
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	220/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 4

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:	04
		Página	221/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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.


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:	04
		Página	222/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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)

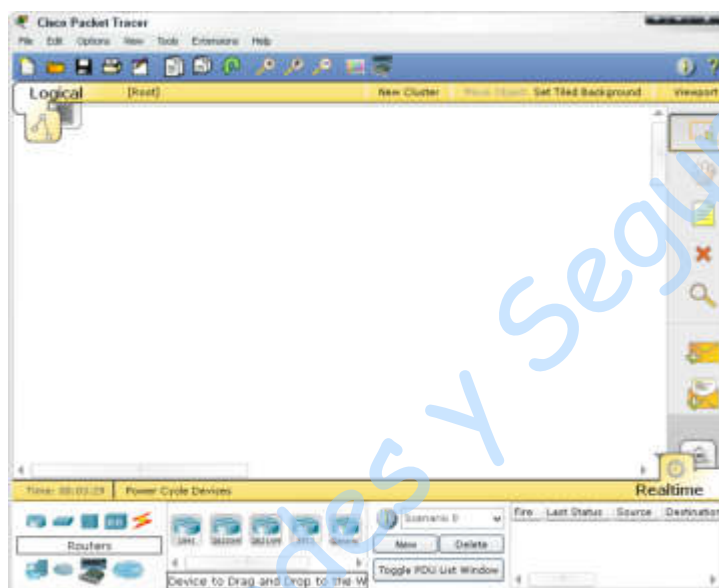



Figura No. 1. Interfaz gráfica de PT

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:	04
		Página	223/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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.).

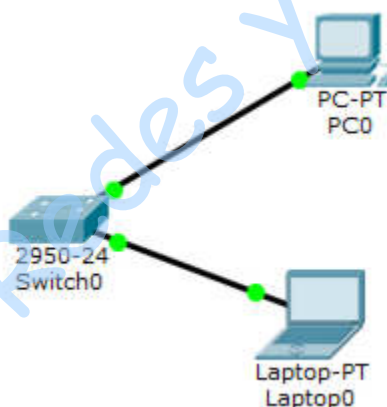


Figura No. 3. Topología básica


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:	04
		Página	224/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

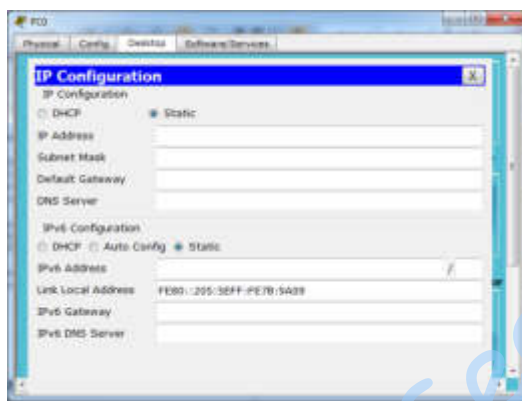


Figura No. 4. Configuración de la PC.

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:

- Deshabilitar los puertos (interfaces) que no se utilicen.
- 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:	04
		Página	225/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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).

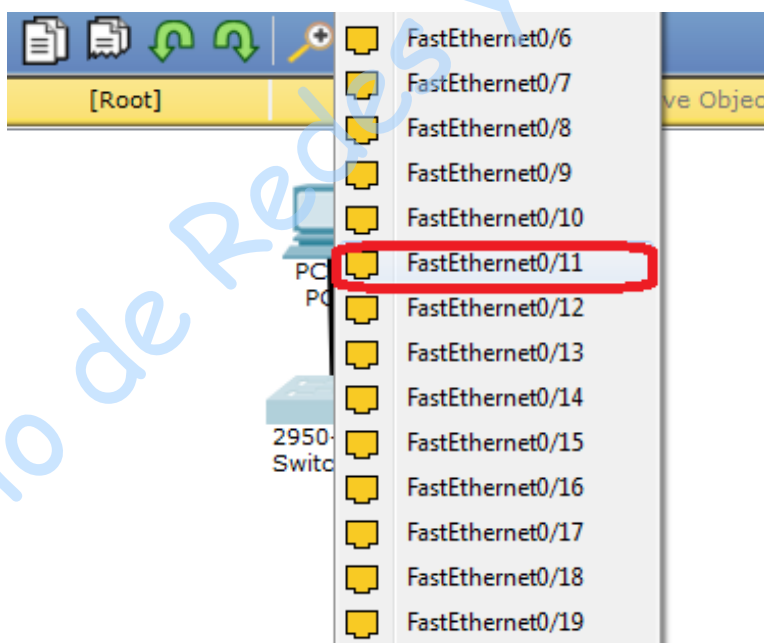




Figura No. 5. Añadiendo y conectando la nueva PC en el puerto 11

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	226/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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:	04
		Página	227/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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:	04
		Página	228/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

