DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES PRACTICAS CCNP

DANIEL EDUARDO RENGIFO CASTAÑEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA ECBTI

INGENIERIA EN TELECOMUNICACIONES

IBAGUÉ

2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

DANIEL EDUARDO RENGIFO CASTAÑEDA

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA ECBTI
INGENIERIA EN TELECOMUNICACIONES
IBAGUÉ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

Ibagué, 22 de mayo de 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VTP: son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable

DTP: es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560. Los switches de otros proveedores no admiten el DTP. DTP maneja la negociación de enlaces troncales solo si el puerto del switch vecino está configurado en un modo de enlace troncal que admite DTP.

VLAN: Una red de área local virtual (VLA N) es una red de switch que es dividida en segmentos lógicamente por la función, el área, o la aplicación, sin consideración alguna hacia las ubicaciones físicas de los usuarios. Los VLA N son un grupo de host o los puertos que pueden ser situados dondequiera en una red sino comunicar como si estén en el mismo segmento físico. Los VLA N ayudan a simplificar la Administración de redes dejándole mover un dispositivo a un nuevo VLA N sin el cambio de ningunas conexiones físicas.

BGP: es un protocolo de gateway exterior (EGP), usado para realizar el ruteo entre dominios en las redes TCP/IP.

GLBP: es un protocolo propietario de Cisco que intenta superar las limitaciones de los protocolos de router redundantes existentes añadiendo la funcionalidad de balanceo de carga.

NVRAM: es uno de los componentes de configuración interna de un router. Se usa para almacenar un archivo de configuración de respaldo/inicio

RESUMEN

En este trabajo se realiza la descripción de cada uno de los pasos que se deben seguir para la configuración de los escenarios propuestos, los cuales corresponden a la prueba de habilidades prácticas del diplomado de profundización CISCO CCNP. En el primer escenario se hace la configuración entre routers vecinos con el protocolo de Gateway exterior (BGP), para permitir el intercambio de información de ruteo entre sí. Y en el desarrollo del segundo escenario se lleva a cabo la configuración de switches mediante el protocolo VTP, el cual sirve para centralizar en un solo switch la administración de todas las VLANs, y éstas se configurarán de forma manual en cada switch. De igual forma de se lleva a cabo la configuración del protocolo de enrutamiento DTP, para que se habilite de manera automática en los switches.
Los desarrollos de los escenarios anteriores ya se han puesto en práctica, por medio de los laboratorios en el transcurso del diplomado, poniéndose a prueba el nivel de solución que se puede dar a problemas relacionados en Redes y Electrónica en el mundo del Networking.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this work, a description is made of each of the steps that must be followed to configure the proposed scenarios, which correspond to the practical skills test of the CISCO CCNP deepening diploma course.

In the first scenario, the configuration is made between neighboring routers with the Exterior Gateway Protocol (BGP), to allow the exchange of routing information with each other. And in the development of the second scenario, the configuration of the switches is carried out using the VTP protocol, which serves to centralize the administration of all the VLANs in a single switch, and these will be configured manually on each switch. In the same way, the configuration of the DTP routing protocol is carried out, so that it is automatically enabled on the switches.

The developments of the previous scenarios have already been put into practice, through the laboratories during the course of the diploma, testing the level of solution that can be given to problems related to Networks and Electronics in the world of Networking.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics

INTRODUCCIÓN

En el desarrollo de la siguiente actividad evaluativa se pone en práctica los conocimientos adquiridos durante el curso del diplomado de CISCO, donde se pretende establecer niveles básicos de seguridad de acuerdo a estrategias mediante el uso de hardware y software, con el fin de proteger la integridad de la información frente a cualquier tipo de ataque que se pueda presentar en un instante de tiempo determinado; en especial en soluciones de red que involucren el uso de aplicaciones cliente-servidor.

Los conocimientos adquiridos con el diplomado CISCO tienen el objetivo de desarrollar capacidades de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP, y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones a través de las redes de datos estableciendo alternativas a problemas de interconectividad.

Mediante el desarrollo de la Prueba de Habilidades se pretende poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking, donde se realizan actividades de configuración de los switchs por medio de VLAN para su conectividad y envío de datos aplicando los protocolos VTP y DTP para un buen direccionamiento entre dispositivos, de igual forma se usan comandos IOS de configuración avanzada en routers (con direccionamiento IPv4 e IPv6) para protocolos de enrutamiento BGP

