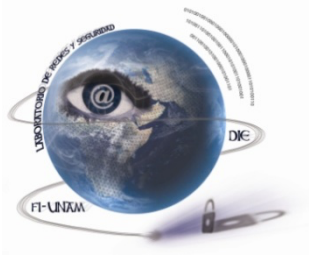




Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. María Alejanda Zuñiga Medel

Asignatura: Redes de Datos Seguras

Grupo: 08

No de Práctica(s): Optativa 4

Integrante(s): Martínez Rojas José Eduardo

Mateos Ruiz Jesus Daniel

Villafañe Pérez Pamela Irais

Navarrete Acosta Cristopher Antonio


*No. de Equipo de
cómputo empleado:*

Semestre: 2022-1

Fecha de entrega: 30/oct/2021

Observaciones:


CALIFICACIÓN: _____

	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 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:	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)

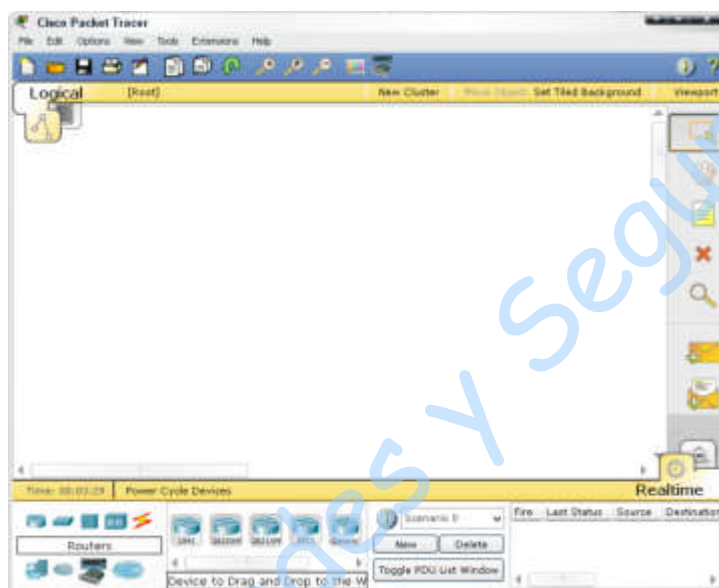


Figura No. 1. Interfaz gráfica de PT

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.)

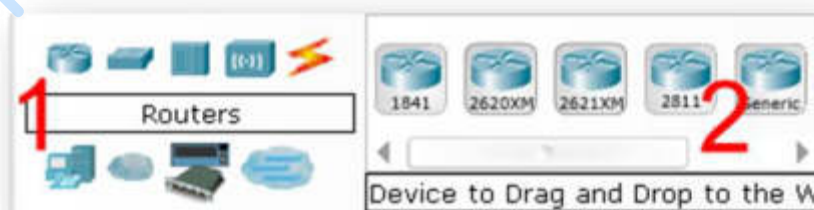



Figura No. 2. Secciones de dispositivos

	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.).

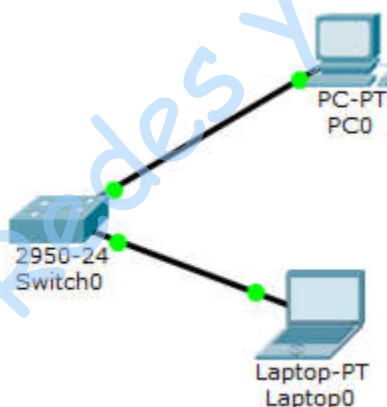


Figura No. 3. Topología básica


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			

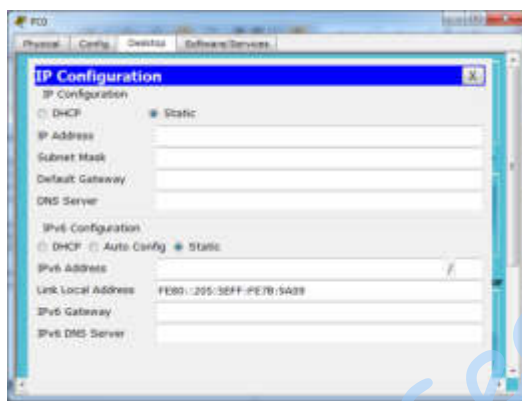


Figura No. 4. Configuración de la PC.

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.

Configura una interfaz de router. La interfaz de router está apagada de manera predeterminada. Apaga y enciende los puertos

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).

