DATOS DE LA ACTIVIDAD							
No. de Actividad:	**3.4**	**Práctica 5**	Seguridad en VLAN la Capa 2				
Unidad:	3: Configuración de SSH y VPN						
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:	30/05/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet.		CP1-1	

1. Objetivo(s) de la actividad

- Conecte un nuevo enlace redundante entre SW-1 y SW-2.
- Habilitar Trunking y configurar la seguridad en el nuevo enlace troncal entre SW-1 y SW-2.
- Crear una nueva VLAN de administración (VLAN 20) y agregar una PC de administración a esa VLAN.
- Implementar en ACL para evitar el acceso de usuarios externos a la VLAN de administración.

2. Introducción

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

3. 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, (recuerda 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

4. Resumen

Seguridad en VLANs

VLANs (Red de área local y virtual), consiste en dos o más redes de ordenadores que se comportan como si estuviesen conectados al mismo equipo informático, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local, es decir, un administrador puede disponer de varias VLANs dentro de un mismo router, agrupando los equipos de un determinado segmento de red. Los principales tipos de VLAN se componen por estáticas y dinámicas, siendo las VLAN estáticas las que se configuran manualmente mediante la asignación de puertos a una VLAN, y las dinámicas usan una base de datos que almacena una asignación de VLAN a MAC para determinar la VLAN a la que está conectado un host en particular, permitiendo que los hosts se muevan dentro de la red en lugar de las redes estáticas.

Tipos de VLAN

Las redes de área local virtuales se pueden clasificar según el nivel del modelo OSI:

- VLAN de nivel 1

Define una red virtual según el puerto del switch utilizado, también conocida como “port switching”, suele ser la más habitual y la que implementan la mayoría de los switches del mercado.

- VLAN de nivel 2

Define una red virtual según las direcciones MAC de los equipos. Frente a la VLAN por puerto, tiene la ventaja de que los equipos pueden cambiar de puerto, pero hay que asignar todas las direcciones MAC una a una.

- VLAN de nivel 3

Hay diferentes tipos de VLAN de nivel 3, dentro de esta se encuentran:
-- VLAN basada en la dirección de red que conecta subredes según la dirección IP de los equipos.
-- VLAN basada en protocolo, permite crear una red virtual por tipo de protocolo utilizado.

Si configura una red de área local virtual (VLAN), las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales.

1. Al usar VLAN, separe los clústeres sensibles de sistemas del resto de la red. De esta manera, se reduce la probabilidad de que los usuarios tengan acceso a la información almacenada en esos clientes y servidores.
2. Asigne un número de VLAN nativo único a los puertos de enlace troncal.
3. Limite las VLAN que se pueden transportar mediante un enlace troncal a las que son estrictamente necesarias.
4. Desactive el protocolo de enlace troncal (VTP) de VLAN, si es posible. De lo contrario, configure lo siguiente para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.
5. Utilice configuraciones de VLAN estáticas, cuando sea posible.
6. Desactive los puertos de conmutador no utilizados y asígneles un número de VLAN que no esté en uso.

Posibles ataques por medio de VLAN:

VLAN Hopping

Es una vulnerabilidad de seguridad que puede aparecer en entornos LAN, donde los Switch están conectados por puertos troncales. Además, trataremos algunas posibilidades de configuración para evitar el problema de seguridad.
Un atacante intenta obtener acceso a una VLAN no autorizada mediante la adición de dos etiquetas en los paquetes salientes desde el cliente, esto se llama doble etiquetado. Estas etiquetas se agregan a los paquetes que identifican a qué VLAN pertenecen (VLAN ID).
La primera etiqueta (802.1Q) es leída por el puerto de línea externa en el primer switch al que el cliente-atacante está conectado, donde es eliminada y no se vuele a etiquetar por otra y la envía al siguiente switch, en el segundo troncal se lee la segunda etiqueta que envía tráfico desde el atacante a los clientes con el mismo ID de VLAN como la segunda etiqueta y por ende estos datos serán reenviados.
Forma de evitarla: Configuración de ACL – listas de control de acceso con direccionamiento e incluso con filtrado de MAC address. También podemos configurar los puertos libres del switch en modo shutdown y asociarlos a una VLAN que no tenga tráfico de datos. Los puertos Troncales se configurarán con una VLAN nativa que no emita tráfico de datos. ACTIVADO – NO NEGOCIANDO

