DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.7**	**Práctica 4**	Seguridad en la Capa 2				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	30/04/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet.		CP1-1	

1. Objetivo(s) de la actividad

- Conocer los tipos de listas de control de acceso.

2. Introducción

Las restricciones en los dispositivos de red permiten implementar la seguridad desde el enfoque físico, en la interconectividad de la red.

3. Objetivos

- Asignar el Switch Central como el puente raíz.
- Asegurar Parámetros de Spanning-Tree para prevenir ataques de manipulación STP.
- Activar el control de tormentas para evitar las tormentas de Broadcast.
- Habilitar la seguridad del puerto para prevenir los ataques de desbordamiento de la tabla de direcciones MAC.

4. Instrucciones de la actividad

1. Usar el archivo de ejemplo de prácticas para realizar el reporte esta actividad.
2. Tomar impresiones de pantalla completa de la actividad, (recuerdas ir haciendo las impresiones conforme vas realizando la práctica en el simulador), con tu nombre en la impresión.
3. Subir el reporte terminado de WORD y el archivo de PACKET TRACERT, dar clic para marcar como entregada la actividad.

5. Resumen

LDAP

LDAP son las siglas de Lightweight Directory Access Protocol. Es un protocolo de aplicación estándar de la industria y neutral para el proveedor que se utiliza para acceder y administrar servicios de información de directorio y proporciona un medio para administrar la membresía de usuarios y grupos almacenados en Active Directory. Fue desarrollado por Tim Howes, Steve Kille y Wengyik Yeong en 1993. Originalmente, LDAP era solo un protocolo de red utilizado para obtener datos de un directorio X.500 (una serie de estándares de redes informáticas que cubren los servicios de directorio electrónico).El Protocolo ligero de acceso a directorios (LDAP) es un protocolo de Internet que funciona en TCP / IP y se utiliza para acceder a la información de los directorios. El protocolo LDAP se utiliza básicamente para acceder a un directorio activo.

Kerberos

Kerberos proporciona un servidor de autenticación centralizado cuya función es autenticar a los usuarios en los servidores y los servidores a los usuarios. En la autenticación Kerberos, el servidor y la base de datos se utilizan para la autenticación del cliente. Kerberos se ejecuta como un servidor de confianza de terceros conocido como Centro de distribución de claves (KDC). Cada usuario y servicio de la red es un principal.

Referencias

Ernesto. A. (31/10/2019). Lightweight Directory Access Protocol (LDAP) Recuperado el 27/04/2021 de: https://www.geeksforgeeks.org/lightweight-directory-access-protocolldap/

(17/09/2020). Kerberos. Recuperado el 27/04/2021 de: https://www.geeksforgeeks.org/kerberos/

