

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	1/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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. Jaqueline López Barrientos Ing. Edgar Martínez Meza M.C. Cintia Quezada Reyes	M.C. Alejandro Velázquez Mena	11 de enero de 2019

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	2/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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	47
Práctica 6. Encaminamiento y análisis de paquetes	68
Práctica 7. Configuración básica del router	84
Práctica 8. TCP Y UDP	106
Práctica 9. SSH: Secure Shell	127
Práctica 10. Funciones de la capa de presentación	148
Práctica 11. Servidor DHCP	161
Prácticas Optativas	178

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	3/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 4/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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 construirá 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).

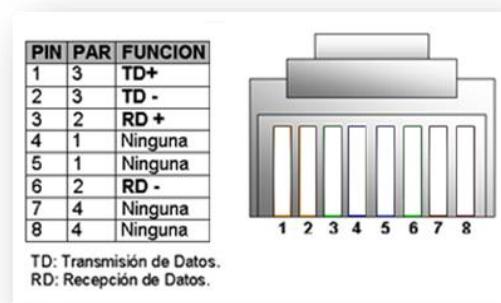


Figura No. 1. Transmisión y Recepción de Datos

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: 03 Página 5/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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:

- 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*

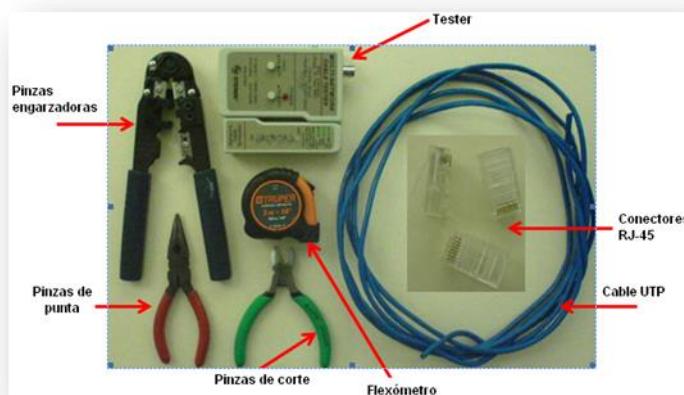


Figura No. 2. Material necesario

4.- Desarrollo:

Modo de trabajar

La construcción de los cables se realizará de manera individual.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 6/298 8.3 11 de enero de 2019
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).

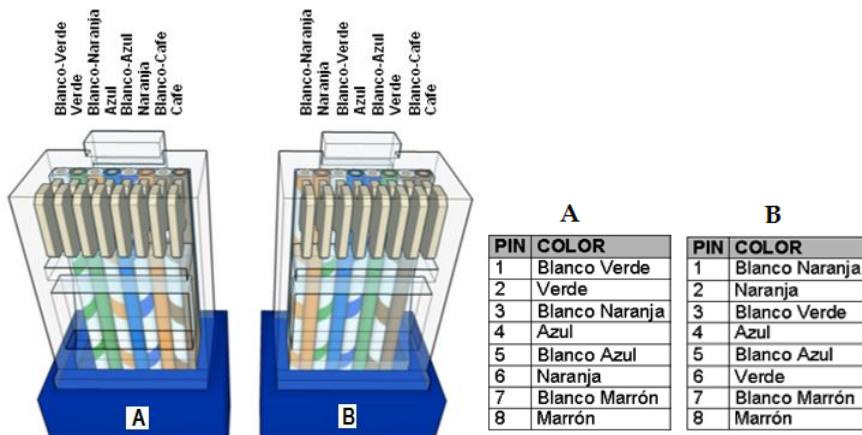


Figura No. 3. Configuración del cableado T568-A y T568-B

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: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 7/298 8.3 11 de enero de 2019
Facultad de Ingeniería			Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

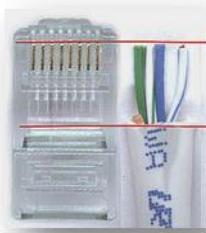


Figura No. 4 Distancia de corte de los alambres.

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:	03
		Página	8/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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).

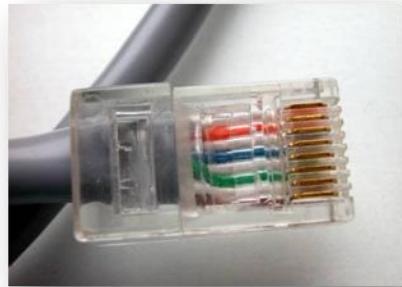


Figura No. 7. Cable de conexión finalizado.

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:	MADO-31
		Versión:	03
		Página	9/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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?



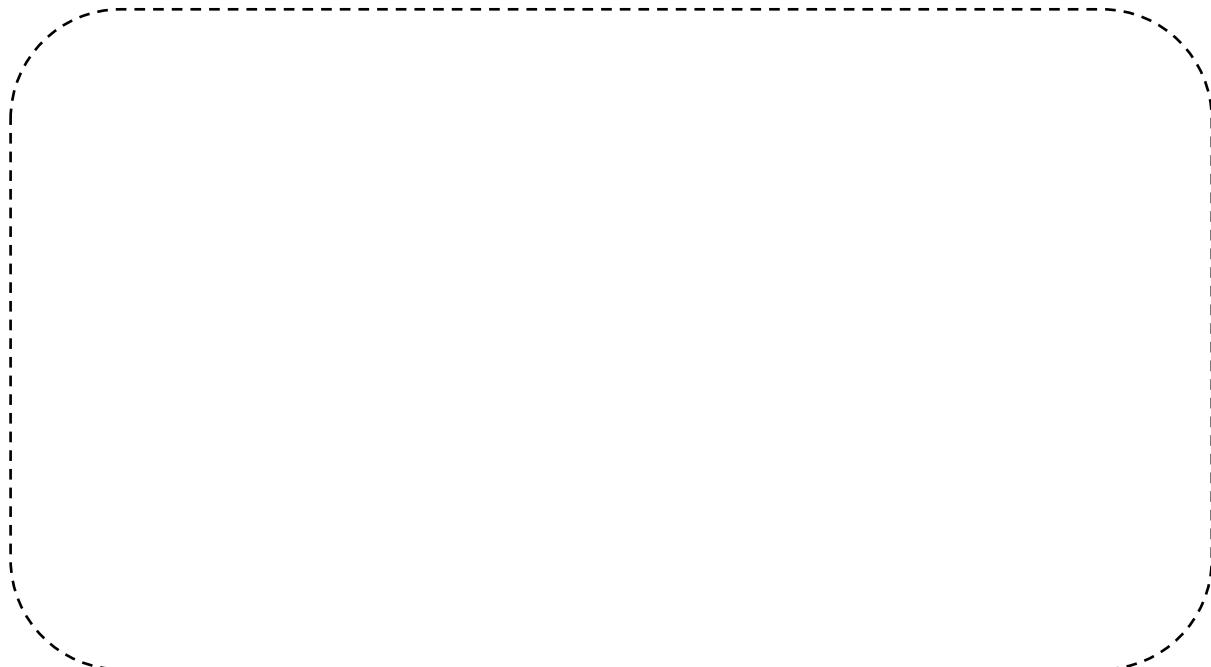
2. Investigue la configuración para un cable cruzado en redes de tipo Gigabit Ethernet.



7.- Conclusiones

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	10/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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



PRÁCTICA 1

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	11/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:	03
		Página	12/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	13/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 conocerá aspectos generales del cableado estructurado mediante la instalación de un *jack* y un panel de parcheo, utilizando 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: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 14/298 8.3 11 de enero de 2019
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:

- 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.

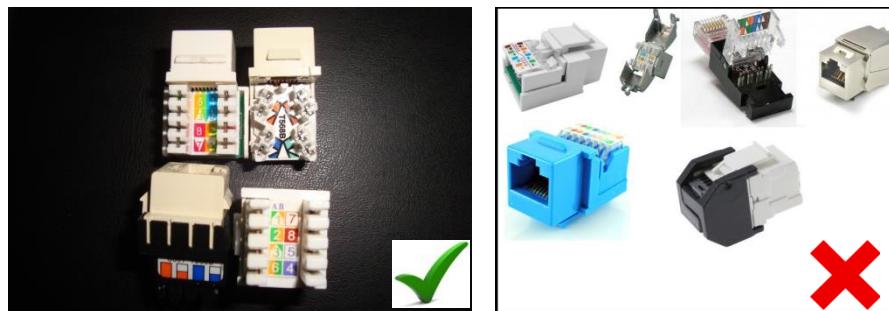


Figura No. 1a. Jacks

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

Equipo del Laboratorio:

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 15/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

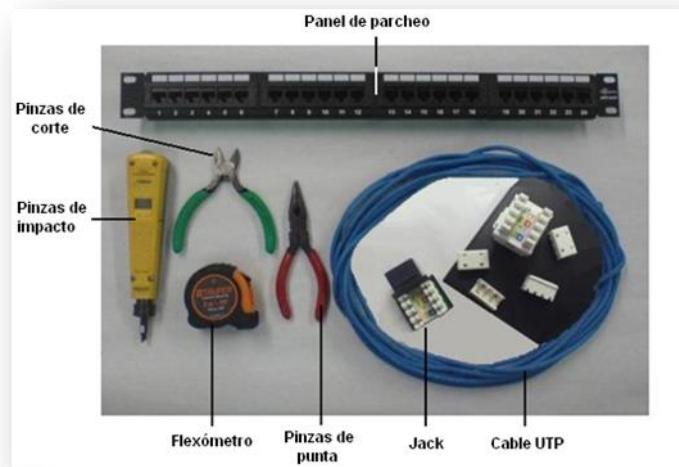


Figura No. 1b. Material necesario

4.- Desarrollo:

Modo de trabajar

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

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).

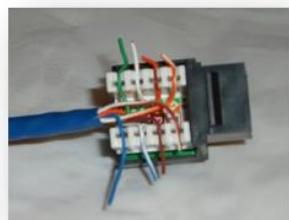


Figura No. 2. Construcción del *jack*

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	16/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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 el profesor.

5.- Pruebas

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

6.- Cuestionario

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	17/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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



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



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



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	18/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	19/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31
		Versión:	03
		Página	20/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	21/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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 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, conmutadores, 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:	03
		Página	22/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:

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

4.- Desarrollo

Modo de trabajar

La práctica se desarrollará en equipos.

4.1 Identificación del cableado estructurado en el laboratorio

En este ejercicio el alumno 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:	03
		Página	23/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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:	03
		Página	24/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	25/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	26/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31	
		Versión:	03	
		Página	27/298	
		Sección ISO	8.3	
		Fecha de emisión	11 de enero de 2019	
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

Ante 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:	03
		Página	28/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31
		Versión:	03
		Página	29/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	30/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 manipulará equipos de interconexión como lo son los hubs y switches.
- El alumno analizará el comportamiento del hub y del switch al momento de transmitir información mediante la herramienta de simulación de redes Cisco Packet Tracer Student en su versión más reciente.

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 adecúa 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:	03
		Página	31/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:

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

Equipo del Laboratorio:

- Software de simulación de redes Cisco Packet Tracer Student.
- Software Analizador de paquetes Wireshark

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 32/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- Switches Ethernet, FastEthernet o Gigabit Ethernet
- Hub

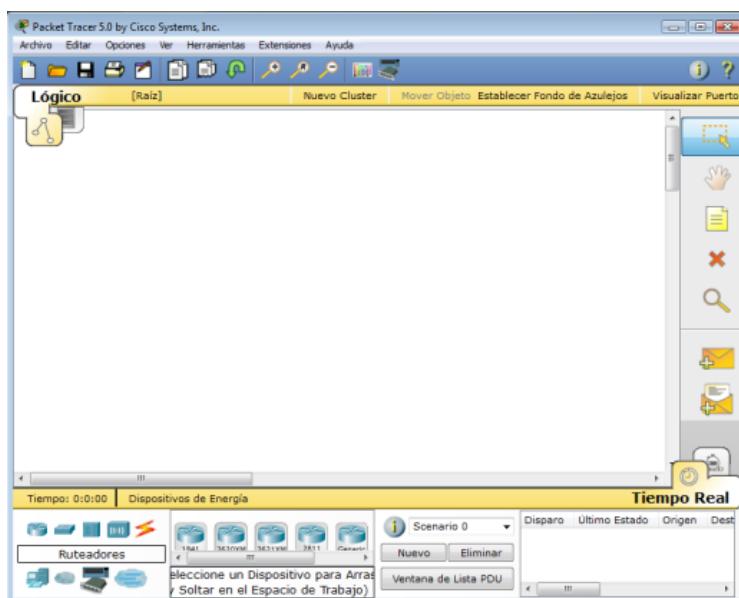
4.- Desarrollo:

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Análisis del rendimiento de un hub

- 4.1.3 Encienda el sistema y elija la opción de cargar *Windows*.
- 4.1.4 Inicie sesión en una cuenta con privilegios de administrador.
- 4.1.5 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.
- 4.1.6 Ejecute la aplicación Cisco Packet Tracer Student. (Ver Figura No. 1)



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 33/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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:

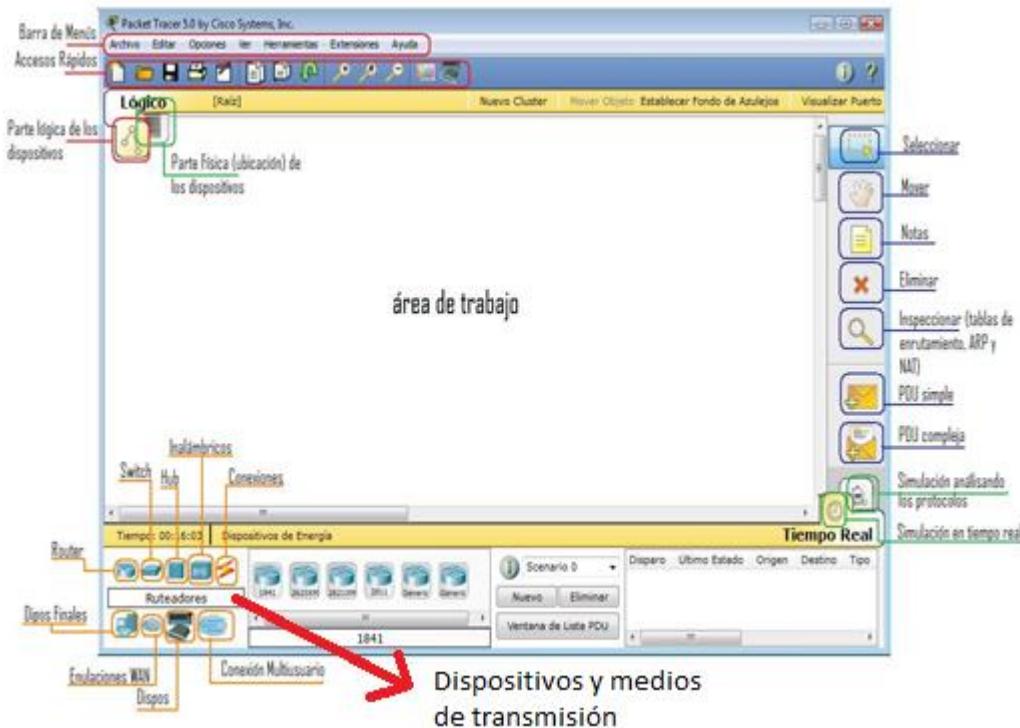


Figura No. 2. Área de trabajo del Simulador de CISCO Packet Tracer

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

- 4.1.7** Arrastre un switch 2950-24, un hub generic 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 profesor.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 34/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

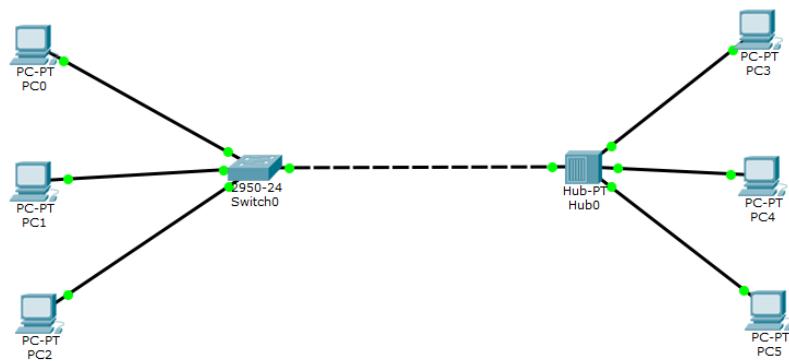


Figura No. 3 Creando la topología en Cisco Packet Tracer.

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

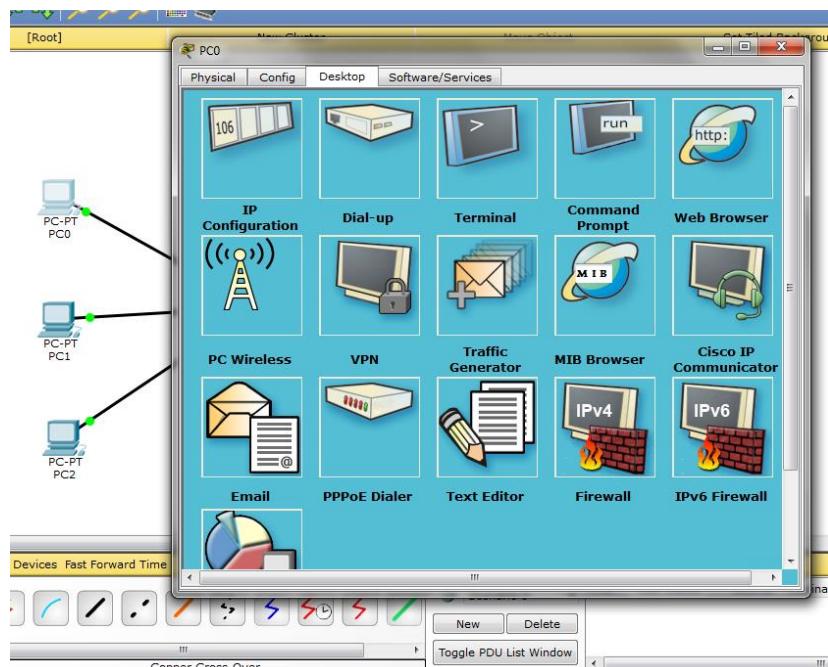


Figura No. 4 Pestaña de configuración de dispositivo.

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 35/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

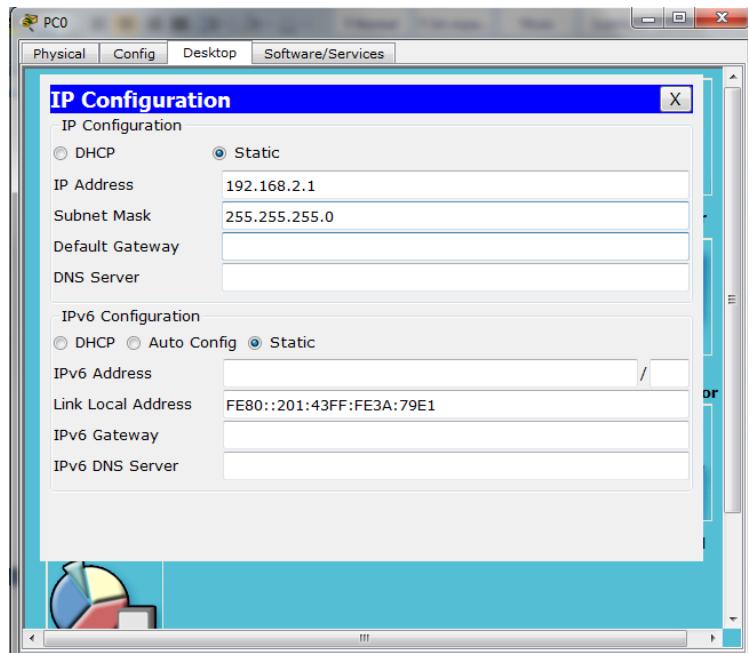


Figura No. 5 Configuración de direcciones.

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

4.1.11 Vaya a la pestaña Simulation en el ángulo inferior derecho del área de trabajo de Packet Tracer (ver figura No. 6), 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.

<p>INGENIERIA</p>	<p>Manual de prácticas del Laboratorio de Redes de Datos Seguras</p>	<p>Código: MADO-31 Versión: 03 Página 36/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019</p>
<p>Facultad de Ingeniería</p>		<p>Área/Departamento: Laboratorio de Redes y Seguridad</p>
<p>La impresión de este documento es una copia no controlada</p>		

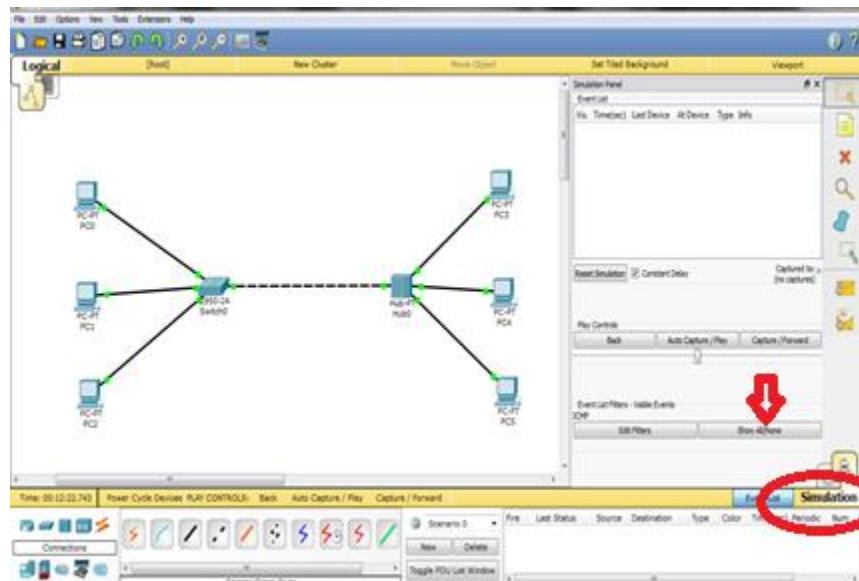


Figura No. 6 Pestaña de simulación de Packet Tracer.

4.1.12 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).

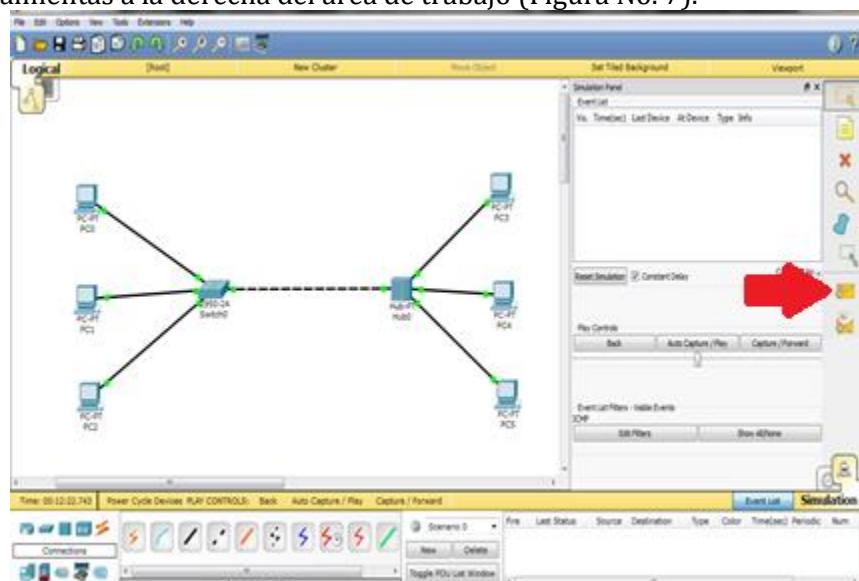


Figura No. 7 Add Simple PDU (P)

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 37/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.1.14 Presione el Botón Capture/Forward para comenzar la simulación (ver figura No. 8).

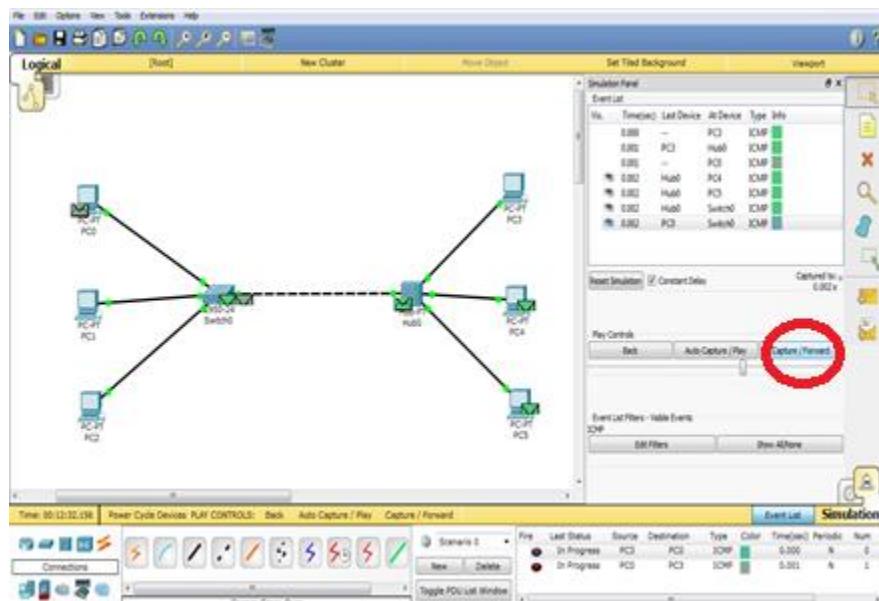
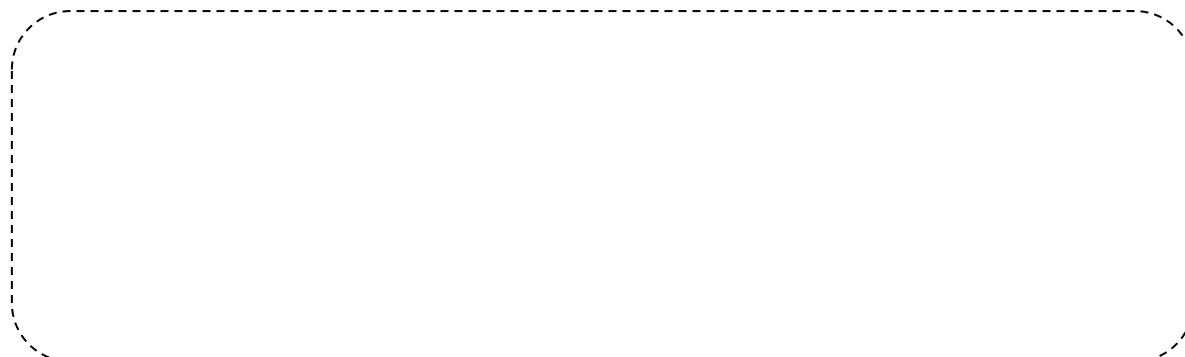


Figura No. 8 Simulación de Packet Tracer en curso.

4.1.15 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.