Snooping attack

Estos ataques pueden ocurrir sobre varios protocolos permitiendo a un atacante realizar ataques de man-in-the-middle (MITM), de tal manera que tras el ataque todo el tráfico fluye por el equipo del atacante antes de enviárselo al router, switch o equipo de destino. Donde el atacante adquiere control y permisos para leer, insertar y modificar las comunicaciones.
El ataque de DHCP Spoofing lo podremos evitar mediante la característica DHCP Snooping de Cisco, mientras que los ataques de ARP Spoofing los podremos evitar mediante las técnicas de inspección dinámica ARP que viene por defecto en los nuevos switches.
Forma de evitarlos: Se pueden evitar configurando IP Source Guard que uniéndolo a DHCP Snooping el switch conocerá la asociación IP – MAC por puerto, evitando los ataques MitM.

Referencias

(14/08/2020) Seguridad VLANs en entornos virtuales. Recuperado el 24/05/2021 de: https://www.infosecuritymexico.com/es/blog/seguridad-vlans-virtuales.html

Seguridad en las VLANs. Recuperado el 24/05/2021 de: https://techclub.tajamar.es/seguridad-vlans-tipos-ataques/

5. Material y Equipo

- Computadora
- Acceso a Packet Tracer

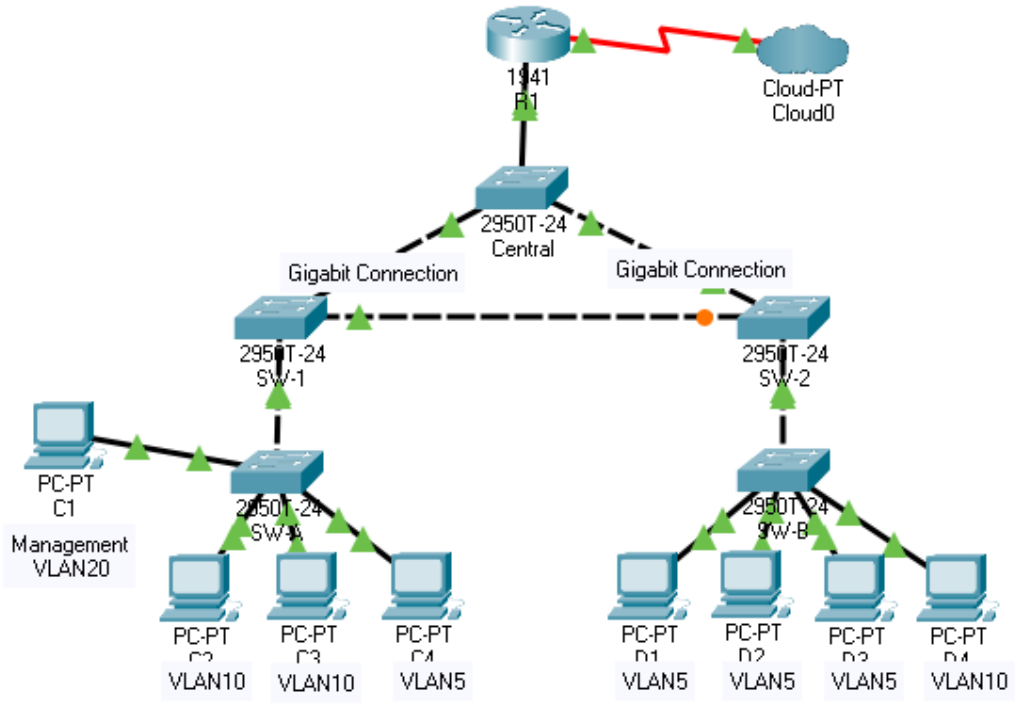
6. Desarrollo

- Tabla de Comandos

Tabla de Comandos
`switchport mode trunk`
`switchport trunk native vlan "N"`

switchport nonegotiate
vlan “N”
interface vlan “N”
switchport access vlan “N”
interface GigabitEthernet0/0.”N” (subinterface)
encapsulation dot1q “N”

- Topología



- Tabla de direcciones

Dispositivo	Interface / vlan	IP	Mascara
R1	G0/0.1	192.168.20.100	255.255.255.0
	G0/0.2	192.168.20.100	255.255.255.0
	G0/0.3	192.168.20.100	255.255.255.0
SW-A	vlan20	192.168.20.1	255.255.255.0
SW-B	vlan20	192.168.20.2	255.255.255.0
SW-1	vlan20	192.168.20.3	255.255.255.0
SW-2	vlan20	192.168.20.4	255.255.255.0
Central	Vlan20	192.168.20.5	255.255.255.0
C1	F0/1 – vlan20	192.168.20.50	255.255.255.0

