HABILIDADES PRÁCTICAS

DIPLOMADO DE PROFUNDIZACIÓN CISCO

(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

Presentado por:

DARWIN ALBERTO CERON ANACONA

Tutor:

JUAN CARLOS VESGA

UNIVERSIDA NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIA ECBTI

PROGRAMA DE INGENIERIA ELECTRONICA

2016

INTRODUCCION

"Networking es más que una palabra. Es el símbolo de un cambio social."

Es de notar que actualmente las redes de computadores han ganado un terreno muy grande en el ámbito de la informática, tanto que ya se hace indispensable en toda empresa, institución educativa u hogares el uso de Internet y la conexión a servidores para poder realizar las labores diarias. Es por eso que las redes en todos sus aspectos, que contempla desde su topología física como lógica hasta aspectos muy importantes como las configuraciones, el direccionamiento, la seguridad, los controles en el envío y recepción de paquetes, la utilización de herramientas que permiten analizar el flujo de la información y que tanto nos congestiona el canal de nuestra red se han convertido en un campo de acción bastante interesante para cualquier ingeniero de sistemas.

En estas prácticas se pretende adquirir las capacidades necesarias para el desarrollo de las guías y mediante el uso de las herramientas dispuestas para su aplicación. En primer lugar se pretende que el alumno conozca las acciones (secuencias de intercambio de paquetes, vulnerabilidades y transmisiones de datos) generadas por la ejecución de las órdenes de red más frecuentes. En segundo lugar, dado que por la red viajan multitud de paquetes, será necesario seleccionar aquellos que nos resulten de interés. En tercer lugar, se pretende introducir al alumno en la interpretación y manejo del contenido de los de datos y para afianzar los conceptos y técnicas utilizados en estas guías. Todo ello permitirá poner en práctica los conocimientos adquiridos a lo largo del trabajo colaborativo 1, adquiriendo una mayor comprensión de los procesos que ocurren en la red cuando se llevan a cabo diversas acciones a nivel de usuario.

OBJETIVOS

General

Implementar todas las habilidades prácticas, teóricas y experiencia que hemos adquirido durante el desarrollo de este diplomado para dar soluciones a los problemas de Networking.

Específicos

Cumplir con los siguientes objetivos específicos, para la adquisición de competencias y habilidades ante problemas típicos de Networking

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Inicializar dispositivos de Networking
- Cálculo de rutas resumidas IPv4 e IPv6

RESUMEN

El presente trabajo es parte de la estrategia de aplicación con el fin de poner en práctica los conocimientos que hemos adquirido a lo largo del diplomado; a través de los ejercicios propuestos ponemos en práctica los conocimientos que adquirimos en los anteriores momentos que como se sabe el diplomado está estructurado a modo de secuencia para una mejor comprensión de los contenidos y conceptos que hacen parte del curso.

Aprendimos a conocer los elementos que conforman una red (Router, Switch, PC, hubo, etc...), a diseñar una topología de red y la configuración de cada elemento ya que las redes en la actualidad tienen un impacto significativo en nuestras vidas por que han cambiado nuestra forma de vivir, trabajar y divertirnos.

Teniendo en cuenta las necesidades y los avances producidos en una sociedad sumamente compleja, resulta de gran importancia destacar tanto la transmisión de información como la necesidad de que esta llegue a su destino en el momento preciso mediante el uso de las redes.

De hecho todas las sociedades por definición han sido y serán sociedades de la comunicación, es importante conocer cómo funciona la tecnología en la era de la telecomunicaciones que clase de protocolos se usan como lenguaje de máquinas en la conversión de la voz humana a información digital quien diría lo que viaja de forma física y a través del aire son unos y ceros.

TABLA DE CONTENIDOS

Calculating Summary Routes with IPv4 and IPv6

Práctica de laboratorio: cálculo de rutas resumidas IPv4 e IPv6

Topología

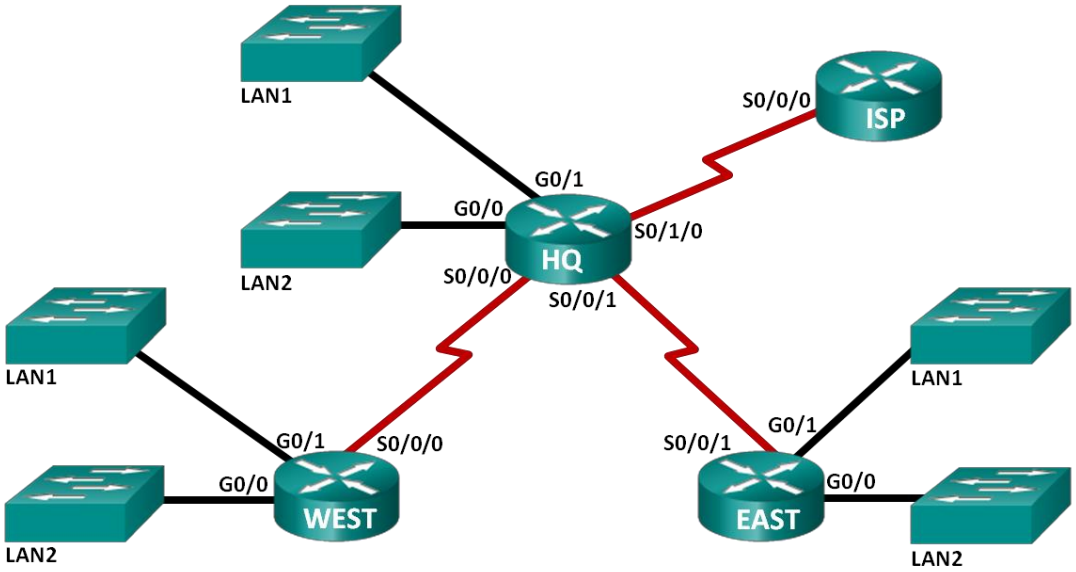


Tabla de direccionamiento

Subred	Dirección IPv4	Dirección IPv6
LAN1 de HQ	192.168.64.0/23	2001:DB8:ACAD:E::/64
LAN2 de HQ	192.168.66.0/23	2001:DB8:ACAD:F::/64
LAN1 de EAST	192.168.68.0/24	2001:DB8:ACAD:1::/64
LAN2 de EAST	192.168.69.0/24	2001:DB8:ACAD:2::/64
LAN1 de WEST	192.168.70.0/25	2001:DB8:ACAD:9::/64
LAN2 de WEST	192.168.70.128/25	2001:DB8:ACAD:A::/64
Enlace desde HQ a ESTE	192.168.71.4/30	2001:DB8:ACAD:1000::/64
Enlace desde HQ a WEST	192.168.71.0/30	2001:DB8:ACAD:2000::/64
Enlace desde HQ a ISP	209.165.201.0/30	2001:DB8:CC1E:1::/64

Objetivos

Parte 1: calcular rutas resumidas IPv4

- Determinar la ruta resumida para las LAN de HQ.
- Determinar la ruta resumida para las LAN ESTE.