DESARROLLO

1. ESCENARIO 1

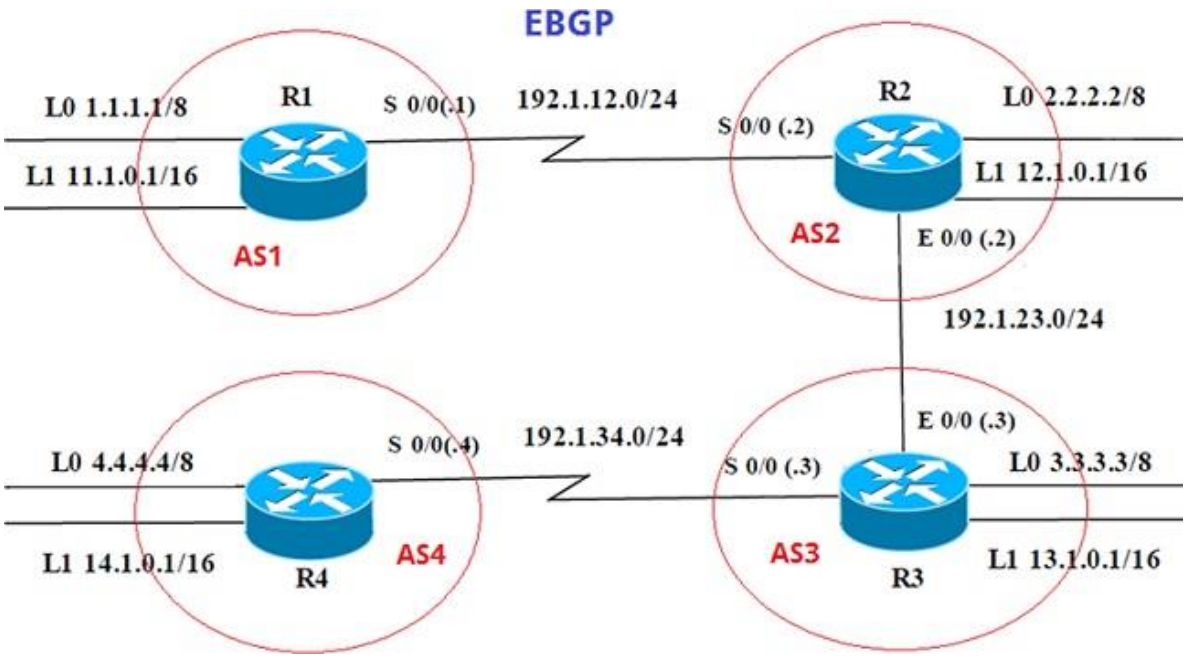


Figura 1 Escenario 1

Tabla 1 Información para configuración de Router 1

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

Tabla 2 Información para configuración de Router 2

Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 3 Información para configuración de Router 3

Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

Tabla 4 Información para configuración de Router 4

Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

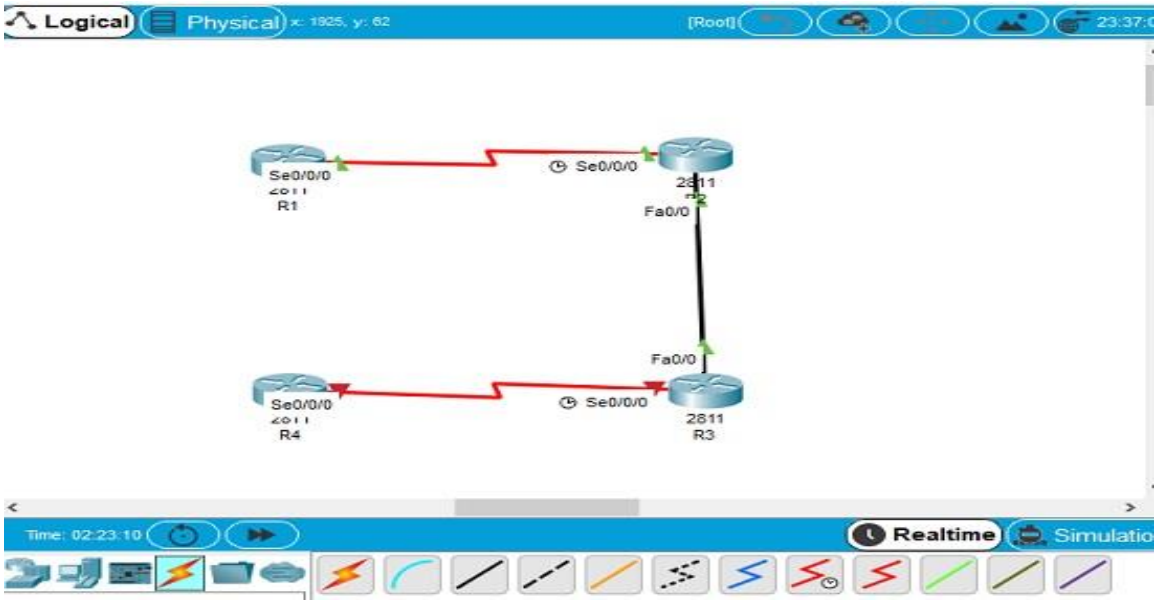


Figura 2 Simulación de escenario 1

Configuración Router 1:

Router>en
Router#conf t
Router(config)#hostname R1

R1(config)#int lo 0
R1(config-if)#
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#int lo 1

