**En este laboratorio 7, se realizará la configuración física de una topología de red sencilla.**

**Objetivos:**

**Se realizará la configuración de un router y un switch de manera segura para acceso remoto.**

**Vamos a establecer niveles de seguridad en el switch**

**Elementos importantes de configurar en un switch** está el hostname, los passwords de consola, line vty 0 15 máximo número de conexiones de forma remota.

**telnet** no es seguro porque envía información al canal de comunicaciones en texto plano y esta información puede ser tomada por un tercero para hackear mi red.

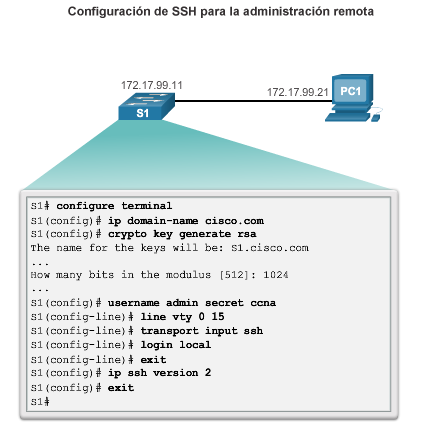
El **protocolo ssh** utiliza el **puerto 22** y tiene un protocolo de comunicación segura, ya que toda la información debe viajar encriptada. Utilizaremos el **algoritmo de encriptación RSA.**

El día de hoy se instalará un **servicio SSH** que llevará a cabo la comunicación utilizando un **algoritmo de criptografía conocido como RSA**

Los switches 2960 soportan la posibilidad de tener comunicaciones seguras utilizando el protocolo SSH utilizando el puerto 22.

SSH es un protocolo de comunicación segura entre un origen y un destino, y se utiliza para accesos remotos.

**Los parámetros de configuración a utilizar son:**

****

**Para conectarnos de manera remota segura, utilizando el protocolo ssh se tiene que crear una base de datos. La base de datos se crea en la primera línea y puede tener más de un usuario.**

3. username **admin** secret **ccna SE ESTABLECE USUARIO Y PASSWORD**

1. Line vty 0 15

4. transport input ssh **SE ESTABLECE COMO PROTOCOLO DE COMUNICACIONES O PARA ACCESO REMOTO SSH.**

2. Login local **SE DEBE CREAR UNA BASE DE DATOS**

**El otro elemento importante de comunicación o de seguridad, es que vamos a utilizar una llave criptada que utiliza el algoritmo RSA. RSA por default trabaja con 1024 bits para encriptar, por default está configurado con 512 si le doy enter:**

**crypto key generate rsa**

**FINALMENTE SE REQUIERE DE UN DOMINIO DONDE BUSCAR LA BASE DE DATOS EN ESTE CASO cisco.com SE DEBE DAR DE ALTA ESTE DOMINIO DE NOMBRE**