- Determinar la ruta resumida para las LAN OESTE.
- Determinar la ruta resumida para las LAN de HQ, ESTE y OESTE.

Parte 2: calcular rutas resumidas IPv6

- Determinar la ruta resumida para las LAN de HQ.
- Determinar la ruta resumida para las LAN ESTE.
- Determinar la ruta resumida para las LAN OESTE.
- Determinar la ruta resumida para las LAN de HQ, ESTE y OESTE.

Información básica/situación

Las rutas resumidas reducen el número de entradas en las tablas de routing y hacen que el proceso de búsqueda en dichas tablas sea más eficaz. Este proceso también disminuye los requisitos de memoria del router. Se puede usar una sola ruta estática para representar unas pocas rutas o miles de rutas.

En esta práctica de laboratorio, determinará las rutas resumidas de diferentes subredes de una red. Después determinará la ruta resumida de toda la red. Determinará rutas resumidas para direcciones IPv4 e IPv6. Debido a que IPv6 usa valores hexadecimales, tendrá que convertir el valor hexadecimal en valor binario.

Recursos necesarios

- 1 computadora (Windows 7, Vista o XP, con acceso a Internet)
- Optativo: calculadora para convertir los valores hexadecimales y decimales en valores binarios

Parte 1. calcular rutas resumidas IPv4

En la parte 1, determinará las rutas resumidas que se pueden utilizar para reducir el tamaño de las tablas de routing. Después de cada conjunto de pasos, complete las tablas con la información apropiada de direccionamiento IPv4.

Paso 1. Indique la máscara de subred de la dirección IP de la LAN1 de HQ y la LAN2 de HQ en formato decimal.

LAN1 de HQ: 255.255.254.0

LAN2 de HQ: 255.255.254.0

Paso 2. Indique la dirección IP de la LAN1 de HQ y la LAN2 de HQ en formato binario.

LAN1 de HQ: 11000000.10101000.01000000.00000000

LAN2 de HQ: 11000000.10101000.01000010.00000000

Paso 3. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? 22

b. Indique la máscara de subred para la ruta resumida en formato decimal.

255.255.252.0

Paso 4. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

a. Indique los bits binarios coincidentes de las subredes de la LAN1 de HQ y la LAN2 de HQ.
b. Agregue ceros para conformar el resto de la dirección de red en formato binario.
c. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de HQ	192.168.64.0	255.255.254.0	**11111111.11111111.11111110.00000000**
LAN2 de HQ	192.168.66.0	**255.255.254.0**	**11111111.11111111.11111110.00000000**
Dirección de resumen de las LAN de HQ	**192.168.64.0**	**255.255.252.0**	**11111111.11111111.11111100.00000000**

Paso 5. indicar la máscara de subred de la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato decimal.

Paso 6. indicar la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato binario.

LAN1 ESTE: 11000000.10101000.01000100.00000000

LAN2 ESTE: 11000000.10101000.01000101.00000000

Paso 7. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

d. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? 23
e. Indique la máscara de subred para la ruta resumida en formato decimal.

255.255.254.0

Paso 8. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

f. Indique los bits binarios coincidentes de las subredes de la LAN1 ESTE y la LAN2 ESTE.
g. Agregue ceros para conformar el resto de la dirección de red en formato binario.
h. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección de subred en formato binario
LAN1 de EAST	192.168.68.0	**255.255.255.0**	**11111111.11111111.11111111.00000000**
LAN2 de EAST	192.168.69.0	**255.255.255.0**	**11111111.11111111.11111111.00000000**

Dirección de resumen de las LAN ESTE	192.168.68.0	255.255.254.0	11111111.11111111.11111110.00000000

Paso 9. indicar la máscara de subred de la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato decimal.

LAN1 OESTE: 255.255.255.128

LAN2 OESTE: 255.255.255.128

Paso 10. indicar la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato binario.

LAN1 OESTE: 11000000.10101000.01000110.00000000

LAN2 OESTE: 11000000.10101000.01000110.10000000

Paso 11. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

i. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? 24

j. Indique la máscara de subred para la ruta resumida en formato decimal.

255.255.255.0

Paso 12. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

k. Indique los bits binarios coincidentes de las subredes de la LAN1 OESTE y la LAN2 OESTE.

l. Agregue ceros para conformar el resto de la dirección de red en formato binario.

m. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de WEST	192.168.70.0	255.255.255.128	11111111.11111111.11111111.10000000
LAN2 de WEST	192.168.70.128	255.255.255.128	11111111.11111111.11111111.10000000
Dirección de resumen de las LAN OESTE	192.168.70.0	255.255.255.0	11111111.11111111.11111111.00000000

Paso 13. indicar la dirección IP y la máscara de subred de la ruta resumida de HQ, ESTE y OESTE en formato decimal.

HQ= 192.168.64.0 255.255.252.0

ESTE= 192.168.68.0 255.255.254.0

OESTE= 192.168.70.0 255.255.255.0

Paso 14. indicar la dirección IP de la ruta resumida de HQ, ESTE y OESTE en formato binario.

HQ= 11111111.11111111.01000000.00000000

ESTE= 11111111.11111111.01000100.00000000

OESTE= 11111111.11111111.01000110.00000000

Paso 15. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

n. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres redes? 21

o. Indique la máscara de subred para la ruta resumida en formato decimal.

255.255.248.0

Paso 16. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

p. Indique los bits binarios coincidentes de las subredes de HQ, ESTE y OESTE.

q. Agregue ceros para conformar el resto de la dirección de red en formato binario.

r. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
HQ	192.168.64.0	255.255.252.0	**11111111.11111111.11111100.00000000**
EAST	192.168.68.0	255.255.254.0	**11111111.11111111.11111110.00000000**
WEST	192.168.70.0	255.255.255.0	**11111111.11111111.11111111.00000000**
Ruta resumida de la dirección de red	192.168.64.0	255.255.248.0	**11111111.11111111.11111000.00000000**

Parte 2. calcular rutas resumidas IPv6

En la parte 2, determinará las rutas resumidas que se pueden utilizar para reducir el tamaño de las tablas de routing. Después de cada conjunto de pasos, complete las tablas con la información apropiada de direccionamiento IPv6.

