UF2. Administració de dispositius de xarxa

NF3. Seguretat al switch

NF3.2. Configuracions de seguretat al switch

Laboratori1. Configuració de seguretat al switch

Nom: Cognoms:

Índex de la pràctica

Entrega

- Format PDF amb el nom del fitxer: **UF2_NF3.2_L1_Cognom_Nom.pdf**
- Es valorarà positivament que l'activitat sigui ordenada, estructurada i ben documentada, amb captures de pantalla quan sigui el cas.
- Es valorarà positivament que documentis els inconvenients que trobis i la solució que hagis donat.
- Es valorarà negativament aquelles activitats que es presenten incompletes.

Introducció

En aquest laboratori treballarem les diferents característiques de la seguretat de capa 2 que podem implementar en un switch. Els objectius que perseguim aconseguir són els següents:

Part 1: Configurar els dispositius de xarxa.

- Connectar la xarxa.
- Configurar R1.
- Configurar i verificar els paràmetres bàsics del switch.

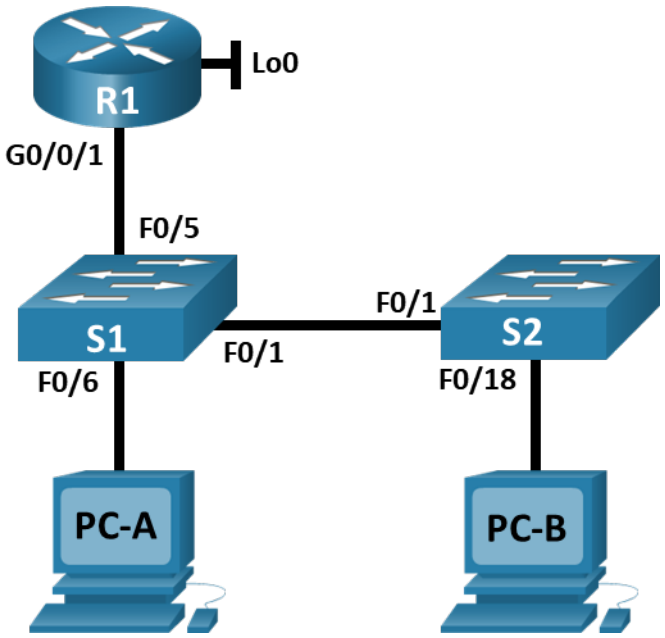
Part 2: Configurar les VLAN als Switches.

- Configurar la VLAN 10.
- Configurar la SVI per a VLAN 10.
- Configurar la VLAN 333 amb el nom Nativa a S1 i S2.
- Configurar la VLAN 999 amb el nom Sith a S1 i S2.

Part 3: Configurar la seguretat al Switch.

- Implementar l'enllaç troncal 802.1Q.
- Configurar els ports d'accés.
- Assegurar i deshabilitar els ports del switch no utilitzats.
- Documentar i implementar funcions de seguretat dels ports.
- Implementar la seguretat DHCP snooping.
- Implementar PortFast i la protecció BPDU.
- Verificar la connectivitat extrem a extrem.

Topologia



Taula d'assignació de direccions

Dispositius	Interface / VLAN	Direcció IP	Màscara de Subxarxa
R1	G0/0/1	192.168.10.1	255.255.255.0
	Loopback0	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

Recursos necessaris

- 2 Switchs (Cisco 2960 amb IOS Release 15.2 lanbasek9 o semblant).
- 1 Router (Cisco 4221 amb imatge universal Cisco IOS XE version 16.9.3 o semblant)
- 2 PC (windows o linux amb un programa d'emulació de terminal, MiniCom, Tera Term, ...).
- Cables de consola per a configurar els dispositius amb IOS Cisco mitjançant els ports de consola.
- Cables Ethernet, tal i com es mostra a la topologia (podem utilitzar cable directe entre routers donat que fan detecció automàtica, en cas contrari hauria de ser creuat).

Tasques a realitzar

APARTAT 1. Muntar la topologia i configurar els paràmetres bàsics dels dispositius

Pas1: Realitzar les connexions segons marca la topologia i engegar tots els dispositius

1. En cas de que prèviament s'hagin guardat configuracions als switchs o router, hauràs de reinicialitzar-los i carregar la configuració predeterminada.

Pas2: Configurar els paràmetres del router

1. Accedeix al router mitjançant el port de consola i entra al mode EXEC privilegiat
2. Copiar la següent configuració bàsica i pegar-la al router des del mode de configuració global.

```
no ip domain-lookup
hostname nom_grup_R1
service password-encryption
enable secret bolson
banner motd #Di amigo i entra. #
```

3. L'accés al port de la consola també s'ha de restringir amb una contrasenya. Utilitza "*comarca"* com a password d'inici de sessió. Per evitar que els missatges de consola interrompin les comandes es pot utilitzar l'opció logging synchronous.
4. Configura les línies de terminal (vty) per a que el router permeti accés telnet. Utilitza "brandivino" com a password.
5. Exclou les nou primeres direccions utilitzables de la xarxa 192.168.10.0/24, i també les direccions que s'assignaran a la VLAN 10 del S1 i S2.
6. Crea un grup DHCP amb el nom "Numenor_R1".
7. Especifica la xarxa que admet aquest servidor DHCP.
8. Configura com a nom de domini "hobbiton.com"
9. Configura la porta d'enllaç predeterminada amb la @IP del R1.
10. Configura les interfaces del router tal i com s'indica a la taula de direccions.
11. Configura la interface Gigabit com a font confiable de retransmissió DHCP amb la comanda **ip dhcp relay information trusted**
12. Configura l'hora del router. Copia la configuració en execució a la configuració d'inici.