Ip domain-name cisco.com

**Se puede trabajar con una versión avanzada de protocolo ssh que es la versión 2: En esta práctica no está incluido.**

Ip ssh versión 2

**RSA es protocolo que trabaja con un algoritmo de criptografía que utiliza 1024 bits**

**ssh -l dirección**

**En el simulador sería así o desde interfaz de línea de comandos:**

**ssh –l admin 172.16.99.11, aquí solo nos pide el password.**

**Desde físico nos va a pedir el usuario admin y el passwrod**

**El protocolo ssh puede ser analizado utilizando los siguientes comandos:**

**COMO ESTÁ CONFIGURADO EL PROTOCOLO SSH. Para analizar el contenido de su configuración**

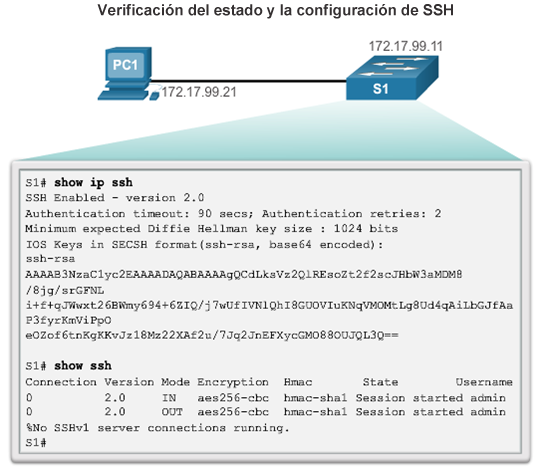
**sh ip ssh**

**El comando**

**sh ssh**

**NOS MUESTRA COMO ESTÁ FUNCIONANDO DE ENTRADA Y DE SALIDA, INFORMACIÓN DEL DEL USERNAME, LA VERSIÓN. ME PERMITE VER LAS SESIONES QUE TENGO ESTABLECIDAS DE ACUERDO A LAS PERSONAS DADAS DE ALTA EN LA BASE DE DATOS.**

**Ya que en la base de datos podemos dar de alta varios usuarios. EN este ejemplo solamente tengo un usuario admin.**

****

Por qué es importante establecer seguridad,

**2 principios básicos de la seguridad:**

1. **Cuando quiero establecer una conexión de forma remota, debo utilizar un protocolo seguro como ssh.**
2. **El segundo mecanismo de seguridad cuando solamente se le permite a un conjunto de dispositivos verídicos para poder conectarse al switch. Y esto lo conseguimos con el nivel más básico de las comunicaciones, utilizando la dirección mac.**

Todos los equipos tienen una dirección mac que los hace únicos (mi cel, mi pc, etc) dentro de ese segmento de red. La dirección mac de mi celular, por la cantidad de dispositivos que pueden existir puede ser una dirección mac duplicada que se encuentre en otro lugar del mundo, por ejemplo China, si yo llevo mi celular a China y me conecto en algún lugar donde alguien más tiene el mismo número de dispositivo se generará algún conflicto.

**A un switch se le puede asignar a cada puerto una sola dirección mac. Solamente un equipo es el** que tiene derecho para conectarse a través de ese outlet. Permitir solamente a un dispositivo conectarse a un puerto. En un banco si desconectamos una compu, y queremos conectar la nuestra no va a ser posible, ya que ese outlet está ligado con una dirección mac. Eso no pasa en el tec que cuando nos conectamos en cualquier outlet nos es permitido obtener direccionamiento ip y nuestra mac trabaja sin ningún conflicto.

Cuando es necesario establecer un mecanismo de seguridad y solamente permitir a un dispositivo con una mac específica conectarse en ese puerto. En caso de que tratemos de conectar un equipo con una mac diferente, esto provoca un conflicto y el switch se protege de manera inmediata bloqueando el puerto.

Esto se consigue cuando configuramos el comando:

1. **switchport port-security mac-address***dirección-mac*

donde se define con claridad cuál es la mac que cada puerto va a poder acceder.

Recordemos que por puerto solamente podemos asignar una única dirección mac. Donde se tiene una relación uno a uno.

1. También la MAC se puede aprender de manera dinámica y permite conectar cualquier dispositivo.
2. En el switch se tiene una tabla de las direcciones MAC donde hay una relación a qué puerto le corresponde que MAC y si es dinámico está tabla se puede borrar después de cierto tiempo en que no haya actividad para que alguien más pueda conectarse.

Los switches también pueden aprender las MACs de manera dinámica.

**switchport port-security mac-address sticky**

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.

SwA(config-if)# switchport port-security mac-address DIRECCION-MAC

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.

SwA(config-if)# switchport port-security

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.

SwA(config-if)# switchport port-security mac-address sticky [DIRECCION-MAC]

Dile al switch que haga “sticky learn” ó en español «aprendizaje pegajoso» para las direcciones MAC aprendidas de forma dinámica usando dentro de la interfaz el comando **switchport port-security mac-address sticky**.

**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.

**Que pasa cuando un puerto está protegido por la configuración de port security y trata de conectarse un dispositivo con una mac no permitida.**

El puerto automáticamente se da de baja. Y la única forma de levantarlo es utilizando la instrucción no shut.