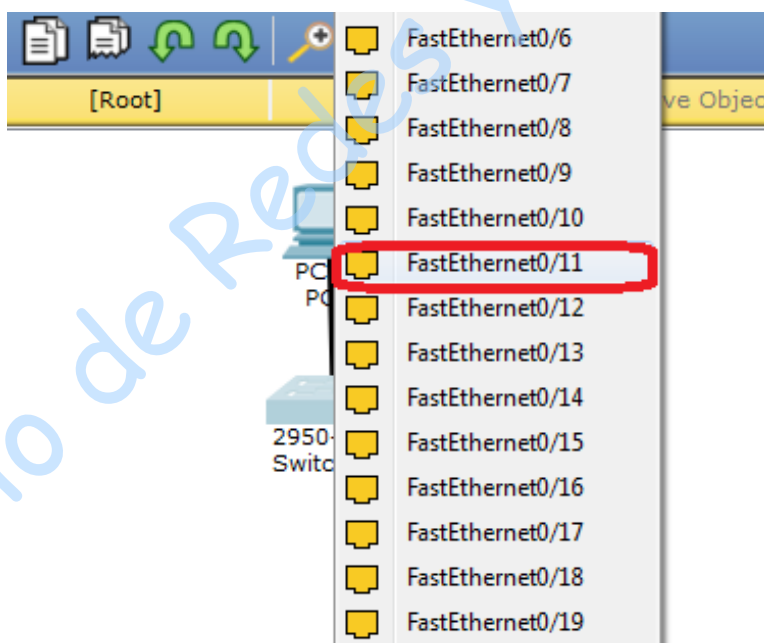



Figura No. 5. Añadiendo y conectando la nueva PC en el puerto 11

	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			


Dado que en el switch está deshabilitado el puerto Fa0/11, no va estar conectado a la switch con el cable o no tendrá acceso. ya que deshabilitamos esos puertos igual si quisiéramos del puerto 11-24 al switch no funcionarían ya que deshabilitamos esos puertos pero los puertos del 0-11 siguen On.

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:

```
Switch>enable
Switch#config t
Switch(config)#interface range Fa0/11-24
Switch(config-if-range)#no shutdown
Switch(config-if-range)#end
Switch#
```