R1(config-if)#

R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shut

Configuración Router 2:
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#int lo 1

R2(config-if)#

R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#int f0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut

Configuración Router 3:
Router>en
Router#conf t
Router(config)#hostname R3
R3(config)#int lo 0

R3(config-if)#

R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#int lo 1

```
R3(config-if)#

R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#int f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shut

R3(config-if)#

R3(config-if)#exit
R3(config)#int s0/0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
```

Configuración Router 4:

```
Router>en
Router#conf t
Router(config)#hostname R4
R4(config)#int lo 0

R4(config-if)#

R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#int lo 1

R4(config-if)#

R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#int s0/0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shut
```

1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

BGP R1:
R1>en
R1#conf t
R1(config)#router bgp 1
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#bgp router-id 22.22.22.22

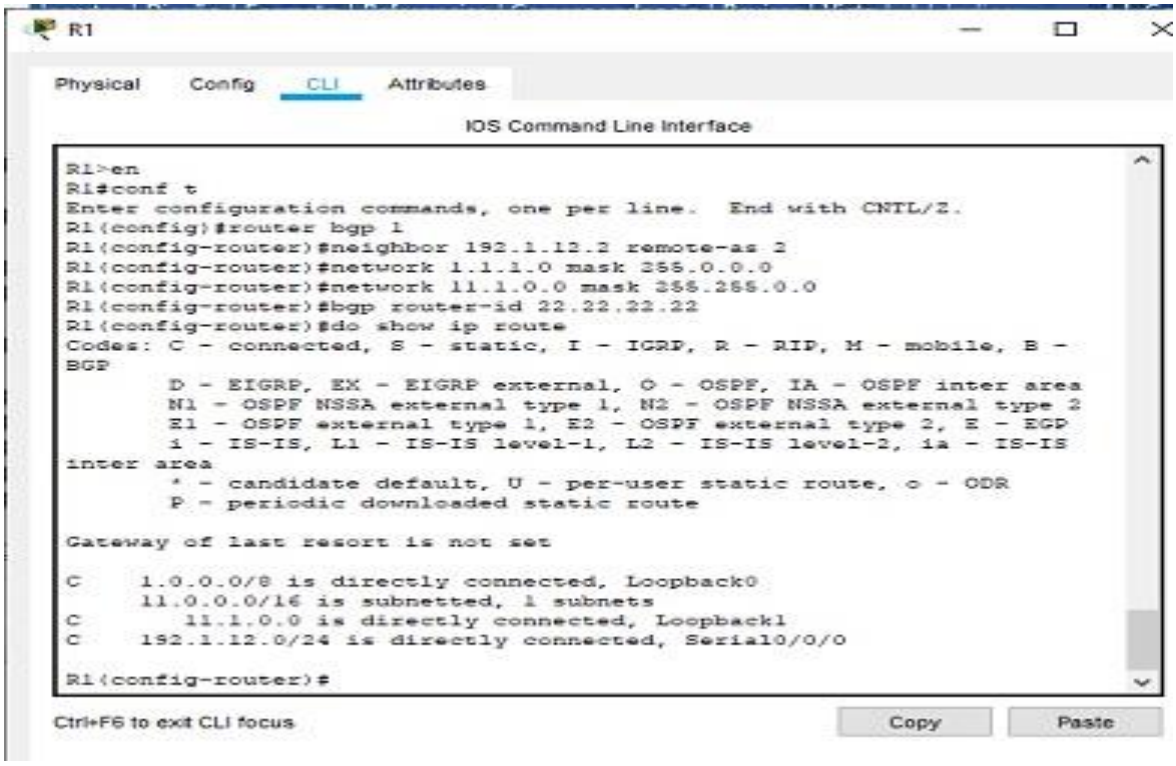


Figura 3 Comando show ip route en R1

BGP R1:
R2>en
R2#conf t
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

R2(config-router)#network 2.2.2.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#bgp router-id 33.33.33.33