Topología

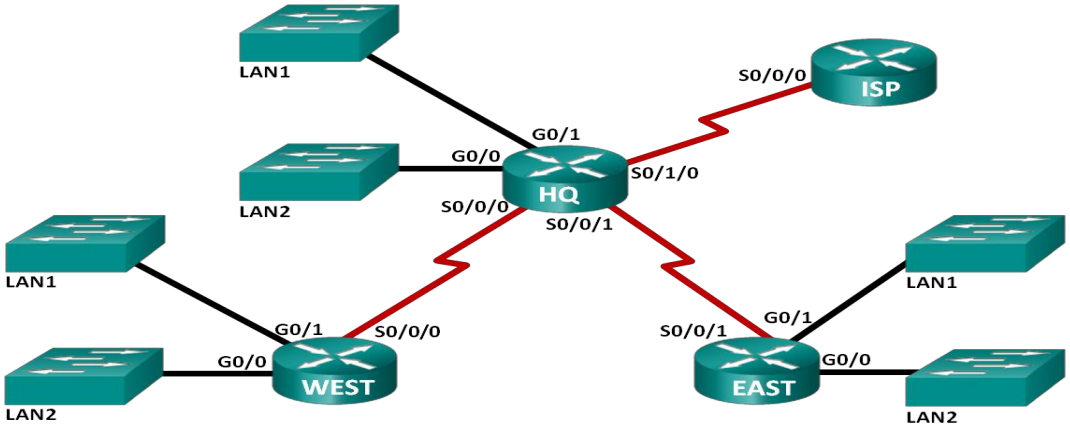


Tabla de direccionamiento

Subred	Dirección IPv6
LAN1 de HQ	2001:DB8:ACAD:E::/64
LAN2 de HQ	2001:DB8:ACAD:F::/64
LAN1 de EAST	2001:DB8:ACAD:1::/64
LAN2 de EAST	2001:DB8:ACAD:2::/64
LAN1 de WEST	2001:DB8:ACAD:9::/64
LAN2 de WEST	2001:DB8:ACAD:A::/64
Enlace desde HQ a ESTE	2001:DB8:ACAD:1000::/64
Enlace desde HQ a WEST	2001:DB8:ACAD:2000::/64
Enlace desde HQ a ISP	2001:DB8:CC1E:1::/64

Paso 1. indicar los primeros 64 bits de la máscara de subred de la dirección IP de la LAN1 de HQ y la LAN2 de HQ en formato hexadecimal.

LAN1 de HQ 2001:DB8:ACAD:E

LAN2 de HQ 2001:DB8:ACAD:F

Paso 2. indicar la ID de subred (bits 48 a 64) de la LAN1 de HQ y la LAN2 de HQ en formato binario.

LAN1 de HQ 0000000000001110

LAN2 de HQ 0000000000001111

Paso 3. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred?
15

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

8193.3512.44205.14/63

Paso 4. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

c. Indique los bits binarios de la ID de subred coincidentes para las subredes LAN1 de HQ y LAN2 de HQ.

d. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

e. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
LAN1 de HQ	2001:DB8:ACAD:E::/64	2001:DB8:ACAD:E/64	0000000000001110
LAN2 de HQ	2001:DB8:ACAD:F::/64	2001:DB8:ACAD:F/64	0000000000001111
Dirección de resumen de las LAN de HQ	2001:DB8:ACAD:E::/63	2001:DB8:ACAD:E/63	0000000000001110

Paso 5. indicar los primeros 64 bits de la máscara de subred de la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato hexadecimal.

LAN1 de ESTE 2001:DB8:ACAD:1

LAN2 de ESTE 2001:DB8:ACAD:2

Paso 6. indicar la ID de subred (bits 48 a 64) de la LAN1 ESTE y la LAN2 ESTE en formato binario.

LAN1 de ESTE 0000000000000001

LAN2 de ESTE 0000000000000010

Contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

f. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred?
14

g. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

8193.3512.44205.0/62

Paso 7. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

h. Indique los bits binarios coincidentes de las subredes de la LAN1 ESTE y la LAN2 ESTE.

i. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

j. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
LAN1 de EAST	2001:DB8:ACAD:1::/64	2001:DB8:ACAD:1/64	0000000000000001
LAN2 de EAST	2001:DB8:ACAD:2::/64	2001:DB8:ACAD:2/64	0000000000000010
Dirección de resumen de las LAN ESTE	2001:DB8:ACAD::/62	2001:DB8:ACAD:0/62	0000000000000000

Paso 8. indicar los primeros 64 bits de la máscara de subred de la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato decimal.

LAN1 de OESTE 2001:DB8:ACAD:9

LAN2 de OESTE 2001:DB8:ACAD:A

Paso 9. indicar la ID de subred (bits 48 a 64) de la LAN1 OESTE y la LAN2 OESTE en formato binario.

LAN1 de OESTE 0000000000001001

LAN2 de OESTE 0000000000001010

Paso 10. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

k. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred?
14

l. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

8193.3512.44205.8/62

Paso 11. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

m. Indique los bits binarios coincidentes de las subredes de la LAN1 OESTE y la LAN2 OESTE.

n. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

o. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
LAN1 de WEST	2001:DB8:ACAD:9::/64	2001:DB8:ACAD:9/64	0000000000001001
LAN2 de WEST	2001:DB8:ACAD:A::/64	2001:DB8:ACAD:A/64	0000000000001010
Dirección de resumen de las LAN OESTE	2001:DB8:ACAD:8::/62	2001:DB8:ACAD:8/62	0000000000001000

Paso 12. indicar la dirección IP de la ruta resumida y los primeros 64 bits de la máscara de subred de HQ, ESTE y OESTE en formato decimal.

Paso 13. indicar la ID de subred de la ruta resumida de HQ, ESTE y OESTE en formato binario.

Paso 14. contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de subred para la ruta resumida.

p. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres ID de subred?
12

q. Indique la máscara de subred de los primeros 64 bits de la ruta resumida en formato decimal.

