TECNOLÓGICO NACIONAL DE MÉXICO

**Instituto Tecnológico de La Paz**

**Ingeniería en Sistemas Computacionales**

**Tópicos Avanzados De Seguridad En Red**

**M.S.C. Armando Yuen Coria**

***Alumnos***

**Enrique Missael Ramos Sepúlveda**

**Jesús Ignacio Gutiérrez Honesto**

**Practica Port Security**

La Paz B.C.S a 25 de septiembre de 2019

Tabla de contenido

[TÍTULO DE LA PRACTICA 3](#_Toc20259642)

[COMPETENCIAS 3](#_Toc20259643)

[OBJETIVO 3](#_Toc20259644)

[INTRODUCCIÓN 3](#_Toc20259645)

[MARCO TEÓRICO 3](#_Toc20259646)

[PROCEDIMIENTO 4](#_Toc20259647)

[RESULTADOS 4](#_Toc20259648)

[CONCLUSIÓN 4](#_Toc20259649)

[BIBLIOGRAFÍA 4](#_Toc20259650)

# TÍTULO DE LA PRACTICA

Port Security

# COMPETENCIAS

Conocimientos básicos de Packet Tracert, y estructuras de una red LAN.

# OBJETIVO

Que los Alumnos aprendan a filtrar las conexiones de los dispositivos dentro de una red local.

# INTRODUCCIÓN

El presente trabajo es un reporte de practica de la materia de Tópicos Avanzados De Seguridad En Red, el tema a tratar es Port Security el cual es una función en los Cisco switch destinada a limitar la cantidad de direcciones MAC que se pueden conectar a través de un puerto, el ejemplo mostrado es realizado en la herramienta Packet Tracert de Cisco.

# MARCO TEÓRICO

Con el objetivo de incrementar la seguridad en una red LAN es posible implementar seguridad de puertos en los switches de capa de acceso, de manera de permitir que a cada puerto se conecte sólo la estación autorizada. Para ello Cisco provee port security, un mecanismo bastante potente y sencillo.

Dirección MAC segura estática

* Se configura manualmente.
* Se agrega a la tabla de direcciones MAC.
* Se guarda en la running-config.
* Se puede hacer permanente guardando la configuración.

Dirección MAC segura dinámica

* Se aprende del tráfico que atraviesa la interfaz.
* Se la guarda en la tabla de direcciones MAC.
* Se pierde cuando se reinicia el equipo.

Dirección MAC segura sticky

* Se la puede configurar de forma manual o dinámica.
* Se la guarda en la tabla de direcciones MAC.
* Se almacena en la running-config.
* Se puede hacer permanente guardando la configuración.

**Acciones a tomar si se produce una violación**

Es importante tener en cuenta que por violación se entiende uno de los siguientes dos casos:

* Se alcanzó la cantidad máxima de direcciones MAC permitidas.
* Una dirección MAC que se aprendió en un puerto se aprende por otro puerto diferente.
* Los modos en los que se puede establecer un puerto para decidir qué acción tomar en el caso de una violación son, entonces:

Protect: una vez que se alcanzó el máximo de direcciones MAC en un puerto, todo el tráfico de orígenes desconocidos (es decir, de direcciones MAC que no sean válidas para ese puerto) es descartado. No obstante, se continúa enviando el tráfico legal normalmente. No se notifica al administrador de esta situación.

Restrict: el mismo comportamiento que el caso anterior, pero con la diferencia que se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

Shutdown: en este caso el puerto se da de baja dejándolo en estado err-disabled (deshabilitado por error). Además, se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

Shutdown VLAN: la única diferencia con el caso anterior es que se deshabilita la VLAN en ese puerto en lugar de dar de baja el puerto completo. Es particularmente atractivo para los puertos de trunk.

En el caso del Switch SFE2000P las especificaciones del Port Security son las siguientes:

La seguridad de la red se puede aumentar limitando el acceso a un puerto específico solo a usuarios con direcciones MAC específicas. Las direcciones MAC se pueden aprender dinámicamente o configurar estáticamente. La seguridad de puerto bloqueado supervisa los paquetes recibidos y aprendidos que se reciben en puertos específicos. El acceso al puerto bloqueado está limitado a usuarios con direcciones MAC específicas. Estas direcciones se definen manualmente en el puerto o se aprenden en ese puerto hasta el punto en que está bloqueado. Cuando se recibe un paquete en un puerto bloqueado, y la dirección MAC de origen del paquete no está vinculada a ese puerto (o se aprendió en un puerto diferente o es desconocido para el sistema), se invoca el mecanismo de protección y puede proporcionar varias opciones. Los paquetes no autorizados que llegan a un puerto bloqueado son:

• Reenviado

• Desechado sin trampa

• Desechado con trampa

• Causa de cierre del puerto

La seguridad de puerto bloqueado también permite almacenar una lista de direcciones MAC en el archivo de configuración. La lista de direcciones MAC se puede restaurar después de que el dispositivo se haya reiniciado. Los puertos deshabilitados se activan desde la Página de Seguridad del Puerto.

# PROCEDIMIENTO

# RESULTADOS

# CONCLUSIÓN

# BIBLIOGRAFÍA