6. Material y Equipo

- Computadora
- Acceso a Packet Tracer

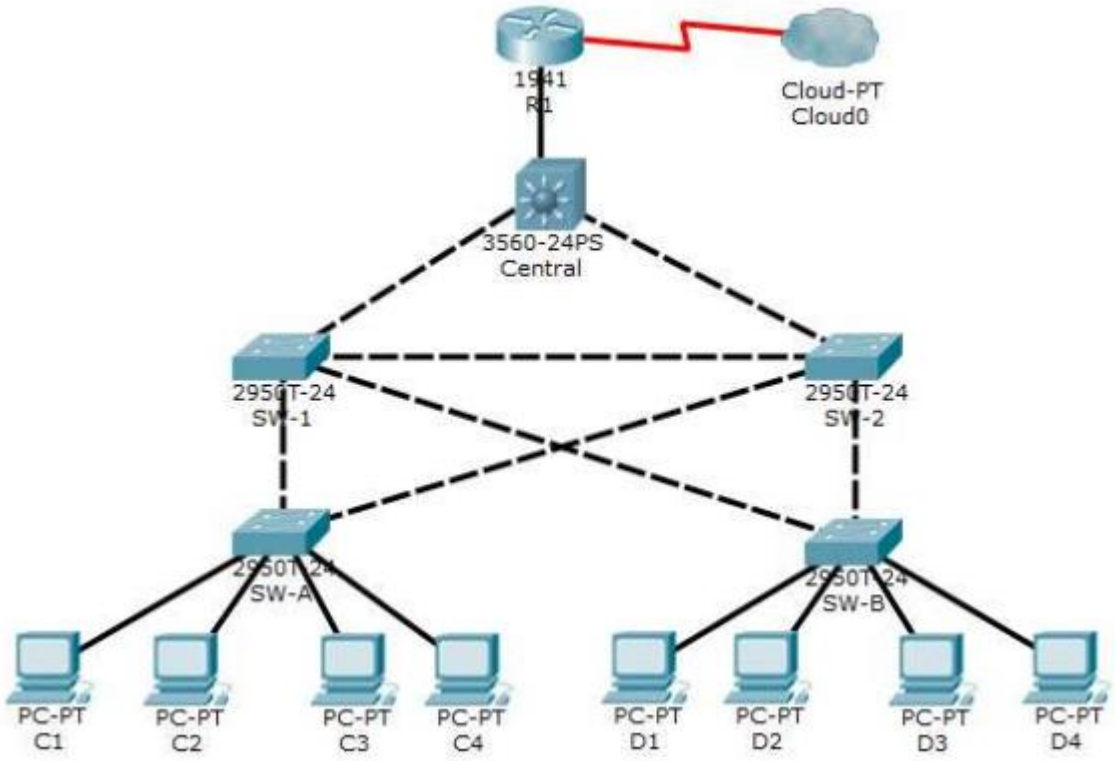
7. Desarrollo

- Tabla de Comandos

Tabla de Comandos
`spanning-tree vlan 1 root primary`
`interface range fi/Ri - Rf`
`spanning-tree guard root`
`spanning-tree portfast`
`spanning-tree bpduguard enable`
`switchport mode access`
`switchport port-security`
`switchport port-security maximum 2`
`switchport port-security violation shutdown`

```
switchport port-security mac-address sticky
```

• Topología



• Procedimiento

Part 1: Configure Root Bridge

Step 1: Determine the current root bridge.

From **Central**, issue the **show spanning-tree** command to determine the current root bridge, to see the ports in use, and to see their status.

Which switch is the current root bridge?

Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Step 2: Assign Central as the primary root bridge.

Using the **spanning-tree vlan 1 root primary** command, and assign **Central** as the root bridge.

Step 3: Assign SW-1 as a secondary root bridge.

Assign **SW-1** as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

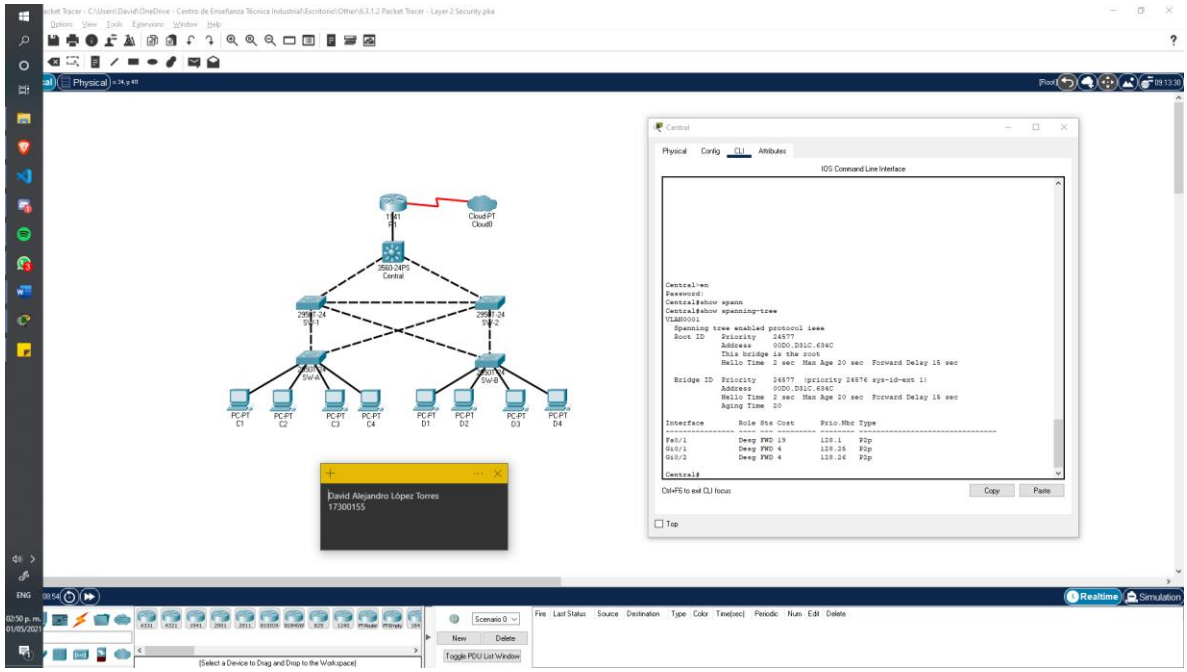
Step 4: Verify the spanning-tree configuration.

