for ARM CPU \(ARMv8/AArch64\)](#)

NOTE: To simplify your hands-on lab environment, the CSE-LABVM, Security Workstation, CyberOps VM, and Cisco CyberOps Workstation VM are also available as a unified single virtual machine - Cybersecurity LabVM Workstation. You do not need to download and install multiple virtual machines, only this one.

System Requirements:

Computer with either Windows, Mac or Linux operating systems, 64 bit Intel or AMD CPU with PVV Virtualization Support, 4 GB of free RAM, 15 GB of free disk space, Oracle VM VirtualBox software

Or Apple computer with M1/M2 CPU, 15 GB of free disk space, UTM VM Virtualization software

© 2023 Cisco. All rights reserved.
[About Us](#) [Terms and Conditions](#) [Privacy Statement](#) [Cookie Policy](#) [Data Protection](#) [Trademarks](#) [Help](#)

Figura No. 8. Instalación

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	477/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

b) Proceso para la utilización de Cisco Packet Tracer

2.1 Al ejecutar la aplicación Cisco Packet Tracer aparecerá la Figura No. 9, debe seleccionar la opción Skills for All

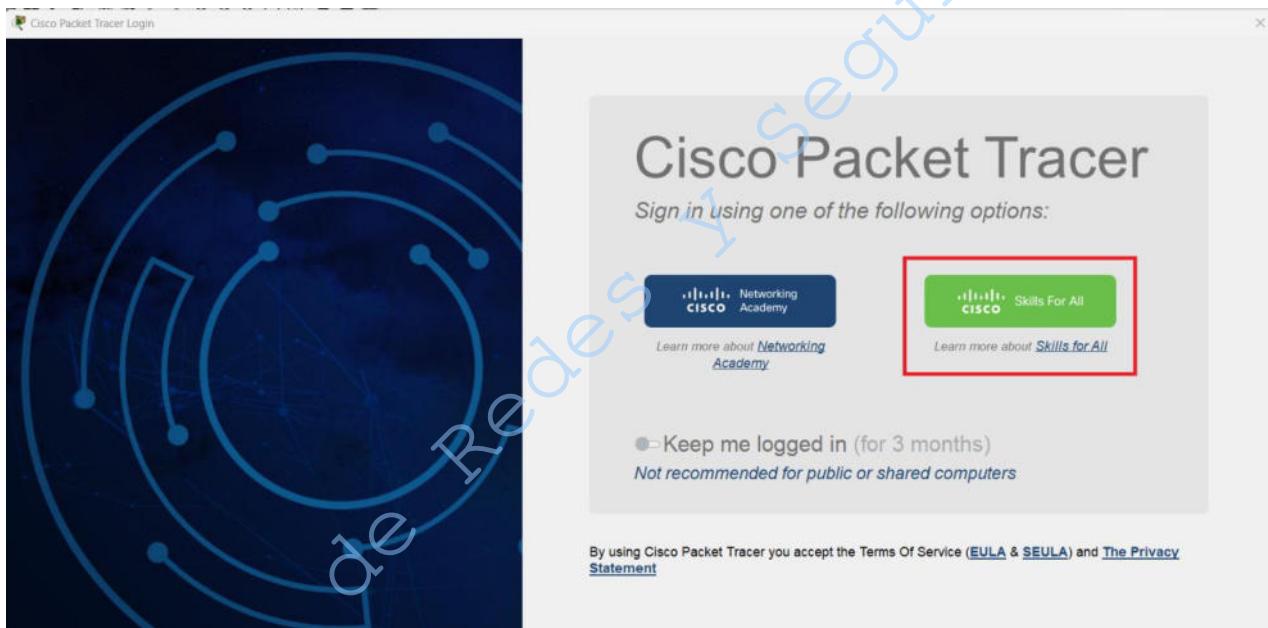


Figura No. 9. Cisco Packet Tracer

2.2 Será dirigido a la página que se observa en la Figura No. 10, en ella deberá ingresar su correo electrónico y contraseña correspondientes a la cuenta creada.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	06
		Página	478/479
		Sección ISO	8.3
		Fecha de emisión	11 de agosto de 2023
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