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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	38/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	

La impresión de este documento es una copia no controlada



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 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 Capture Options y configure de la siguiente manera (Ver Figura No. 9):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 39/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

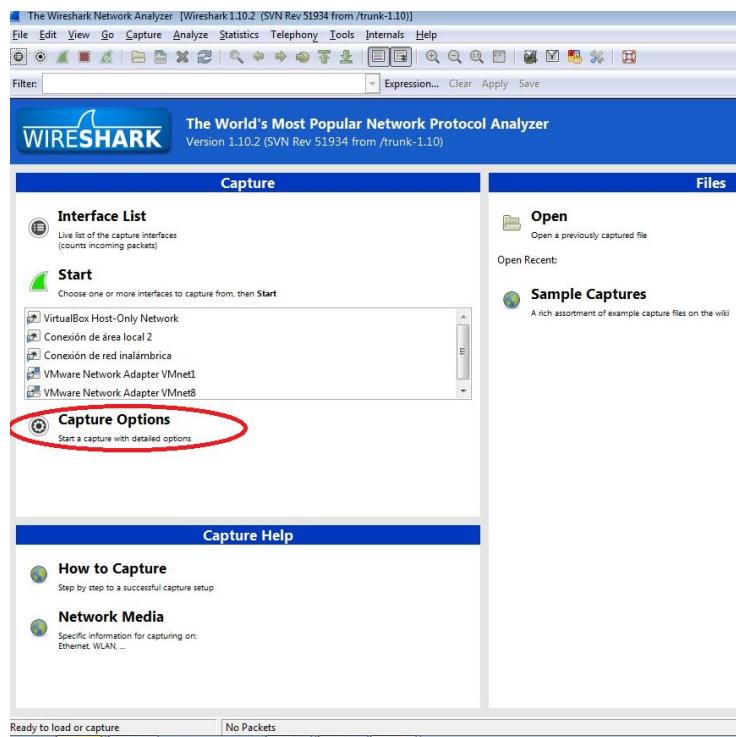


Figura No. 9 Iniciando una captura.

4.2.7 En la siguiente pantalla seleccione y habilite la tarjeta de red que se está usando (Interface) dando clic sobre el cuadro que está debajo de la palabra Capture. (Ver Figura No. 10). Verifique que debajo de Interface, aparezca la dirección IP correspondiente al equipo de cómputo que está utilizando (Conexión de área local 2, verificar la etiqueta pegada en el monitor de la PC), de no ser así, deberá seleccionar otra tarjeta de red donde aparezca la dirección IP correspondiente, 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: 03 Página 40/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada		

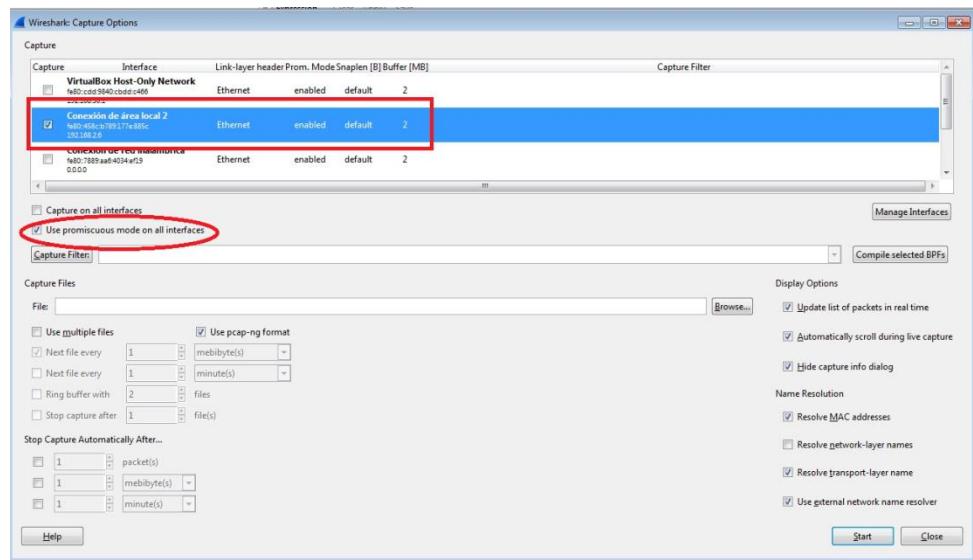


Figura No. 1.10. Seleccionando la Interfaz adecuada.

- 4.2.8** Despues de esto verifique que la captura en modo promiscuo esté activada (Use promiscuous mode on all interfaces) y presione start (Figura No. 10).
- 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 Compartir. Seleccione el botón que dice Compartir. (Ver Figura No. 11)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 41/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

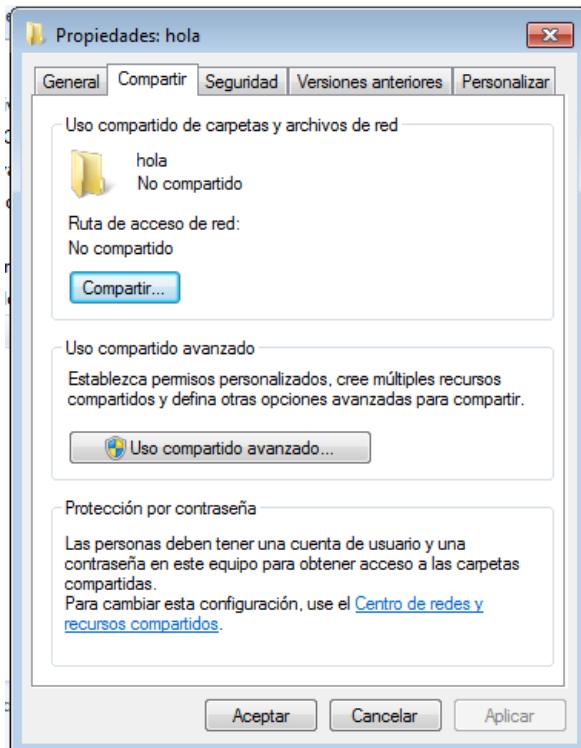


Figura No. 11. Propiedades de la carpeta

4.2.9.5 Seleccione Todos y dé clic en el botón Agregar. (Ver Figura No. 12)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 42/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

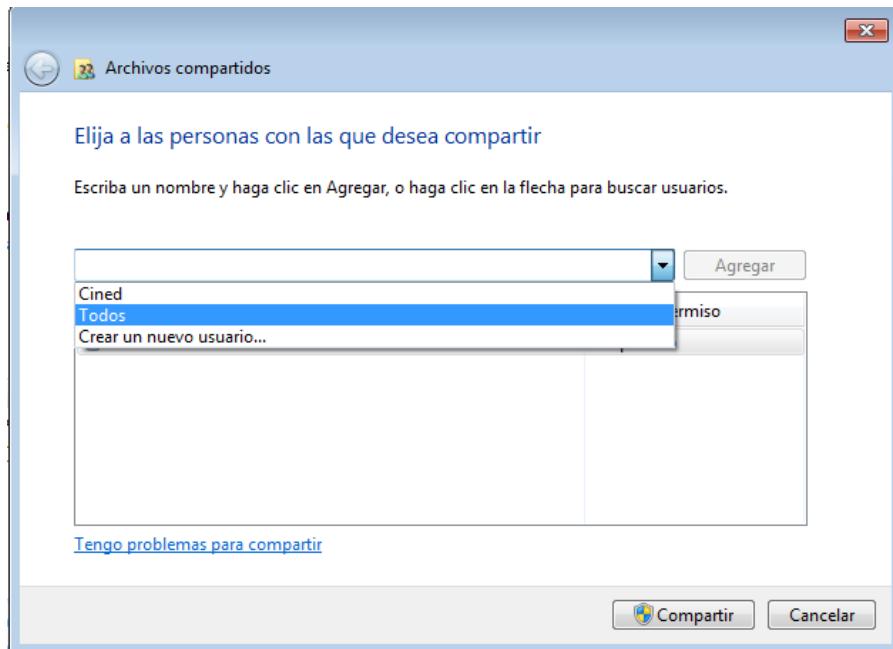


Figura No. 12. Permisos de la carpeta

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. 13).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 43/298 8.3 11 de enero de 2019
Facultad de Ingeniería			Area/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

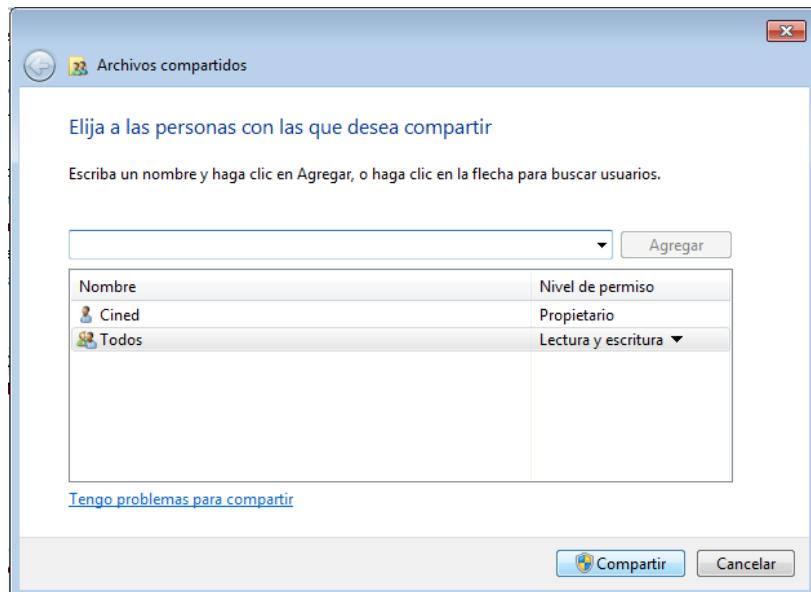


Figura No. 13. Nivel de permiso

4.2.9.7 Abra el menú principal y escriba en Buscar programas y archivos **\\\192.168.2.X\NombreDeLaCarpetaEnLaMáquinaRemota** (Ver Figura No. 14)

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: 03 Página 44/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

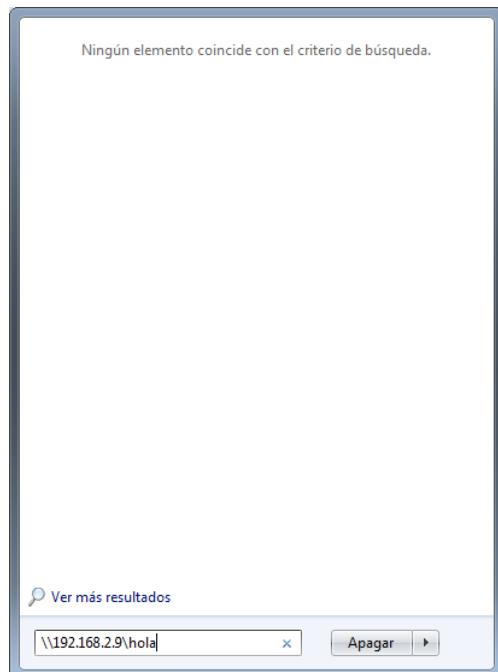


Figura No. 14 Ventana de búsqueda

- 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	45/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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:	03
		Página	46/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	47/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	48/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 al finalizar la práctica podrá configurar una tarjeta de red.
- El alumno 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 pasarlos a la capa física.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	49/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:

- Cable cruzado (crossover) construido en la práctica 1
- Un cable directo, norma B 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 desarrollará 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).

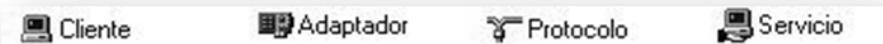


Figura No. 1. Íconos para los componentes de red.

- 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: 03 Página 50/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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)

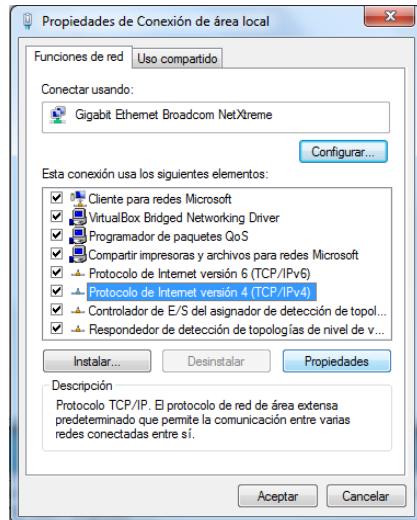


Figura No. 3. Propiedades de conexión de área local.

- 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**).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 51/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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 profesor (Dirección IP, Máscara de subred, Puerta de enlace predeterminada, Servidor DNS). (Ver Figura No. 4)

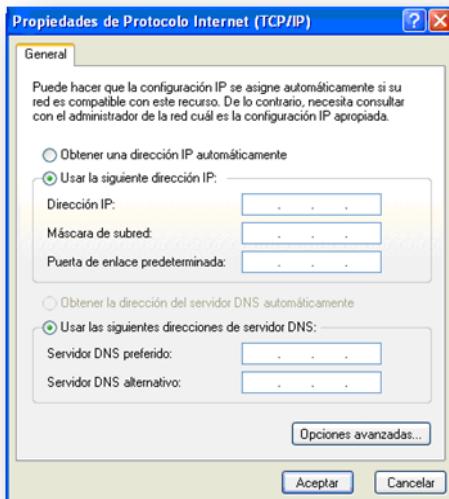


Figura No. 4. Propiedades del protocolo TCP/IP.

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:	03
		Página	52/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Código:</td><td>MADO-31</td></tr> <tr> <td>Versión:</td><td>03</td></tr> <tr> <td>Página</td><td>53/298</td></tr> <tr> <td>Sección ISO</td><td>8.3</td></tr> <tr> <td>Fecha de emisión</td><td>11 de enero de 2019</td></tr> </table>	Código:	MADO-31	Versión:	03	Página	53/298	Sección ISO	8.3	Fecha de emisión	11 de enero de 2019
Código:	MADO-31											
Versión:	03											
Página	53/298											
Sección ISO	8.3											
Fecha de emisión	11 de enero de 2019											
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad										
La impresión de este documento es una copia no controlada												

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

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

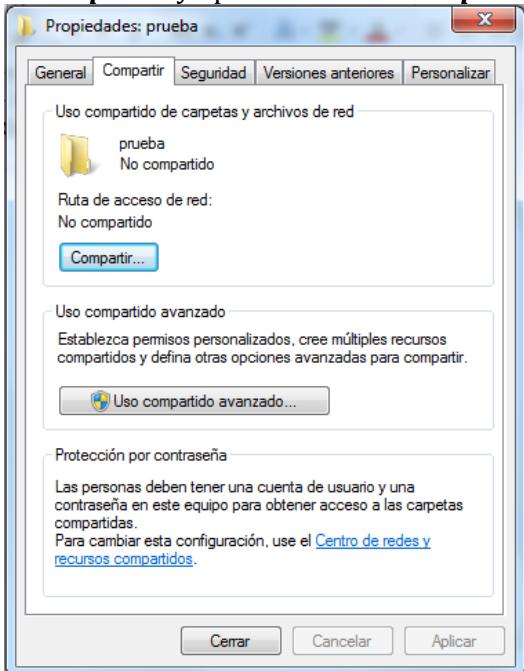
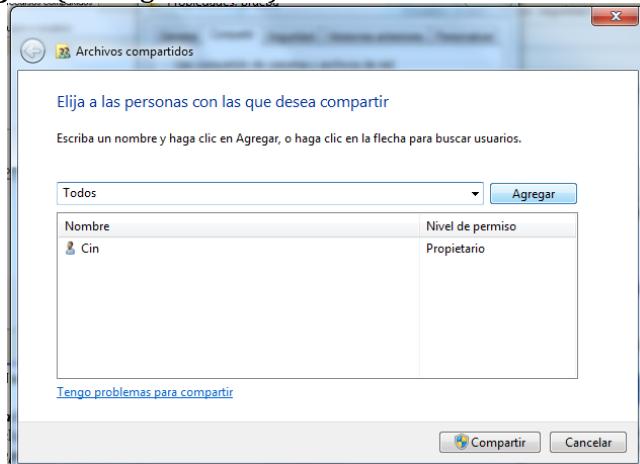


Figura No. 6. Propiedades de la carpeta

4.2.3.5 En la ventana **Elija a las personas con las que desea compartir** escriba **Todos** 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: 03 Página 54/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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).

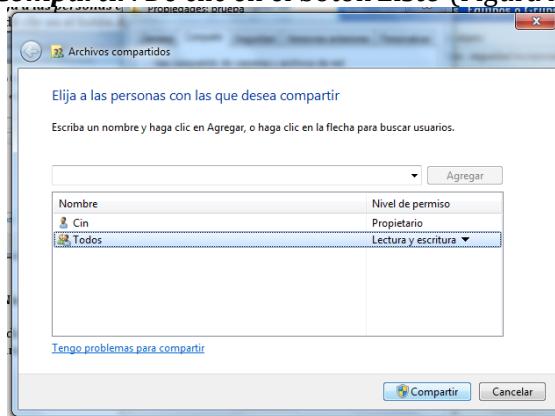


Figura No. 8. Selección de grupos, usuarios o equipos

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	55/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

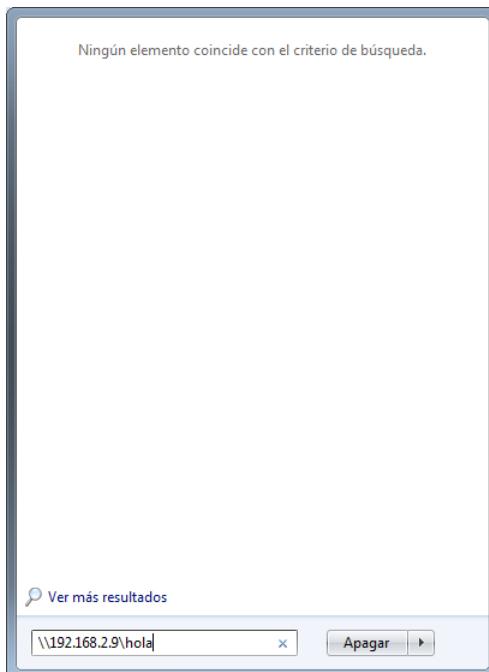


Figura No. 9 Ventana de comandos

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

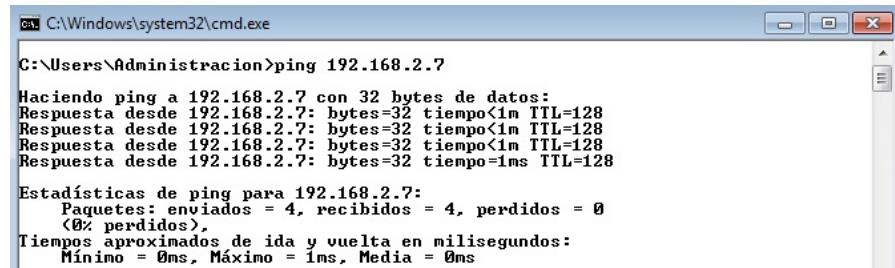
4.2.4 Conecte el cable cruzado (crossover) a dos computadoras.

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 56/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```
C:\Windows\system32\cmd.exe
C:\Users\Administracion>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<1ms TTL=128
Respuesta desde 192.168.2.7: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.2.7: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.2.7: bytes=32 tiempo=1ms 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:
        Minimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura No. 10. Ejecución del comando ping

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:

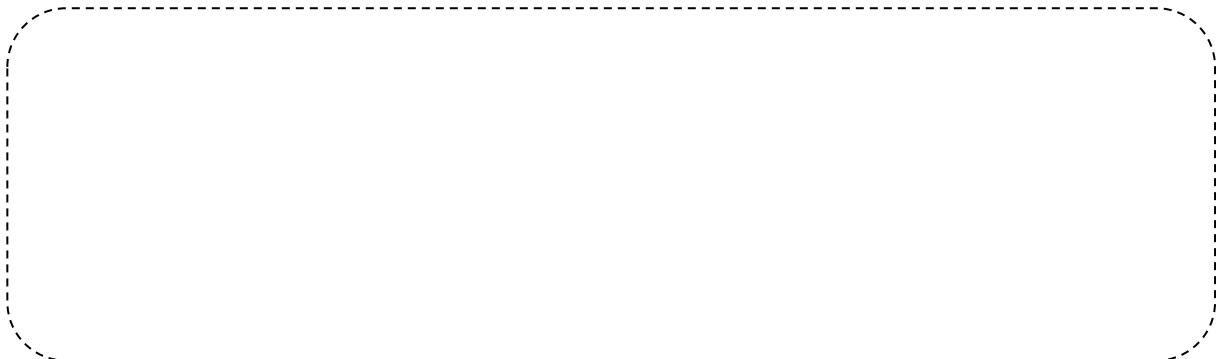
4.2.8 Ejecute nuevamente el comando ping, pero ahora agregue el parámetro -t (Figura No. 11). Mientras se ejecuta, desconecte el cable de red y observe la salida del comando. Escriba a continuación el resultado y mencione la importancia del comando ping para realizar pruebas de conectividad en redes.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 57/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```
C:\Windows\system32\cmd.exe
C:\Users\Administracion>ping -t 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<1ms TTL=128
Estadísticas de ping para 192.168.2.7:
    Paquetes: enviados = 11, recibidos = 11, perdidos = 0
        (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Minimo = 0ms, Máximo = 0ms, 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

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).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 58/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

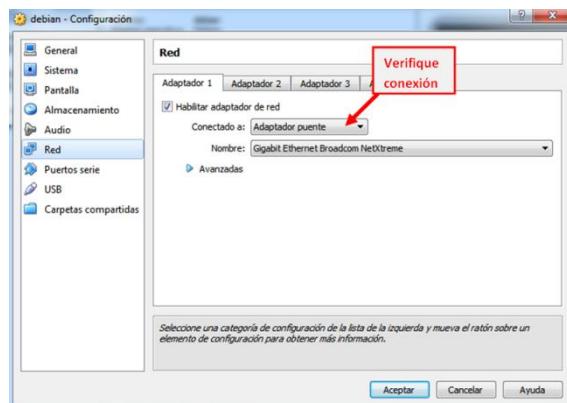


Figura No. 12. Conexión de red.

4.3.2 Encienda la máquina virtual

4.3.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No.13), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

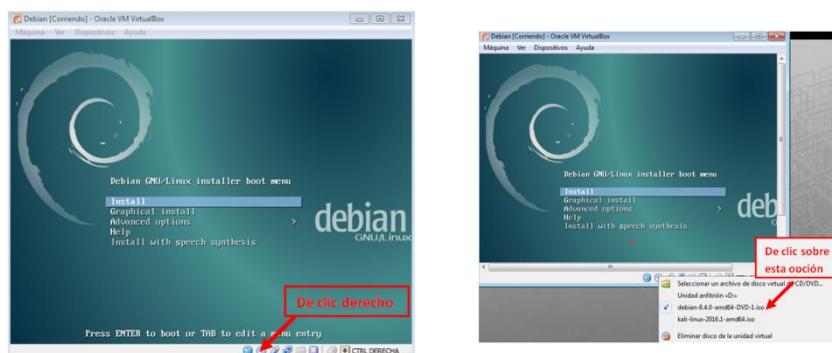


Figura No. 13. Inicio de Máquina Virtual.

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. 14)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 59/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes#
```

Figura No. 14. Terminal de comandos como root.

4.3.6 Teclee los siguientes comandos para borrar cualquier configuración previa:

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

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

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

4.3.8 Verifique y anote la versión del kernel de su máquina. Teclee el siguiente comando: (Ver figura No.15)

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



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# uname -r
3.16.0-4-amd64
root@debian:/home/redes#
```

Figura No. 15. Visualización de la versión del kernel.

Versión del kernel:_____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 60/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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. 16), 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/version_kernel/kernel/drivers/net
```



```
root@debian:/home/redes# ls /lib/modules/3.16.0-4-amd64/kernel/drivers/net
appletalk    hamradio    mdio.ko      slip       vxlan.ko
arcnet       hippi       mii.ko      sungem_phy.ko wan
bonding      hyperv      netconsole.ko team      wimax
can          ieee802154 nlmon.ko    tun.ko     wireless
dummy.ko     ifb.ko      phy        usb       xen-netback
eql.ko       irda        plip       veth.ko   xen-netfront.ko
ethernet    macvlan.ko  ppp        virtio_net.ko
fddi        macvtap.ko sb1000.ko  vmxnet3
```

Figura No. 16. Listado de drivers

- 4.3.11 Comente el resultado obtenido.**
-
-
-
-

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	61/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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

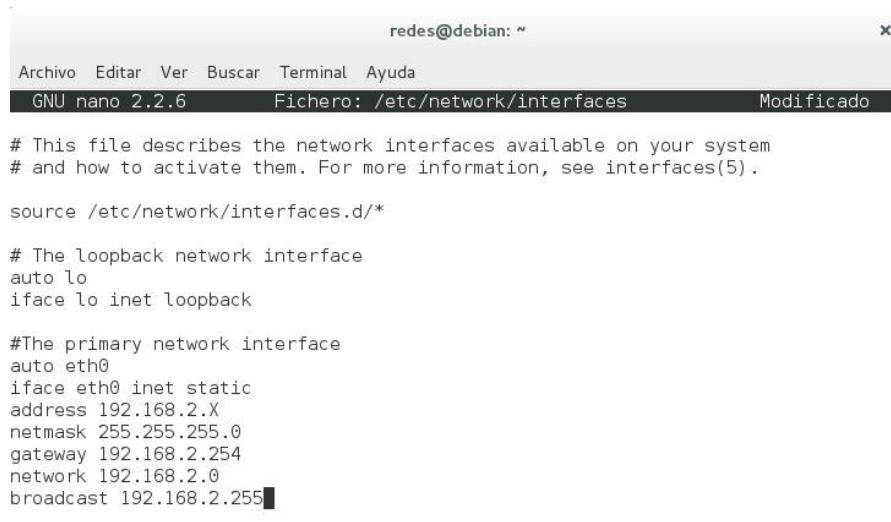
4.4.1.1 Edite el archivo **/etc/network/interfaces**, coloque lo siguiente: (Si los parámetros no aparecen en el archivo, tecléelos) (Ver Figura No. 17)

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

```
#The primary network interface
auto eth0
iface eth0 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



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6           Fichero: /etc/network/interfaces      Modificado

# 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/*

# The loopback network interface
auto lo
iface lo inet loopback

#The primary network interface
auto eth0
iface eth0 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
```

Figura No. 17 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:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 62/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

auto:

iface **** inet :

address:

gateway:

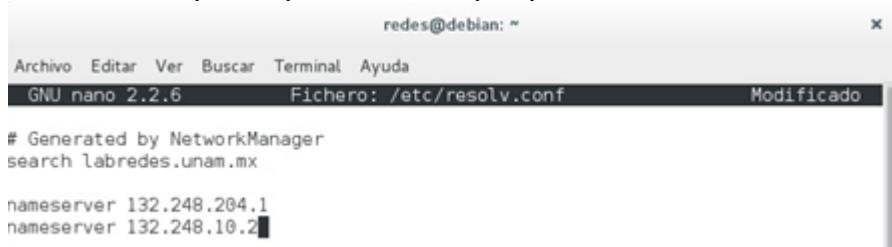
netmask:

network:

broadcast:

4.4.1.4 Dentro del archivo **resolv.conf** coloque los DNS (Ver Figura No. 18)

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



```
# Generated by NetworkManager
search labredes.unam.mx

nameserver 132.248.204.1
nameserver 132.248.10.2
```

Figura No. 18 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 eth0

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

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

root@debian:/home/redes# ifconfig eth0 up

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 63/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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



4.5 Pruebas y aplicaciones

4.5.1 Para comprobar la configuración actual de la NIC, utilice el siguiente comando(Ver Figura No. 19):

root@debian:/home/redes# ifconfig

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:14:b0:9e
          inet addr:192.168.2.35 Bcast:192.168.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe14:b09e/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:4540 errors:0 dropped:0 overruns:0 frame:0
            TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:342999 (334.9 KiB) TX bytes:12266 (11.9 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:34 errors:0 dropped:0 overruns:0 frame:0
            TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:3539 (3.4 KiB) TX bytes:3539 (3.4 KiB)
```

Figura No. 19. Ejecución del comando “ifconfig”

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	64/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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

4.5.2 Teclee el comando

```
root@debian:/home/redes # ifconfig eth0 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

- 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?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 65/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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. 24)

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# ping 192.168.2.35
PING 192.168.2.35 (192.168.2.35) 56(84) bytes of data.
64 bytes from 192.168.2.35: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 192.168.2.35: icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from 192.168.2.35: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 192.168.2.35: icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from 192.168.2.35: icmp_seq=5 ttl=64 time=0.056 ms
```

Figura No. 24 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	66/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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

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: 03 Página 67/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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 sirve el protocolo TCP/IP?
9. ¿Cuál es el significado e importancia de WINS?
10. ¿Por qué es importante conocer el modelo del chipset de la NIC?
11. ¿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.
12. ¿Cómo se desactiva un firewall en el sistema operativo Linux?
13. ¿Cómo se desactiva un firewall en el sistema operativo Windows?
14. Investigar los pasos para instalar el controlador de tarjeta de red en Windows
15. En el administrador de dispositivos investigue los diferentes íconos que señalan los problemas en los dispositivos y su significado (Figura No. A)

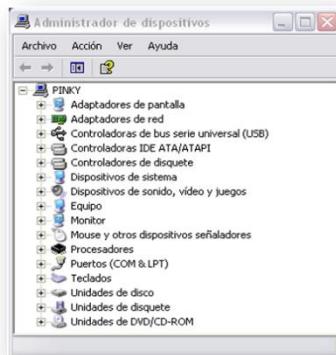


Figura No. A. Administrador de dispositivos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	68/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	69/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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 conocerá los fundamentos del monitoreo de redes, encapsulado de unidades a diferentes niveles y demultiplexación de las mismas.
- El alumno aplicará filtros adecuados en el análisis de paquetes.
- El alumno 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.