Issue the **show spanning-tree** command to verify that **Central** is the root bridge.

```
Central# show spanning-tree
VLAN0001
   Spanning tree enabled protocol ieee
   Root ID  Priority      24577
            Address       00D0.D31C.634C
            This bridge is the root
            Hello Time  2 sec  Max Age  20 sec   Forward Delay  15 sec
```

Which switch is the current root bridge?

Based on the new root-bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)



Part 2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

Step 1: Enable PortFast on all access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the **SW-A** and **SW-B**, use the **spanning-tree portfast** command.

Step 2: Enable BPDU guard on all access ports.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports. Enable BPDU guard on **SW-A** and **SW-B** access ports.

Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard enable** command in interface configuration mode or the **spanning-tree portfast bpduguard default** command in global configuration mode. For grading purposes in this activity, please use the **spanning-tree bpduguard enable** command.

Step 3: Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the **show spanning-tree** command to determine the location of the root port on each switch.

On **SW-1**, enable root guard on ports F0/23 and F0/24. On **SW-2**, enable root guard on ports F0/23 and F0/24.

Part 3: Configure Port Security and Disable Unused Ports

Step 1: Configure basic port security on all ports connected to host devices.

This procedure should be performed on all access ports on **SW-A** and **SW-B**. Set the maximum number of learned MAC addresses to **2**, allow the MAC address to be learned dynamically, and set the violation to **shutdown**.

Note: A switch port must be configured as an access port to enable port security.

Why is port security not enabled on ports that are connected to other switch devices?

Step 2: Verify port security.

