UNIVERSIDAD PRIVADA DEL VALLE
LABORATORIO DE REDES Y COMUNICACIÓN DE DATOS II
PRÁCTICA Nº 9

CONFIGURACIÓN DE SEGURIDAD EN EL SWITCH

1. CONOCIMIENTO TEÓRICO REQUERIDO. –

Para lograr una configuración de seguridad efectiva en un switch Cisco, es esencial contar con un sólido conocimiento teórico respaldado por el material proporcionado por Netacad.com. Este conocimiento debe abarcar varios aspectos cruciales. En primer lugar, se requiere una comprensión profunda de los conceptos de VLAN y cómo se utilizan para segmentar el tráfico en la red. Esto implica conocer cómo crear, asignar puertos a VLAN específicas y aplicar prácticas de segmentación para evitar el movimiento no autorizado entre segmentos.

Además, es fundamental dominar las listas de control de acceso (ACL) y su implementación. Esto incluye aprender cómo configurar ACLs basadas en direcciones IP, protocolos y puertos, y cómo aplicarlas en interfaces y puertos específicos para filtrar y controlar el flujo de tráfico de manera precisa. El conocimiento sobre la autenticación de dispositivos a través de protocolos como 802.1X y el uso de port security también es vital. Esto implica entender cómo configurar la autenticación en los puertos y establecer políticas de seguridad para mitigar amenazas como ataques de "spoofing" de direcciones MAC y garantizar que solo dispositivos autorizados accedan a la red. En resumen, el conocimiento teórico requerido en la configuración de seguridad en un switch Cisco, según Netacad.com, involucra una comprensión profunda de VLANs, ACLs, autenticación de dispositivos y otras funciones de seguridad esenciales para crear un entorno de red protegido y resistente ante posibles riesgos.

2. COMPETENCIAS. -

Parte 1: Configurar los dispositivos de red.

- Conectar la red
- Configurar R1
- Configurar y verificar los parámetros básicos del switch

Parte 2: Configurar las VLAN en los Switches.

- Configurar la VLAN 10.
- Configurar el SVI para VLAN 10.
- Configurar la VLAN 333 con el nombre Native en S1 y S2.
- Configurar la VLAN 999 con el nombre ParkingLot en S1 y S2.

Parte 3: Configurar la seguridad del Switch.

- Implemente el enlace troncal 802.1Q.
- Configure los puertos de acceso.

- Asegure y deshabilite los puertos del switch no utilizados.
- Documentar e implementar funciones de seguridad de los puertos.
- Implemente la seguridad de DHCP snooping.
- Implemente PortFast y la protección BPDU.
- Verifique la conectividad de extremo a extremo.

3. MATERIALES, REACTIVOS Y EQUIPOS. –

EQUIPOS			
Cantidad	Unidad	Descripción	Observaciones
1	Pza	Router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.4 o comparable)	La práctica es para 1 grupo de 2 estudiantes, la capacidad del Laboratorio es de 10 grupos
2	Pza	SWITCH CISCO (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)	
2	Pza	PC (Windows con un programa de emulación de terminal, como Tera Term)	
INSUMOS			
Cantidad	Unidad	Descripción	Observaciones
2	Pza	CABLE DE CONSOLA	La práctica es para 1 grupo de 2 estudiantes, la capacidad del Laboratorio es de 10 grupos
4	Pza	CABLE ETHERNET	

4. TECNICA O PROCEDIMIENTO. –

Parte 2: Configurar los dispositivos de red.

Paso 2: Conecte la red.

a. Realice el cableado de red tal como se muestra en la topología.
b. Inicializar los dispositivos.

Paso 3: Configurar R1

e. Cargue el siguiente script de configuración en R1.

```
enable
configure terminal
hostname R1
```

```
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 description Link to S1 Port 5
 ip dhcp relay information trusted
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
línea con 0
 logging synchronous
 exec-timeout 0 0
```

f. Verifique la configuración en ejecución en R1 con el siguiente comando:

R1# **show ip interface brief**

c. Verifique que el direccionamiento IP y las interfaces estén en un estado activo / activo (solucione los problemas según sea necesario).