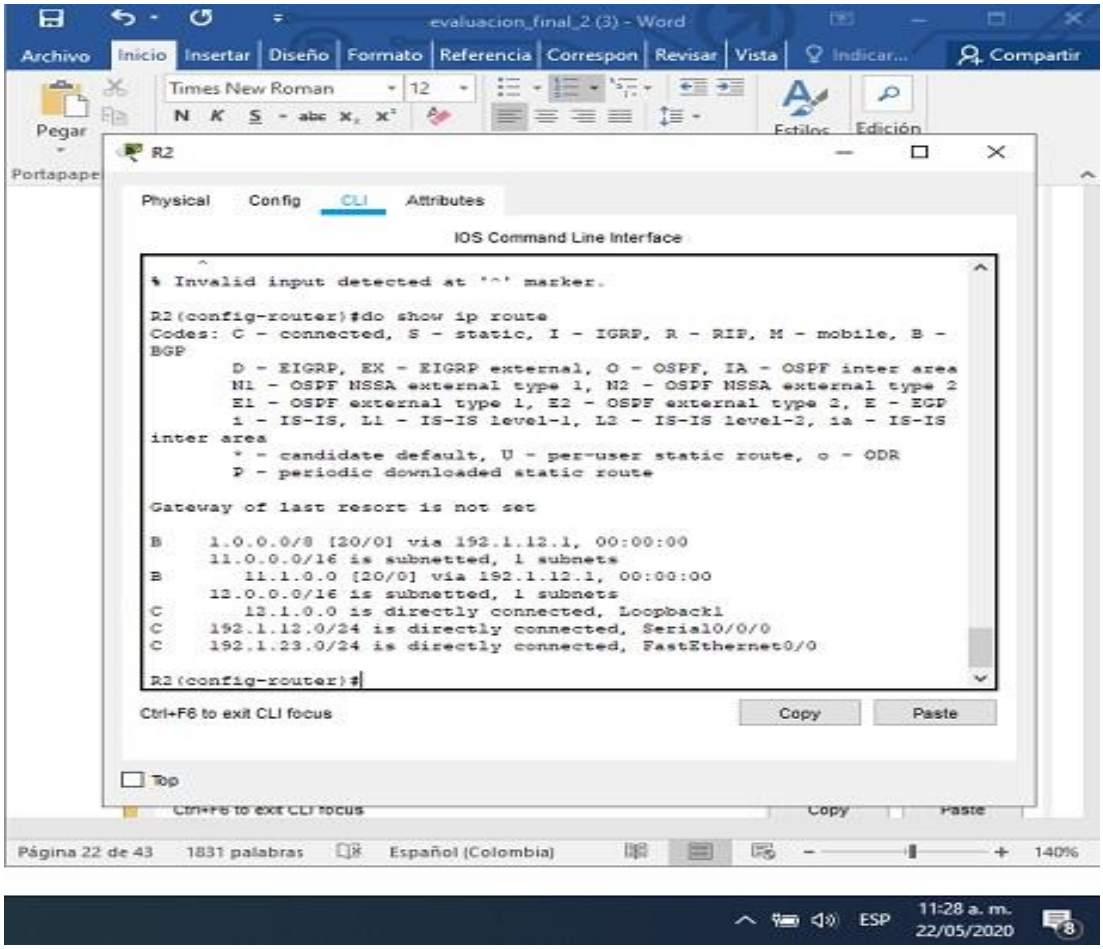


Figura 4 Comando show ip route en R2

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

R2:
R2>en
R2#conf t
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-a 3

R3:
R3>en
R3#conf t
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#network 3.3.3.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#bgp router-id 44.44.44.44