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			

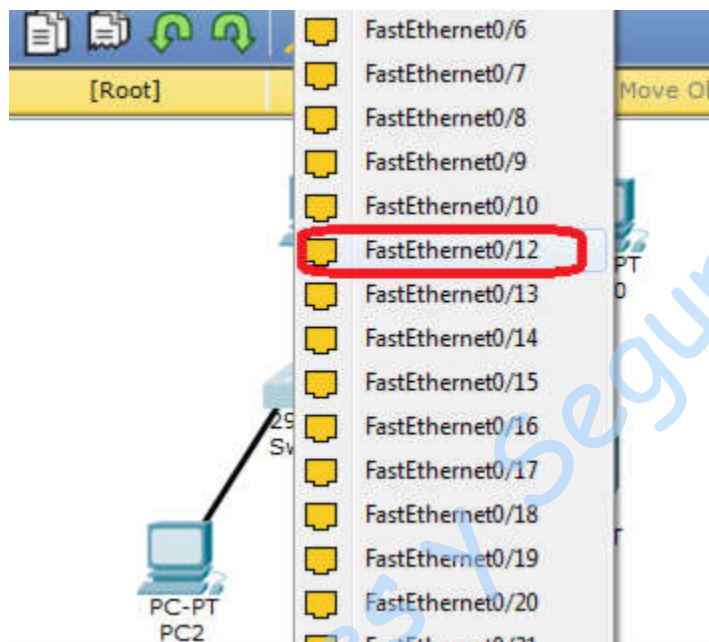



Figura No. 6. Añadiendo y conectando la nueva PC en el puerto 12

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			

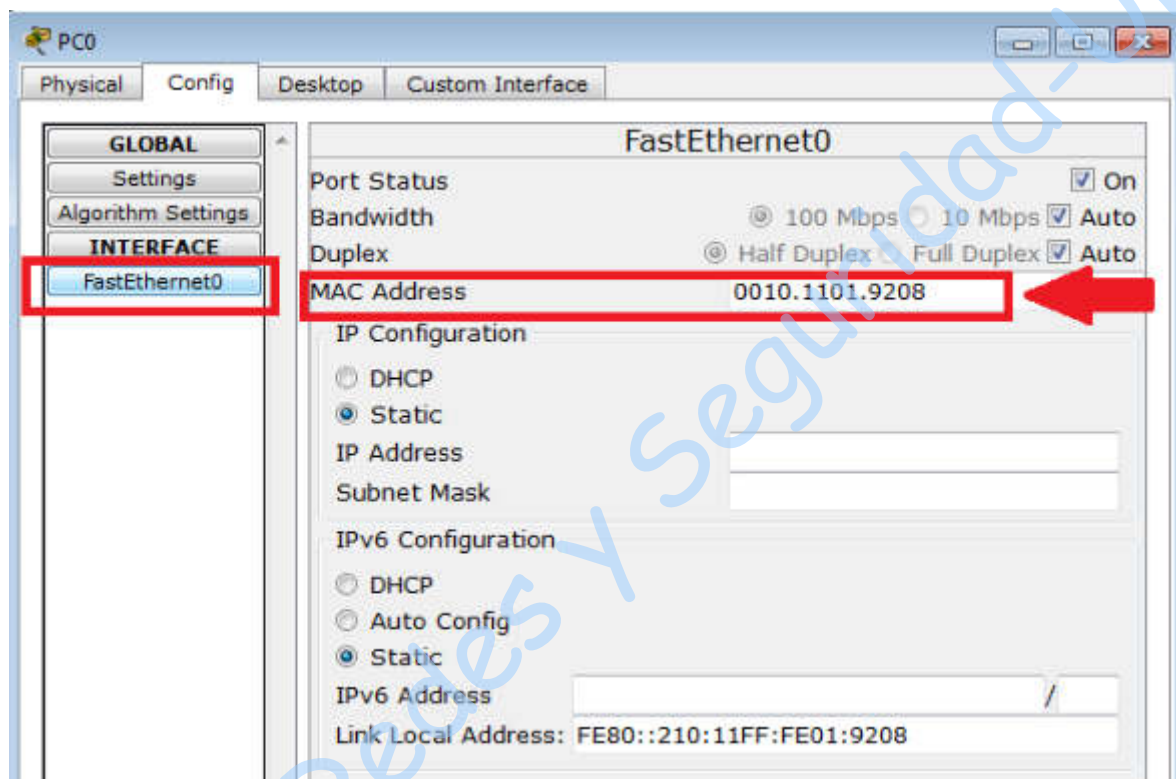



Figura No. 7. Obtener Dirección MAC

```
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.

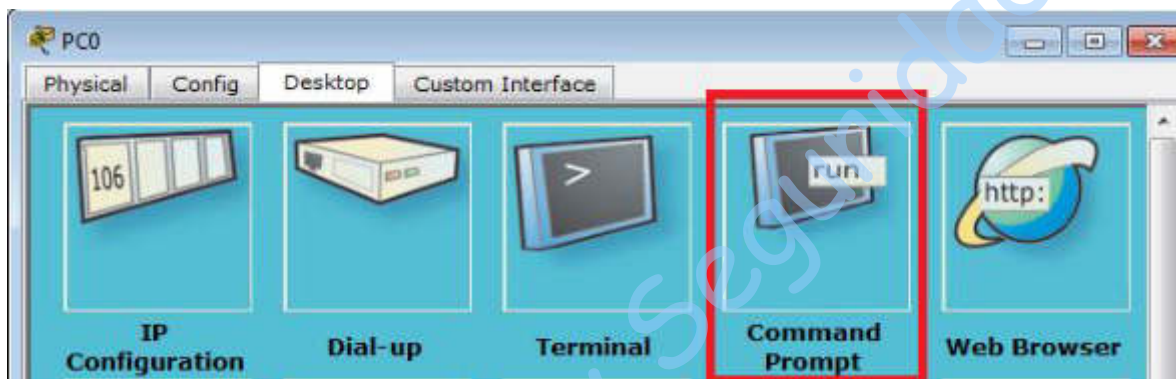


Figura No. 8. Command Prompt

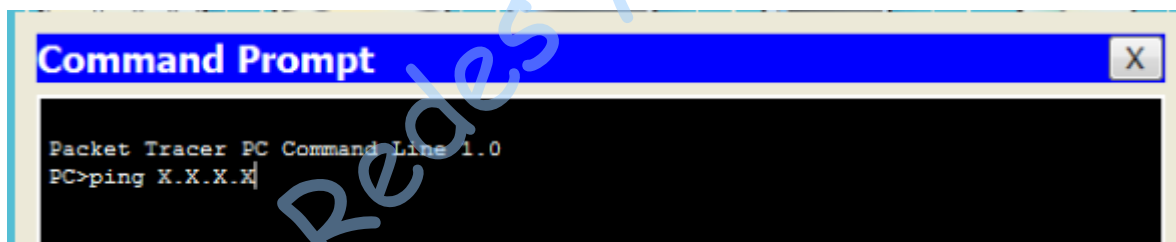



Figura No. 9. Ping

- 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.

esta opción leera y aprendera la primera mac-address que se conecte, switchport port-security mac-address