Paso 4: Configure y verifique los parámetros básicos del switch.

g. Configure el nombre de host para los switches S1 y S2.

h. Evite búsquedas DNS no deseadas en ambos switches.

i. Configure las descripciones de interfaz para los puertos que están en uso en S1 y S2.

a. Establezca la puerta de enlace predeterminada para la VLAN de administración en 192.168.10.1 en ambos switches.

Parte 3: Configure las VLAN en los Switches.

Paso 2: Configure la VLAN 10.

Agregue la VLAN 10 a S1 y S2 y asigne un nombre a la VLAN de administración **Management.**

Paso 3: Configure el SVI para VLAN 10.

Configure la dirección IP de acuerdo con la Tabla de Direccionamiento para SVI para VLAN 10 en S1 y S2. Habilite las interfaces SVI y proporcione una descripción para la interfaz.

Paso 4: Configure la VLAN 333 con el nombre Native en S1 y S2.

Paso 5: Configure la VLAN 999 con el nombre ParkingLot en S1 y S2.

Paso 6: Implemente el enlace 802.1Q.

a. En ambos switches, configure el enlace troncal en F0/1 para usar la VLAN 333 como la VLAN nativa.

b. Verifique que el enlace troncal esté configurado en ambos switches.

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan
Fa0/1 en 802.1q trunking 333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999

S2# **show interface trunk**

Port Mode Encapsulation Status Native vlan
Fa0/1 en 802.1q trunking 333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999

c. Deshabilite la negociación DTP en F0/1 en S1 y S2.

d. Verifique con el comando **show interfaces** .

S1# **show interfaces f0/1 switchport | include Negotiation**
Negotiation of Trunking: Off
S2# **show interfaces f0/1 switchport | include Negotiation**
Negotiation of Trunking: Off

Paso 7: Configure los puertos de acceso.

a. En S1, configure F0/5 y F0/6 como puertos de acceso asociados con la VLAN 10.

b. En S2, configure F0/18 como un puerto de acceso asociado con la VLAN 10.

Paso 2: Asegure y deshabilite los puertos de conmutación no utilizados.

a. En S1 y S2, mueva los puertos no utilizados de la VLAN 1 a la VLAN 999 y desactive los puertos no utilizados.

b. Verifique que los puertos no utilizados estén deshabilitados y asociados con la VLAN 999 emitiendo el comando **show interfaces status** .

S1# **show interfaces status**
Port Name Status Vlan Duplex Speed Type
Fa0/1 Link to S2 connected trunk a-full a-100 10/100BaseTX
Fa0/2 disabled 999 auto auto 10/100BaseTX
Fa0/3 disabled 999 auto auto 10/100BaseTX
Fa0/4 disabled 999 auto auto 10/100BaseTX
Fa0/5 Link to R1 connected 10 a-full a-100 10/100BaseTX
Fa0/6 Link to PC-A connected 10 a-full a-100 10/100BaseTX
Fa0/7 disabled 999 auto auto 10/100BaseTX
Fa0/8 disabled 999 auto auto 10/100BaseTX
Fa0/9 disabled 999 auto auto 10/100BaseTX
Fa0/10 disabled 999 auto auto 10/100BaseTX
<output omitted>
S2# **show interfaces status**
Port Name Status Vlan Duplex Speed Type
Fa0/1 Link to S1 connected trunk a-full a-100 10/100BaseTX
Fa0/2 disabled 999 auto auto 10/100BaseTX
Fa0/3 disabled 999 auto auto 10/100BaseTX
<output omitted>
Fa0/14 disabled 999 auto auto 10/100BaseTX
Fa0/15 disabled 999 auto auto 10/100BaseTX
Fa0/16 disabled 999 auto auto 10/100BaseTX
Fa0/17 disabled 999 auto auto 10/100BaseTX
Fa0/18 Link to PC-B connected 10 a-full a-100 10/100BaseTX
Fa0/19 disabled 999 auto auto 10/100BaseTX
Fa0/20 disabled 999 auto auto 10/100BaseTX
Fa0/21 disabled 999 auto auto 10/100BaseTX
Fa0/22 disabled 999 auto auto 10/100BaseTX
Fa0/23 disabled 999 auto auto 10/100BaseTX
Fa0/24 disabled 999 auto auto 10/100BaseTX
Gi0/1 disabled 999 auto auto 10/100/1000BaseTX
Gi0/2 disabled 999 auto auto 10/100/1000BaseTX