8193.3512.44205.0/60

Paso 15. copiar los bits binarios coincidentes y luego agregar todos ceros para determinar la dirección de red resumida.

r. Indique los bits binarios coincidentes de las subredes de HQ, ESTE y OESTE.

s. Agregue ceros para conformar el resto de la dirección de ID de subred en formato binario.

t. Indique las direcciones de red resumidas en formato decimal.

Subred	Dirección IPv6	Máscara de subred de los primeros 64 bits	ID de subred en formato binario
HQ	2001:DB8:ACAD:E::/63	2001:DB8:ACAD:E/63	0000000000001110
EAST	2001:DB8:ACAD::/62	2001:DB8:ACAD:0/62	0000000000000000
WEST	2001:DB8:ACAD:8::/62	2001:DB8:ACAD:8/62	0000000000001000
Ruta resumida de la dirección de red	2001:DB8:ACAD::/60	2001:DB8:ACAD:0/60	0000000000000000

Reflexión

1. **¿Qué diferencia existe entre determinar la ruta resumida para IPv4 y determinarla para IPv6?**

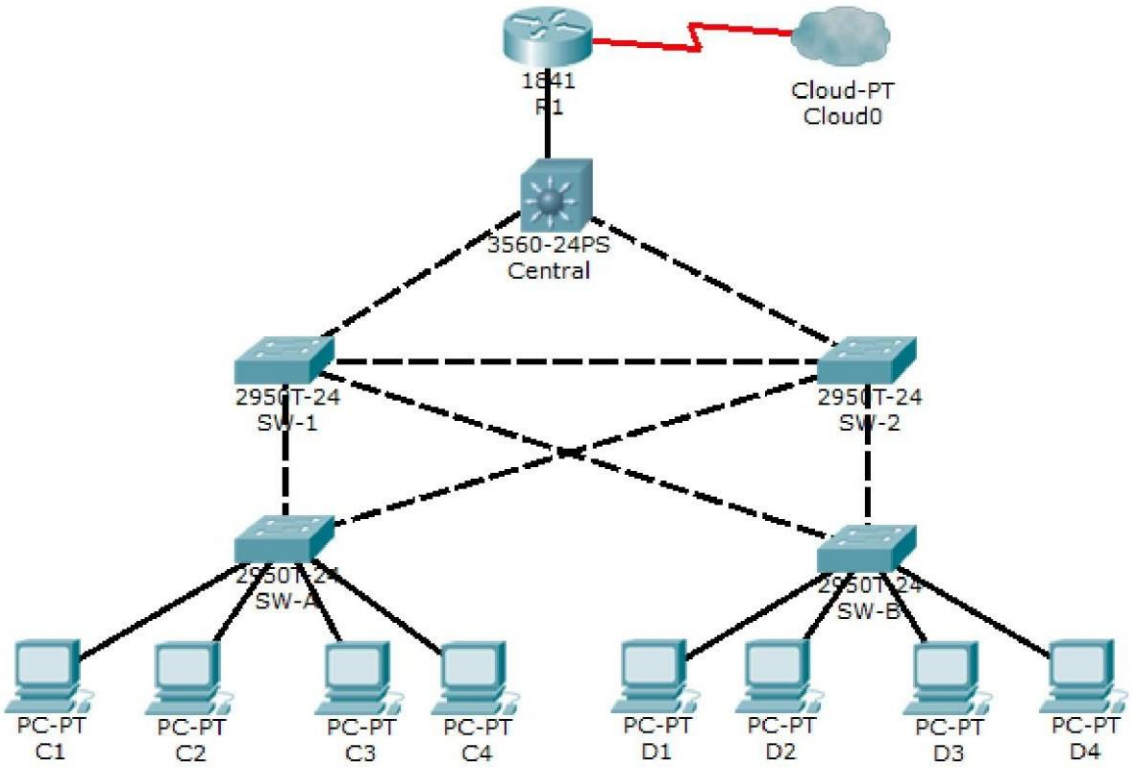
   La principal diferencia es que la IPv4 usa 32 bits y la IPv6 usa 128 bits. La IPv4 se convierte de decimal a binario y la IPv6 requiere más pasos para convertir de hexadecimal a binario.

2. **¿Por qué las rutas resumidas son beneficiosas para una red?**

   Porque hacen que el proceso de búsqueda en la tabla de routing sea más eficaz y reducen los requisitos de memoria del router

6.5.1.2 Packet Tracer - Layer 2 Security_Instructor

Topology



Objectives

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable storm control to prevent broadcast storms.
- Enable port security to prevent MAC address table overflow attacks.

Background / Scenario

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent against spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. In addition, the network administrator would like to enable storm control to prevent broadcast storms. Finally, to prevent against MAC address table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses that can be learned per switch port. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

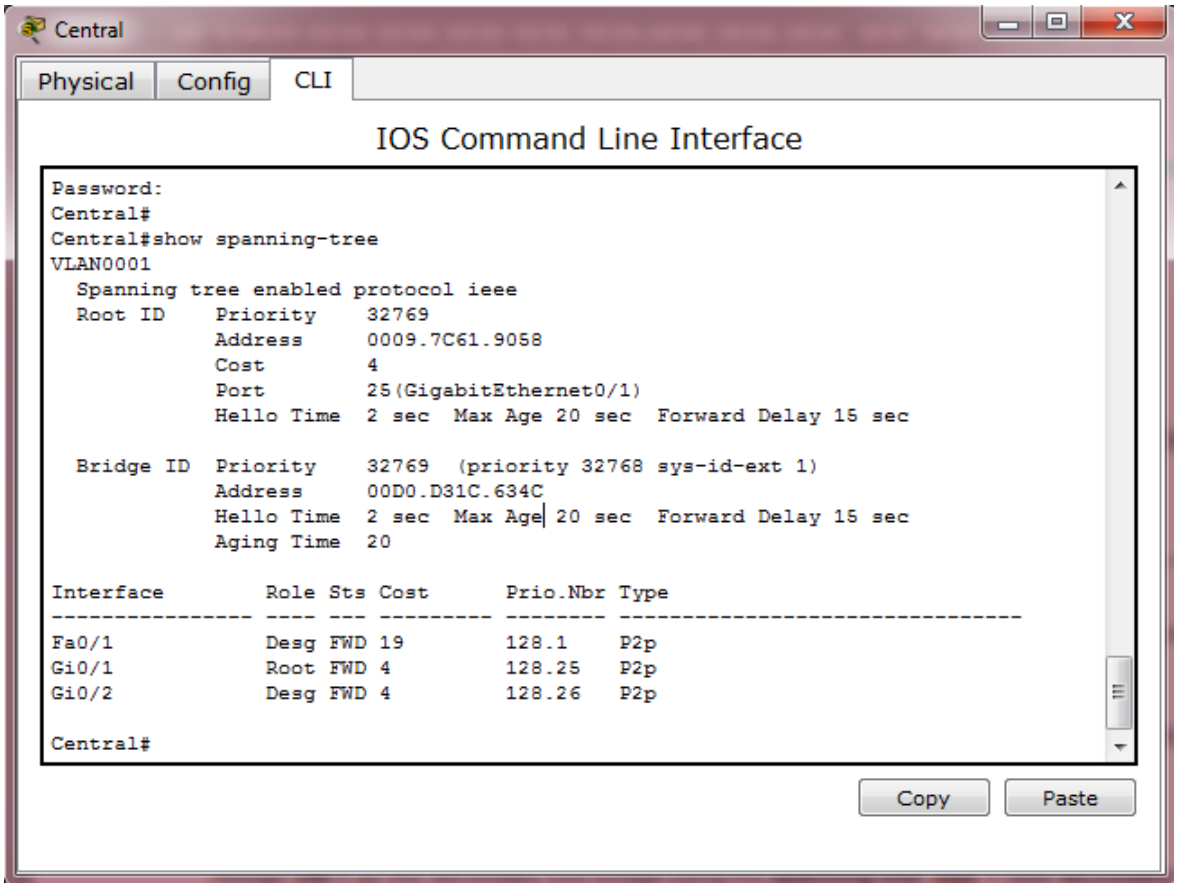
All switch devices have been preconfigured with the following:

- Enable password: ciscoenpa55
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

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 and to see the ports in use and their status.



Which switch is the current root bridge?

Current root is SW-1

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, assign **Central** as the root bridge. Central(config)# **spanning-tree vlan 1 root primary**

```
Central#
Central#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)#spanning-tree vlan 1 root primary
Central(config)#
```

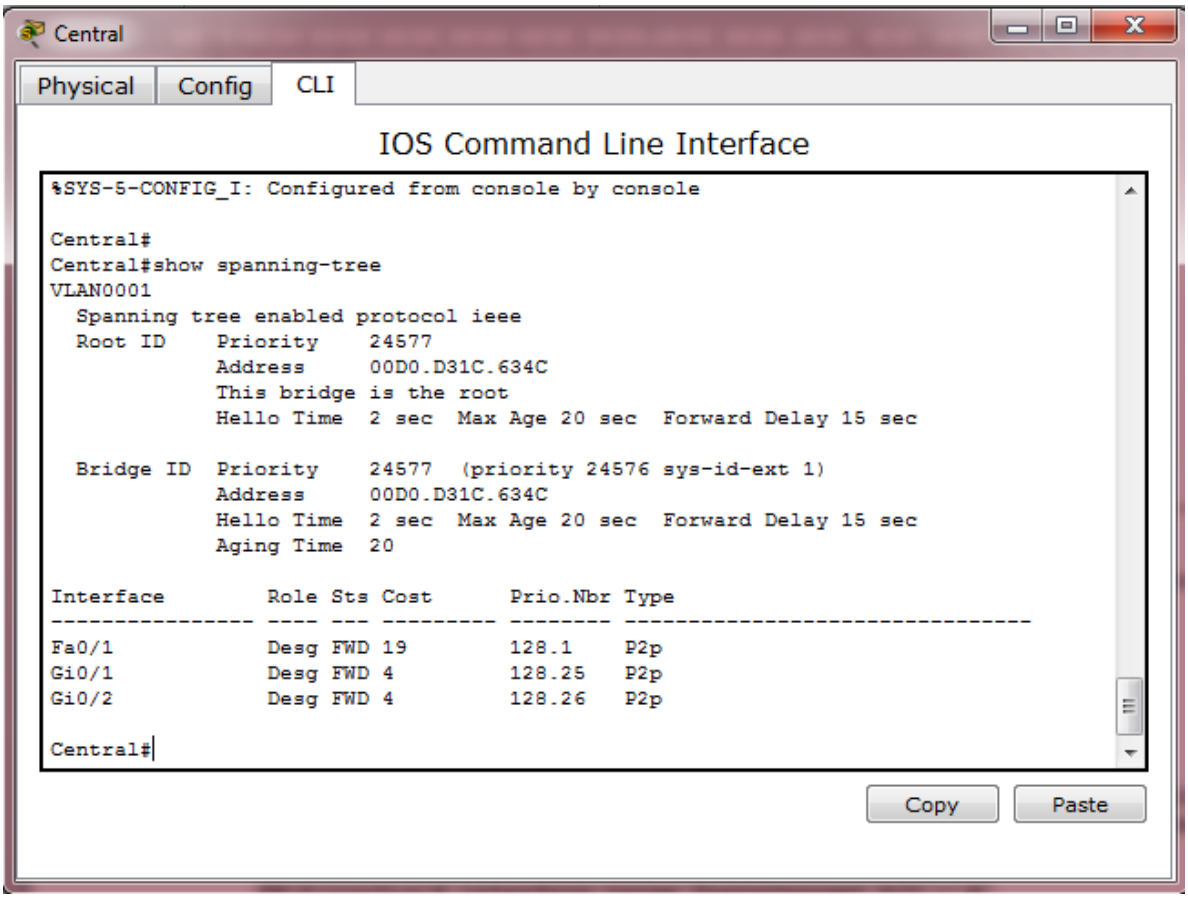
Step 3: Assign SW-1 as a secondary root bridge.

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

```
SW-1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#spanning-tree vlan 1 root secondary
SW-1(config)#
```

Step 4: Verify the spanning-tree configuration.