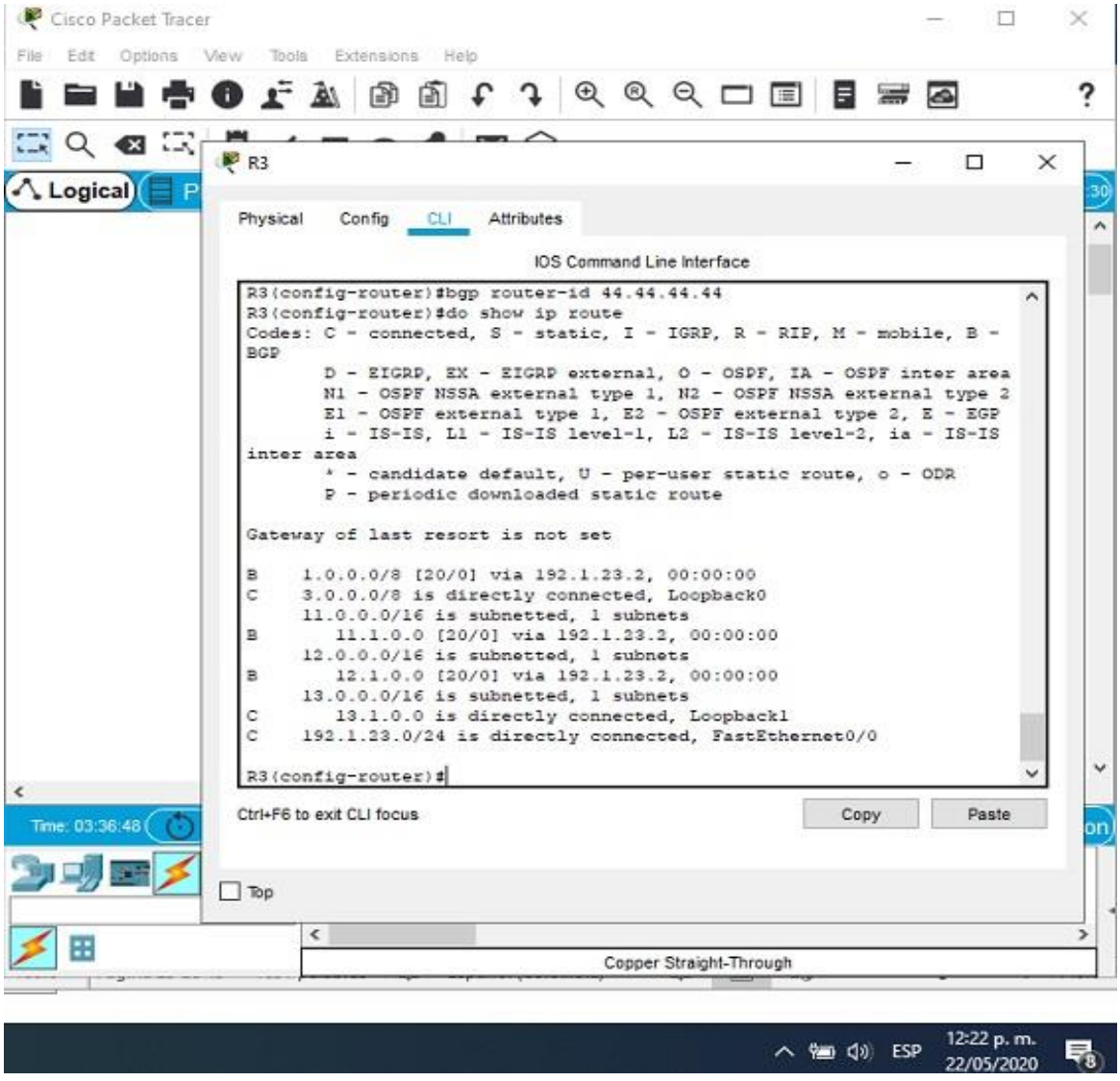


Figura 5 Comando show ip route R3

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP.

Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

R4:
R4>en
R4# conf t
R4(config)#router bgp 4
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#network 4.4.4.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#bgp router 66.66.66.66