Paso 3: Documentar e implementar funciones de seguridad portuaria.

Las interfaces F0/6 en S1 y F0/18 en S2 están configuradas como puertos de acceso. En este paso, también configurará la seguridad del puerto en estos dos puertos de acceso.

a. En S1, haga el comando**show port-security interface f0/6** para mostrar la configuración de seguridad de puerto predeterminada para la interfaz F0/6. Registre sus respuestas en la tabla a continuación.

Configuración de seguridad de puerto predeterminada	
Característica	**Configuración Predeterminada**
Seguridad de puertos	
Número máximo de direcciones MAC	
Modo de Violación	
Tiempo de Vencimiento	
Tipo de Vencimiento	
Vencimiento seguro de la dirección estática	
Dirección MAC Sticky	

b. En S1, habilite la seguridad del puerto en F0/6 con la siguiente configuración:
   - Número máximo de direcciones MAC: **3**
   - Tipo de violación: **restrict**
   - Tiempo de vencimiento: **60 min**
   - Tipo de vencimiento: **inactivity**

c. Verifique la seguridad del puerto en S1 F0/6.

S1# **show port-security interface f0/6**
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Restrict
Aging Time : 60 mins
Aging Type : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 3
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0022.5646.3411:10
Security Violation Count : 0
S1# **show port-security address**
Secure Mac Address Table

Vlan Mac Address Type Ports Remaining Age

(mins)
--- ----------- --- ----- -------------
10 0022.5646.3411 SecureDynamic Fa0/6 60 (I)

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192

d. Habilite la seguridad del puerto para F0/18 en S2. Configure el puerto para agregar direcciones MAC aprendidas en el puerto automáticamente a la configuración en ejecución.

e. Configure las siguientes configuraciones de seguridad de puerto en S2 F 0/18:
   - Número máximo de direcciones MAC: **2**
   - Violation type: **Protect**
   - Tiempo de vencimiento: **60 min**

f. Verifique la seguridad del puerto en S2 F0/18.

S2# **show port-security interface f0/18**
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 60 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0022.5646.3413:10
Security Violation Count : 0

S2# **show port-security address**
Secure Mac Address Table

Vlan Mac Address Type Ports Remaining Age
(mins)
--- ----------- --- ----- -------------
10 0022.5646.3413 SecureSticky Fa0/18 -

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192

Paso 4: Implemente la seguridad de DHCP snooping.

a. En S2, habilite la inspección DHCP y configure la inspección DHCP en la VLAN 10.

b. Configure el puerto troncal en S2 como un puerto confiable.

c. Limite el puerto no confiable, F18 en S2, a cinco paquetes DHCP por segundo.

a. Verifique la inspección DHCP en S2.

S2# **show ip dhcp snooping**
Switch DHCP snooping is enabled
DHCP snooping está configurado en las siguientes VLANs;
10
DHCP snooping es operacional en las siguientes VLANs;
10
DHCP snooping está configurado en las siguientes interfaces L3
Inserción de opción 82 habilitada
circuit-id default format: vlan-mod-port
remote-id: 0cd9.96d2.3f80 (MAC)
La Opción 82 en puertos no confiables no es permitida.
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping está configurado en las siguientes interfaces L3
Interface Trusted Allow option Rate limit (pps)
---------- ------- ---------- ----------
FastEthernet0/1 yes yes unlimited
Custom circuit-ids:
FastEthernet0/18 no no 5
Custom circuit-ids:

b. Desde el símbolo del sistema en la PC-B, suelte y luego renueve la dirección IP.