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



Current root is Central

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

Part 2: Protect Against STP Attacks

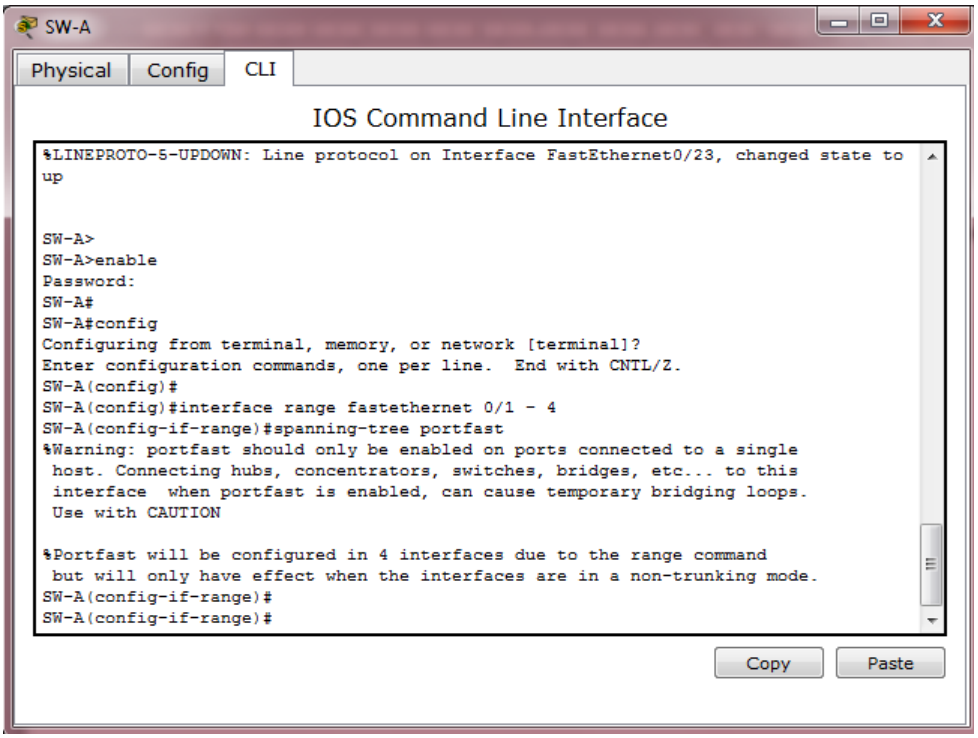
Secure the STP parameters to prevent STP manipulation attacks.

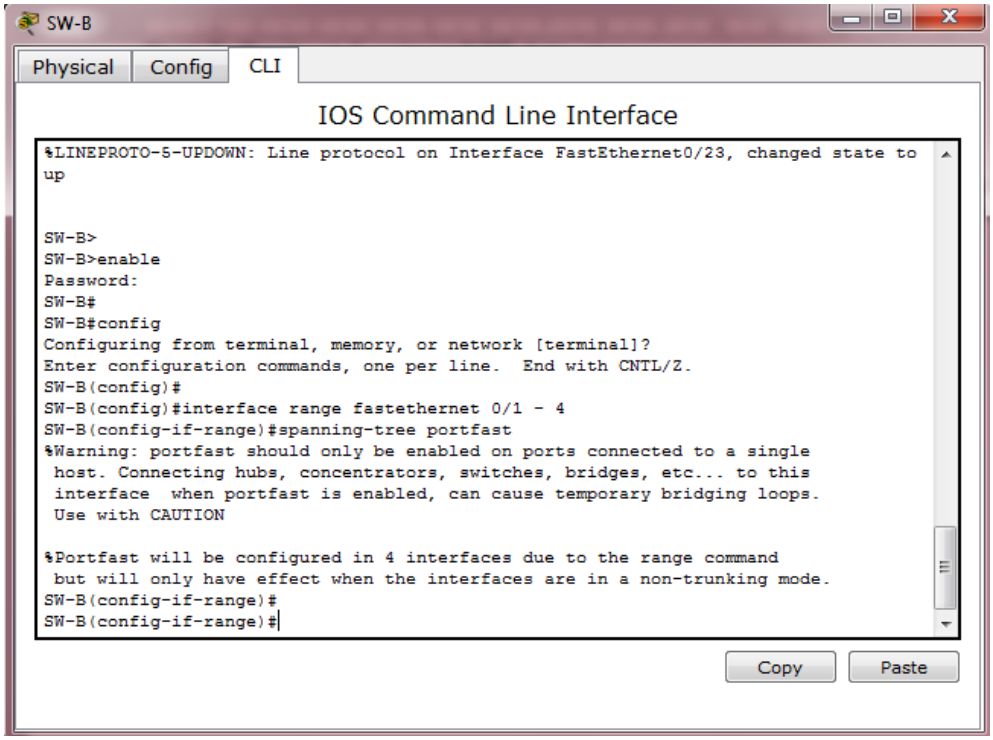
Step 1: Enable PortFast on all access ports.

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.

SW-A(config)# **interface range fastethernet 0/1 - 4**
SW-A(config-if-range)# **spanning-tree portfast**

SW-B(config)# **interface range fastethernet 0/1 - 4**
SW-B(config-if-range)# **spanning-tree portfast**


SW-A
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
SW-A>
SW-A>enable
Password:
SW-A#
SW-A#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW-A(config)#
SW-A(config)#interface range fastethernet 0/1 - 4
SW-A(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast will be configured in 4 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW-A(config-if-range)#
SW-A(config-if-range)#
Copy
Paste


SW-B
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
SW-B>
SW-B>enable
Password:
SW-B#
SW-B#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW-B(config)#
SW-B(config)#interface range fastethernet 0/1 - 4
SW-B(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast will be configured in 4 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW-B(config-if-range)#
SW-B(config-if-range)#
Copy
Paste

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.

SW-A(config)# **interface range fastethernet 0/1 - 4**
SW-A(config-if-range)# **spanning-tree bpduguard enable**

SW-B(config)# **interface range fastethernet 0/1 - 4**
SW-B(config-if-range)# **spanning-tree bpduguard enable**

```
SW-A(config)#interface range fastethernet 0/1 - 4
SW-A(config-if-range)#spanning-tree bpduguard enable
SW-A(config-if-range)#
```

```
SW-B(config)#interface range fastethernet 0/1 - 4
SW-B(config-if-range)#spanning-tree bpduguard enable
SW-B(config-if-range)#
```

Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard enable** command in the interface configuration mode or the **spanning-tree portfast bpduguard default** command in the 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 Fa0/23 and Fa0/24. On **SW-2**, enable root guard on ports Fa0/23 and Fa0/24.

SW-1(config)# **interface range fa0/23 - 24**
SW-1(config-if-range)# **spanning-treeguard root**

SW-2(config)# **interface range fa0/23 - 24**
SW-2(config-if-range)# **spanning-treeguard root**

```
SW-1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-1(config)#interface range fa0/23 - 24
SW-1(config-if-range)#spanning-tree guard root
SW-1(config-if-range)#
```

```
SW-2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#interface range fa0/23 - 24
SW-2(config-if-range)#spanning-tree guard root
SW-2(config-if-range)#
```

Part 3: Enable Storm Control

Step 1: Enable storm control for broadcasts.

a. Enable storm control for broadcasts on all ports connecting switches (trunk ports).

b. Enable storm control on interfaces connecting **Central**, **SW-1**, and **SW-2**.
Set a **50** percent rising
suppression level using the **storm-control broadcast** command.