Traceroute

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	70/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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: 03 Página 71/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

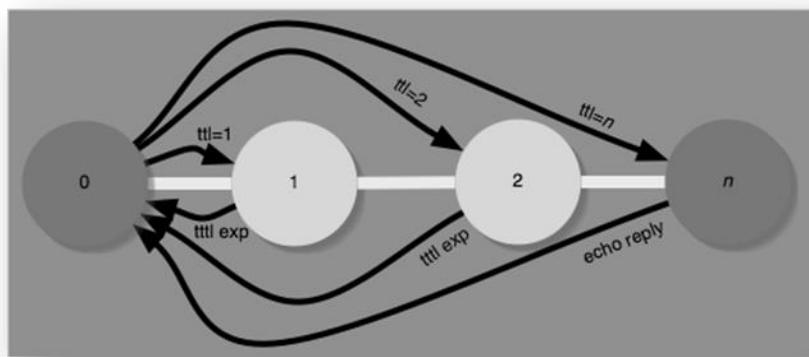


Figura No.1. Funcionamiento de traceroute

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:	03
		Página	72/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 73/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

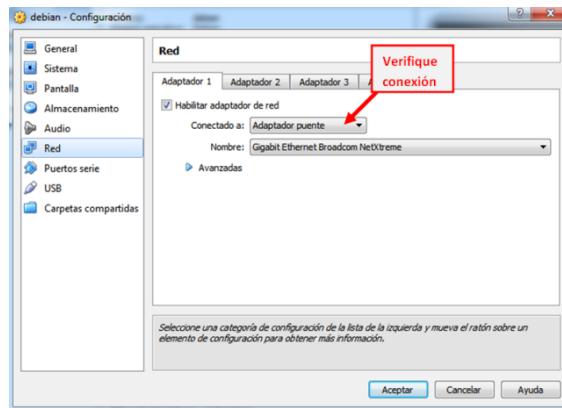


Figura No. 2. Conexión de red.

4.1.2 Encienda la máquina virtual

4.1.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 3), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

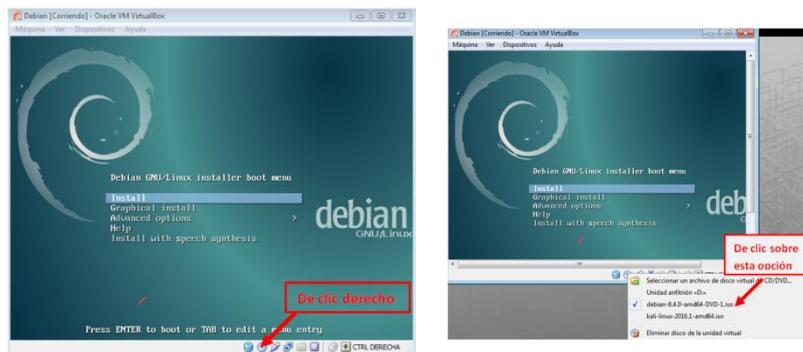


Figura No. 3. Inicio de Máquina Virtual.

4.1.4 Inicie sesión como usuario redes. 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. 4)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 74/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes#
```

Figura No. 4. Terminal de comandos.

4.1.6 Verifique que la conexión a la red esté habilitada (Ver Figura No. 5).

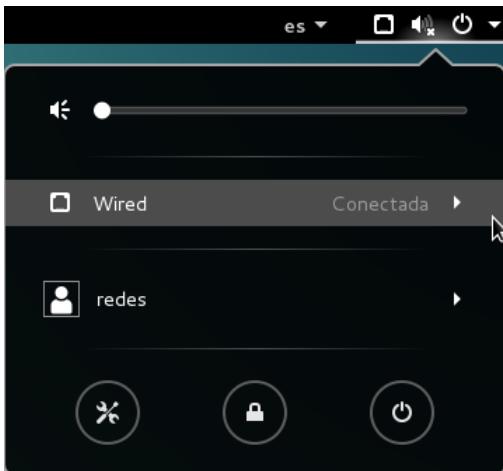
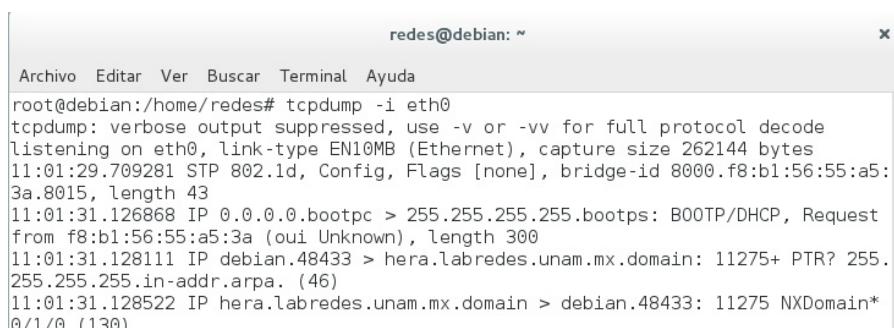


Figura No. 5. Conexión a la red.

4.1.7 Monitoree la interfaz de red, para ello teclee el siguiente comando (Figura No. 6)

root@debian:/home/redes# tcpdump -i eth0



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:01:29.709281 STP 802.1d, Config, Flags [none], bridge-id 8000.f8:b1:56:55:a5:3a.8015, length 43
11:01:31.126868 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from f8:b1:56:55:a5:3a (oui Unknown), length 300
11:01:31.128111 IP debian.48433 > hera.labredes.unam.mx.domain: 11275+ PTR? 255.
255.255.255.in-addr.arpa. (46)
11:01:31.128522 IP hera.labredes.unam.mx.domain > debian.48433: 11275 NXDomain*
0/1/0 (130)
```

Figura No. 6. Tcpdump.

NOTA: Teclee **ctrl+c** para detener la captura

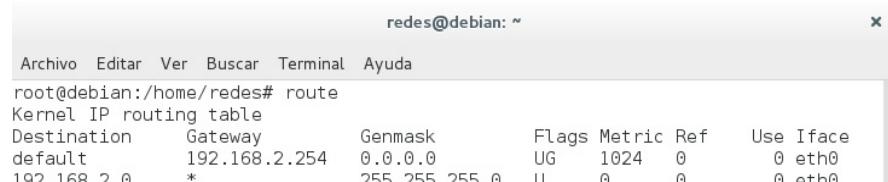
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 75/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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



- 4.1.9** Visualice la configuración actual de la tabla de encaminamiento. (Ver Figura No. 7)
Teclee lo siguiente:

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



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
default         192.168.2.254  0.0.0.0       UG    1024   0        0 eth0
192.168.2.0     *              255.255.255.0 U     0        0        0 eth0
```

Figura No. 7. 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. 8)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	76/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# traceroute www.google.com
traceroute to www.google.com (74.125.21.99), 30 hops max, 60 byte packets
 1  192.168.2.254 (192.168.2.254)  1.349 ms  1.177 ms  1.045 ms
 2  ve52.iimas-dist.unam.mx (132.248.52.254)  10.417 ms  10.328 ms  10.244 ms
 3  1010-iimas.redunam.unam.mx (132.247.237.101)  1.722 ms  1.605 ms  1.487 ms
 4  201-174-135-89.transtelco.net (201.174.135.89)  2.422 ms  2.294 ms  2.130 ms
 5  ustx-mca-pae.transtelco.net (201.174.254.237)  14.717 ms ustx-mca-pae.transtelco.net (201.174.254.201)  14.614 ms 14.495 ms
 6  201-174-250-36.transtelco.net (201.174.250.36)  86.185 ms 201-174-244-149.transtelco.net (201.174.244.149)  28.548 ms 201-174-244-165.transtelco.net (201.174.244.165)  26.410 ms
 7  209.85.173.184 (209.85.173.184)  30.379 ms  29.344 ms  29.183 ms
 8  108.170.240.145 (108.170.240.145)  29.048 ms 108.170.240.82 (108.170.240.82)  28.886 ms 108.170.240.81 (108.170.240.81)  31.396 ms
 9  216.239.62.213 (216.239.62.213)  29.465 ms 108.170.228.79 (108.170.228.79)  60.015 ms 59.808 ms
10  209.85.240.17 (209.85.240.17)  48.782 ms  47.667 ms 209.85.249.44 (209.85.249.44)  59.119 ms
11  216.239.56.166 (216.239.56.166)  47.399 ms 209.85.142.149 (209.85.142.149)  47.685 ms 216.239.56.166 (216.239.56.166)  46.611 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  yv-in-f99.1e100.net (74.125.21.99)  45.916 ms  47.230 ms  46.568 ms
root@debian:/home/redes#
```

Figura No. 8 Comando traceroute

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



4.1.13 Ciérre la máquina virtual

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	77/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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). 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



- 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:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 78/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



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 En la siguiente pantalla seleccione y habilite la tarjeta de red que se está usando (Interface) dando clic sobre el cuadro que está debajo de la palabra Capture. Verifique que debajo de Interface, aparezca la dirección IP correspondiente al equipo de cómputo que está utilizando (Conexión de área local 2, verificar la etiqueta pegada en el monitor de la PC), de no ser así, deberá seleccionar otra tarjeta de red donde aparezca la dirección IP correspondiente, evite seleccionar aquellas que correspondan a las tarjetas inalámbricas o virtuales. Deshabilite la opción Use promiscuous mode on all interfaces. Oprima Start (Ver Figura No. 9)

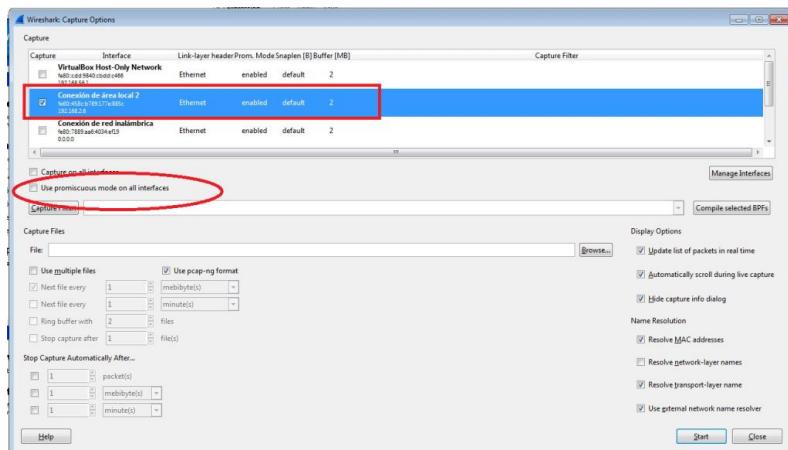


Figura No. 9. Opciones de captura.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 79/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.8.4 Dé clic en la opción *Expression...* y seleccione del menú la siguiente opción: *ARP/RARP - Address Resolution Protocol-> arp.proto.type-Protocol type*. Dé clic en *OK* (Ver Figura No. 10)

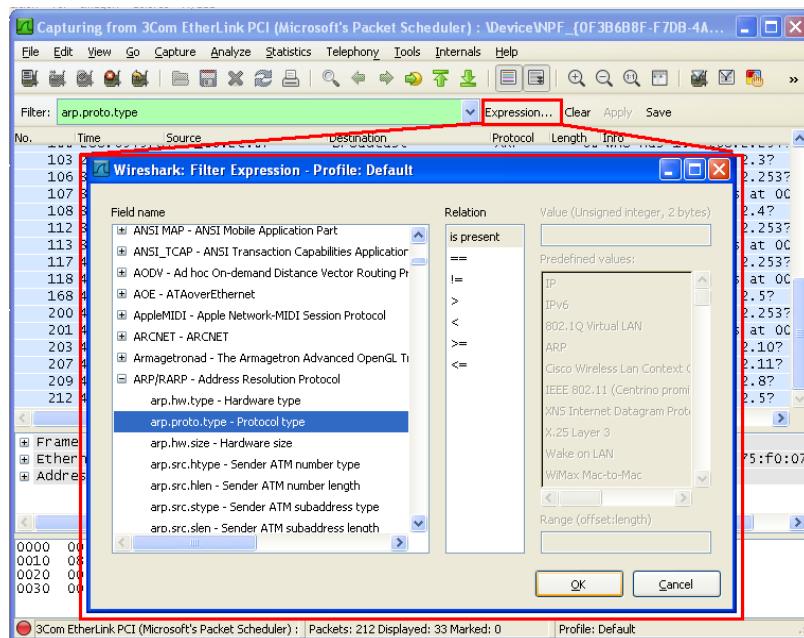


Figura No. 10. Filtro ARP.

4.2.8.5 Seleccione la opción *Apply* (Ver figura No. 11)



Figura No. 11. Aplicación del filtro ARP.

4.2.8.6 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.

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

```
C:\> arp -a
```

4.2.8.8 Detenga la captura de Wireshark.

4.2.8.9 Realice una tabla con el contenido de la tabla del comando ARP del paso **4.2.8.7**.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 80/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			



4.2.8.10 Analice la información del paso anterior y comente

4.2.8.11 Vuelva a Wireshark y observe las tramas recibidas

4.2.8.12 Localice una trama ARP REQUEST y su correspondiente ARP REPLAY. 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 REPLAY, indique cuál es el funcionamiento del protocolo ARP (Figura No. 12):

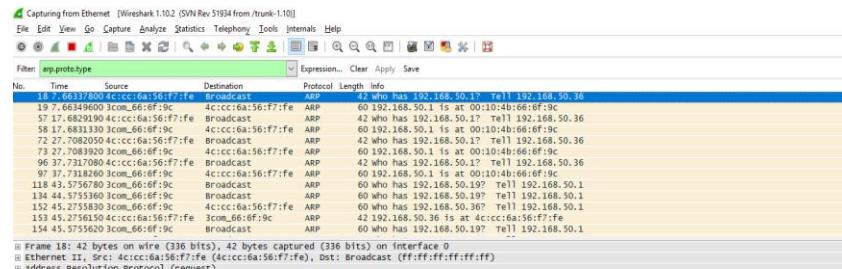


Figura No. 12 Tramas ARP REQUEST y ARP REPLAY

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	81/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

4.2.9 Si 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*?

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

6.-Conclusiones

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	82/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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



PRÁCTICA 6

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	83/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Encaminamiento y análisis de paquetes

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. Defina el concepto de encaminamiento
5. Investigue el objetivo y funcionamiento del protocolo ARP
6. Descargue el software NeoTrace (o equivalente) y visualice en el mapa el camino que siguen los paquetes hacia un servidor localizado en:
 - a. Hawaii
 - b. Londres
 - c. India

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	84/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: Versión: Página: Sección ISO Fecha de emisión	MADO-31 03 85/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

1.- Objetivo de Aprendizaje

- El alumno 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 Student.

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 serials 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:	03
		Página	86/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 Student
- Router Cisco 877

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:	03
		Página	87/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

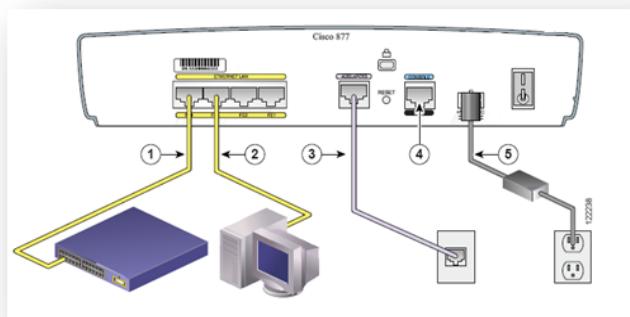


Figura No. 2. Componentes del router CISCO

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: 03 Página 88/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

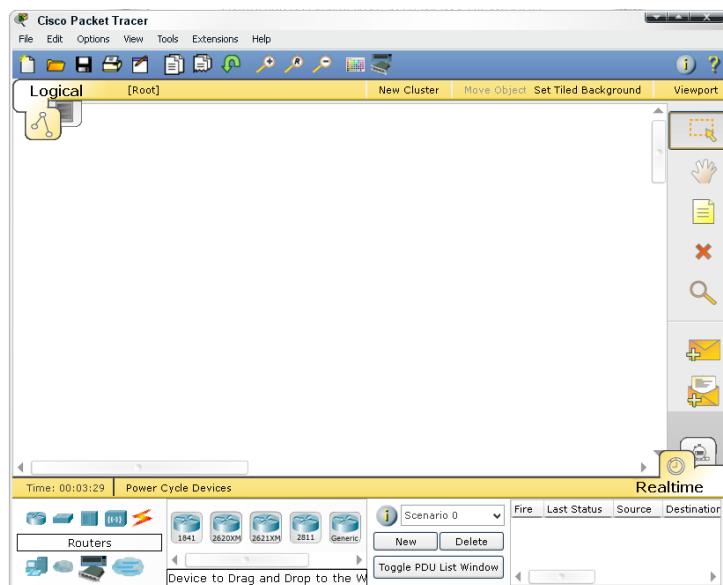


Figura No. 3. Interfaz gráfica de PT

- 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.)

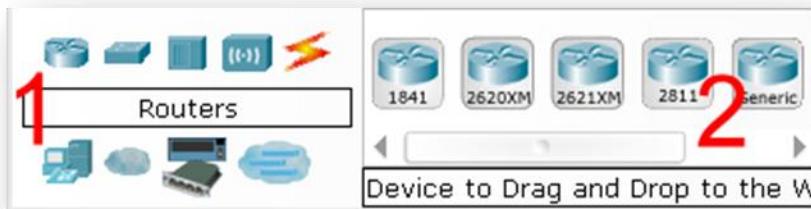


Figura No. 4. Secciones de dispositivos

- 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 89/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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:

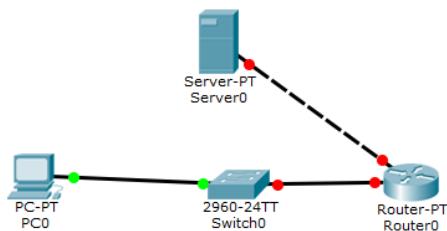


Figura No. 5 Topología

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: Generic, es indispensable que seleccione el primer router genérico que aparece en la lista, al colocarlo en el área lógica observe que diga Router-PT) y un switch 2960.

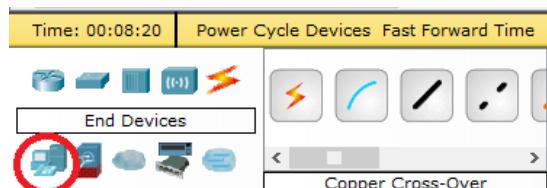


Figura No. 6 End Devices

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)

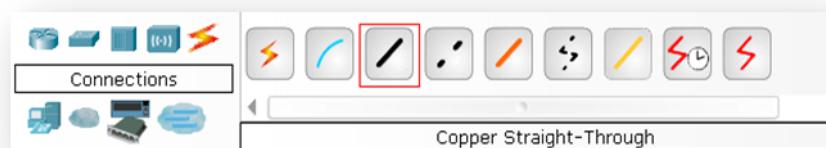


Figura No. 7. Tipos de cables de conexión.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 90/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Area/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 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)

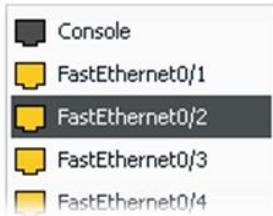


Figura No. 8. Puertos del switch

- 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 FastEhternet0.

- 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 profesor.

- 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 91/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

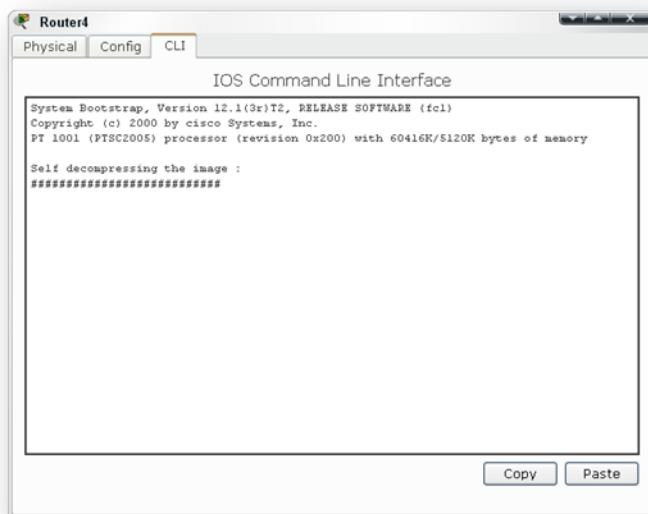


Figura No. 9. Interfaz de consola del router.

- 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	

- 4.3.5** Los routers funcionan con tres modos básicos:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	92/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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**

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**.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	93/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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.

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	94/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			



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

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	95/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 desee 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
```

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	96/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	97/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:	03
		Página	98/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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

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 _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	99/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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.

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 100/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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):

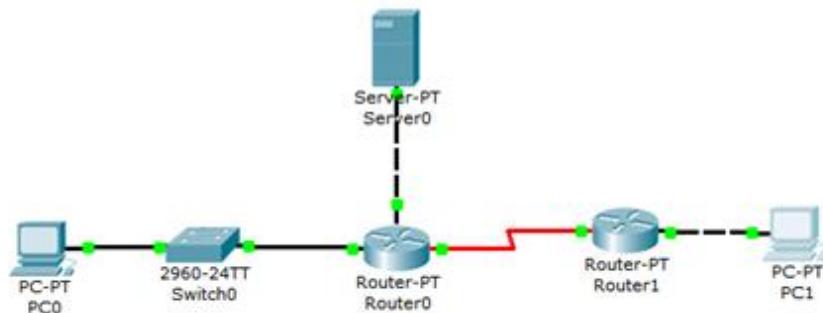


Figura No. 10 Topología de red final

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).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	101/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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
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:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	102/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

- 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)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	103/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

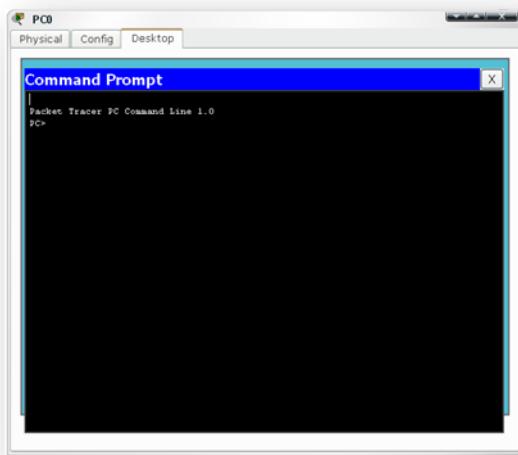


Figura No. 11. Command Prompt

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?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	104/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

5.-Conclusiones

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

(Large dashed rectangular area for writing conclusions)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	105/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	106/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	107/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 podrá utilizar un programa que le permita enviar y recibir información utilizando los protocolos TCP y UDP y reafirmando conceptos teóricos.
- El alumno 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:

- 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.

4.1 Preparación del programa Sock

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 108/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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)

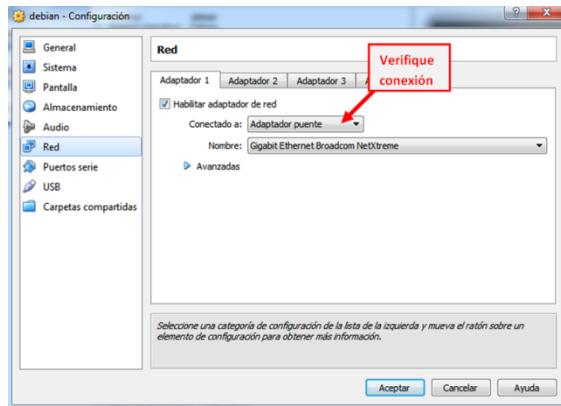


Figura No. 1. Conexión de red.

4.1.2 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 2), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

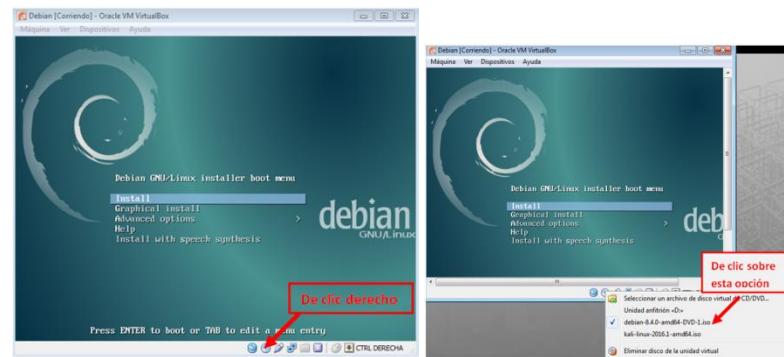


Figura No. 2. Inicio de Máquina Virtual.

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. 14)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	109/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

redes@debian:~\$ su

- 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 eth0 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: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 110/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes# service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled)
  Active: active (running) since mar 2017-05-23 21:19:02 MDT; 9min ago
    Process: 849 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
  Main PID: 388 (sshd)
    CGroup: /system.slice/sshd.service
            └─388 /usr/sbin/sshd -D

may 23 21:19:09 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:09 debian sshd[388]: Server listening on :: port 22.
may 23 21:19:29 debian sshd[388]: Received SIGHUP; restarting.
may 23 21:19:29 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:29 debian sshd[388]: Server listening on :: port 22.
may 23 21:19:29 debian sshd[388]: Received SIGHUP; restarting.
may 23 21:19:29 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:29 debian sshd[388]: Server listening on :: port 22.
root@debian:/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
```

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/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:	03
		Página	111/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# rm -rf prac*
root@debian:/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@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ mkdir practica
redes@debian:~$
```

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@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ cp sock-1.1.tar.tar /home/redes/practica/
```

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:	03
		Página	112/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
redes@debian: ~/practica
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ cd practica/
redes@debian:~/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@debian:~/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
```

```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica$ cd sock-1.1/
redes@debian:~/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@debian:~/practica/sock-1.1$
```

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 113/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 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

```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ make
gcc -g -O2 -Wall -W-no-parentheses -Wstrict-prototypes -Wno-unused -lssl -lre
solv sock.c -o sock
sock.c: In function 'sigchld_handler':
sock.c:215:21: warning: unused parameter 'sig' [-Wunused-parameter]
    sigchld_handler(int sig)
                ^
sock.c: In function 'main':
sock.c:461:37: warning: pointer targets in passing argument 3 of 'accept' differ
in signedness [-Wpointer-sign]
    int ns = accept(sk, sa_incoming, &l);
                           ^
In file included from sock.c:18:0:
/usr/include/x86_64-linux-gnu/sys/socket.h:243:12: note: expected 'socklen_t * __restrict__' but argument is of type 'int *'
extern int accept (int __fd, __SOCKADDR_ARG __addr,
                    ^
```

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@debian:~/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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	114/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 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@debian: ~/practica/sock-1.1$ ./sock :22
SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u1
```

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.