## Acciones de Violación para la Seguridad en el Puerto

**switchport port-security violation {protect | restrict | shutdown}**

|  |  |  |  |
| --- | --- | --- | --- |
| **Opciones de comandos para la violación de puerto con switchport port-security violation** | **Protegido (protect)** | **Restringido (restrict)** | **Shutdown\*** |
| Descartar tráfico ofensivo | Si | Si | Si |
| Envía mensajes de registro y SNMP | No | Si | Si |
| Incrementa el contador de violación por cada violación de trama que llega | No | Si | Si |
| Deshabilita la interfaz poniéndola en estado err-disable y descartando todo el tráfico | No | No | Si |

\*shutdown es la acción de configuración por defecto.

**Para verificar la información de seguridad de los puertos del switch hay un conjunto de comando que podemos utilizar:**

**Sh port-security interface fa 0/18**

En la práctica del día de hoy trabajaremos con un concepto conocido como la vlan 99

**Notas importantes del día de hoy:**

**Por default al momento que arracamos un switch que no tiene configuración todos los puertos se encuentran conectados activos en la vlan 1. La vlan 1 incluye por default los siguientes elementos:**

1. **Todos los puertos pertenecen a la vlan 1**
2. **La vlan de gestión es la número 1.**
3. **La vlan 1 todos sus puertos están activos cuando estos son conectados.**

**Características importantes:**

* **Cualquier persona que desee entrar al sistema va a intentar entrar por la vlan 1.**
* **Las vlans son redes virtuales que como su nombre lo dice son lógicas programables. La vlans es un método para crear redes lógica independientes dentro de una misma red física.**
* **El id máximo que le puedo dar a una vlan es 4094. La primeras 1000 están dedicadas para las conexiones de tipo fastethernet / gigaethernet.**

En el laboratorio hay que crear un topología como la que se muestra en la imagen, el router a insertar es un modelo 4321 para que sea consistente con la práctica y las interfaces a utilizar g0/0/0, g0/0/1 y el switch 2960

En la primera parte se tienen las configuraciones globales del router y del switch.

Estos son los comandos que vamos a utilizar para tener una comunicación remota via telnet con nuestro switch:

**line vty 0 15**

**password cisco**

**login**

**Vamos a tener una administración distinta, ya no vamos a trabajar con la vlan 1, vamos a tener una migración a una vlan distinta, con la intención de que no van a poder encontrar. Para cisco, el estándar es que la vlan 99 es considerada una vlan de administración.**

Podemos cambiar el nombre y el número desde 1 hasta 1000.

**Tres notas importantes sobre las vlans:**

1. **Las vlan se pueden nombrar**
2. **Para poder configurar la vlan se requiere de una dirección ip.**
3. **Hay que hacer los movimientos en los puertos para asignarlos a esa vlan.**

**Si la vlan no tiene puertos conectados la vlan no se levanta y aparecerá como down. Por mas que le digan no shutdown si no tenemos puertos asociados no se va a levantar.**

Cuando conectamos una PC a la vlan, la vlan se levanta.

Mover los puertos es definir de qué tipo son:

**Hay dos tipos de puertos:**

1. **Son de acceso (primer nivel de una arquitectura de red es de acceso,)**
2. **Son de tipo trunk (el puerto puede ser troncal)**

Para mover el puerto primero tengo que entrar a la interface

S1(config)# interface f0/5

S1(config-if)# switchport mode access DEFINIR EL PUERTO DE ACCESO

S1(config-if)# switchport access vlan 99 INDICAR ESE PUERTO PERTENECE A LA VLAN 99

S1(config-if)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 99

S1(config-if)# end

Si no tenemos puerta de enlace predeterminada no vamos a poder acceder desde el exterior.

Generar la criptografía, si le damos enter tomará por default el valor numérico de 512, pero si queremos incrementar el número de bits hay que escribir 1024 y después enter. Para tener una criptografía utilizando 1024 bits.

: **ssh –l admin 172.16.99.11**

**Poner el password, acceder al switch con modo enable y hacer sh run y copiarlo en mi práctica.**

**Hay que anexar pruebas de pings y el acceso por ssh.**