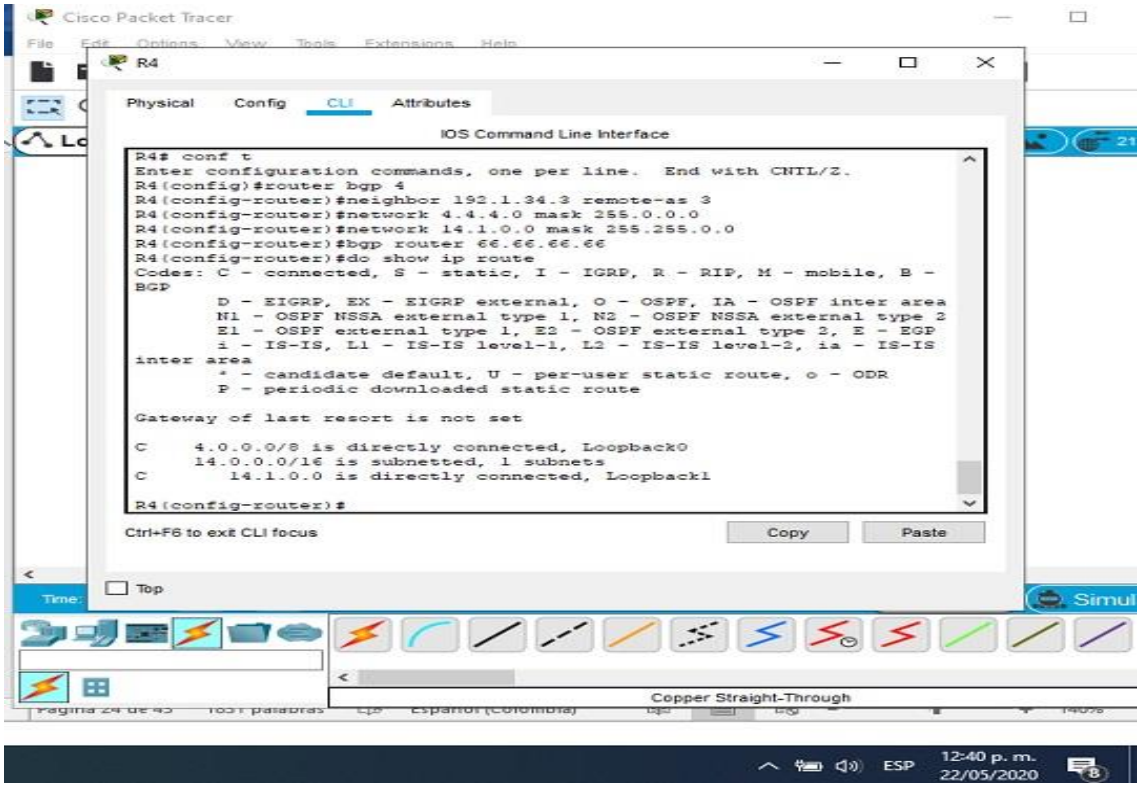


Figura 6 Comando show ip route en R4

2. ESCENARIO 2

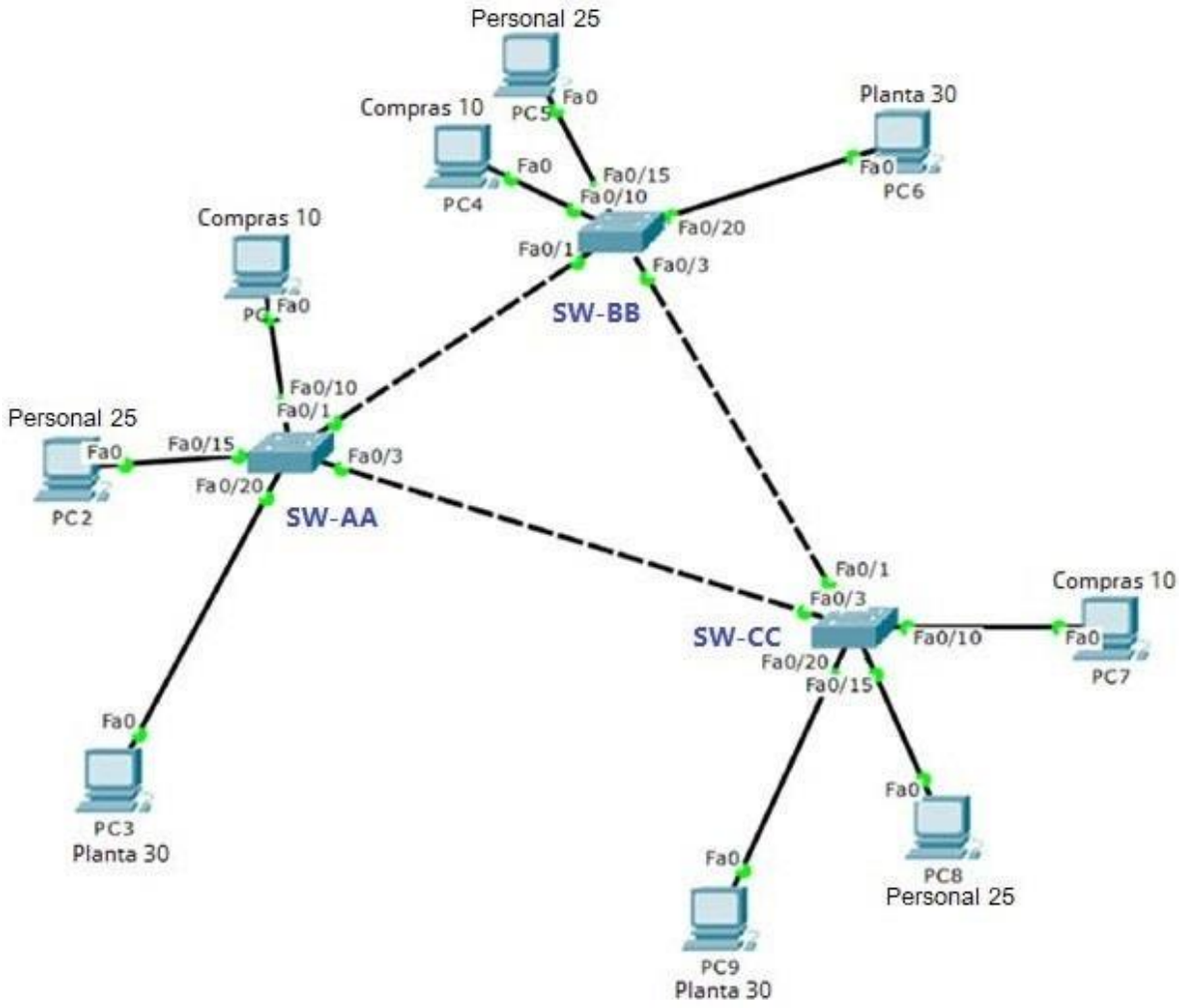


Figura 7 Escenario 2

A. Configurar VTP:

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

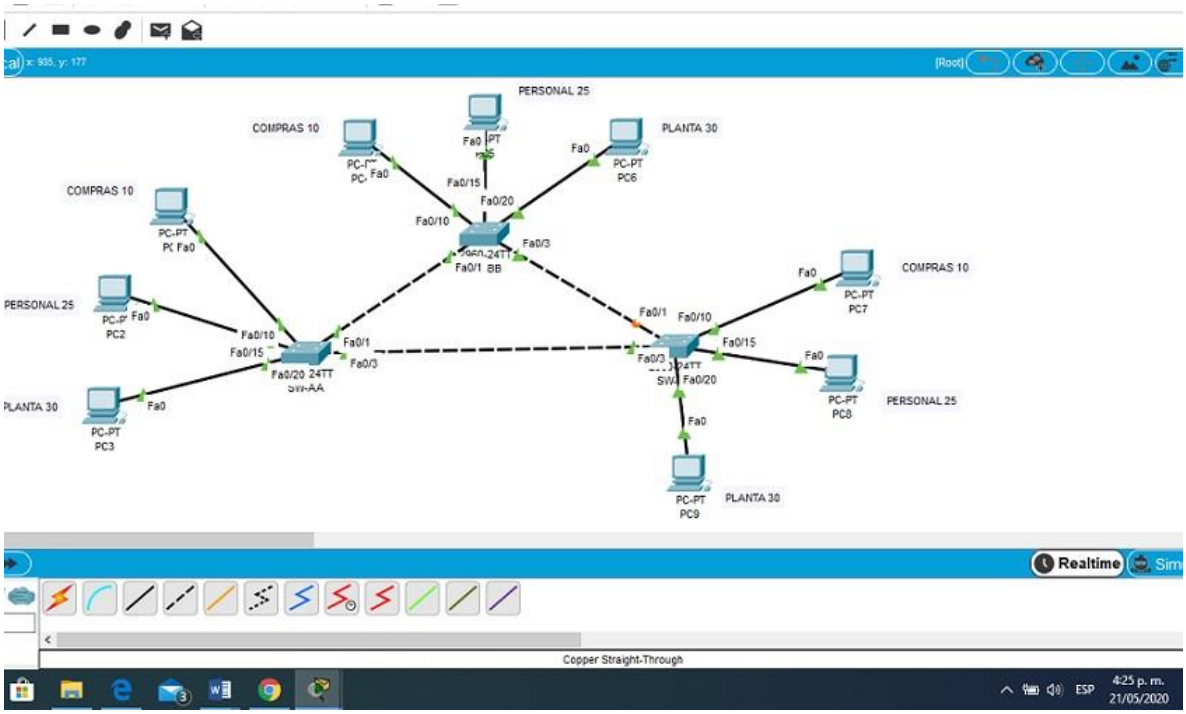


Figura 8 Simulación escenario 2

Configuración Switch SW-BB

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name compras
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name personal
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name planta

SW-BB(config-vlan)#exit

SW-BB(config)#vtp domain VPT

Changing VTP domain name from NULL to VPT

SW-BB(config)#

SW-BB(config)#EXIT

Configuración Switch SW-AA

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vlan 10
SW-AA(config-vlan)#name compras
SW-AA(config-vlan)#exit
SW-AA(config)#vlan 25
SW-AA(config-vlan)#name personal
SW-AA(config-vlan)#exit
SW-AA(config)#vlan 30
SW-AA(config-vlan)#name planta
SW-AA(config-vlan)#exit
SW-AA(config)#vtp domain VPT
Changing VTP domain name from NULL to VPT
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#
SW-AA#

Configuración Switch SW-CC

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vlan 10
SW-CC(config-vlan)#name compras
SW-CC(config-vlan)#exit
SW-CC(config)#vlan 25
SW-CC(config-vlan)#name personal
SW-CC(config-vlan)#exit
SW-CC(config)#vlan 30
SW-CC(config-vlan)#name planta
SW-CC(config-vlan)#exit
SW-CC(config)#vtp domain VPT

Changing VTP domain name from NULL to VPT