C2	F0/1 – vlan10	192.168.10.1	255.255.255.0
C3	F0/1 – vlan10	192.168.10.2	255.255.255.0
C4	F0/1 – vlan5	192.168.5.1	255.255.255.0
D1	F0/1 – vlan5	192.168.5.2	255.255.255.0
D2	F0/1 – vlan5	192.168.5.3	255.255.255.0
D3	F0/1 – vlan5	192.168.5.4	255.255.255.0
D4	F0/1 – vlan10	192.168.10.3	255.255.255.0

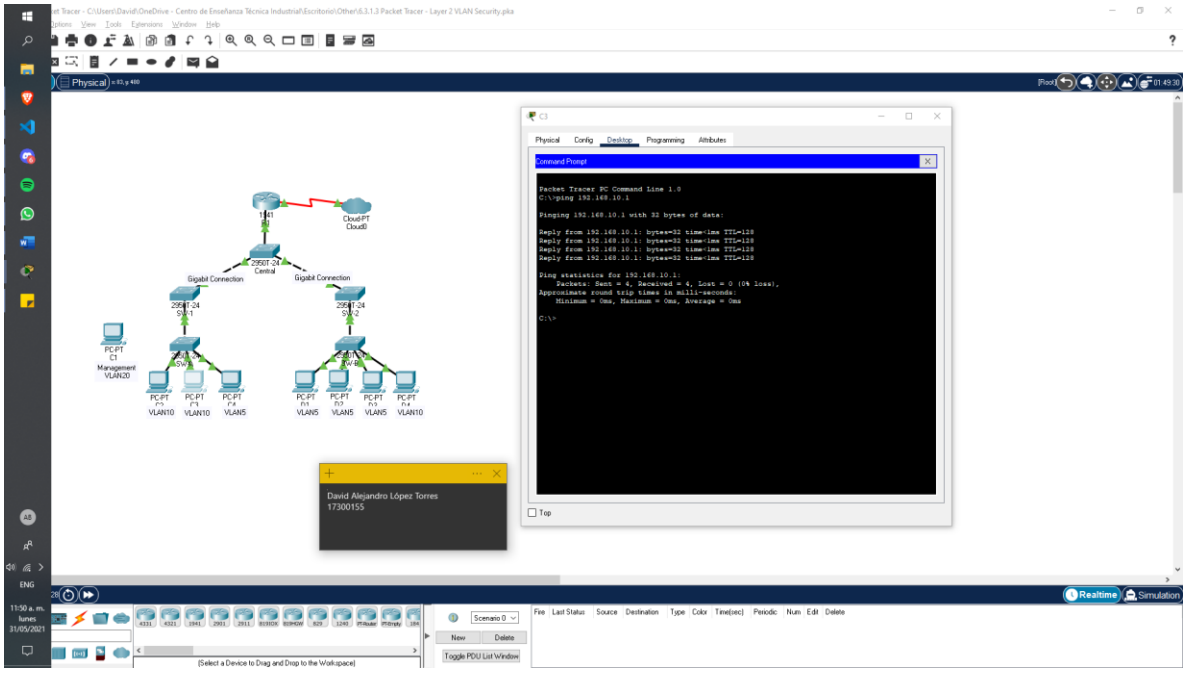
- Procedimiento

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.