SW-1(config)# **interface range gi1/1 , fa0/1 , fa0/23 - 24**
SW-1(config-if)# **storm-control broadcast level 50**

SW-2(config)# **interface range gi1/1 , fa0/1 , fa0/23 - 24**
SW-2(config-if)# **storm-control broadcast level 50**

Central(config-if)# **interface range gi0/1 , gi0/2 , fa0/1**
Central(config-if)# **storm-control broadcast level 50**

```
SW-1(config)#
SW-1(config)#interface range gi0/1 , fa0/1 , fa0/23 - 24
SW-1(config-if-range)#storm-control broadcast level 50
SW-1(config-if-range)#
```

```
SW-2(config)#
SW-2(config)#interface range gi0/1 , fa0/1 , fa0/23 - 24
SW-2(config-if-range)#storm-control broadcast level 50
SW-2(config-if-range)#
```

```
Central(config)#
Central(config)#interface range gi0/1 , gi0/2 , fa0/1
Central(config-if-range)#storm-control broadcast level 50
Central(config-if-range)#
```

- En la configuración de los switches SW-1 y SW-2 se indica que se configuren las interfaces g1/1…, pero están habilitadas las interfaces g0/1…

Step 2: Verify storm control configuration.

Verify your configuration with the **show storm-control broadcast** and the **show run** commands.

Part 4: 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 address 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.

SW-A(config)# **interface range fa0/1 - 22**

SW-A(config-if-range)# **switchport mode access**

SW-A(config-if-range)# **switchport port-security**

SW-A(config-if-range)# **switchport port-security maximum 2**

SW-A(config-if-range)# **switchport port-security violation shutdown**

SW-A(config-if-range)# **switchport port-security mac-address sticky**

SW-B(config)# **interface range fa0/1 - 22**
SW-B(config-if-range)# **switchport mode access** SW-B(config-if-range)# **switchport port-security**

SW-B(config-if-range)# **switchport port-security maximum 2**

SW-B(config-if-range)# **switchport port-security violation shutdown** SW-B(config-if-range)# **switchport port-security mac-address sticky**

```
SW-A>enable
Password:
SW-A#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range fa0/1 - 22
SW-A(config-if-range)#switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address sticky
SW-A(config-if-range)#
```

```
SW-B>enable
Password:
SW-B#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)#
SW-B(config)#
SW-B(config)#interface range fa0/1 - 22
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport port-security
SW-B(config-if-range)#switchport port-security maximum 2
SW-B(config-if-range)#switchport port-security violation shutdown
SW-B(config-if-range)#switchport port-security mac-address sticky
SW-B(config-if-range)#
```

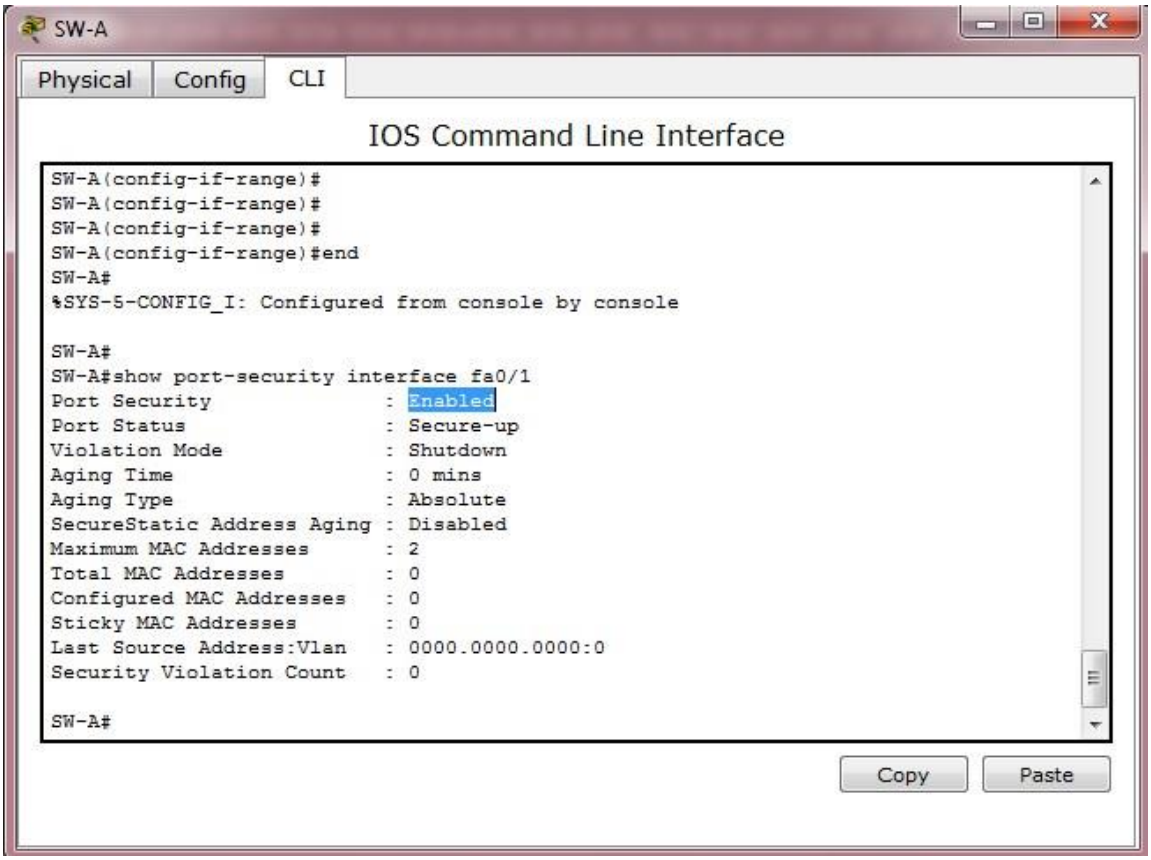
Why would you not want to enable port security on ports connected to other switches or routers?

Ports connected to other switch devices and routers can, and should, have a multitude of MAC addresses learned for that single port. Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality.

Los puertos de conexión con otros dispositivos de conmutación switches y routers pueden, y deben, tener una multitud de direcciones MAC aprendidas para un solo puerto. Limitar el número de direcciones MAC que se pueden aprender en estos puertos puede afectar significativamente la funcionalidad de red.