sticky le dice al switch que de forma dinámica aprenda la dirección MAC de origen y agregue los comandos port-security al running-config.

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			

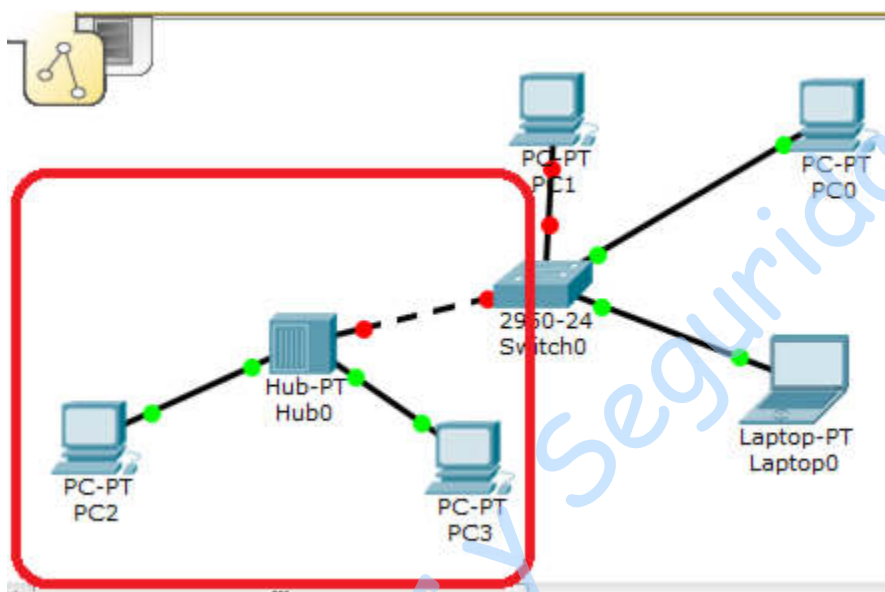



Figura No. 10. Añadiendo y conectando el hub en el puerto 12

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.

El protocolo vio que hubo un cambio que hay 2 dispositivos conectados por medio del hub lo que significa que uno no pertenece al puerto que se conectó, por lo que se aplicó el protocolo de seguridad y como es un violación shutdown apago el puerto.

	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.