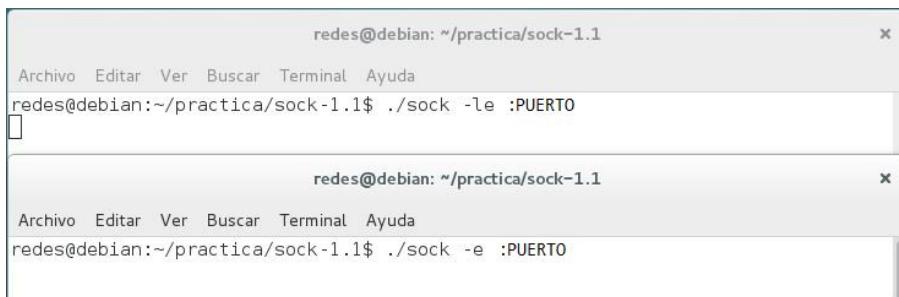
```
redes@debian:~/practica/sock-1.1$ ./sock -l :PUERTO
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	115/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

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

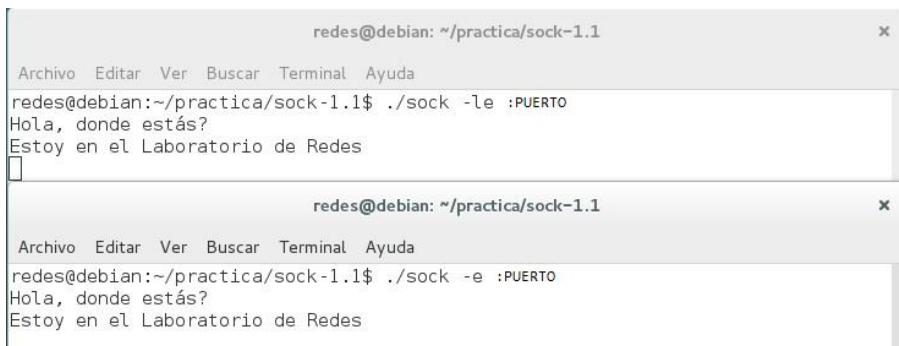


```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -le :PUERTO

redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/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@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -le :PUERTO
Hola, donde estás?
Estoy en el Laboratorio de Redes

redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -e :PUERTO
Hola, donde estás?
Estoy en el Laboratorio de Redes
```

Figura No. 14. Comunicación entre terminales

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	116/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Salga con CTRL + C

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.

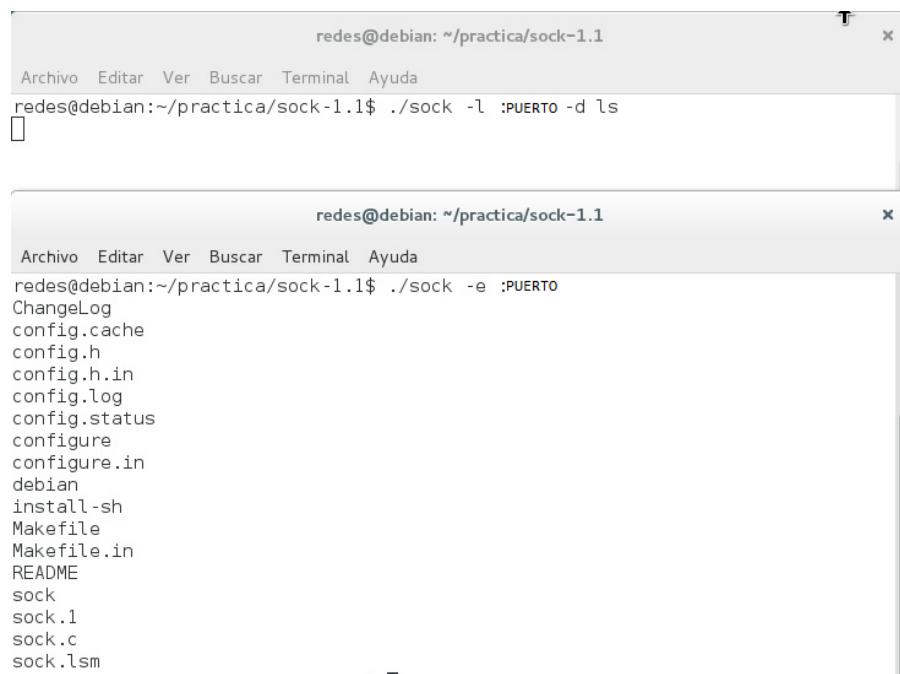
redes@debian:~/practica/sock-1.1\$./sock -l :PUERTO -d ls

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: 03 Página 117/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



```

redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -l :PUERTO -d ls
[Output is empty]

redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -e :PUERTO
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

```

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.

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:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	118/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

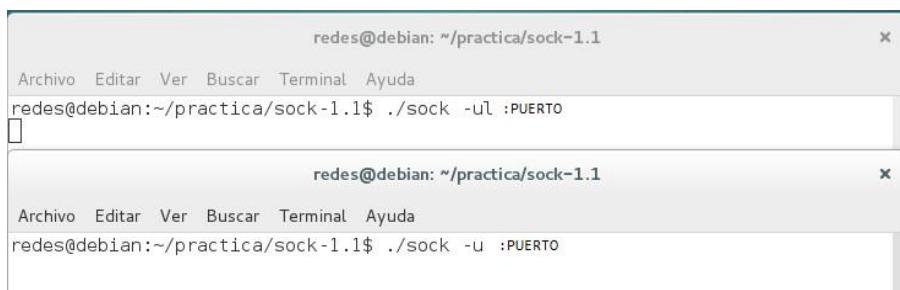
NOTA: PUERTO deberá sustituirse por un número que esté dentro del rango de puertos 1024-65535.

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

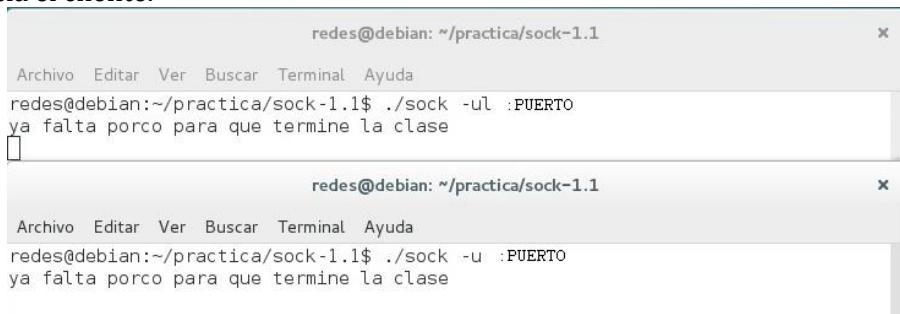
redes@debian:~/practica/sock-1.1\$./sock -u :PUERTO



```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -ul :PUERTO
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/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.



```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -ul :PUERTO
ya falta porco para que termine la clase
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -u :PUERTO
ya falta porco para que termine la clase
```

Figura No. 17. Comunicación entre terminales.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 119/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

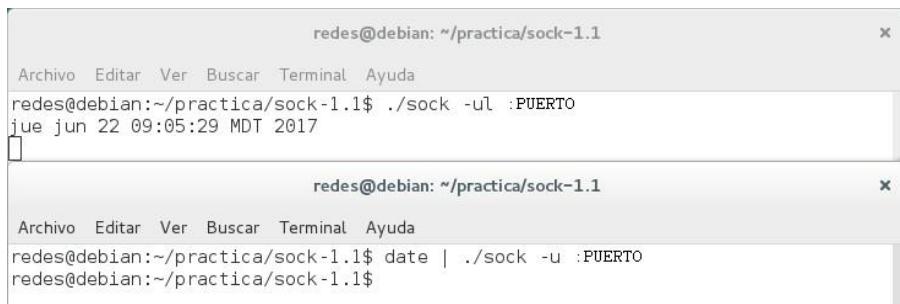
Comente lo que sucede

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@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -u :PUERTO
jue jun 22 09:05:29 MDT 2017
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ date | ./sock -u :PUERTO
redes@debian:~/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.

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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	120/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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'



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

4.5.3 Conéctese a la máquina que le indique su 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: 03 Página 121/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ssh -l redes 192.168.2.37
The authenticity of host '192.168.2.37 (192.168.2.37)' can't be established.
ECDSA key fingerprint is 60:a8:23:16:f6:72:63:ee:0c:69:78:83:fc:59:e9:84.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.37' (ECDSA) to the list of known hosts.
redes@192.168.2.37'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@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -e 192.168.2.35: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: 03 Página 122/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
-rw-r--r-- 1 redes redes 1134 jun 12 2001 ChangeLog
-rw-r--r-- 1 redes redes 1413 jun 22 08:32 config.cache
-rw-r--r-- 1 redes redes 460 jun 22 08:32 config.h
-rw-r--r-- 1 redes redes 386 jun 19 1998 config.h.in
-rw-r--r-- 1 redes redes 3638 jun 22 08:32 config.log
-rwxr--xr-x 1 redes redes 7916 jun 22 08:32 config.status
-rw xr--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 204632 jun 22 09:55 dibujo.jpg
-rwxr--xr-x 1 redes redes 4771 jun 19 1998 install-sh
-rw-r--r-- 1 redes redes 823 jun 22 08:32 Makefile
-rw-r--r-- 1 redes redes 714 jun 12 2001 Makefile.in
-rw-r--r-- 1 redes redes 826 jun 12 2001 README
-rwxr--xr-x 1 redes redes 37520 jun 22 08:33 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@debian:~/practica/sock-1.1$ 
```

```

redes@debian: ~/practica/sock-1.1
Terminal Ayuda
$ 1134 jun 12 2001 ChangeLog
$ 1413 jun 22 10:19 config.cache
$ 460 jun 22 10:19 config.h
$ 386 jun 19 1998 config.h.in
$ 3638 jun 22 10:19 config.log
$ 7916 jun 22 10:19 config.status
$ 50279 jun 12 2001 configure
$ 493 jun 12 2001 configure.in
$ 4096 jun 12 2001 debian
$ 204632 jun 22 10:55 imagen2.jpg
$ 4771 jun 19 1998 install-sh
$ 823 jun 22 10:19 Makefile
$ 714 jun 12 2001 Makefile.in
$ 826 jun 12 2001 README
$ 37520 jun 22 10:19 sock
$ 2876 jun 12 2001 sock.1
$ 9612 jun 12 2001 sock.c
$ 498 jun 12 2001 sock.lsm
redes@debian:~/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 sí 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
```

```

redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -ul :PUERTO>dibujo2.jpg

```

Figura No.23. Recepción del archivo

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

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	123/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ssh -l redes 192.168.2.37
redes@192.168.2.37'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.
Last login: Thu Jun 22 10:15:40 2017 from 192.168.2.35
redes@debian:~$
```

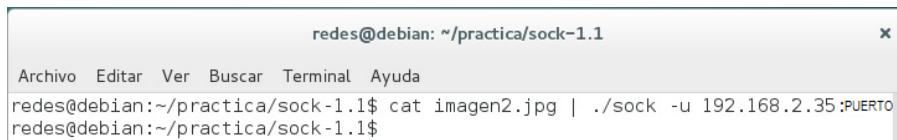
Figura No. 24. Conexión por medio de ssh

- 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@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ cat imagen2.jpg | ./sock -u 192.168.2.35:PUERTO
redes@debian:~/practica/sock-1.1$
```

Figura No.25. Envío del archivo

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 124/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

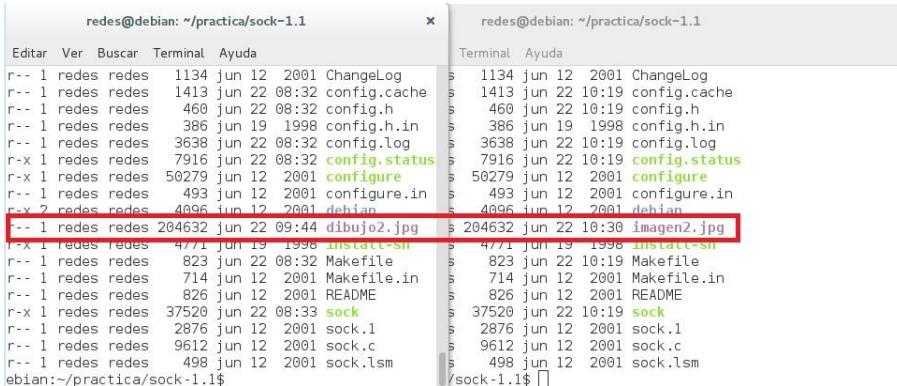
- 4.5.9** A continuación, finalice la orden del paso 4.5.8 pulsando <Ctrl>+<c> en el primer shell (asegúrese de que la ha seleccionado primero, haciendo clic con el ratón). (Ver figura No. 26).



```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~/practica/sock-1.1$ ./sock -ul :PUERTO>dibujo2.jpg
^C
redes@debian:~/practica/sock-1.1$
```

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@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
r-- 1 redes redes 1134 jun 12 2001 ChangeLog
r-- 1 redes redes 1413 jun 22 08:32 config.cache
r-- 1 redes redes 460 jun 22 08:32 config.h
r-- 1 redes redes 386 jun 19 1998 config.h.in
r-- 1 redes redes 3639 jun 22 08:32 config.log
r-x 1 redes redes 7916 jun 22 08:32 config.status
r-x 1 redes redes 50279 jun 12 2001 configure
r-- 1 redes redes 493 jun 12 2001 configure.in
r-- 2 redes redes 4096 jun 12 2001 debian
r-- 1 redes redes 204632 jun 22 09:44 dibujo2.jpg
r-- 1 redes redes 4771 jun 19 1998 install-sh
r-- 1 redes redes 823 jun 22 08:32 Makefile
r-- 1 redes redes 714 jun 12 2001 Makefile.in
r-- 1 redes redes 826 jun 12 2001 README
r--x 1 redes redes 37520 jun 22 08:33 sock
r-- 1 redes redes 2876 jun 12 2001 sock.1
r-- 1 redes redes 9612 jun 12 2001 sock.c
r-- 1 redes redes 498 jun 12 2001 sock.lsm
ebian:~/practica/sock-1.1$
```

```
redes@debian: ~/practica/sock-1.1
Terminal Ayuda
s 1134 jun 12 2001 ChangeLog
s 1413 jun 22 10:19 config.cache
s 460 jun 22 10:19 config.h
s 386 jun 19 1998 config.h.in
s 3638 jun 22 10:19 config.log
s 7916 jun 22 10:19 config.status
s 50279 jun 12 2001 configure
s 493 jun 12 2001 configure.in
s 4096 jun 12 2001 debian
s 204632 jun 22 10:30 imagen2.jpg
s 4771 jun 19 1998 install-sh
s 823 jun 22 10:19 Makefile
s 714 jun 12 2001 Makefile.in
s 826 jun 12 2001 README
s 37520 jun 22 10:19 sock
s 2876 jun 12 2001 sock.1
s 9612 jun 12 2001 sock.c
s 498 jun 12 2001 sock.lsm
/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).



```
redes@debian: ~/practica/sock-1.1
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ cd practica/sock-1.1/
redes@debian:~/practica/sock-1.1$ exit
logout
Connection to 192.168.2.37 closed.
redes@debian:~/practica/sock-1.1$
```

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	125/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.5.12 Cierre sesión.

5.-Cuestionario

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

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

3. Mencione algunos ejemplos de los usos de TCP y UDP

6.- Conclusiones.

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



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	126/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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. ¿Qué es un puerto?
9. ¿Cuáles son los rangos de puertos existentes?
10. ¿Qué rangos de puertos pueden utilizarse para establecer comunicaciones?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	127/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	128/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 al finalizar la práctica, conocerá la importancia de utilizar el protocolo SSH (Secure Shell) y su herramienta OpenSSH.
- El alumno iniciará una sesión remota a través de SSH, utilizando autenticación por contraseña.
- El alumno iniciará una sesión remota con clave pública, generando las claves.
- El alumno 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:	03
		Página	129/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	130/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 131/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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).

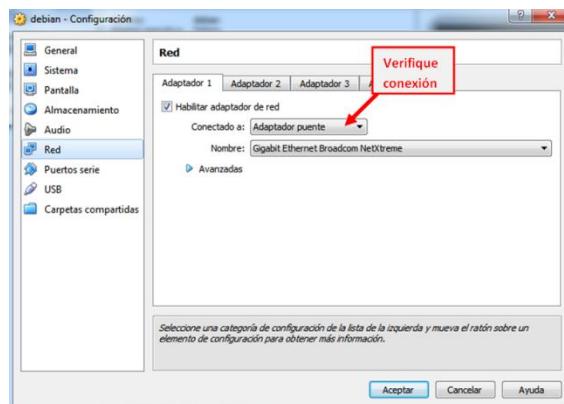


Figura No. 2. Conexión de red.

4.2.2 Encienda la máquina virtual

4.2.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 3), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 132/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

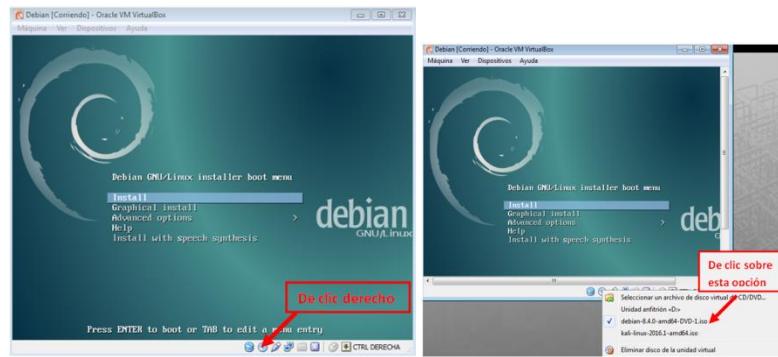


Figura No. 3. Inicio de Máquina Virtual.

- 4.2.4** Entre a sesión como usuario redes (cliente) o estudiante (servidor), según le indique su profesor. La cuenta y la contraseña serán proporcionadas por 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. 4)

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes#
```

Figura No. 4. Terminal de comandos como root.

- 4.2.6** Teclee la contraseña de root. (Ver Figura No. 5)

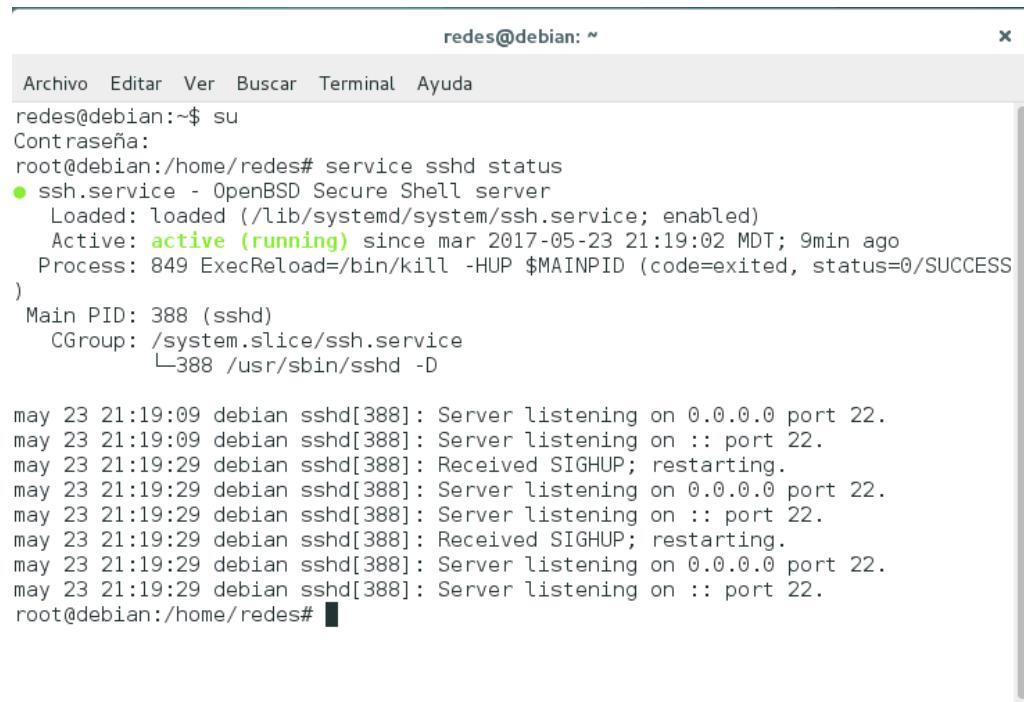
```
redes@Pooh: ~
Archivo Editar Ver Terminal Solapas Ayuda
redes@Pooh:~$ su
Contraseña:
Pooh:/home/redes#
```

Figura No. 5. Cambio de sesión con privilegios

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 133/298 8.3 11 de enero de 2019
Facultad de Ingeniería		Area/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.2.7** Verifique que la aplicación SSH se encuentre instalada (Active: active (running)) (Figura No. 6), para ello teclee:

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



```
redes@debian:~$ su
Contraseña:
root@debian:/home/redes# service sshd status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/sshd.service; enabled)
  Active: active (running) since mar 2017-05-23 21:19:02 MDT; 9min ago
    Process: 849 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
   Main PID: 388 (sshd)
     CGroup: /system.slice/sshd.service
             └─388 /usr/sbin/sshd -D

may 23 21:19:09 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:09 debian sshd[388]: Server listening on :: port 22.
may 23 21:19:29 debian sshd[388]: Received SIGHUP; restarting.
may 23 21:19:29 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:29 debian sshd[388]: Server listening on :: port 22.
may 23 21:19:29 debian sshd[388]: Received SIGHUP; restarting.
may 23 21:19:29 debian sshd[388]: Server listening on 0.0.0.0 port 22.
may 23 21:19:29 debian sshd[388]: Server listening on :: port 22.
root@debian:/home/redes#
```

Figura No. 6. Verificación de SSH

NOTA: En caso de que no se encuentre instalada, debe teclear el siguiente comando para instalarla (Figura No. 7)

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 134/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

redes@Pooh: ~
Archivo Editar Ver Terminal Solapas Ayuda
redes@Pooh:~$ su
Contrasenia:
Pooh:/home/redes# apt-get install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
ssh ya está en su versión más reciente.
0 actualizados, 0 se instalarán, 0 para eliminar y 3 no actualizados.
Pooh:/home/redes#

```

Figura No. 7. Descarga del paquete SSH

4.2.8 Visualice el archivo *sshd_config*. (Ver figura No. 8). Teclee lo siguiente:

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

```

redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# cat /etc/ssh/sshd_config

```

Figura No. 8. Archivo sshd_config

La salida del comando dará algo similar a lo siguiente (Ver figura No. 9). Comente la información obtenida en la pantalla.

```

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::

#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	135/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Figura No. 9 Archivo sshd.config

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. 10):

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

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



Figura No. 10 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. 11).



Figura No. 11 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:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	136/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

Lo que significa que se ha agregado la clave pública del servidor en `/home/redes/.ssh/known_hosts`. (Ver figura No. 12). Luego el cliente solicitará el ingreso de la contraseña:



```
redes@debian:~$ ssh estudiante@192.168.2.48
The authenticity of host '192.168.2.48 (192.168.2.48)' can't be established.
ECDSA key fingerprint is c1:48:55:3e:f1:71:fd:5c:24:34:e3:5e:16:da:1a:61.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.48' (ECDSA) to the list of known hosts.
estudiante@192.168.2.48's password: 
```

Figura No. 12 Acceso al equipo remoto

4.3.3 Teclee la contraseña de la cuenta estudiante, que será proporcionada por el profesor. Finalmente, si la contraseña ingresada es correcta, aparecerá algo similar a lo siguiente: (Ver figura No. 13).



```
redes@debian:~$ ssh estudiante@192.168.2.48
The authenticity of host '192.168.2.48 (192.168.2.48)' can't be established.
ECDSA key fingerprint is c1:48:55:3e:f1:71:fd:5c:24:34:e3:5e:16:da:1a:61.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.48' (ECDSA) to the list of known hosts.
estudiante@192.168.2.48's password:
Connection closed by 192.168.2.48
redes@debian:~$ ssh estudiante@192.168.2.48
estudiante@192.168.2.48'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.
estudiante@debian:~$ 
```

Figura No. 13 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. 14).

estudiante@debian:~\$ exit

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	137/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
estudiante@debian:~$ exit
logout
Connection to 192.168.2.48 closed.
redes@debian:~$ █
```

Figura No. 14 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.

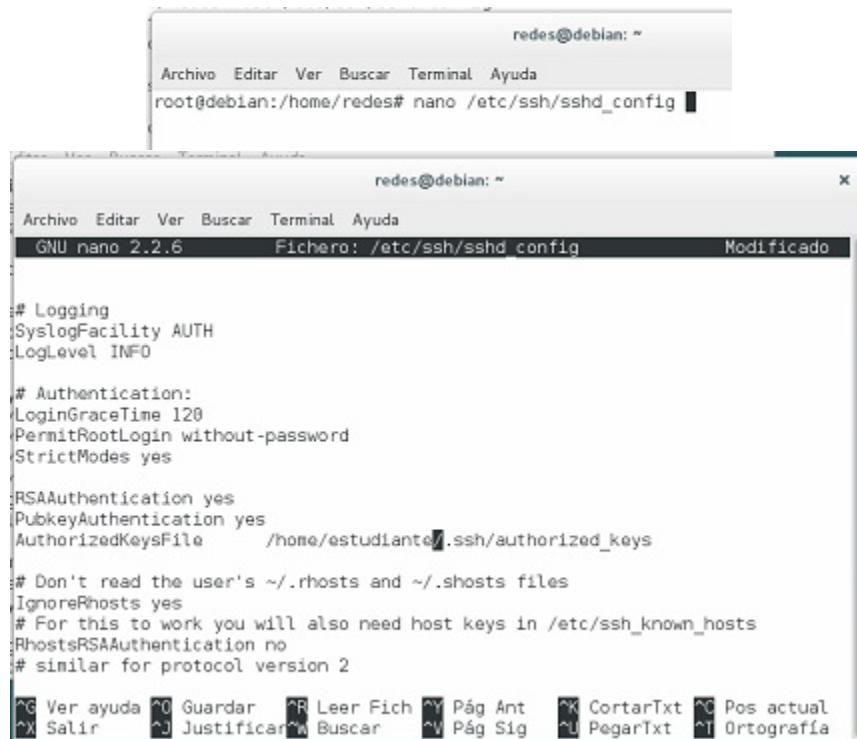
Para ello, edite el archivo `sshd_config` borrando el símbolo # de las siguientes líneas y verificando que estén escritas como se ve a continuación, si alguna falta inclúyala: (Ver Figura No. 15)

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

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	138/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	

La impresión de este documento es una copia no controlada



```

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes

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

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2

```

Figura No. 15 Archivo de configuración

Guarde los cambios (ctrl+o), salga del editor (ctrl+x) y reinicie el servicio (Ver Figura No. 16).

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



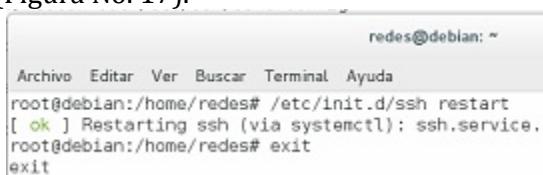
```

root@debian:/home/redes# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl); ssh.service.

```

Figura No. 16 Reiniciando el servicio de SSH

Cierre la sesión de root (Figura No. 17).



```

root@debian:/home/redes# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl); ssh.service.
root@debian:/home/redes# exit
exit

```

Figura No. 17. Cerrando sesión de root

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página Sección ISO Fecha de emisión	MADO-31 03 139/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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. 18).

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

```
| redes@debian:~$ ssh-keygen -t rsa
```

Figura No. 18 Comando para generar las claves

El programa responderá algo similar a lo siguiente: (Ver figura No. 19).