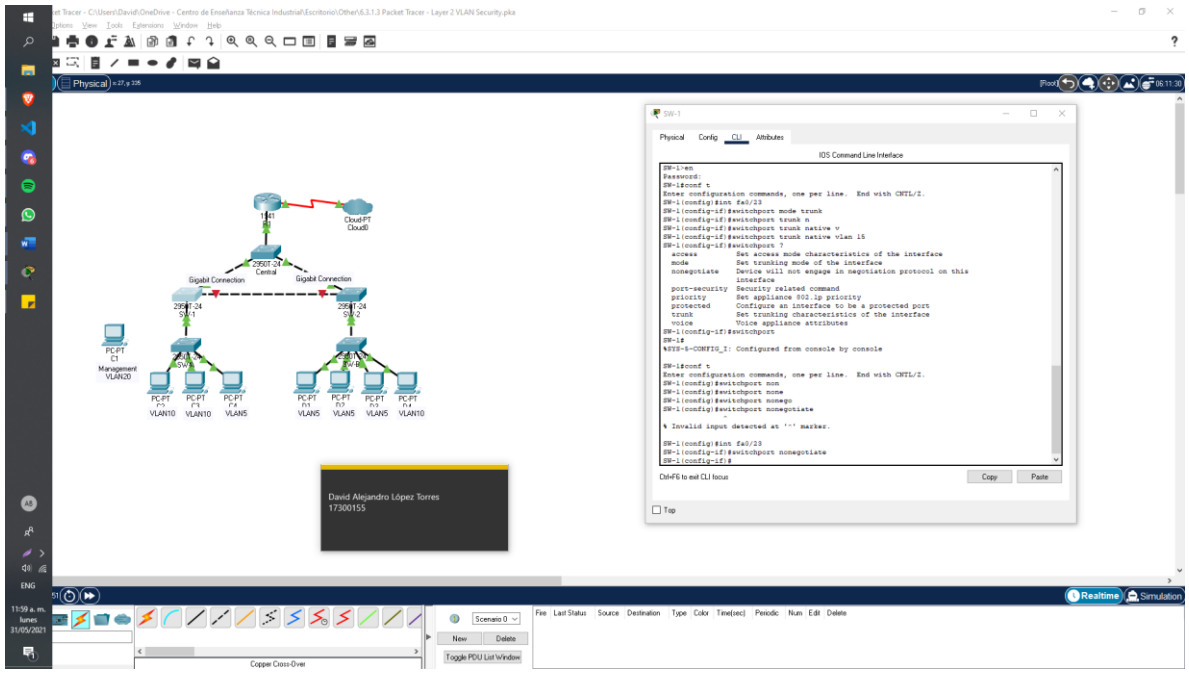
Part 2: Create a Redundant Link Between SW-1 and SW-2

Step 1: Connect SW-1 and SW-2.

Using a crossover cable, connect port F0/23 on **SW-1** to port F0/23 on **SW-2**.

Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both **SW-1** and **SW-2**, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.



Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security purposes, the administrator wants to ensure that all managed devices are on a separate VLAN.

Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on **SW-A**.

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

Step 2: Enable the same management VLAN on all other switches.

a. Create the management VLAN on all switches: **SW-B**, **SW-1**, **SW-2**, and **Central**.

b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

Step 3: Connect and configure the management PC.

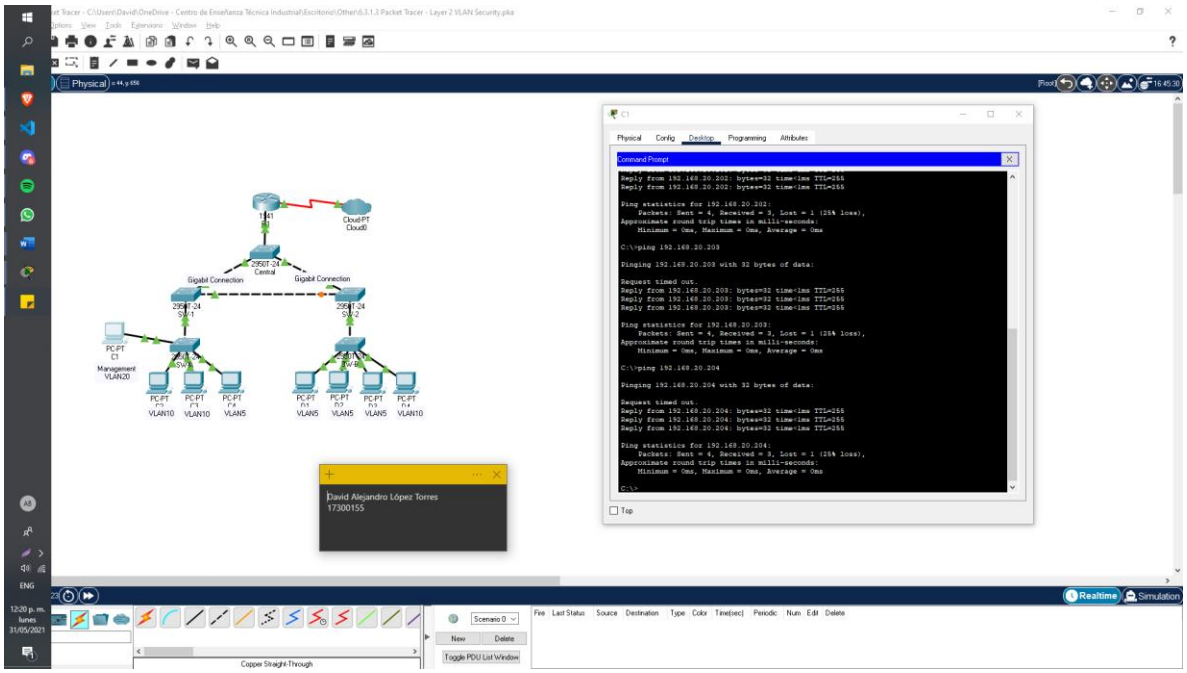
Connect the management PC to **SW-A** port F0/1 and ensure that it is assigned an available IP address within the 192.168.20.0/24 network.