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#

2. Verifique las configuraciones mediante el comando show vtp status.

Switch SW-BB

SW-BB>show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
VTP Operating Mode : Server
VTP Domain Name : VPT
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x9D 0x57 0xE9 0x95 0x3B 0xBE 0x04 0xCC
Configuration last modified by 0.0.0.0 at 3-1-93 01:00:56
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB>

Switch SW-AA

SW-AA>show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
VTP Operating Mode : Client
VTP Domain Name : VPT
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x41 0x56 0x23 0x22 0x03 0xD9 0x01 0x22
Configuration last modified by 0.0.0.0 at 3-1-93 01:28:46
SW-AA>

Switch SW-CC

SW-CC>show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
VTP Operating Mode : Client
VTP Domain Name : VPT
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x3F 0x6F 0x2E 0x25 0xB0 0x7E 0x74 0x85
Configuration last modified by 0.0.0.0 at 3-1-93 01:38:24
SW-CC>

B. Configurar DTP (Dynamic Trunking Protocol)

1. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

SW-AA>en
SW-AA#conf t
SW-AA(config)#int f0/1
SW-AA(config-if)#switchport mode trunk

SW-AA(config-if)#

SW-AA(config-if)#switchport mode ?
access Set trunking mode to ACCESS unconditionally
dynamic Set trunking mode to dynamically negotiate access or trunk mode
trunk Set trunking mode to TRUNK unconditionally

2. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando show interfaces trunk.