C:\Users\Student> **ipconfig /release**
C:\Users\Student> **ipconfig /renew**

c. Verifique el enlace de iDHCP snooping utilizando el comando **show ip dhcp snooping binding**.

S2# **show ip dhcp snooping binding**
MacAddress IpAddress Lease(sec) Type VLAN Interface
---------- ---------- ---------- ---------- ---- ----------
00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18
Total number of bindings: 1

Paso 3: Implemente PortFast y la protección BPDU.

a. Configure PortFast en todos los puertos de acceso que están en uso en ambos switches.

b. Habilite la protección BPDU en los puertos de acceso VLAN 10 S1 y S2 conectados a la PC-A y PC-B.

c. Verifique que la protección BPDU y PortFast estén habilitados en los puertos apropiados.

S1# **show spanning-tree interface f0/6 detail**
Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.6.
<output omitted for brevity>

Number of transitions to forwarding state: 1
The port is in the portfast mode
Link type is point-to-point by default
Bpdu guard is enabled
BPDU: sent 128, received 0

Paso 4: Verifique la conectividad de extremo a extremo.

Verifique la conectividad PING entre todos los dispositivos en la Tabla de Direccionamiento IP. Si los ping fallan, es posible que deba deshabilitar el firewall en los hosts de la PC

5. TIEMPO DE DURACIÓN DE LA PRÁCTICA. –

Se estima 1 sesión de 2 periodos de 50 minutos en laboratorio para la elaboración de esta práctica.

6. MEDICIÓN, CÁLCULOS Y GRAFICOS. –

Topología

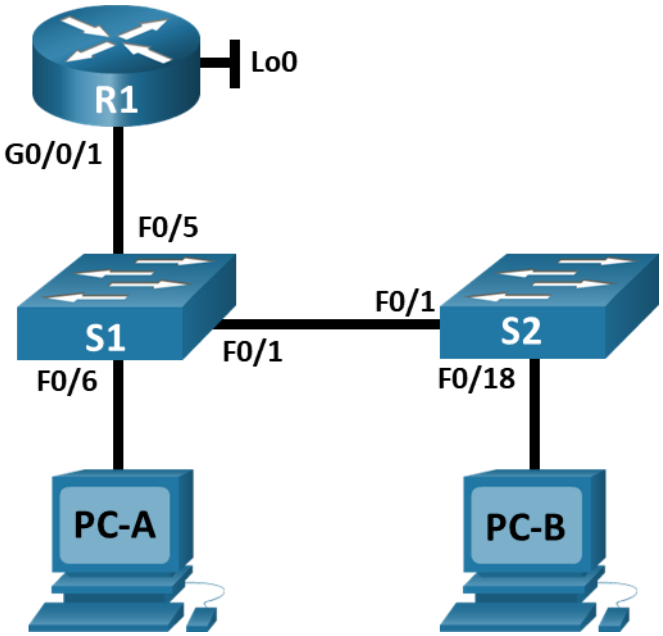

Tabla de asignación de direcciones

Dispositivos	Interface / VLAN	Dirección IP	Máscara de Subred
R1	G0/0/1	192.168.10.1	255.255.255.0
	Bucle invertido 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

7. CUESTIONARIO. –

1. En referencia a Port Security en S2, ¿por qué no hay un valor de temporizador para la edad restante en minutos cuando se configuró el aprendizaje permanente?
2. En referencia a Port Security en S2, si carga el script de configuración en ejecución en S2, ¿por qué la PC-B en el puerto 18 nunca obtendrá una dirección IP a través de DHCP?
3. En referencia a Port Security, ¿cuál es la diferencia entre el tipo de envejecimiento absoluto y el tipo de envejecimiento por inactividad?