Step 4: On SW-A, ensure the management PC is part of VLAN 20.

Interface F0/1 must be part of VLAN 20.

Step 5: Verify connectivity of the management PC to all switches.

The management PC should be able to ping **SW-A**, **SW-B**, **SW-1**, **SW-2**, and **Central**.



Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

a. Create subinterface g0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

b. Assign an IP address within the 192.168.20.0/24 network.

Step 2: Verify connectivity between the management PC and R1.

Be sure to configure the default gateway on the management PC to allow for connectivity.

Step 3: Enable security.

While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that allows only the Management PC to access the router.

b. Apply the ACL to the proper interface(s).

Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

a. Verify only the Management PC can access the router. Use SSH to access **R1** with username **SSHadmin** and password **ciscosshpa55**.

```
PC> ssh -l SSHadmin 192.168.20.100
```

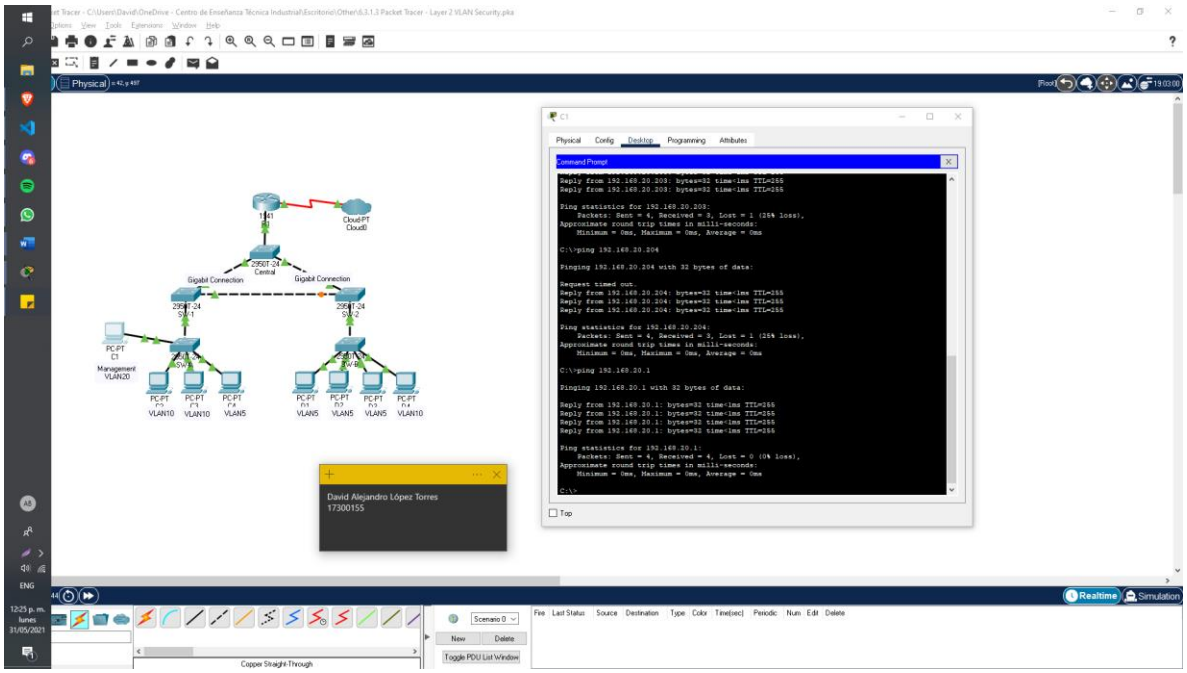
b. From the management PC, ping **SW-A**, **SW-B**, and **R1**. Were the pings successful? Explain.