```
| redes@debian:~$ 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. 19 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. 20).

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

```
redes@debian:~$ 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. 20 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. 21).

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 140/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

redes@debian:~$ 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:
bf:2a:0f:7d:6a:35:b5:86:fe:8d:0b:2a:3b:59:7f:ae  redes@debian
The key's randomart image is:
+---[RSA 2048]---+
|          . |
|          . |
|          . |
|          . |
|          S o . |
|          ...+o |
|          -o,++o |
|          =..+oo.o |
|          .B=.E==.. |
+-----+
redes@debian:~$ 

```

Figura No. 21 Claves generadas satisfactoriamente

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. 22).

```
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



Figura No. 22 Trasferencia de la clave

4.5.2 Para añadir la clave pública al archivo *authorized_keys* realice lo siguiente en el servidor

- a) Realice lo siguiente en el servidor (sesión estudiante):

Teclee:
estudiante@debian:~\$su

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 141/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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

Ahora teclee (Figura No. 23)

```
root@debian:/home/estudiante# cat /home/estudiante/id_rsa.pub>
/home/estudiante/.ssh/authorized_keys
```

```
root@debian:/home/estudiante# cat /home/estudiante/id_rsa.pub >/home/estudiante/
.ssh/authorized_keys
```

Figura No. 23 Añadiendo la clave al archivo authorized_keys

b) Ahora diríjase al cliente (sesión redes) y agregue la clave (Figura No. 24)

```
root@debian:/home/redes# ssh-add /home/redes/.ssh/id_rsa
```



```
redes@debian:~$ ssh-add /home/redes/.ssh/id_rsa
Identity added: /home/redes/.ssh/id_rsa (rsa w/o comment)
```

Figura No. 24 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. 25).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 142/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

redes@debian:~$ ssh estudiante@192.168.2.48
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: Mon Jun 26 17:06:53 2017 from 192.168.2.34
estudiante@debian:~$ █

```

Figura No. 25 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. 26).

```

estudiante@debian:~$ exit
logout
Connection to 192.168.2.48 closed.
redes@debian:~$ █

```

Figura No. 26 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. 27).

*Enter new passphrase (empty for no passphrase):
Enter same passphrase again:*

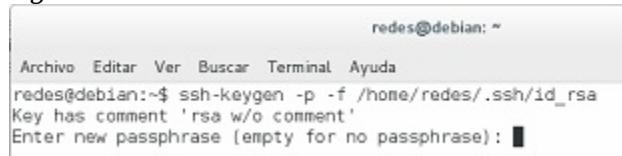


Figura No. 27 Asegurando la clave privada

- 4.7.2** Ingrese la frase clave, usted seleccione una y escriba esta misma en ambas ocasiones.

Frase clave empleada: _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 143/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.7.3 Finalmente informa: (Ver figura No. 28).

```
redes@debian:~$ ssh-keygen -p -f /home/redes/.ssh/id_rsa
Key has comment 'rsa w/o comment'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.
redes@debian:~$
```

Figura No. 28 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. 29).

redes@debian:~\$ eval ‘ssh-agent’

```
redes@debian:~$ eval 'ssh-agent'
SSH_AUTH_SOCK=/tmp/ssh-lgc0TB6koqog/agent.3066; export SSH_AUTH_SOCK;
SSH_AGENT_PID=3067; export SSH_AGENT_PID;
echo Agent pid 3067;
redes@debian:~$
```

Figura No. 29 Utilizando el ssh-agent

4.8.2 Agregue la clave privada de RSA. (Ver figura No. 30). Para ello use el comando *ssh-add*:

redes@debian:~\$ ssh-add /home/redes/.ssh/id_rsa

redes@debian:~\$ ssh-add /home/redes/.ssh/id_rsa

Figura No. 30 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. 31).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 144/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

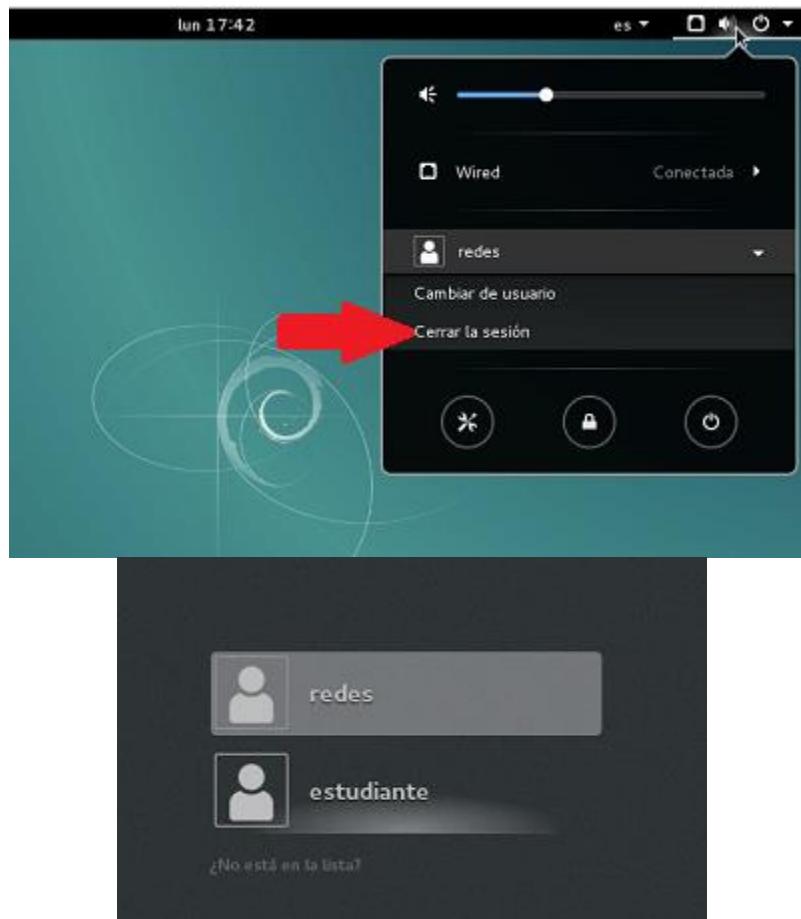


Figura No. 31 Cierre e inicio de sesión en redes

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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	145/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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
```

4.9.2 Desinstalación de ssh

En modo superusuario teclee lo siguiente:

```
root:/home/redes# apt-get autoremove -- purge ssh
```

4.9.3 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
```

4.9.4 Cierre la sesión.

4.9.5 Cuestionario

1. ¿Qué sucedería si escribiera mal la contraseña al querer hacer una conexión remota con ssh?



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	146/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

2. Investigue las características de los algoritmos de cifrado RSA y 3DES

- 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:	03
		Página	147/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31
		Versión:	03
		Página	148/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 149/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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 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 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

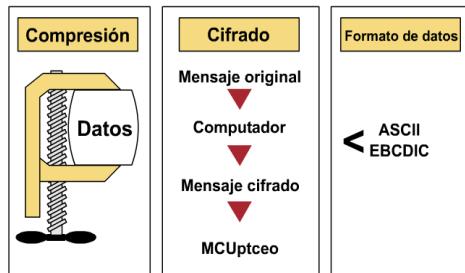


Figura No. 1. Funciones principales de la Capa 6.

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
- *JPEG* (Grupo conjunto de expertos fotográficos): Formato gráfico utilizado con frecuencia para comprimir imágenes fijas de ilustraciones o fotografías complejas

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	150/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:

- Paint
- Mozilla Firefox

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 151/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- AXCrypt

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 e Internet explorer (puede abrir Internet explorer usando Edge en caso de contar con esta aplicación).

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 ambos navegadores

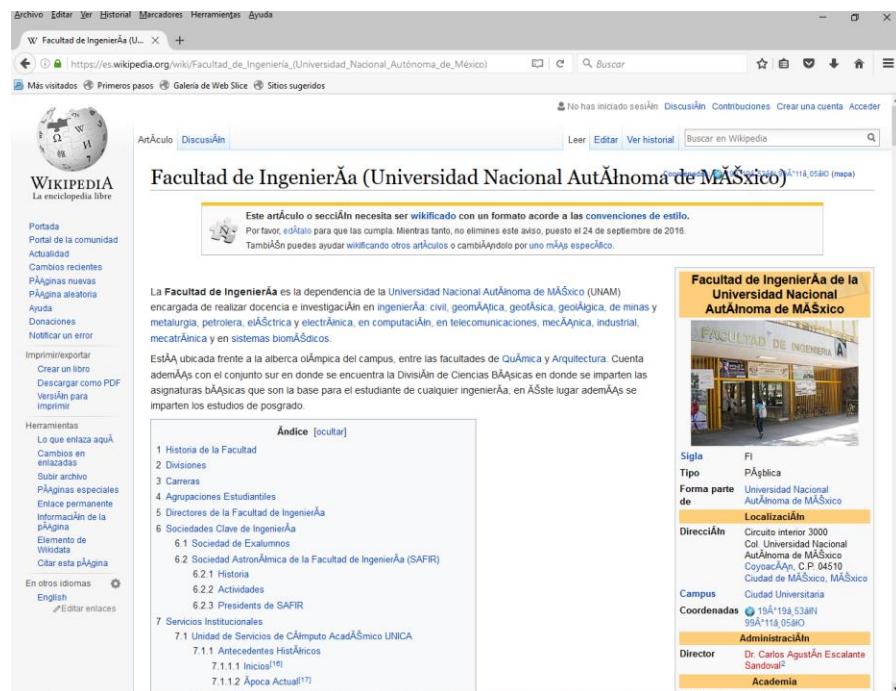


Figura No. 2. Página de Internet con codificación Unicode UTF-8.

4.2.3 En el menú Ver de Mozilla Firefox, elija la opción: Ver > Codificación de Texto> Centroeuopeo (ISO), y espere a que cargue nuevamente la página de Internet (ver Figura No. 3).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página: 152/298 Sección ISO: 8.3 Fecha de emisión: 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

NOTA: Si no observa la Barra de Menú, dé clic derecho en la parte superior del navegador para habilitar esa opción



Este artículo o sección necesita ser wikificado con un formato acorde a las convenciones de estilo. Por favor, editalo para que las cumpla. Mientras tanto, no elimines este aviso, puesto el 24 de septiembre de 2016. También puedes ayudar mejorando otros artículos o cambiándolo por uno más específico.

Facultad de Ingeniería (Universidad Nacional Autónoma de México)

Facultad de Ingeniería de la Universidad Nacional Autónoma de México

Sigla: FI
Tipo: Pájrica
Forma parte de: Universidad Nacional Autónoma de México
Localización: Circuito interior 3000 Col. Universidad Nacional Autónoma de México Coyoacán, C.P. 04510 Ciudad de México, México
Dirección: Circuito interior 3000 Col. Universidad Nacional Autónoma de México Coyoacán, C.P. 04510 Ciudad de México, México
Campus: Ciudad Universitaria
Coordenadas: 19°19'53" N 99°11'05" O
Administración: Dr. Carlos Agustín Escalante Sandoval²
Director: Dr. Carlos Agustín Escalante Sandoval²
Academia:

Figura No. 3. Página de Mozilla Firefox con codificación ISO (Centroeuropéo).

NOTA: El procedimiento para cambiar la codificación puede variar entre versiones de Mozilla Firefox.

4.2.4 En caso de que haga uso de Edge, para abrir Internet explorer debe dar clic sobre los tres puntos ubicados en la parte superior derecha y posteriormente seleccione la opción Abrir con Internet Explorer, haciendo uso de Internet Explorer elija la opción Ver > Codificación> Más> Centroeuropéo (ISO), y espere a que cargue nuevamente la página de Internet (ver Figura No. 3b)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página: 153/298 Sección ISO: 8.3 Fecha de emisión: 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

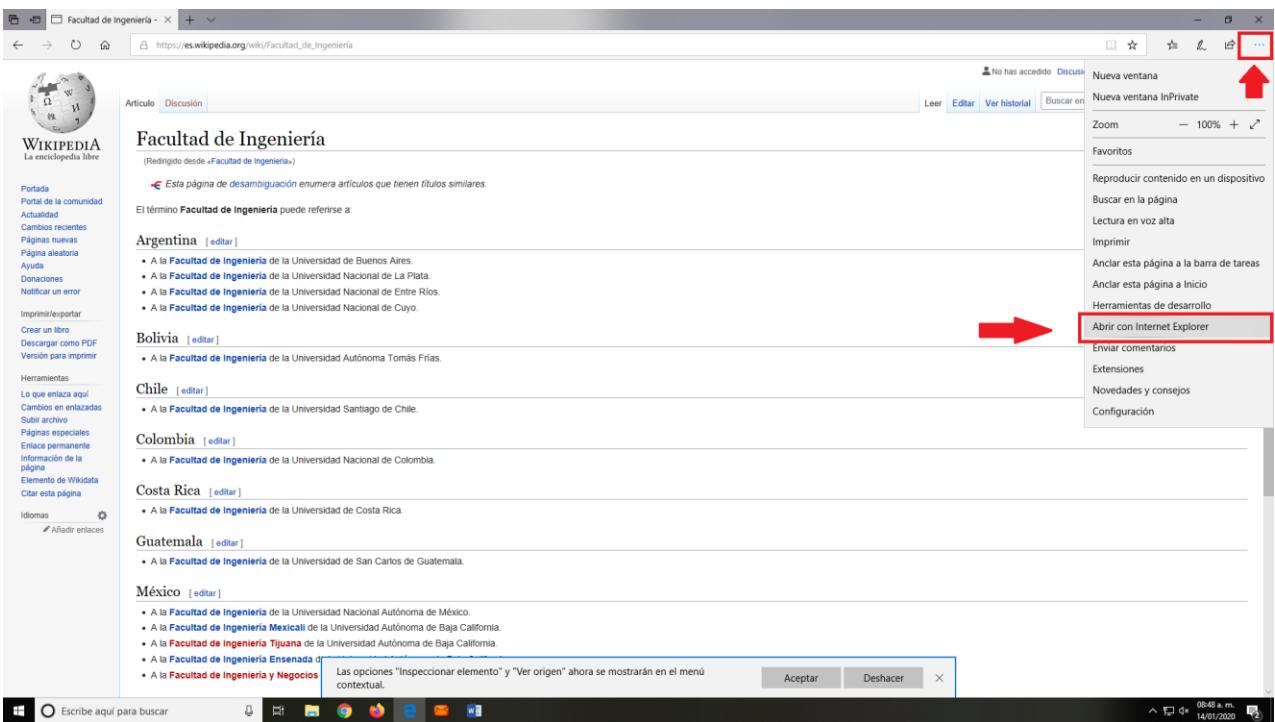


Figura No. 3b. Abrir Internet Explorer desde Edge

4.2.5 Observe la página detenidamente. ¿Fue posible realizar algún cambio en ambos navegadores?, de ser así describa los cambios que hubo entre la página con codificación Unicode e ISO. Si no fue posible cambiar la codificación explique por qué.

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

4.2.9 Del menú Ver de Mozilla Firefox, elija Código fuente de esta página

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 154/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.2.10 Observe el código fuente de la página de Internet. Y describa el funcionamiento de algunas etiquetas de HTML.

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. 4)

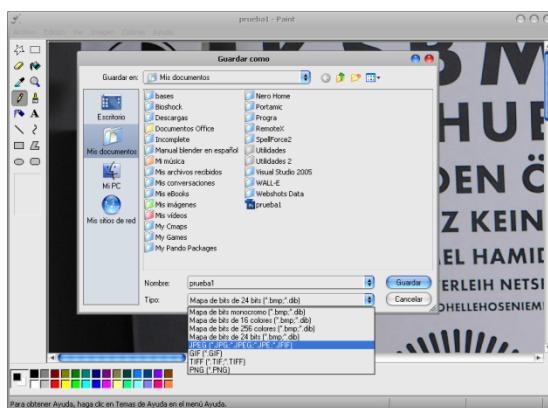


Figura No. 4. Guardando la imagen bmp a jpg.

4.3.3 Abra ambas imágenes en ventanas diferentes. Reajuste las ventanas para poder comparar las imágenes. (ver Figura No. 5)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 155/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

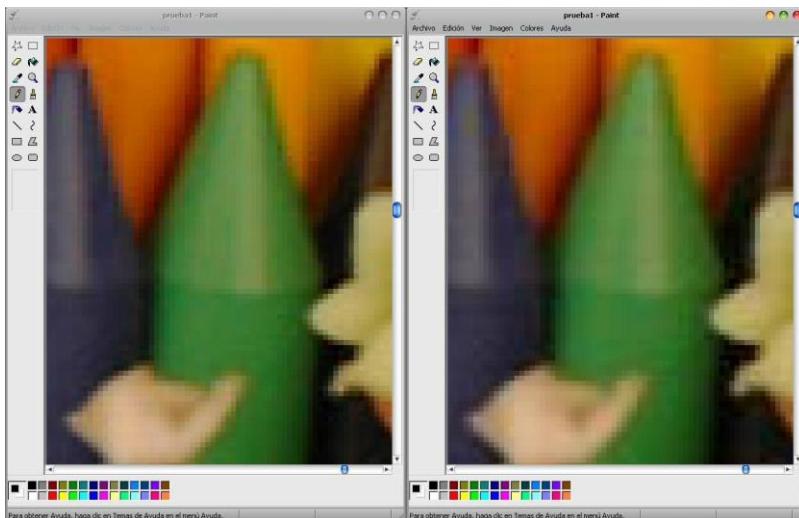


Figura No. 5. Imagen bmp e imagen jpg.

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).

4.3.7 Repita la actividad guardando esta vez la imagen en formato tiff.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 156/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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 click derecho sobre el archivo, y elija la opción *AxCrypt-> Cifrar*. (ver Figura No. 6)



Figura No. 6. Opción de cifrar archivo tras haber instalado AxCrypt.

- 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. 7)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 157/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 7. Ingreso de clave.

4.4.4 Ahora el archivo ha sido reemplazado por un archivo protegido de AxCrypt. 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).

4.4.6 Ahora dé click derecho sobre el archivo, y elija la opción *AxCrypt->Descifrar*. 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 AxCrypt.

4.4.7 Investigue qué tipo de cifrado emplea AxCrypt

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	158/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 el profesor

4.4.10 Cierre la sesión.

5.- Cuestionario

1. ¿Para qué sirve el programa AxCrypt?

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.

4. Menciona en qué situaciones se usaría compresión sin pérdida de datos.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	159/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

5. Investigue la relación entre las formas de codificación de texto que maneja Mozilla Firefox y el código ASCII.

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:	03
		Página	160/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31
		Versión:	03
		Página	161/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	162/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 habrá configurado un servidor DHCP bajo una plataforma Linux.
- El alumno configurará el servidor en sus tres modos de asignación de parámetros.
- El alumno analizará el funcionamiento del servidor y la comunicación con el cliente por medio del analizador de paquetes Wireshark.

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:

- Cables construidos en la práctica 1

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 163/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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).

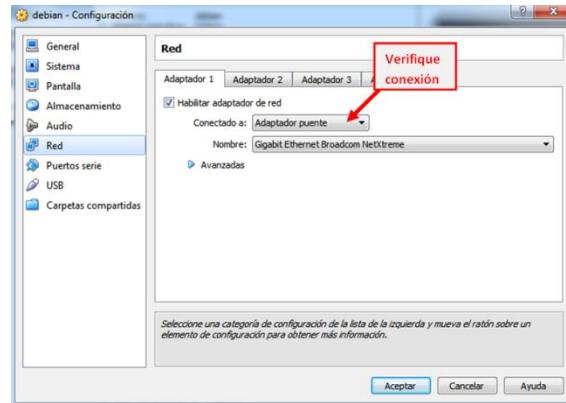


Figura No. 1. Conexión de red.

4.1.2 Encienda la máquina virtual

4.1.3 Elija la opción de cargar Linux, distribución Debian.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 164/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 2), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

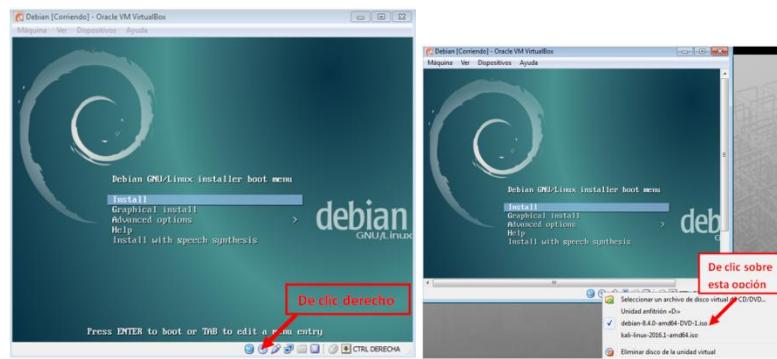


Figura No. 2. Inicio de Máquina Virtual.

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. 3)

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes#
```

Figura No 3. 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
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	165/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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. 4)

root@debian:/home/redes# apt-get install isc-dhcp-server

```

redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# apt-get install isc-dhcp-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  isc-dhcp-server-ldap
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-server
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 267 no actualizados.
Se necesita descargar 0 B/381 kB de archivos.
Se utilizarán 864 kB de espacio de disco adicional después de esta operación.
Preconfigurando paquetes ...
Seleccionando el paquete isc-dhcp-server previamente no seleccionado.
(Leyendo la base de datos ... 145066 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../isc-dhcp-server_4.3.1-6+deb8u2_amd64.deb ...
Desempaquetando isc-dhcp-server (4.3.1-6+deb8u2) ...
Procesando disparadores para systemd (215-17+deb8u4) ...
Procesando disparadores para man-db (2.7.0.2-5) ...
Configurando isc-dhcp-server (4.3.1-6+deb8u2) ...
Job for isc-dhcp-server.service failed. See 'systemctl status isc-dhcp-server.service' and 'journalctl -xn' for details.
invoke-rc.d: initscript isc-dhcp-server, action "start" failed.
root@debian:/home/redes#

```

Figura No. 4. Instalación del servidor DHCP

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:	03
		Página	166/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.

4.3.3 Configure la tarjeta de red del servidor con los siguientes datos (no emplee la forma gráfica sino vía comandos):

Dirección IP: 192.168.1.8
Máscara de red: 255.255.255.0
Red: 192.168.1.0
Broadcast: 192.168.1.255

4.3.4 Reinicie los servicios de la tarjeta de red, ingrese el siguiente comando (Figura No. 5)

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
root@debian:/home/redes#
```

Figura No. 5. Reinicio del servicio

4.3.5 Verifique que pertenezca al mismo segmento de red (Ver la Figura No. 6), ingrese el comando siguiente:

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

```
root@debian:/home/redes# ifconfig
eth0      Link encap:Ethernet Hwaddr 00:0c:29:8:c8:cb
          inet addr:192.168.1.8  Bcast 192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a0c:29ff:fe8:c8%eth0  Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
                  RX packets:1348 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:561 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:200589 (195.8 KiB)  TX bytes:88838 (86.7 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:16436 Metric:1
                  RX packets:12 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:796 (796.0 B)  TX bytes:796 (796.0 B)
```

Figura No. 6 Verificación de la dirección IP.

4.3.6 Cambie el nombre del archivo de configuración original del servidor. Teclee lo siguiente (Figura No. 7):

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 167/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

root@debian:/home/redes# mv /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. 7 Cambio de nombre del archivo de configuración

4.3.7 Cree un nuevo archivo de configuración, para ello teclee lo siguiente:

root@debian:/home/redes# nano /etc/dhcp/dhcpd.conf

4.3.8 Escriba las siguientes líneas dentro del archivo de configuración (ver Figura No. 8)

```
#Archivo de configuración del servidor DHCP
#####
# Subred #####
subnet 192.168.1.0 netmask 255.255.255.0 {
}
```



```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Fichero: /etc/dhcp/dhcpd.conf Modificado
#####
# Archivo de configuracion del servidor DHCP
#####

subnet 192.168.1.0 netmask 255.255.255.0 {
```

Figura No. 8. Configuración inicial

Explique el significado de las líneas agregadas anteriormente

4.3.9 Guarde y salga del editor

4.3.10 Inicie el servicio DHCP. Teclee lo siguiente

root@debian:/home/redes# /etc/init.d/isc-dhcp-server start

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	168/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 Escriba lo siguiente en el lugar adecuado y coloque la dirección MAC del cliente en la línea correspondiente (ver Figura No. 9)

```
option routers 192.168.1.8;
option domain-name-servers 132.248.204.1, 132.248.10.2;
#####
#####Asignación Manual#####
host Equipo1 {
    hardware ethernet MAC_del_cliente;
    fixed-address 192.168.1.101;
}
```

```
Archivo de configuracion del servidor DHCP
#####
#####Subred#####

subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers 192.168.1.8;
    option domain-name-servers 132.248.204.1, 132.248.10.2;
}

#####
#Asignacion Manual#####

host Equipo1 {
    hardware ethernet 00:16:D3:A3:98:7C;
    fixed-address 192.168.1.100;
}
```

Figura No. 9 Asignación Manual



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	169/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Explique el significado de las líneas agregadas anteriormente

4.4.4 Guarde y salga del editor

4.4.5 Reinicie el servicio

```
root@debian:/home/redes# /etc/init.d/isc-dhcp-server restart
```

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. 10)

```
Aaptador de Ethernet Conexión de área local:  
  Sufijo DNS específico para la conexión . . . . . : Intel(R) PRO/100 Ue Network Connection  
  Descripción . . . . . : Intel(R) PRO/100 Ue Network Connection  
  Dirección física . . . . . : 00-16-B3-A3-98-7C  
  DHCP habilitado . . . . . : sí  
  Configuración automática habilitada . . . . . : sí  
  Vínculo: dirección IPv6 local . . . . . : fe80::24b8:8635%7da3:c475x12<Preferido>  
  
  Dirección IPv4 . . . . . : 192.168.1.100<Preferido>  
  Máscara de subred . . . . . : 255.255.255.0  
  Concesión obtenida . . . . . : jueves, 01 de julio de 2010 11:11:14 a.m.  
  La concesión expira . . . . . : jueves, 01 de julio de 2010 11:11:14 p.m.  
  Puerta de enlace predeterminada . . . . . : 192.168.1.8  
  Servidor DHCP . . . . . : 192.168.1.8  
  IAID DHCPv6 . . . . . : 285218515  
  DUID de cliente DHCPv6 . . . . . : 00-01-00-01-13-B7-D4-A9-00-16-B3-98-7C  
  Servidores DNS . . . . . : 132.248.204.1  
  NetBIOS sobre TCP/IP . . . . . : 132.248.10.2  
  . . . . . : habilitado
```

Figura No. 10. Configuración en la computadora cliente.