```
Switch(config)#interface Fa0/13
Switch(config)# switchport mode access
Switch(config)#switchport port-security
Switch(config)#switchport port-security mac-address sticky
Switch(config)#end
Switch(config)#interface Fa0/14
Switch(config)# switchport mode access
Switch(config)#switchport port-security
Switch(config)#switchport port-security mac-address sticky
Switch(config)#end
Switch(config)#interface Fa0/15
Switch(config)# switchport mode access
Switch(config)#switchport port-security
Switch(config)#switchport port-security mac-address sticky
Switch(config)#end
```

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			

Show port security nos muestra todos los puertos que han sido configurados, máximos de elementos, si hay una dirección actual, número de violaciones y la acción de seguridad ya sea shutdown, protect o restrict.

Show port security interface PUERTO: Nos muestra toda la información del puerto escogido si esta habilitado ese rasgo para dicho puerto, el status apagado o encendido el puerto, acción de seguridad como shutdown, protect o restrict que es la acción que hace si hay un dispositivo conectado a ese puerto pero no es el permitido o no es el que tiene la dirección mac registrada, tiempo de caducidad de las direcciones, si está activada está opción para que caduquen cada cierto tiempo las direcciones, máximo número de direcciones MAC, total actual que hay registradas, número de configuraciones MAX, la dirección mac guardada y si el número de violaciones cometidas.

4.4.2 Indique para qué se usa el comando show port-security address

Nos sirve para ver la tabla de direcciones mac guardadas por el rasgo que activamos para nuestro switch port-security donde vemos todas las direcciones mac guardadas o registradas y el puerto al que pertenecen y si se aprenden dinámicamente o son estáticas.


	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.

Martínez Rojas José Eduardo

En resumidas cuentas se pudo entender los mecanismos de seguridad adecuados para la seguridad de los puertos del switch, además se pudo entender como configurar para obtener la seguridad en cada puerto, también apagar y prender los puertos con los comandos adecuados en Cisco packet tracer.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	236/297
		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 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?

1.-Realice una lista con al menos 3 ventajas y desventajas de adquirir un switch administrable en comparación con uno que no tenga dicha característica.

Ventajas

- Mejor confiabilidad, disponibilidad y optimización de la red.
- Son compatibles con métodos de configuración
- Se implementan tecnologías como VLAN. Para segmentar (separar) redes con tráfico de información confidencial.
- Mejora la seguridad perimetral. Teniendo protección físico, detección de tentativas de intrusión y, o disuasión de intrusos.
- Flexibilidad para reaccionar ante el crecimiento de la red

Desventajas

- No consiguen filtrar difusiones o broadcasts, multicasts ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.
- Para una conexión a internet si el ISP solo nos brinda 1 IP pública.
- Solo una maquina tendría internet.
- Muchos conmutadores existentes en el mercado no son configurables

2.-Investigue en qué consiste el ataque conocido como inundación de direcciones MAC (MAC Flooding Attack) y realice un diagrama donde se muestre su funcionamiento.

Los switches emplean una las tablas de direcciones MAC para dirigir los paquetes a destino de manera eficiente, los datos contenidos en estas tablas se aprenden dinámicamente a medida que el switch va gestionando tráfico, asignando las diferentes MAC a sus diferentes puertos dependiendo de a través de cual de ellos se llegue al destino. De esta manera el switch consigue una mayor eficiencia, reduciendo a la vez la carga en la red al solo tener que enviar las tramas a través del puerto adecuado.

Lo que hace un atacante con esta amenaza es crear una inundación, una solicitud masiva para lograr el colapso de esta tabla que mencionamos.

Con esto logran que, en caso de un ataque exitoso, el switch pase a enviar paquetes que reciba a través de todos sus puertos y así poder interceptar el tráfico. Es lo que se conoce también como saturación de direcciones MAC.

Lo que hace el atacante en este caso es bombardear el switch con una gran cantidad de solicitudes, cada una de ellas con una dirección MAC falsa, con el objetivo de saturar rápidamente esa tabla.

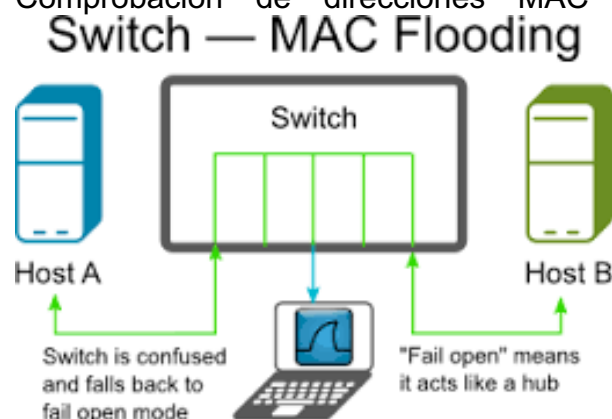
Cuando esto ocurre, el switch comienza a redireccionar tráfico a través de todos los puertos y permite utilizar un sniffer para capturar el tráfico.

La intención es consumir la limitada memoria de lado en el interruptor para almacenar la tabla de direcciones MAC.

Mitigación