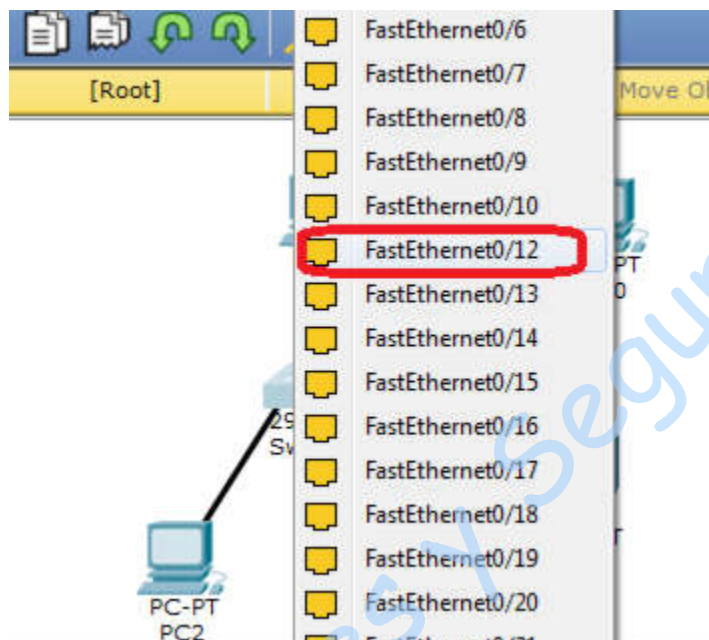



Figura No. 6. Añadiendo y conectando la nueva PC en el puerto 12

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:	04
		Página	229/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