4.4.8 Escriba a continuación lo obtenido en el paso anterior

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	170/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			



Analice y comente al respecto

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** Edite el archivo de configuración. (Paso 4.3.2.2) Borre las líneas adecuadas y agregue las siguientes en el lugar adecuado: (Ver Figura No. 11)

```
#####Asignación Automática#####
range 192.168.1.110 192.168.1.120;
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	171/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	

La impresión de este documento es una copia no controlada

```
# Archivo de configuracion del servidor DHCP
#####
#Subred#####
subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers 192.168.1.8;
    option domain-name-servers 132.248.204.1, 132.248.10.2;
#####
#Asignacion Automatica#####
    range 192.168.1.110 192.168.1.120;
}
```

Figura No. 11. Asignación Automática.

4.5.3 Guarde y salga del editor

4.5.4 Repita los pasos del 4.4.5 al 4.4.7

4.5.5 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. Coloque las siguientes líneas en el lugar adecuado: (Ver Figura No. 12)

```
#####
# Asignación Dinámica #####
range 192.168.1.111 192.168.1.120;
default-lease-time 120;
max-lease-time 122;
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 172/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

```

#Archivo de configuracion del servidor DHCP
#####
##Subred#####
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.8;
option domain-name-servers 132.248.204.1, 132.248.10.2;
#####
##Asignación Dinámica#####
range 192.168.1.111 192.168.1.120;
default-lease-time 120;
max-lease-time 122;
}

```

Figura No. 12. Asignación Dinámica

Analice las líneas agregadas anteriormente y explique su significado:

4.6.3 Guarde y salga del editor.

4.6.4 Repita los pasos del 4.4.5 al 4.4.7

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 173/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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 only** (ver Figura No. 13) **No inicie la captura**

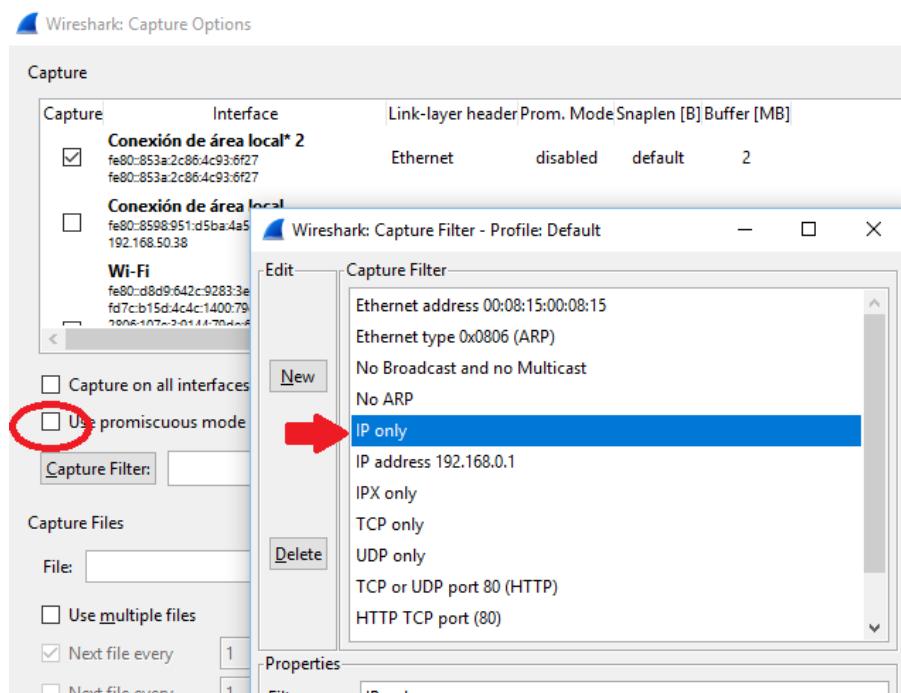


Figura No. 13. Configuración de la captura

¡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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 174/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 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. 14)

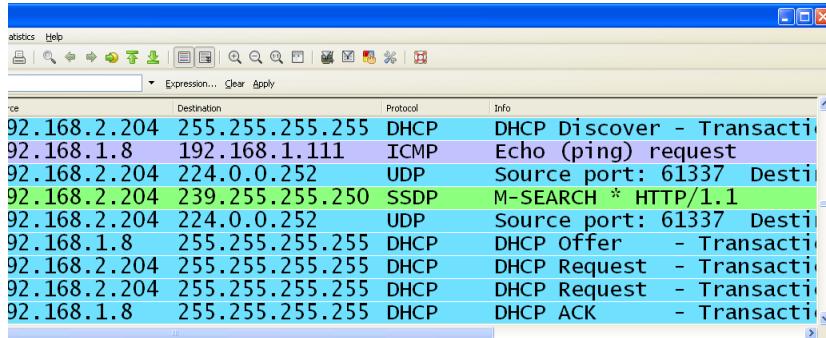


Figura No. 14. Captura de paquetes.

- 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. 15)

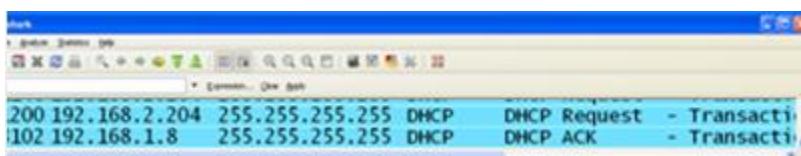


Figura No. 15. Paquetes de actualización de concesión.

- 4.7.11** Analice lo obtenido en el paso anterior observando los detalles de los paquetes capturados. Comente al respecto.
-

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	175/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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-sever
```

4.7.14 Si 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)



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	176/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

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:	03
		Página	177/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31
		Versión:	03
		Página	178/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento:	Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada			

Manual de prácticas optativas del laboratorio 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	M.C. Alejandro Velázquez Mena	11 de enero de 2019

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	179/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Índice de prácticas optativas

Práctica Optativa 1. Normatividad	180
Práctica Optativa 2. Cableado estructurado	191
Práctica Optativa 3. Compartición de archivos por Hub y Switch en Linux	200
Práctica Optativa 4. Políticas de seguridad en las interfaces del switch	221
Práctica Optativa 5. Enrutamiento estático	237
Práctica Optativa 6. Firewall básico	255
Práctica Optativa 7. Configuración básica de una comunicación de Voz IP	273

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	180/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 1

Normatividad

Estándares y Arquitecturas

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	181/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 investigará organismos de estandarización.
- El alumno 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:	MADO-31
		Versión:	03
		Página	182/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	183/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 03 184/298 8.3 11 de enero de 2019
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:	03
		Página	185/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	186/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	187/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
Página	188/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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:	03
		Página	189/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	MADO-31
		Versión:	03
		Página	190/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	191/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 2

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 03 192/298 8.3 11 de enero de 2019
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 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.

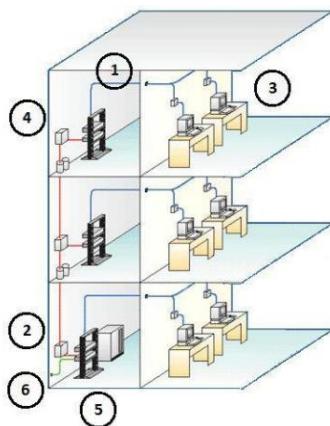


Figura No.1. Subsistemas del cableado estructurado.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: Versión: Página: Sección ISO Fecha de emisión	MADO-31 03 193/298 8.3 11 de enero de 2019
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):

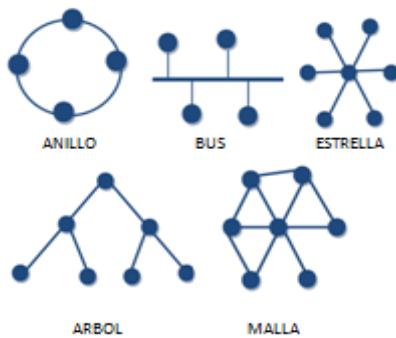


Figura No.2. Topologías de red.

- 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:

- Planos del proyecto indicados por 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:	03
		Página	194/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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 el profesor.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	195/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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 el profesor.

EJERCICIOS OPCIONALES

4.2 Costo de la propuesta del cableado estructurado.

- 4.2.1** 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.

4.2.2 Indique qué consideraciones de seguridad debe tomar en cuenta para su propuesta y por qué.

- 4.2.3** Exponga ante el grupo su propuesta y justifíquela.

4.2.4 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:	03
Página	196/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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:	03
Página	197/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

5.- Cuestionario

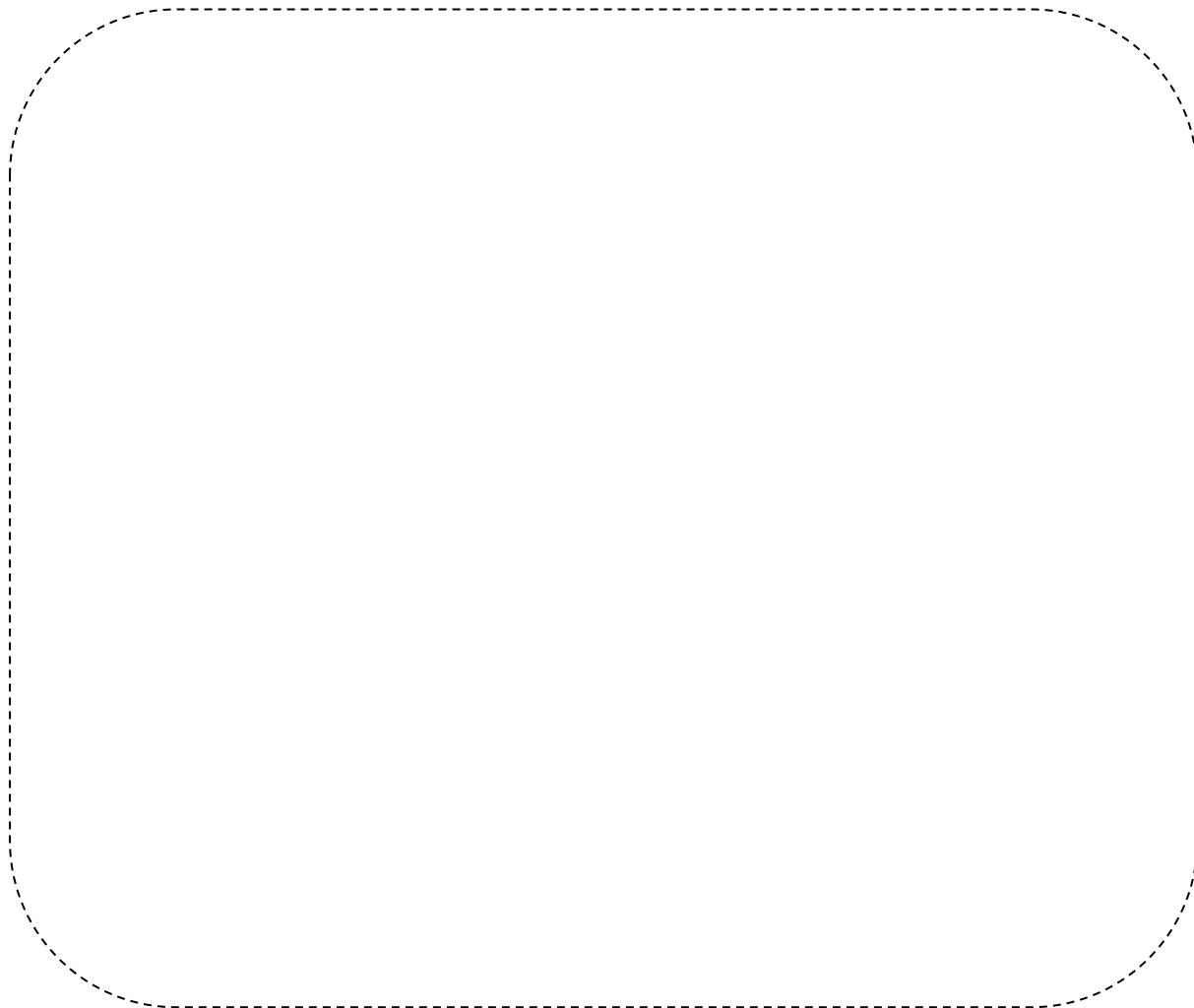
1. ¿Qué consideró para la creación de su propuesta? Argumente su respuesta.

2. ¿Cuáles son las ventajas y desventajas de la topología utilizada en la pregunta anterior?

6.- Conclusiones

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	198/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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:	03
		Página	199/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 2

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:	MADO-31
		Versión:	03
		Página	200/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 3

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:	03
		Página	201/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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:	03
		Página	202/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 203/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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 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).

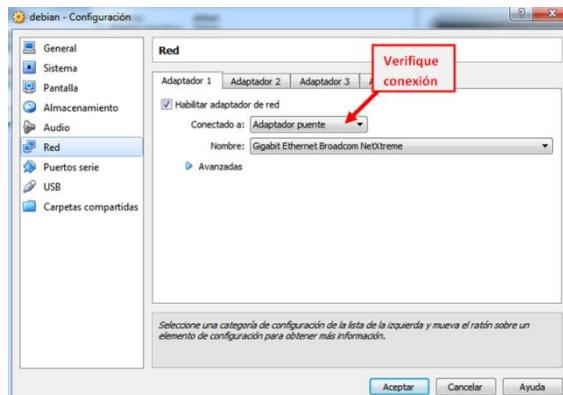


Figura No. 1. Conexión de red.

- 4.1.5 Encienda la máquina virtual
- 4.1.6 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No.2), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 204/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

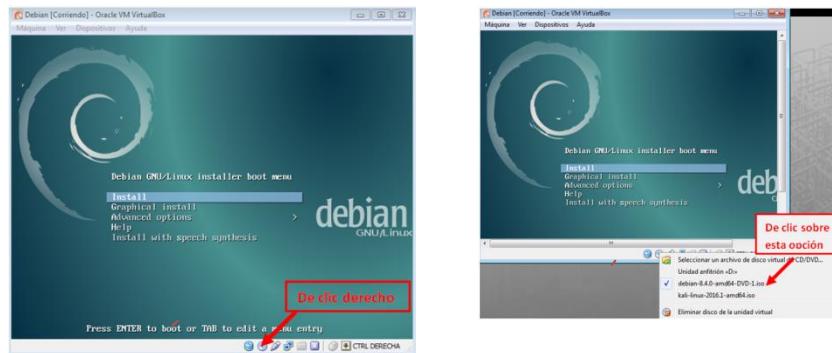


Figura No. 2. Inicio de Máquina Virtual.

- 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. 3)

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes#
```

Figura No. 3. 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

Añote la dirección IP de su máquina _____

4.2 Configuración del servidor y del cliente

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	205/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.1 Designe una máquina como servidor.

Desde el paso 4.2.1.1 hasta el paso 4.2.1.10 se realizarán en el dispositivo designado como servidor

4.2.1.1 Instale samba tecleando el siguiente comando (Figura No. 4):

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes# apt-get install samba
```

Figura No. 4. Instalación de samba

4.2.1.2 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.

4.2.1.3 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.

4.2.1.4 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. 5):

```
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. 5. Creación de contraseña en Linux.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	206/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Anote la contraseña que utilizó _____

4.2.1.5 Indique para qué se usa el comando **smbpasswd** en este caso.



4.2.1.6 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 acceder al archivo de configuración con el siguiente comando (Ver Figura No. 6a) y escribir al final del archivo las siguientes líneas (Ver Figura No. 6b):

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. 6a. Acceso al archivo

```
[nombre_carpeta]
path = /home/redes/
writeable = yes
shares = yes
guest ok = yes
```

Figura No. 6b. Permisos carpeta compartida

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	207/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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



4.2.1.7 Reinicie el servicio de samba con el siguiente comando (Figura No. 7):

```
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. 7. Reinicio del servicio

4.2.1.8 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
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	208/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

4.2.1.9 Para acceder a la carpeta compartida debe emplear la dirección IP que ya había anotado.

4.2.1.10 Abra un navegador web en Linux y teclee la dirección IP de su máquina, se trata de la máquina donde se encuentra la carpeta que acaba de compartir. Para ello escriba en el navegador web lo siguiente (Figura No. 8):

smb://192.168.2.X

NOTA: La X se sustituirá por la dirección de su máquina



Figura No. 8. Acceso a la carpeta compartida

4.2.2 Designe una máquina como cliente.

Desde el paso 4.2.2.1 hasta el paso 4.2.2.5 se realizarán en el dispositivo designado como cliente.

4.2.2.1 Instale samba cliente tecleando lo siguiente (Figura No. 9):

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	209/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# apt-get install smbclient
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Figura No. 9. 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. 10)

root@debian:/home/redes# apt-get update

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# apt-get update
Ign http://httpredir.debian.org jessie InRelease
Obj http://httpredir.debian.org jessie Release.gpg
```

Figura No. 10. 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.

root@debian:/home/redes# ping 192.168.2.X

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# ping 192.168.2.x
```

Figura No. 11. 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.12)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	210/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

root@debian:/home/redes# smbclient --list 192.168.2.X

```
root@debian:/home/redes# smbclient --list 192.168.2.X
Enter root's password:
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.2.14-Debian]

      Sharename      Type      Comment
      -----      ----      -----
      print$        Disk      Printer Drivers
      practica3     Disk
      IPC$          IPC       IPC Service (Samba 4.2.14-Debian)
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.2.14-Debian]

      Server          Comment
      -----          -----
      DEBIAN          Samba 4.2.14-Debian

      Workgroup      Master
      -----          -----
      LABREDES        HUITZILOPOCHTLI
      WORKGROUP       DEBIAN
```

Figura No. 12. Solicitud de listado de carpetas compartidas

NOTA: Recuerde que la X debe sustituirse por la dirección de la máquina servidor.

En esta sección se le solicitará la contraseña que generó la máquina designada como servidor en el punto 4.2.1.4.

4.2.2.5 Abra un navegador web en Linux y teclee la dirección IP de la máquina designada como servidor, se trata de la máquina donde se encuentra la carpeta que se está compartiendo. Para ello escriba en el navegador web (Figura No. 13):

smb://192.168.2.X

NOTA: La X se sustituirá por la dirección de la máquina designada como servidor

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 211/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 13. Acceso a la carpeta compartida

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. 14):

\\192.168.2.X

NOTA: La X debe sustituirse por la dirección IP de la máquina designada como servidor.

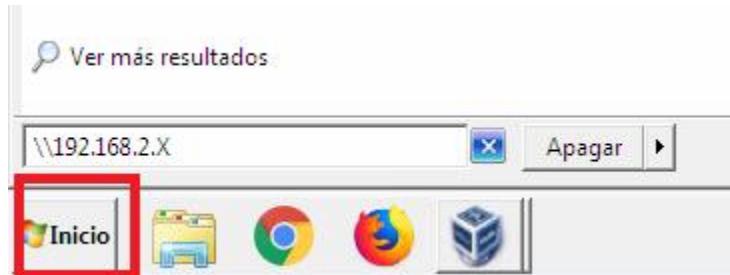


Figura No. 14. Acceso a la máquina designada como servidor

- 4.3.2** Cuando acceda a la máquina designada como servidor se mostrará la carpeta compartida (Figura 15), puede navegar dentro de ella para observar los documentos compartidos

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 212/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

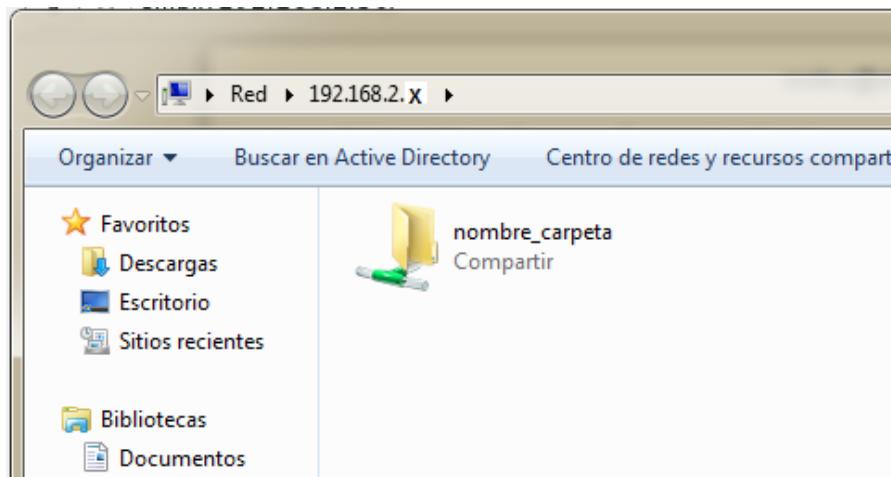


Figura No. 15. Acceso a la carpeta compartida en Windows

4.3.3 Mencione si tuvo algún problema para lograr acceder a la carpeta, de ser así ¿cuál fue su solución?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	213/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3.4 Mencione ¿Qué pasaría si no se solicita contraseña para ingresar?



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:	MADO-31
		Versión:	03
		Página	214/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.



- 4.3.7** ¿Por qué se puede realizar la compartición entre dos sistemas operativos?



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 215/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

EJERCICIO OPCIONAL

Con este ejercicio el alumno visualizará la colisión de los dispositivos en forma simulada por medio del software Cisco Packet Tracer Student en su versión más reciente.

4.4 Construcción de la topología.

- 4.4.1** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 16).

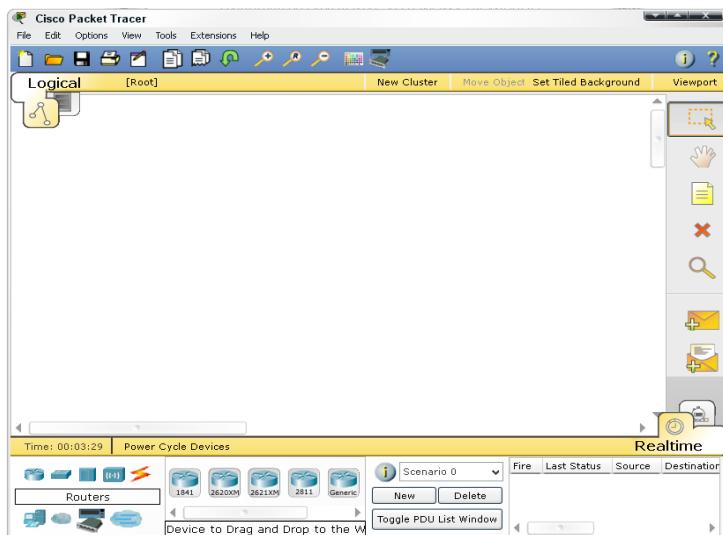


Figura No. 16. Interfaz gráfica de PT

- 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. 17.)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 216/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		



Figura No. 17. 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 profesor realice la topología de red que se observa en la Figura No. 18 agregando al área de trabajo de Packet Tracer los dispositivos siguientes: 1 Switch 2950-24, 6 PC-PT y un Hub -PT.



Figura No. 18. 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.

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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 217/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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. 19). Ingrese los datos designados por su profesor.

4.5.4 Repita los pasos 4.4.1, 4.4.2 y 4.4.3 para las cinco PC restantes.

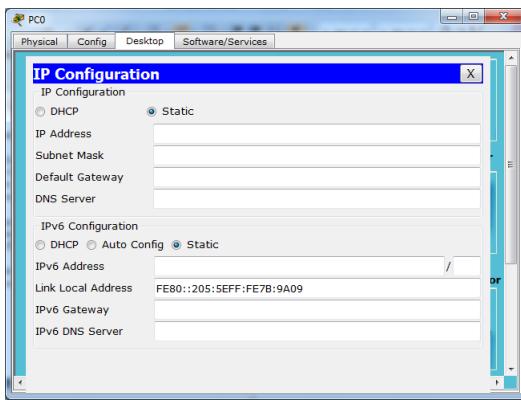


Figura No. 19. Configuración de la PC.

4.5.5 Una vez configurados los equipos de cómputo verifique que exista comunicación. Seleccione una PDU como se observa en la Figura No. 20 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.

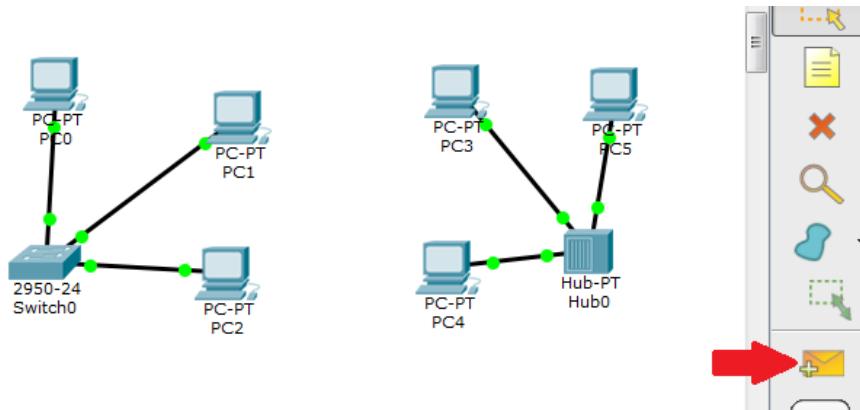


Figura No. 20. Pruebas.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	218/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.5.7 ¿Se logró establecer la comunicación? Explique.

4.5.8 ¿Qué pasaría si no se asignan direcciones IP a las máquinas?

5.- Cuestionario

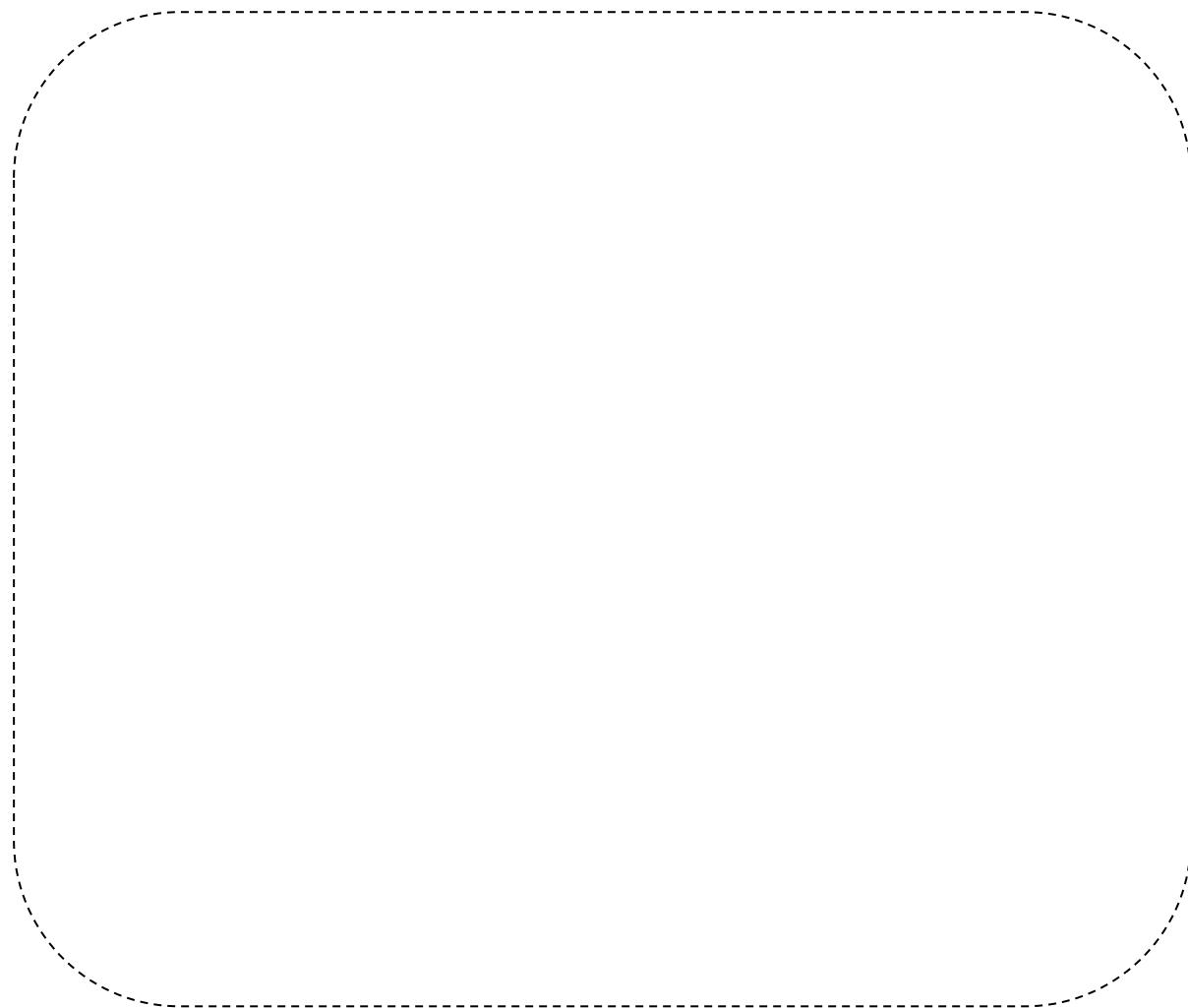
1. ¿Cuál es la diferencia de descarga al compartir archivos entre ambos dispositivos?
Argumente su respuesta

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:	03
		Página	219/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	220/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 3
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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	221/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 4

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:	03
		Página	222/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 implementará mecanismos adecuados de seguridad en los puertos del switch.
- El alumno 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 Student.

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.

4.1 Construcción de la topología

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 223/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.5.13** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 1)

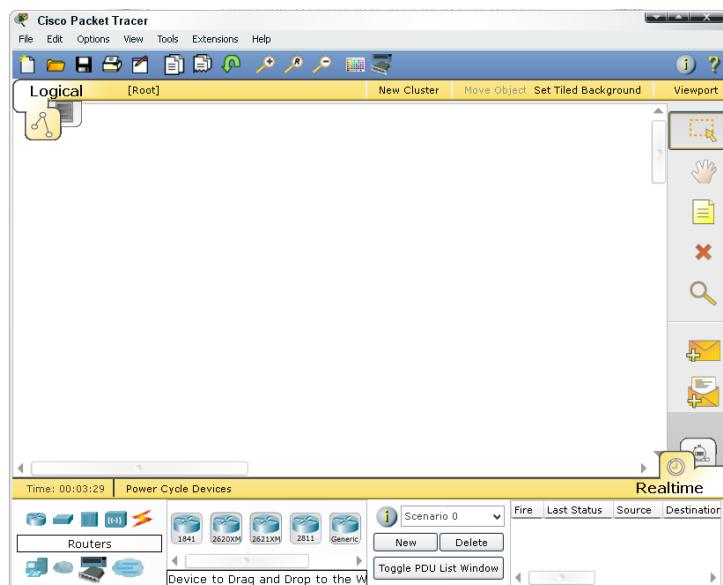


Figura No. 1. Interfaz gráfica de PT

- 4.5.14** 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.

- 4.5.15** 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: MADO-31 Versión: 03 Página 224/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

- 4.5.16** 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.
- 4.5.17** 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.
- 4.5.18** Con ayuda de su 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.).

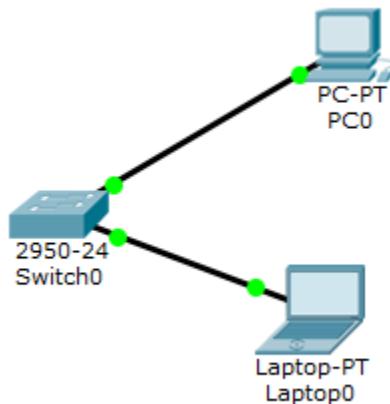


Figura No. 3. Topología básica

- 4.5.19** 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 el profesor.
- 4.5.19.1** Dé clic sobre la PC0 conectada al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.5.19.2** Seleccione la pestaña Desktop y seleccione IP Configuration.
- 4.5.19.3** 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 profesor.
- 4.5.19.4** 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: 03 Página 225/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

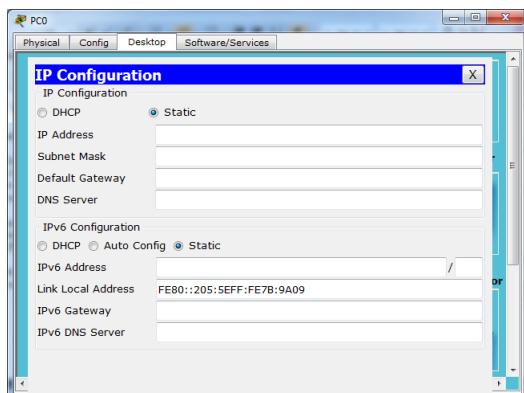


Figura No. 4. Configuración de la PC.

4.5.20 Tomando como base la topología construida se explicarán 2 técnicas para restringir el uso de puertos del switch a dispositivos no autorizados:

- a) Deshabilitar los puertos (interfaces) que no se utilicen.
- b) Implementar políticas de acceso a puertos con port security.

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.

4.6.1 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#

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 226/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.6.2 Explique qué sucede en la ventana CLI cuando se ejecuta el comando shutdown.



4.6.3 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).

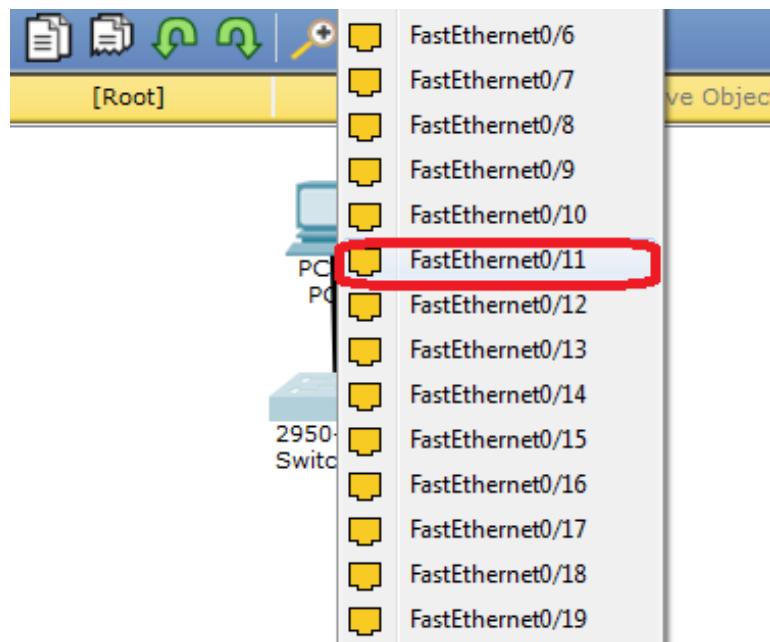


Figura No. 5. Añadiendo y conectando la nueva PC en el puerto 11

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	227/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	

La impresión de este documento es una copia no controlada

- 4.6.4** ¿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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	228/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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.
 - 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.
- 4.7.1** 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.
- 4.7.2** 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).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 229/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

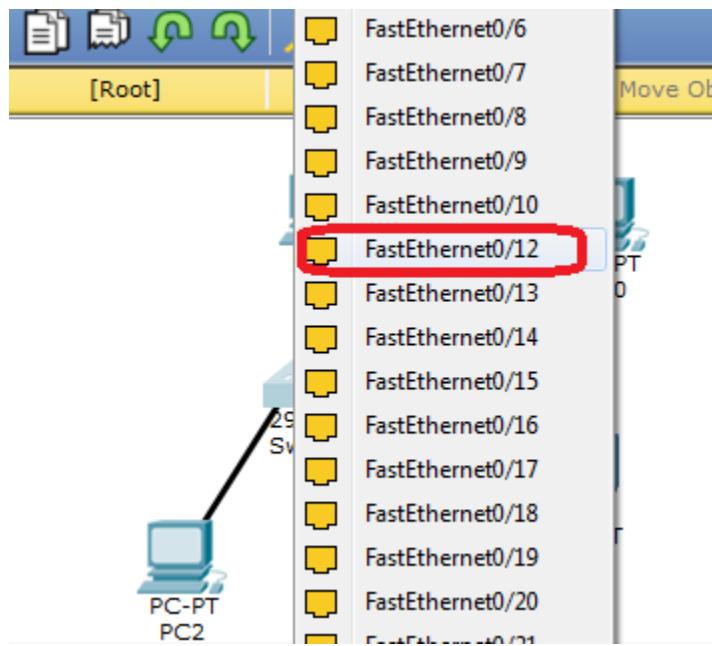


Figura No. 6. Añadiendo y conectando la nueva PC en el puerto 12

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)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 230/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

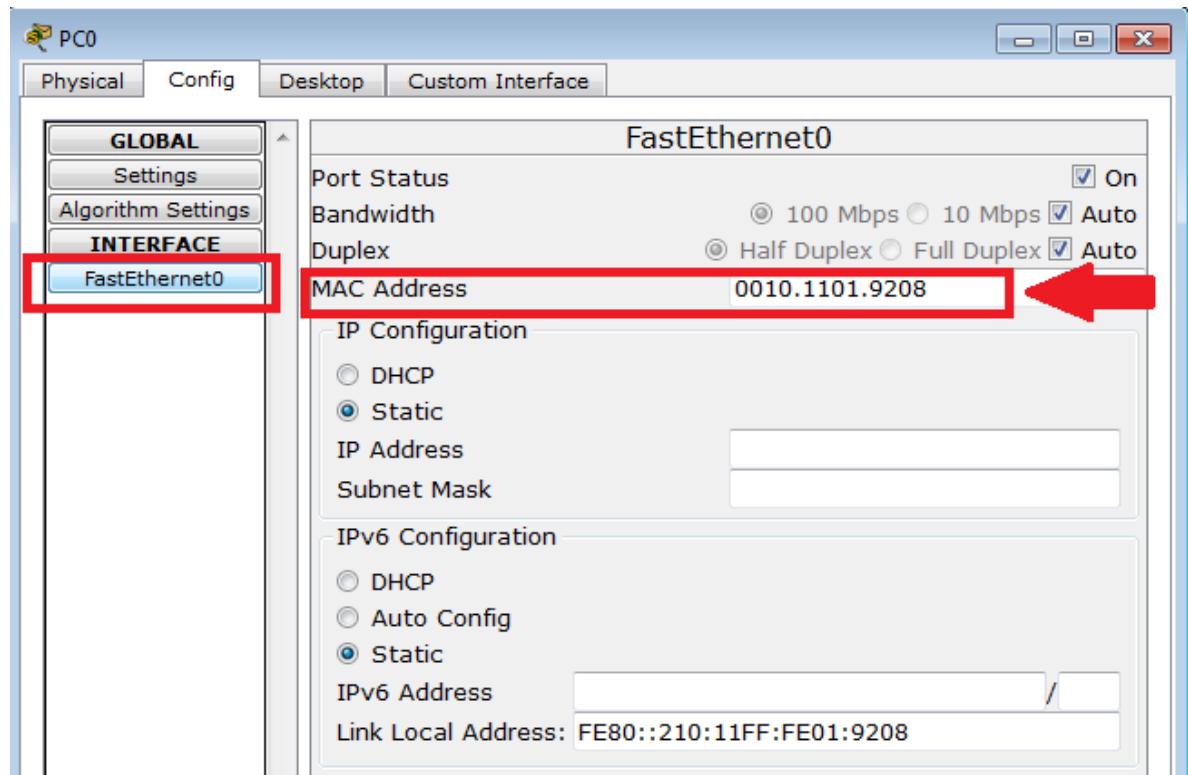


Figura No. 7. Obtener Dirección MAC