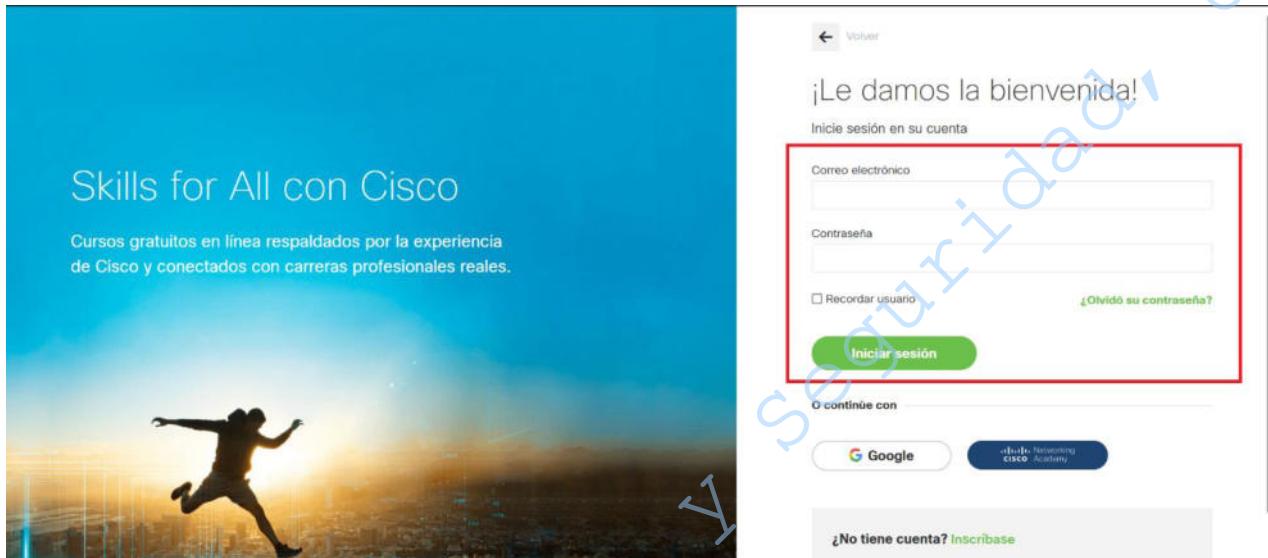


Figura No. 9. Cuenta en Cisco Packet Tracer

2.3 Al ingresar la información del paso anterior visualizará la Figura No 11, podrá cerrar dicha pestaña y comenzar a trabajar en la aplicación Cisco Packet Tracer (Figura No. 12).

You have successfully logged in to Cisco Packet Tracer. You may close this tab.

Figura No. 11. Acceso correcto a Cisco Packet Tracer

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 06 Página 479/479 Sección ISO 8.3 Fecha de emisión 11 de agosto de 2023
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

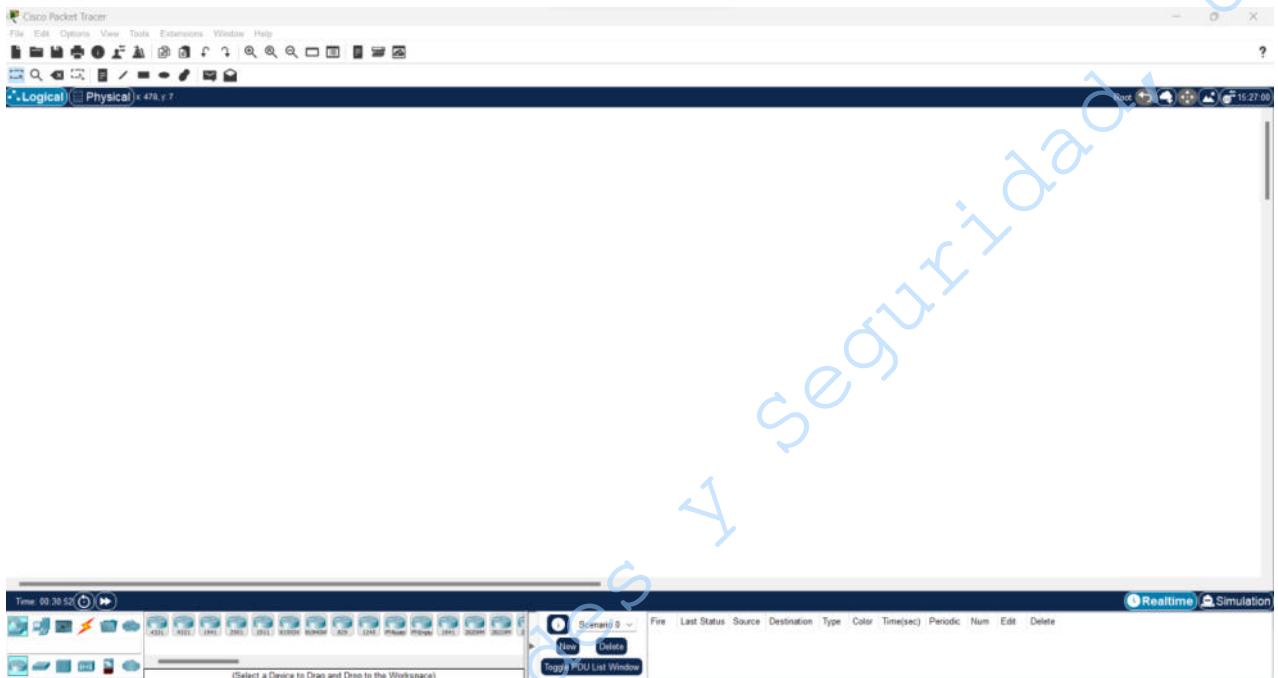


Figura No. 12. Aplicación Cisco Packet Tracer