Pas3: Comprova la configuració en execució de R1

1. Comprova amb la comanda adient l'estat de les interfaces i les @IP assignades.

Pas4: Configurar els paràmetres bàsics per a cada switch

1. Accedeix al switch mitjançant el port de consola i entra al mode EXEC privilegiat.
2. Copiar la següent configuració bàsica i pegar-la al switch des del mode de configuració global.

```
no ip domain-lookup
hostname nom_grup_S1/2
service password-encryption
enable secret bolson
banner motd #Di amigo i entra. #
```

3. L'accés al port de la consola també s'ha de restringir amb una contrasenya. Utilitza "*comarca"* com a password d'inici de sessió. Per evitar que els missatges de consola interrompin les comandes es pot utilitzar l'opció logging synchronous.
4. Configura les línies de terminal (vty) per a que el switch permeti accés telnet. Utilitza "brandivino" com a password.
5. Configura les descripcions de cada interface del switch per als ports que estan en ús.
6. Estableix la porta d'enllaç predeterminada per a la VLAN d'administració amb la @IP de R1.
5. Configura l'hora del switch. Copia la configuració en execució a la configuració d'inici.

APARTAT 2. Configurar les VLAN als switchs

Pas1: Crear la VLAN 10

1. Afegeix la VLAN 10 al switch S1 i S2 i assigna-li el nom "Padawans".

Pas2: Configurar la SVI per a la VLAN10

1. Configura la @IP segons la taula de direccionament per a la VLAN10 a S1 i S2, dona una descripció adient i habilita les interfaces.

Pas3: Configurar la VLAN333 amb el nom Nativa a S1 i S2

Pas4: Configurar la VLAN999 amb el nom Sith a S1 i S2

APARTAT 3. Configura la seguretat del switch

Pas1: Implementar l'enllaç troncal 802.1Q

1. Als dos switchs configura l'enllaç troncal a F0/1 per a que utilitzi la VLAN 333 com la VLAN nativa.
2. Verifica l'estat de l'enllaç troncal als dos switchs
3. Deshabilita la negociació DTP a la interface F0/1 de S1 i S2.
4. Verificar l'acció de la pregunta anterior amb la comana show interfaces i els paràmetres adients per a que només ens mostri que la negociació està deshabilitada.

Pas2: Configurar els ports d'accés

1. A S1, configura F0/5 i F0/6 com a ports d'accés associats a la VLAN10.
2. A S2, configura F0/18 com a port d'accés associat a la VLAN10.

Pas3: Asegurar i deshabilitar els ports d'accés no utilitzats

1. A S1 i S2, assigna els ports no utilitzats de la VLAN1 a la VLAN999 i desactiva'ls.
2. Verifica amb la comanda adient que els ports no utilitzats estan desabilitats i associats a la VLAN999.

Pas4: Documentar i implementar funcions de seguretat
Les interfaces F0/6 a S1 i F0/18 a S2 estan configurades com a ports d'accés, en aquest pas configurarem la seguretat de port en aquests dos ports d'accés

1. A S1 executa la comanda **show port-security interface f0/6** per veure la configuració de seguretat de port predeterminada, emplena amb el resultat d'aquesta comanda la següent taula.

Configuració de seguretat de port predeterminada	
Paràmetre	Valor Predeterminat
Seguretat de port	
Número màxim de direccions MAC	
Mode de Violació	
Temps d'envelliment	
Tipus d'envelliment	
Envelliment segur de la direcció estàtica	
Direcció MAC Sticky	

Important: S'ha d'indicar exactament d'on treieu el valor que doneu a cada paràmetre.

2. A S1 configura i habilita la seguretat del port a F0/6 amb els següents valors.
   - Número màxim de @MAC: 3.
   - Tipus de violació: restrict.
   - Temps d'envelliment: 60 min.
   - Tipus d'envelliment: inactivity.
3. Verifica la seguretat del port al switch S1 per al port F0/6.
4. A S2 configura i habilita la seguretat del port a F0/18. Configura el port per a que afegeixi de forma automàtica a la configuració en execució direccions MAC apreses pel port.
5. Configura els següents paràmetres a la seguretat del port F0/18 del switch S2.
   - Número màxim de @MAC: 2.
   - Tipus de violació: protect.
   - Temps d'envelliment: 60 min.
6. Verifica la seguretat del port al switch S2 per al port F0/18.

Pas5: Implementar la seguretat DHCP snooping

1. A S2, habilita la inspecció DHCP i posteriorment assigna-la a la VLAN 10.
2. Configura el port troncal de S2 com un port confiable.
3. Al port no confiable de S2, limita a cinc els paquets DHCP per segon. Per què és un port no confiable?
4. Utilitza la comanda adient per verificar la inspecció DHCP a S2.
5. Des del terminal del PC-B, allibera la @IP que tinguis assignada, posteriorment fes una petició al servei DHCP del router per a que t'assigni una nova @.
6. Verfica l'enllaç DHCP snoopoing amb la comanda adient. Comenta els resultats obtinguts.

Pas6: Implementar PortFast i la protecció BPDU

1. Configura PortFast a tots els ports d'accés que s'estiguin utilitzant, tant al switch S1 com S2.
2. Habilita la protecció BPDU als ports d'accés de la VLAN10 al switch S1 i S2 connectats al PC-A i PC-B.

3. Verifica que la protecció BPDU i PortFast estigui habilitada als ports pertinents. Comenta els resultats obtinguts

Pas7: Verifica la connectivitat extrem a extrem

1. Verifica la connectivitat mitjançant la comanda ping entre tots els dispositius de la taula de direccionament.