```

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

```

- 4.7.3** 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: 03 Página 231/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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.

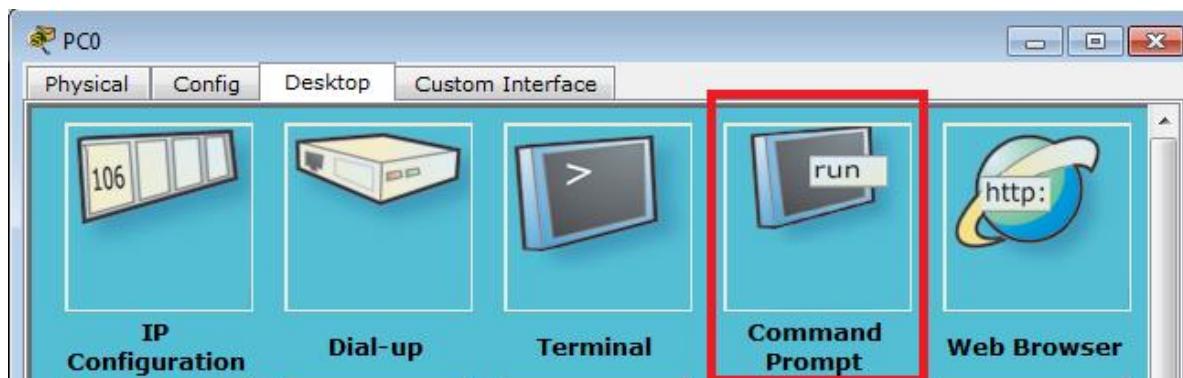


Figura No. 8. Command Prompt

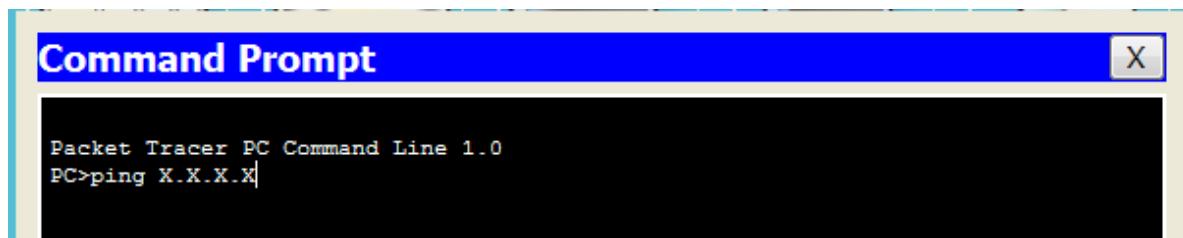


Figura No. 9. Ping

- 4.7.4** 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

```

- 4.7.5** Valide que la nueva PC tiene comunicación con las demás enviando mensajes Ping o con paquetes PDU simples.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	232/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 4.7.6** Indique para qué sirve la opción sticky en este caso.



- 4.7.7** 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: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 233/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

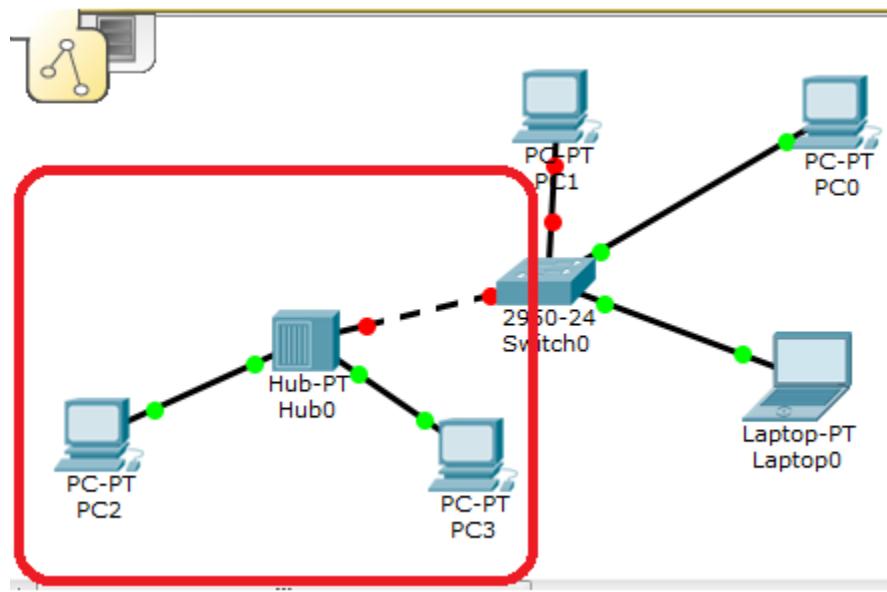


Figura No. 10. Añadiendo y conectando el hub en el puerto 12

- 4.7.8** 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.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	234/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.7.9** 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.



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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	235/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:	MADO-31
		Versión:	03
		Página	236/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	237/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 4
Políticas de seguridad en los puertos del Switch
Cuestionario Previo

12. Realice una lista con al menos 3 ventajas y desventajas de adquirir un switch administrable en comparación con uno que no tenga dicha característica.
13. Investigue en qué consiste el ataque conocido como inundación de direcciones MAC (MAC Flooding Attack) y realice un diagrama donde se muestre su funcionamiento.
14. ¿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?
15. Investigue la sintaxis del comando port security para un switch Cisco.
16. Investigue qué permite realizar la opción sticky de port security.
17. Investigue cómo se podría utilizar la opción sticky de port security como una opción más flexible a MACs fijas.
18. ¿Para qué se utiliza la opción aging de port security?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	238/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 5

Enrutamiento estático

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	239/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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:	03
		Página	240/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 241/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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)

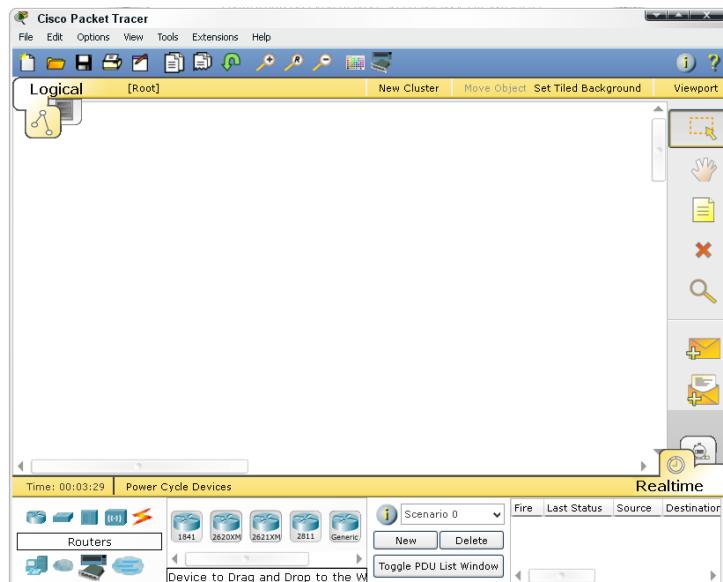


Figura No. 1. Interfaz gráfica de PT

- 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 03 242/298 8.3 11 de enero de 2019
Facultad de Ingeniería	Area/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 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.

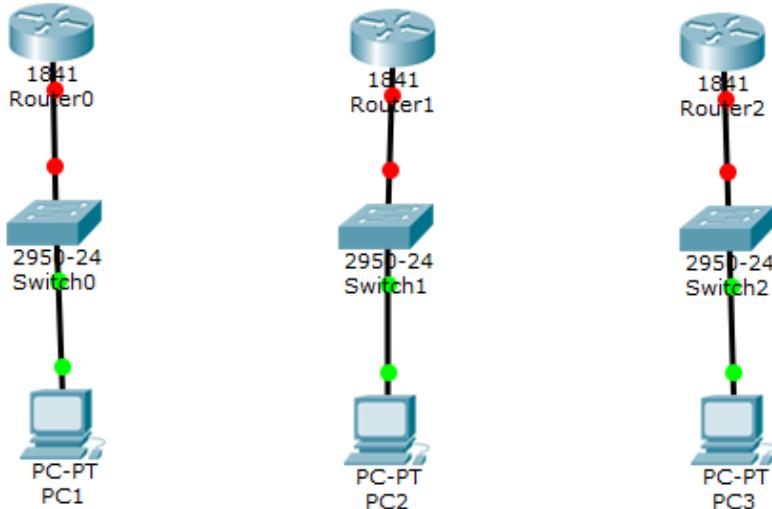


Figura No. 3. Topología de dispositivos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 243/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

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).



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:	03
		Página	244/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

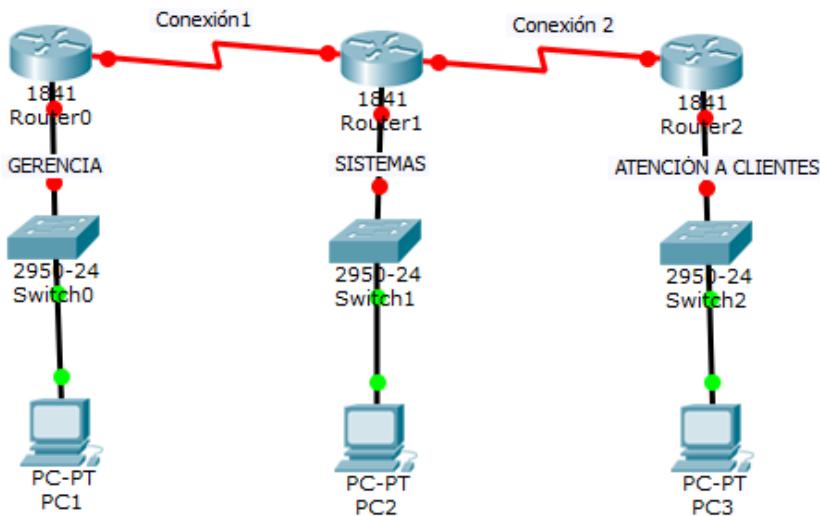


Figura No. 5. Conexión de los routers

4.3 Configuración de las interfaces de los routers

- 4.3.1** Seleccione el Router0 y dé clic 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

Anote la DIR_IP empleada en este caso _____

- 4.3.3** Para configurar la interfaz Serial0/1/0 deben teclearse los siguientes comandos:

```

Router(config)#int Serial 0/1/0
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:	03
		Página	245/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 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
Router(config-if)#no shutdown
Router(config-if)#exit

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	246/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:	03
		Página	247/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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**.

- 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	248/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 Anote 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 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
Router#copy run start
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	249/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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
```

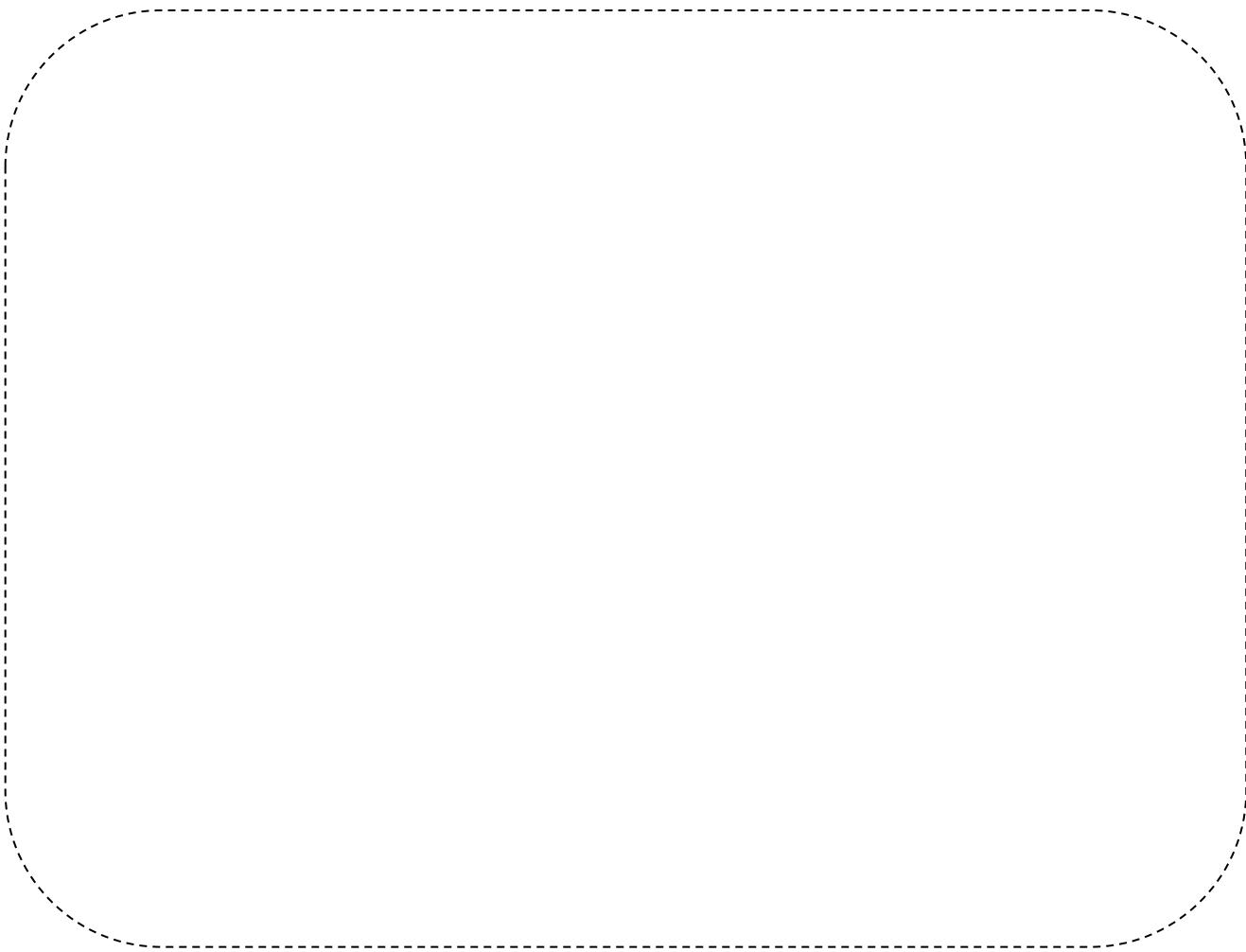
NOTA 1: Reemplace el parámetro **NETWORK** con el segmento de red con el cual desea tener comunicación (red remota), el parámetro **NET_MASK** corresponde a la máscara de subred de la red remota. El parámetro **NEXT_HOP_ADDRESS** corresponde a la dirección de red de la interfaz del router remoto que 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:	03
		Página	250/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 251/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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

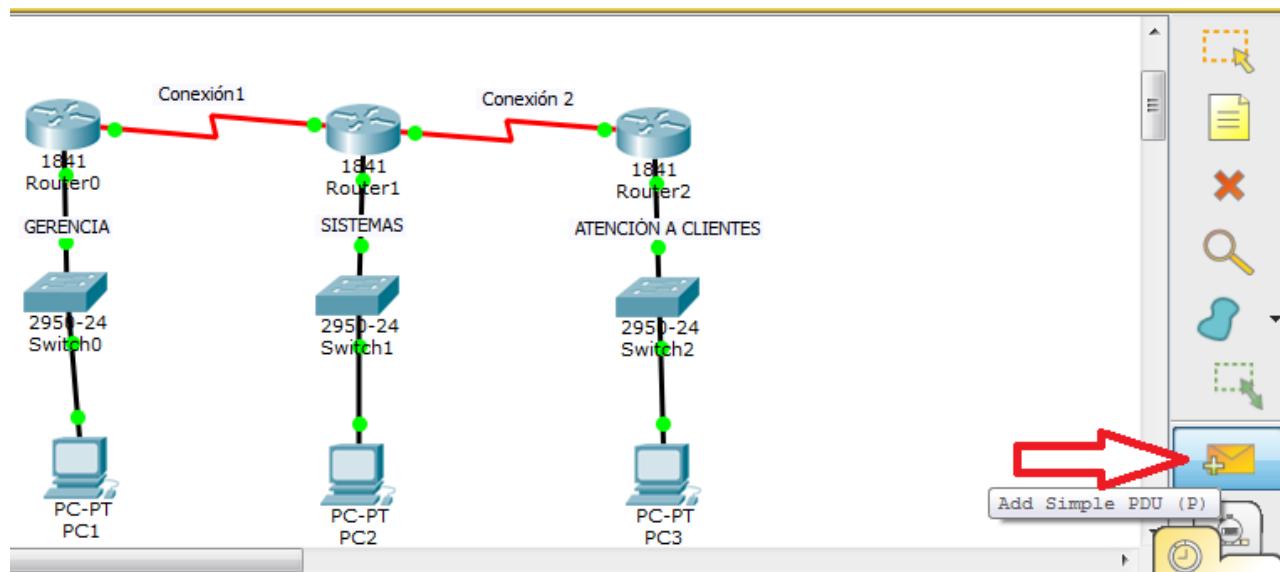


Figura No. 6. Pruebas

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	252/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

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

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?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	253/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Cuestionario

1. ¿Por qué es importante prestar atención al momento de establecer las direcciones IP en las interfaces del router?

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?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	254/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5. Investigue los métodos de seguridad que serían convenientes utilizar en la topología de red que está empleando

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:	03
		Página	255/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 5
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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	256/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 6

Firewall básico

Capa 7 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	257/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 analizará, investigará e implementará mecanismos adecuados de seguridad en los puertos lógicos de entrada de un servidor de red.
- El alumno 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 solo 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:	03
		Página	258/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 Student.