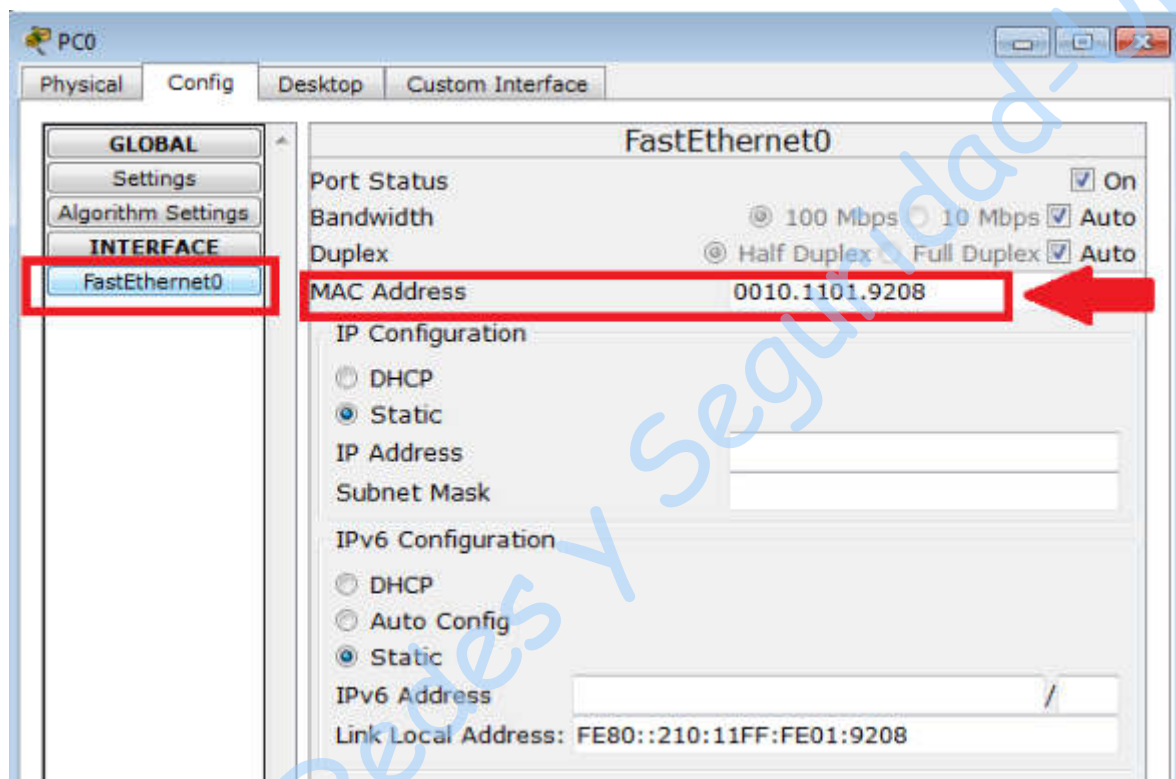



Figura No. 7. Obtener Dirección MAC

```
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:	04
		Página	230/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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.

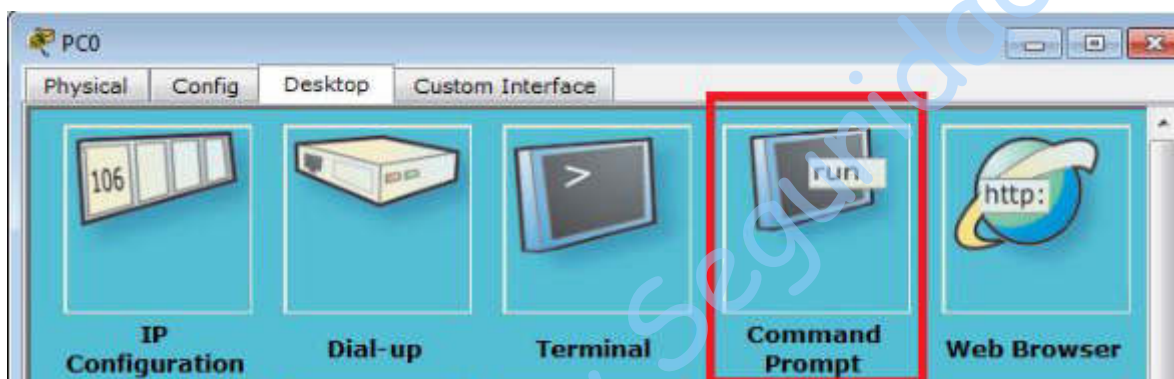


Figura No. 8. Command Prompt

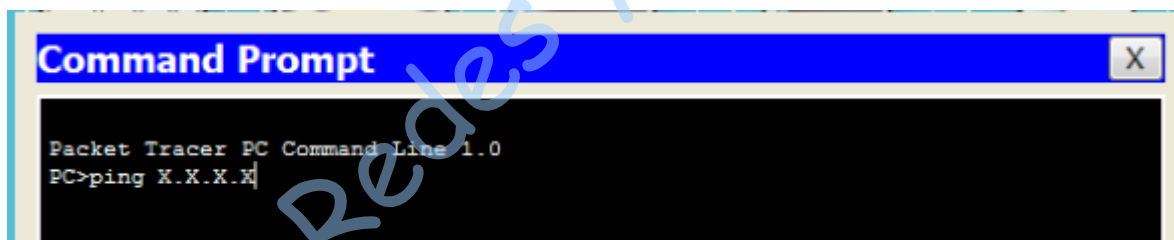



Figura No. 9. Ping

- 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:	04
		Página	231/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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:	MADO-31
		Versión:	04
		Página	232/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

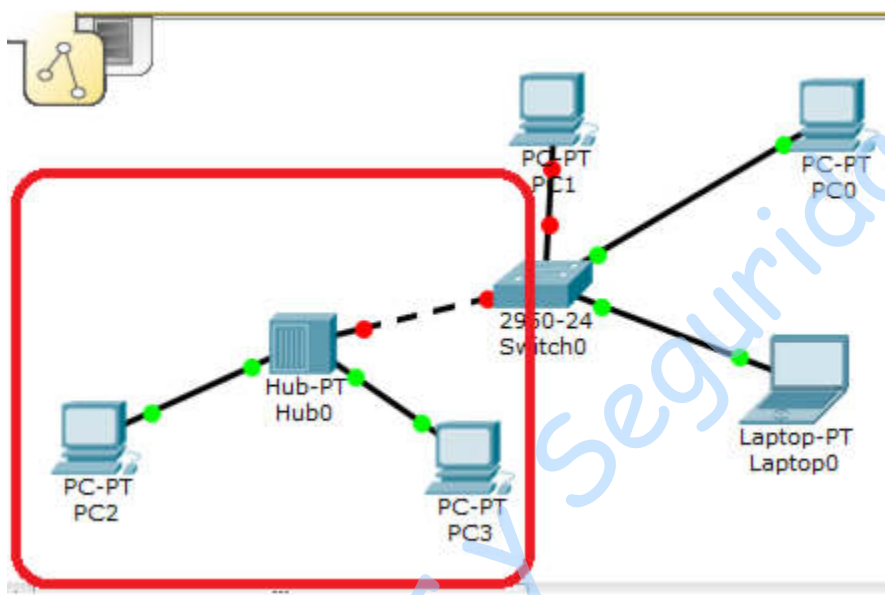



Figura No. 10. Añadiendo y conectando el hub en el puerto 12

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:	04
		Página	233/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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:	04
		Página	234/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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:	04
		Página	235/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
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.