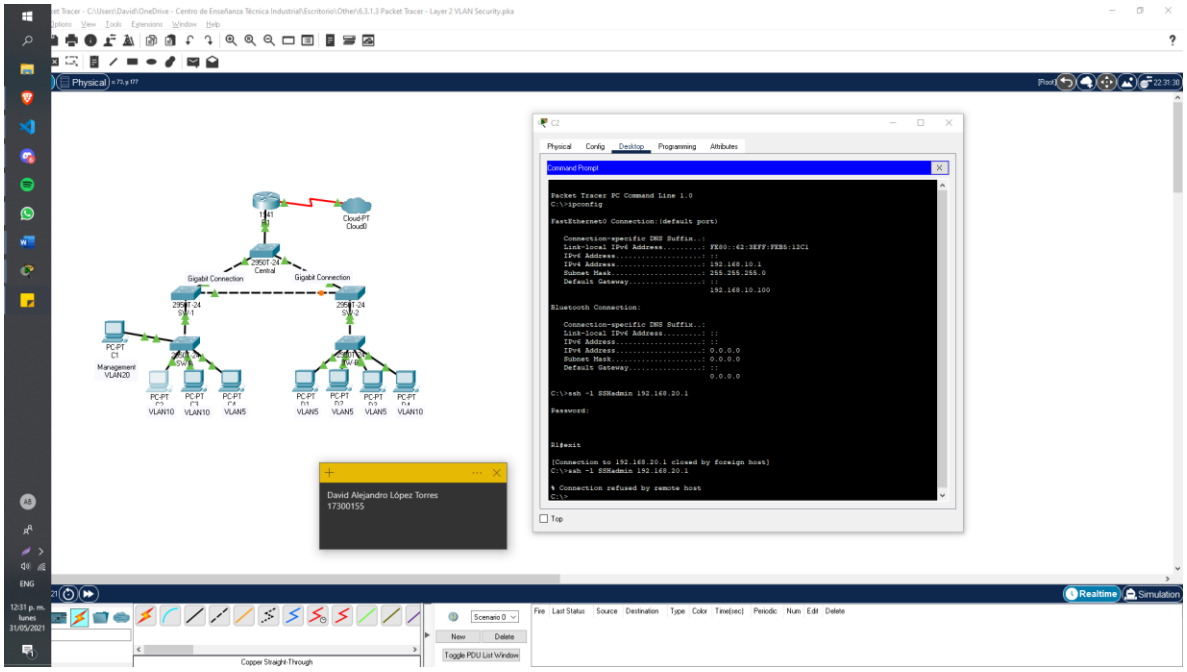
c. From **D1**, ping the management PC. Were the pings successful? Explain.

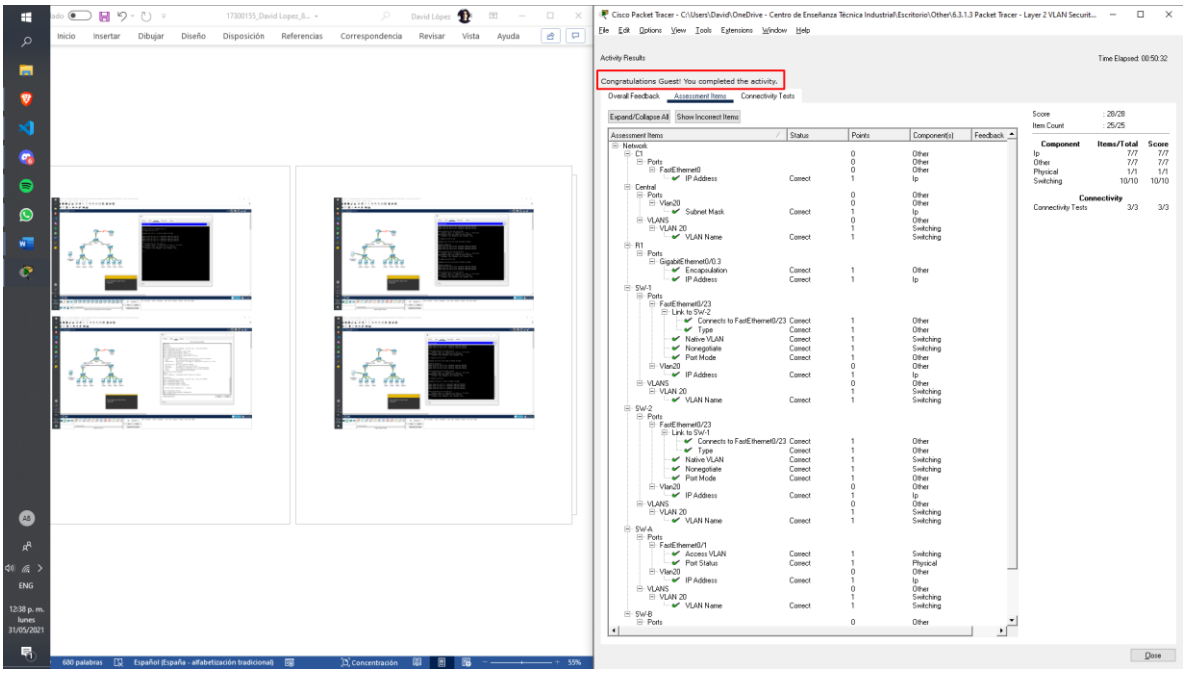
Step 5: Check results.