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: 03 Página 259/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

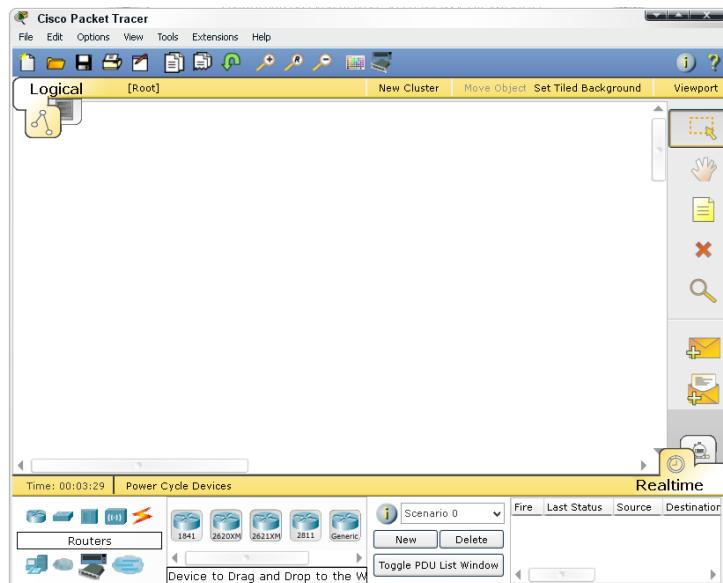


Figura No. 1. Interfaz gráfica de PT

- 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.)

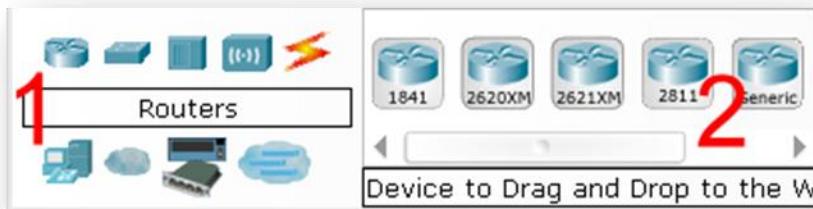


Figura No. 2. Secciones de dispositivos

- 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: Versión: Página: Sección ISO: Fecha de emisión:	MADO-31 03 260/298 8.3 11 de enero de 2019
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 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.

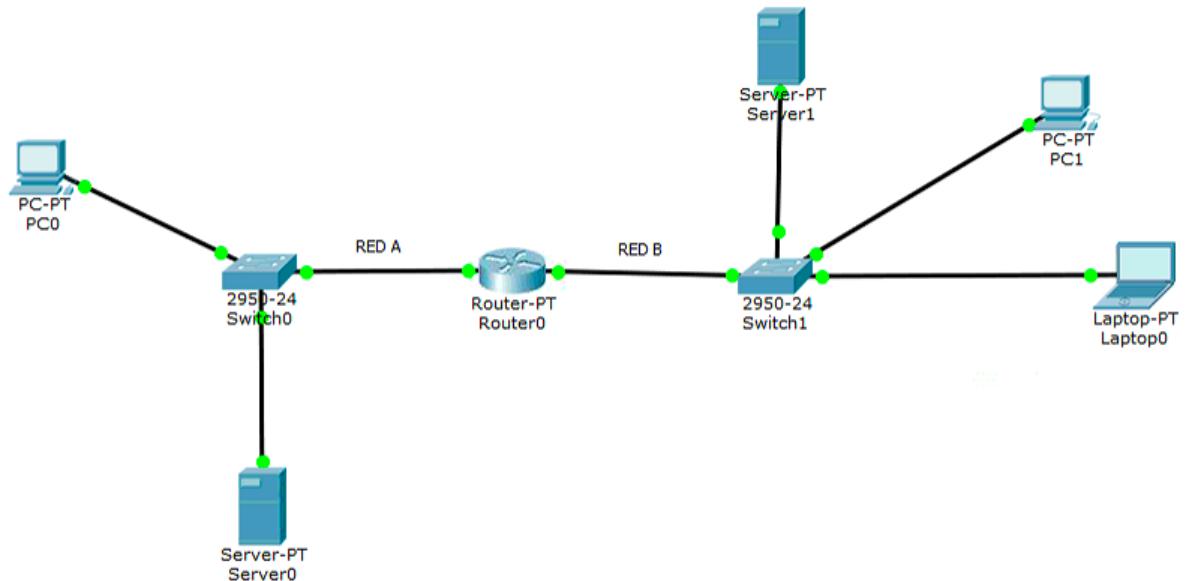


Figura No. 3. Topología básica

- 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:	03
		Página	261/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	262/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	263/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 264/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

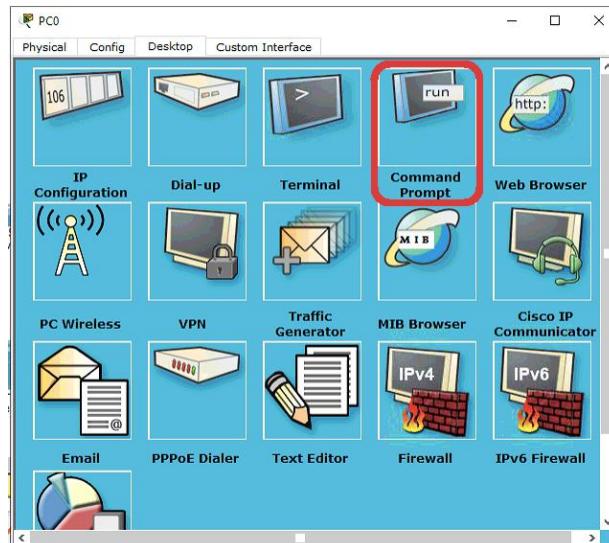


Figura No. 4. Seleccionando la Opción de Command Prompt

- 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 265/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

4.3.18 ¿Se logró establecer la comunicación? Explique

4.3.19 Seleccione nuevamente la pestaña Desktop y posteriormente seleccione la opción de Web Browser como se muestra en la Figura No. 5.

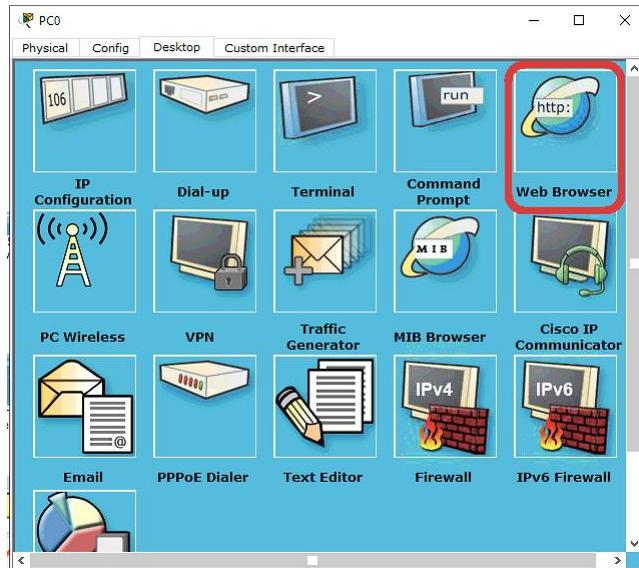


Figura No. 5. Seleccionando la Opción de Web Browser

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



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	266/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

4.3.22 También puede probar la conectividad en el sentido inverso desde la red B hacia la red A. Indique el resultado obtenido.

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.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	267/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

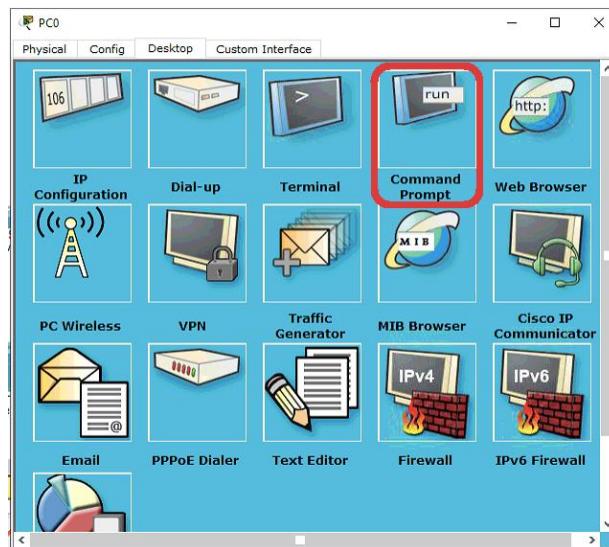


Figura No. 6. Seleccionando la Opción de Command Prompt

- 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.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 268/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería	Area/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada		

- 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.

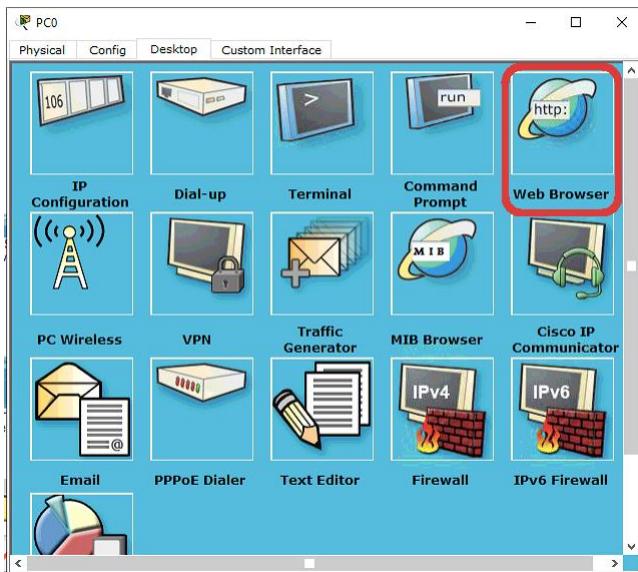


Figura No. 7. Seleccionando la Opción de Web Browser

- 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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	269/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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 el 4.4.7. Ya que la respuesta que se obtiene no es host-unreachable, indique los resultados obtenidos haciendo uso del comando ping.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	270/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4.9 Indique los resultados obtenidos haciendo uso del Web browser.



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.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	271/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

- 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:	03
		Página	272/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	273/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 6

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?

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	274/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería	Área/Departamento: Laboratorio de Redes y Seguridad		
La impresión de este documento es una copia no controlada			

Práctica Optativa 7

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: 03 Página 275/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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 realizará la configuración básica de una VLAN de voz y de datos.
- El alumno 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 Student.

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)

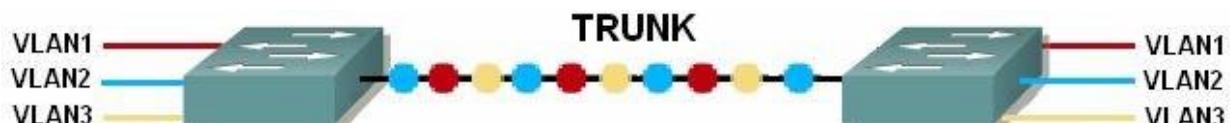


Figura No. 1 Enlace troncal

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:	03
		Página	276/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	277/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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 Student

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 Student (Ver Figura No. 2).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 278/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

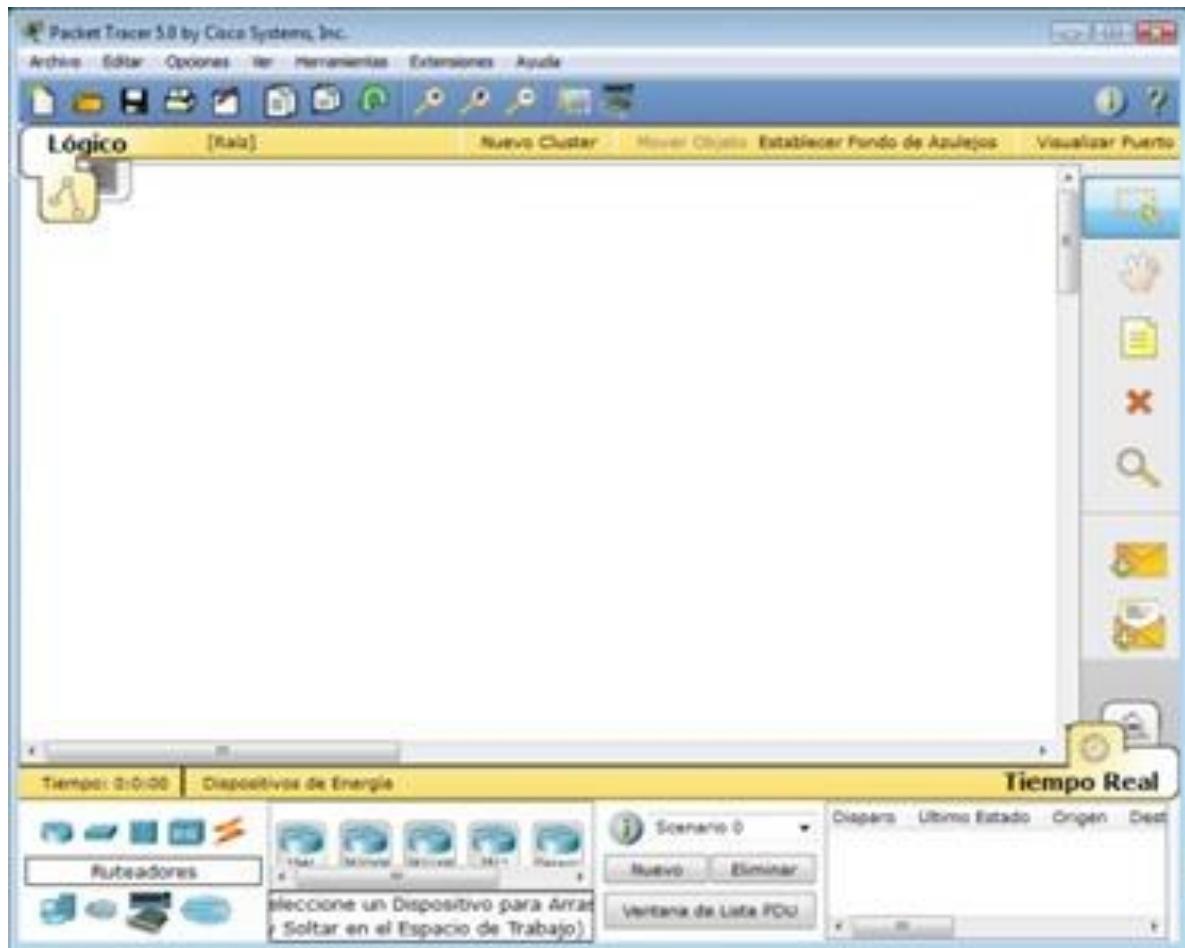


Figura No. 2. Simulador de Cisco Packet Tracer Student

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 279/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

El objetivo de la Figura No. 3 será conocer la aplicación y los elementos importantes:

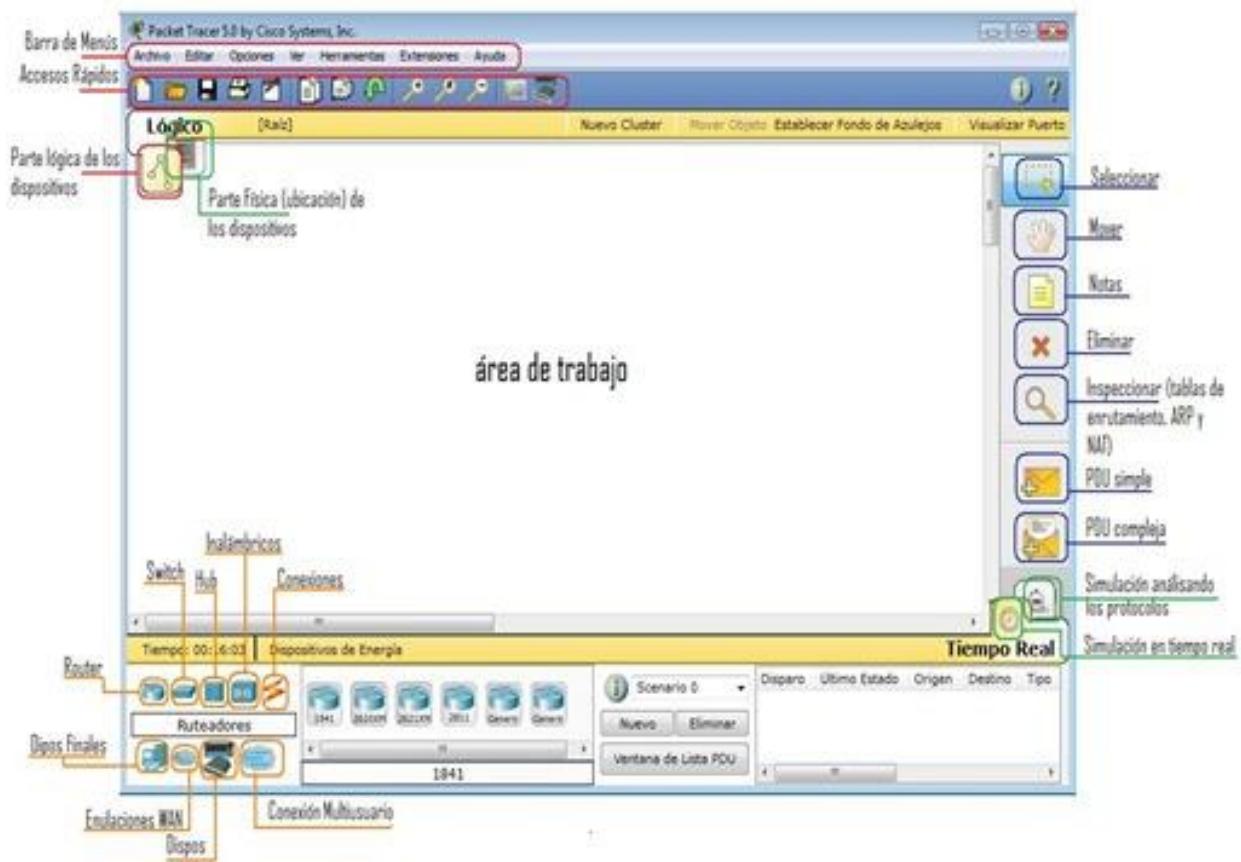


Figura No. 3. Área de Trabajo del simulador de Cisco Packet Tracer Student

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 280/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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

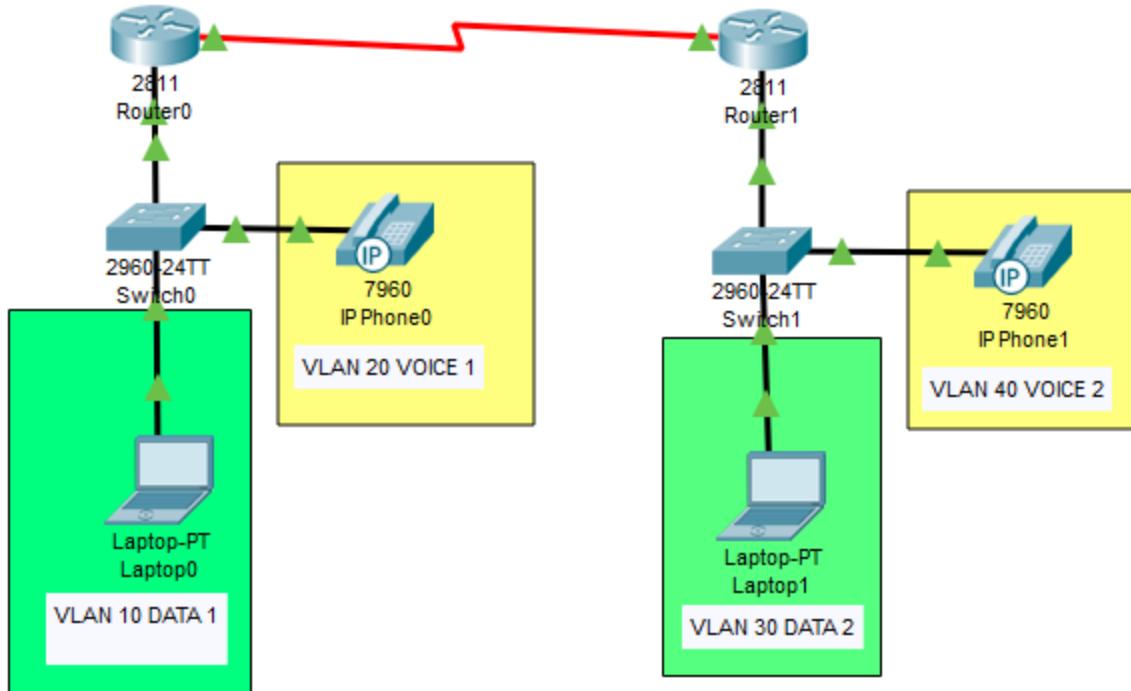


Figura No. 4 Topología de Red.

- 4.1.5** Las conexiones deben realizarse con base en la tabla No. 1.

NOTA: Con ayuda de su 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:	03
		Página	281/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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: 03 Página 282/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

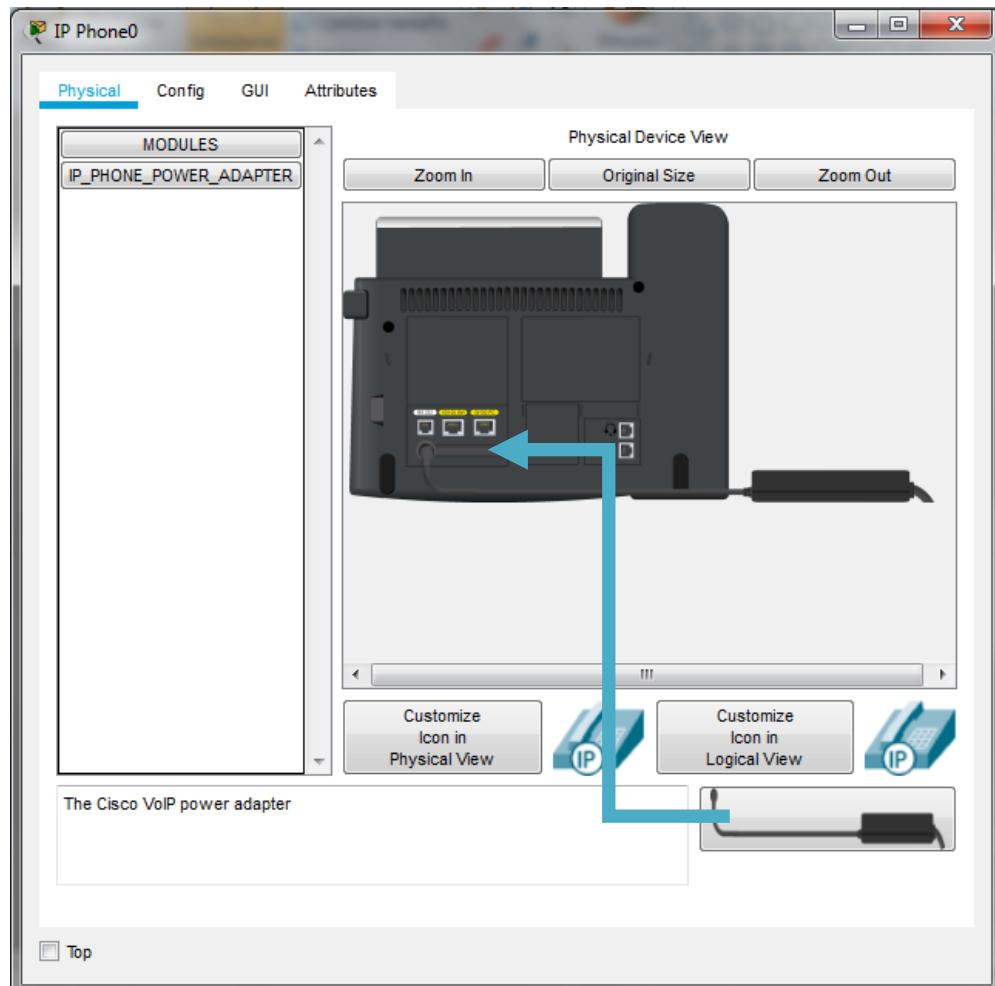


Figura No. 5. Conexión del cable de corriente

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.

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).

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	283/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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 solo 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
Switch0>
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	284/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 solo 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
	VLAN 40	VOICE2	40

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	285/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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:	03	
		Página	286/298	
		Sección ISO	8.3	
		Fecha de emisión	11 de enero de 2019	
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 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 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.

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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	287/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 asigne 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
Router0(dhcp-config)#exit
```

Donde:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	288/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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.

4.7 Configuración de las subinterfaces de las VLAN en el router.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	289/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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

4.7.3 Asigne direcciones IP en la Interfaz Serial de cada router. Para ello teclee los siguientes comandos para el router0:

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	290/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

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: 03 Página 291/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad
La impresión de este documento es una copia no controlada		

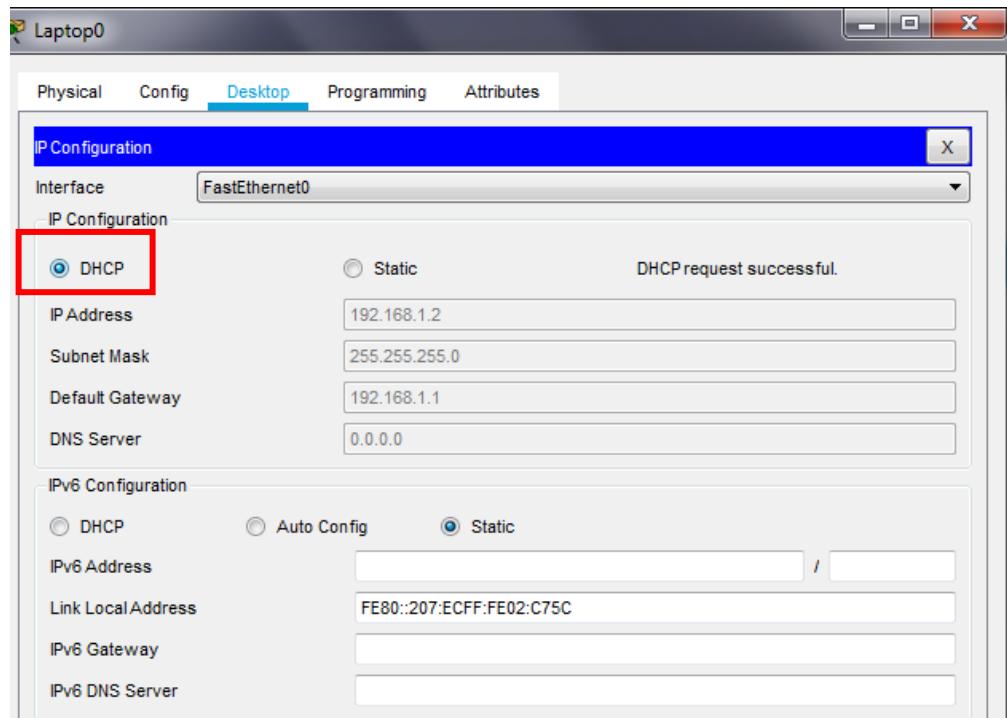


Figura No. 6. Asignación por DHCP

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
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

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	292/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 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.

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
```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	293/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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.

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 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: 03 Página 294/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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:	03
		Página	295/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	296/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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:	03
		Página	297/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
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.



	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	03
		Página	298/298
		Sección ISO	8.3
		Fecha de emisión	11 de enero de 2019
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA OPTATIVA 7
Configuración básica de una comunicación de Voz IP
Cuestionario Previo

- Investigue cuáles son los diferentes tipos de VLAN que se pueden implementar en una RED.
- 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?

- Analice los siguientes comandos que se utilizan en el router e indique a qué se hace referencia cada línea.

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

- Investigue qué comandos se deben utilizar para habilitar la seguridad de los puertos de un switch en cisco packet tracer, en modo dinámico.

- Investigue cuáles son los comandos para configurar la contraseña en modo EXEC privilegiado.

- Investigue para qué sirven los comandos **ephone-dn** y **telephony-service**