Step 2: Verify port security.

On **SW-A**, issue the **show port-security interface fa0/1** command to verify that port security has been configured.



Step 3: Disable unused ports.

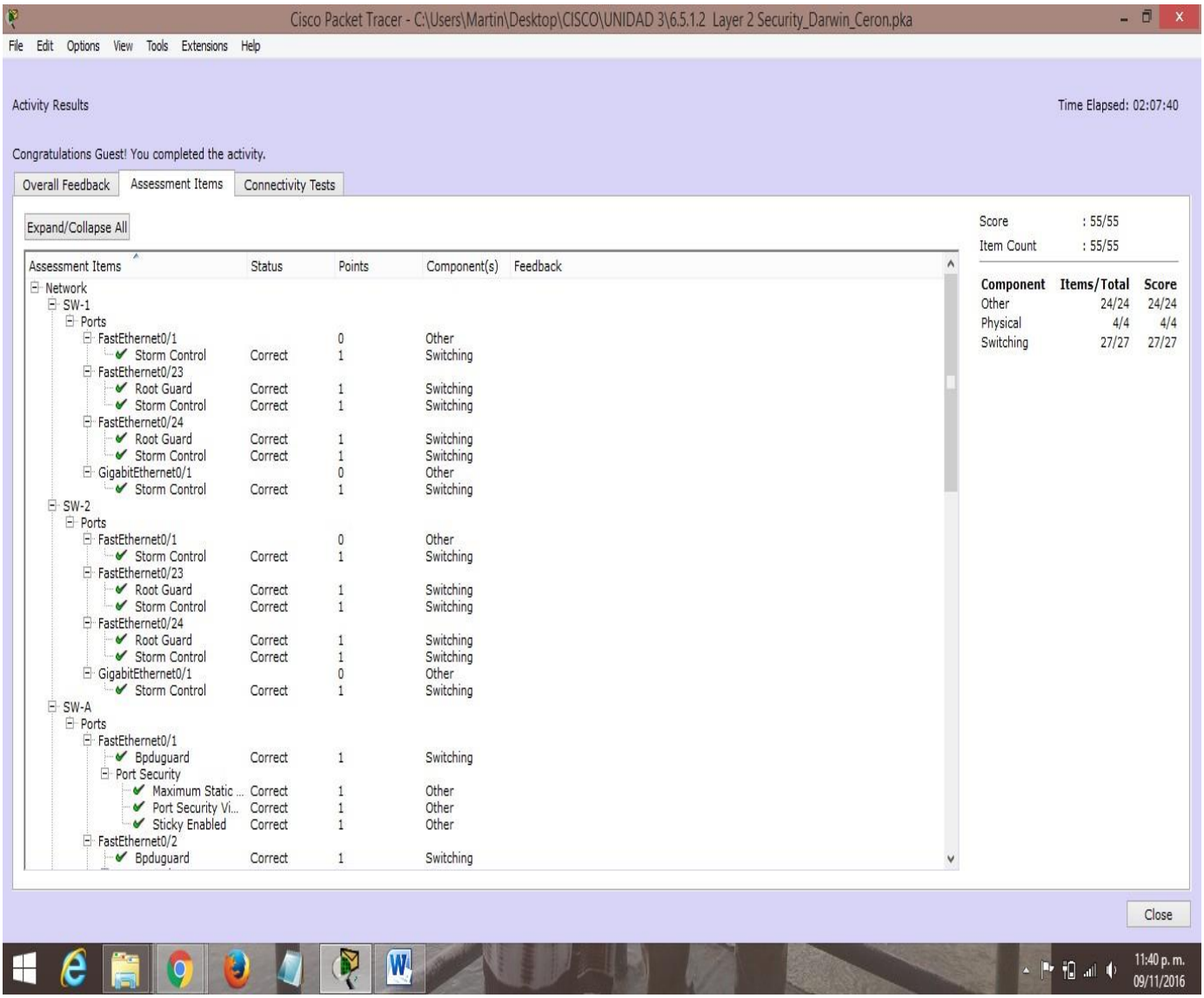
Disable all ports that are currently unused.

SW-A(config)# **interface range fa0/5**
- 22 SW-A(config-if-range)#
shutdown

SW-B(config)# **interface range fa0/5**
- 22 SW-B(config-if-range)#
shutdown

Step 4: Check results.

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



CONCLUSIONES

- ✓ Los estudios previos sobre el diseño de la arquitectura de red ayudó a diseñar el atractivo topología, las características de seguridad también se consideran en el disposición de la topología.

- ✓ En segundo lugar el uso de Seguridad y Política de contraseñas para proporcionar seguridad en la arquitectura estudiado e implementado en 5 juegos de políticas diferentes que pasar a los routers.

- ✓ En los extremos de la red, tanto topologías, la uno sin política de seguridad y el uno con él son simulados utilizando Experimento Cisco Packet Tracer, los resultados de la simulación demuestran que ambas arquitecturas son el trabajo correctamente y los resultados muestran la configuración correcta interconexión de los componentes de la red.

- ✓ En resumen este trabajo proporciona la solución para la seguridad incumplimientos en la empresa estudiada, proporcionando la mejora en la topología de la red de la seguridad perspectiva y la asignación de la política a sus routers.

REFERENCIAS BIBLIOGRAFICAS

- ✓ Shaughnessy, T., Velte, T., & Sáchez García, J. I. (2000). Manual de CISCO.
- ✓ Ariganello, E., & Sevilla, B. (2011). Redes CISCO - guía de estudio para la certificación CCNP (No. 004.6 A73).
- ✓ Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software.
- ✓ CISCO. (s.f.). Principios básicos de routing y switching: Listas de Control de Acceso. (2017), Tomado de: ttps://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1
- ✓ Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: https://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html#11.0
- ✓ DHCP. Principios de Enrutamiento y Conmutación. (2014) Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1
- ✓ Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv4 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx
- ✓ Segui, F. B. (2015). Configuración DHCP en routers CISCO. Chamorro Serna, L., Montaño Torres, O., Guzmán Pérez, E. H., Daza Navia, M. Y., & Castillo Ortiz, O. F. (2018). Diplomado de Profundización Cisco-Enrutamiento en soluciones de red. Es.wikipedia.org. (2018). Open Shortest Path First. [online] disponible en: https://es.wikipedia.org/wiki/Open_Shortest_Path_First [28 May 2018].