Para evitar este ataque, los principales fabricantes de switches incorporan en sus modelos funciones llamadas de Port Security. Estas funcionalidades no las encontraremos en switches básicos de bajo coste, pero se entiende que estos no se van a utilizar en la empresa o en entornos proclives a sufrir este tipo de ataques.

- Limitación en cada puerto de la cantidad de direcciones MAC que se pueden aprender para que en el momento que se alcance el máximo se descarten los paquetes de direcciones no conocidas.
- Asignación estática de direcciones MAC en los puertos para que solo paquetes de ciertas MAC sean procesados.
- Deshabilitación de puertos que no estén en uso.
- Aprendizaje de direcciones MAC persistentes, que al conectar un dispositivo a un puerto, este aprenda la MAC del mismo y no acepte la conexión de ningún otro dispositivo.
- Detección de violaciones de seguridad, que en el caso que se produzcan se apague el puerto.
- Comprobación de direcciones MAC contra un servidor de AAA.



3.-¿Cómo se puede utilizar el ataque de inundación de direcciones MAC para hacer que un switch se comporte como HUB y realizar una escucha de todo el tráfico de los nodos conectados?

La máquina del atacante está conectada a una boca del switch que pertenece a la VLAN 10. Mediante un ataque de floods MAC addresses en esa boca del switch inyecta muchos paquetes con MAC de origen y destinos aleatorios que el switch intenta memorizar. Cuando la tabla CAM (content addressable memory) alcanza su límite el switch empieza a operar como un hub emitiendo las tramas de procedentes de la VLAN 10 a todas las bocas que pertenezcan a dicha VLAN incluyendo la de los switches adyacentes que también tengan bocas para la VLAN 10. Permitiendo a un sniffer capturar todo el tráfico de esa y solo esa VLAN durante el periodo de tiempo que se mantenga el flujo de tramas con MAC aleatorias o durante el tiempo que tarda el switch en ir borrando MAC de su tabla CAM al considerarlas caducadas.

4.-Investigue la sintaxis del comando port security para un switch Cisco.

set port security *mod_num/port_num* enable [*mac_addr*]
set port security *mod_num/port_num* maximum *num_of_mac*

Ejemplo cisco packet tracer

Switch>enable

Switch#config t

Switch(config)#interface Fa0/12 //elige puerto

Switch(config)# switchport mode access //active modo acceso

Switch(config)#switchport port-security //active o habilita el port-security

Switch(config)#switchport port-security mac-address Dir_MAC //asignamos la dirección mac

Switch(config)#switchport port-security maximum 1 //número de direcciones

Switch(config)#switchport port-security violation shutdown Switch(config)#end

5.-Investigue qué permite realizar la opción sticky de port security.

El administrador puede habilitar el switch para que aprenda dinámicamente la dirección MAC y la «pegue/stick» a la configuración en ejecución/running usando el siguiente comando:

Switch(config-if)# **switchport port-security mac-address sticky**

Guardando la configuración en ejecución, la dirección MAC aprendida dinámicamente será enviada a la NVRAM.

6.-Investigue cómo se podría utilizar la opción sticky de port security como una opción más flexible a MACs fijas.

S1(config)#interface Fa0/12 //elige Puerto

S1(config)# switchport mode access //active modo acceso

S1(config-if)# switchport port-security //activamos port-security

S1(config-if)# switchport port-security maximum 4 // Número de direcciones seguras para el puerto

S1(config-if)# switchport port-security mac-address sticky DIRECCIÓN MAC
//asignamos direcciones mac fijas.

S1(config-if)# end

7.-¿Para qué se utiliza la opción aging de port security?

Port security aging se puede usar para establecer el tiempo en que caduca las direcciones seguras estáticas y dinámicas de un puerto. Se admiten dos tipos de envejecimiento por puerto:

- Absolute – Las direcciones seguras en el puerto se eliminan después del tiempo de caducidad especificado.
- Inactivity – Las direcciones seguras en el puerto se eliminan solo si están inactivas durante el tiempo de caducidad especificado.

Utiliza aging para eliminar las direcciones MAC seguras en un puerto seguro sin eliminar manualmente las direcciones MAC seguras existentes. También se pueden aumentar los límites de tiempo de vencimiento para asegurar que se mantengan las direcciones MAC seguras del pasado, incluso mientras se añaden nuevas direcciones MAC. El vencimiento de las direcciones seguras configuradas estáticamente puede activarse o desactivarse en cada puerto.

Bibliografía

CYBERSEGURIDAD(2020) Mac Flooding. Consultado el:28/10/2021 Recuperado de:
<https://www.cyberseguridad.net/mac-flooding-ataques-informaticos-vii>

s.a (2017) Mac Flooding. Consultado el:28/10/2021 Recuperado de:
<https://sites.google.com/site/wikiejemploalccna2017/ventajas-y-desventajas>

CISCO.(2007).Configuring Port Security Consultado el:28/10/2021 Recuperado de:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/sec_port.html

CCNA.(2018).Implementar Port Security Consultado el:28/10/2021 Recuperado de:
<https://ccnadesdecero.es/implementar-port-security/>