a. On **SW-A**, issue the command **show port-security interface f0/1** to verify that port security has been configured.

```
SW-A# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

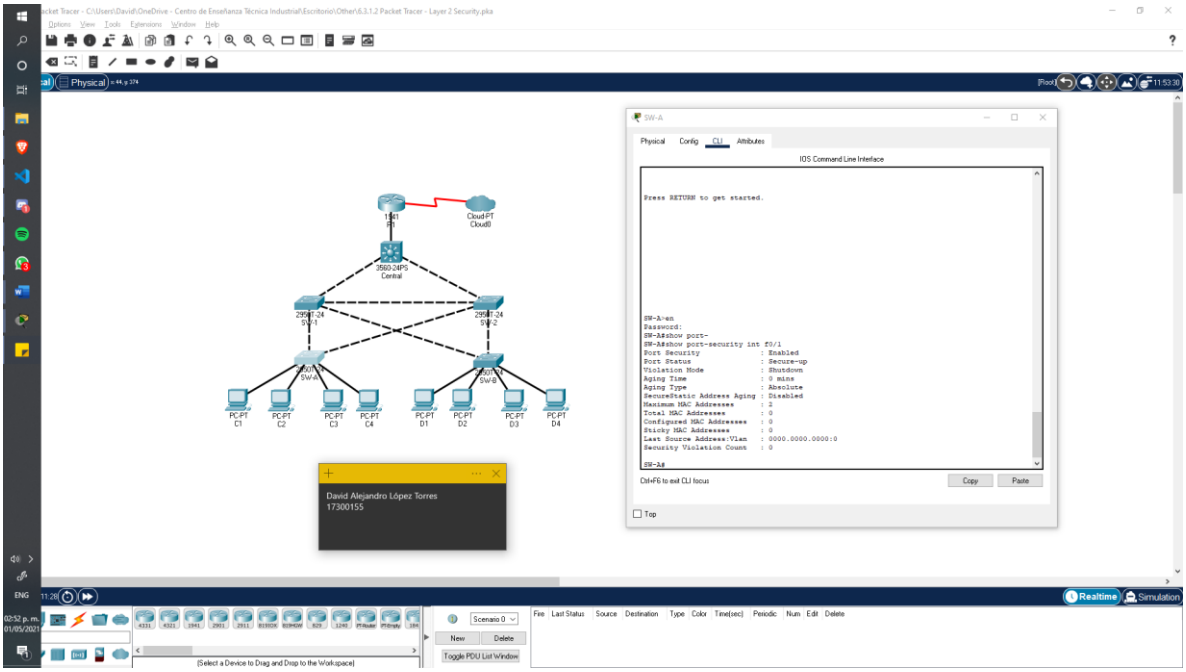
b. Ping from **C1** to **C2** and issue the command **show port-security interface f0/1** again to verify that the switch has learned the MAC address for **C1**.

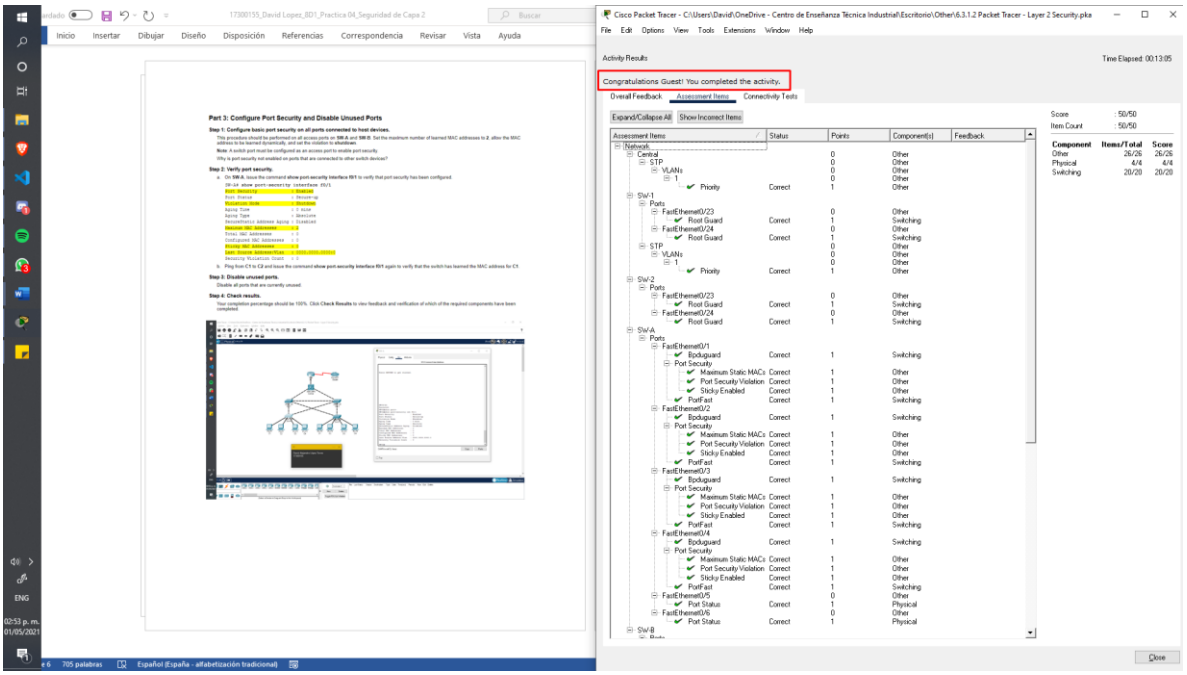
Step 3: Disable unused ports.

Disable all ports that are currently unused.

Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to view feedback and verification of which of the required components have been completed.





8. Observaciones

No hubo muchas diferencias a las indicaciones mostradas en las instrucciones y su correspondiente implementación, solo La característica “Spanning-Tree” BPDU guard, puede ser activada en cada puerto individual utilizando el comando “spanning-tree bpduguard enable” en el modo de configuración de interfaz, de otra forma puede marcar un error de sintaxis.

9. Conclusiones

Con esta práctica se ha implementado una configuración de seguridad en los switches y no solo en los routers de la red. Hemos visto cómo configurar adecuadamente los puertos puede ser de gran utilidad para evitar potenciales ataques STP. Además, prevenimos el “spoofing” y los “rogué switches” activando el guardia BPDU. Por último, deshabilitamos los puertos que no se están utilizando. Es importante resaltar que esta configuración es complementaria a las diferentes implementaciones que hemos visto ya con los routers, por lo que representa una extensión a la seguridad de nuestra red.

10. Referencias

Ernesto. A. (31/10/2019). Lightweight Directory Access Protocol (LDAP) Recuperado el 27/04/2021 de: https://www.geeksforgeeks.org/lightweight-directory-access-protocolldap/

(17/09/2020). Kerberos. Recuperado el 27/04/2021 de: https://www.geeksforgeeks.org/kerberos/