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

If all components appear to be correct and the activity still shows incomplete, it could be due to the connectivity tests that verify the ACL operation.


Physical
C1
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.20.203:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.20.204
Pinging 192.168.20.204 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.204: bytes=32 time<1ms TTL=255
Reply from 192.168.20.204: bytes=32 time<1ms TTL=255
Reply from 192.168.20.204: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.20.204:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.20.1
Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.20.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top
1841
Cloud-PT Cloud0
2950T-24 Central
Gigabit Connection
Gigabit Connection
2960T-24 SW-1
2960T-24 SW-2
2960T-24 SW-3
2960T-24 SW-4
PC-PT C1
Management VLAN20
PC-PT PC-1 VLAN10
PC-PT PC-2 VLAN10
PC-PT PC-3 VLAN5
PC-PT PC-4 VLAN5
PC-PT PC-5 VLAN5
PC-PT PC-6 VLAN5
PC-PT PC-7 VLAN5
PC-PT PC-8 VLAN10
David Alejandro López Torres
17300155
Realtime
Simulation
Copper Straight-Through


Physical
C2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::62:3EFF:FE85:12C1
IPv6 Address.....: ::
IPv4 Address.....: 192.168.10.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
192.168.10.100
Bluetooth Connection:
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
C:\>ssh -l SSHadmin 192.168.20.1
Password:
C:\>exit
[Connection to 192.168.20.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.20.1
% Connection refused by remote host
C:\>
Top
1841
Cloud-PT Cloud0
2950T-24 Central
Gigabit Connection
Gigabit Connection
2960T-24 SW-1
2960T-24 SW-2
2960T-24 SW-3
2960T-24 SW-4
PC-PT C1
Management VLAN20
PC-PT PC-1 VLAN10
PC-PT PC-2 VLAN10
PC-PT PC-3 VLAN5
PC-PT PC-4 VLAN5
PC-PT PC-5 VLAN5
PC-PT PC-6 VLAN5
PC-PT PC-7 VLAN5
PC-PT PC-8 VLAN10
David Alejandro López Torres
17300155
Realtime
Simulation
Copper Straight-Through



7. Observaciones

Al implementar las VLANs con sus respectivas medidas de seguridad pudimos observar como un diseño temprano que tome en cuenta la existencia de estos recursos de red puede facilitar mucho que se desarrolle el diseño que se tenía planteado. Además, siguiendo los pasos de la actividad no hubo mayor complicación para conseguir el objetivo de la actividad.

8. Conclusiones

Con el desarrollo de esta práctica hemos comprendido la importancia de una correcta gestión de las VLANs en caso de ser implementadas para añadir seguridad y cumplir con los principios de integridad y confidencialidad dentro de la red de trabajo. Además, la última parte nos ayudó a reforzar nuestros conocimientos relacionados a las listas de acceso y pudimos apreciar como es posible combinar las diferentes herramientas de seguridad que hemos abordado para generar una mejor protección de la red

9. Referencias

(14/08/2020) Seguridad VLANs en entornos virtuales. Recuperado el 24/05/2021 de: https://www.infosecuritymexico.com/es/blog/seguridad-vlans-virtuales.html

Seguridad en las VLANs. Recuperado el 24/05/2021 de: https://techclub.tajamar.es/seguridad-vlans-tipos-ataques/