SW-AA:

SW-AA>show int trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
Port Vlans allowed on trunk
Fa0/1 1-1005

Port Vlans allowed and active in management domain
Fa0/1 1,10,25,30

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,25,30
SW-AA>

SW-BB:

SW-BB(config-if)#switchport mode dynamic desirable

SW-BB(config-if)#

SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config-if)#do show int trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 desirable n-802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-1005

Port Vlans allowed and active in management domain
Fa0/1 1,10,25,30

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,25,30

3. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA

SW-AA>en
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#int f0/3
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#

4. Verifique el enlace "trunk" el comando show interfaces trunk en SW-AA.

SW-AA(config-if)#do show int trunk
Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1
Fa0/3 on 802.1q trunking 1

Port Vlans allowed on trunk
Fa0/1 1-1005
Fa0/3 1-1005

Port Vlans allowed and active in management domain
Fa0/1 1,10,25,30
Fa0/3 1,10,25,30

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,25,30
Fa0/3 1,10,25,30

5. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

SW-BB:

SW-BB>en
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#int f0/3
SW-BB(config-if)#switchport mode trunk

SW-CC:

SW-CC>en
SW-CC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#int f0/1
SW-CC(config-if)#switchport mode trunk

C. Agregar VLANs y asignar puertos.

1. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

SW-AA:

SW-AA>en
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.

SW-AA(config)#int f0/10

SW-AA(config-if)#switchport access vlan 10

SW-BB:

SW-BB>en
SW-BB#conf t
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name admon
SW-BB(config-vlan)#exit
SW-BB(config)#int f0/10
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#int f0/15
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#int f0/20
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#

2. Verifique que las VLANs han sido agregadas correctamente.

SW-BB(config-if)#do show vlan brief

VLAN Name Status Ports
1 default active Fa0/2, Fa0/4, Fa0/5, Fa0/6
Fa0/7, Fa0/8, Fa0/9, Fa0/11
Fa0/12, Fa0/13, Fa0/14, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
10 compras active Fa0/10
25 personal active Fa0/15
30 planta active Fa0/20
99 admon active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
SW-BB(config-if)#

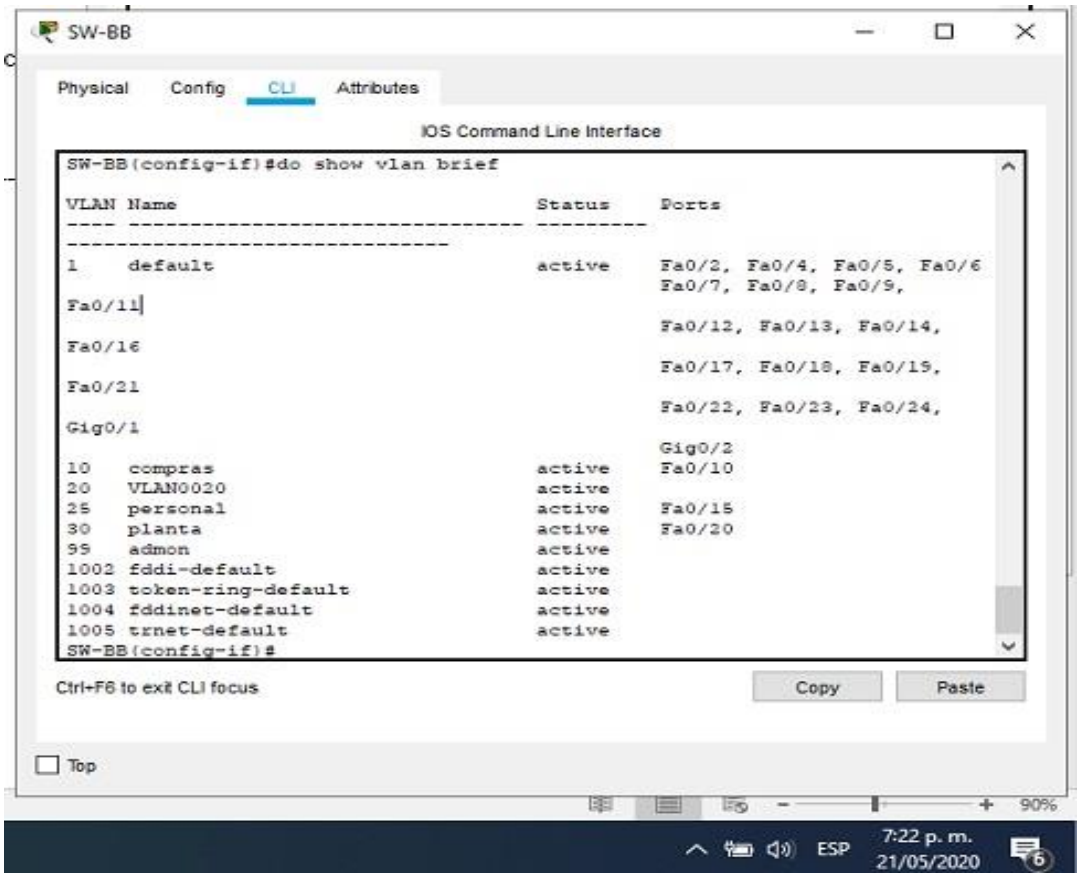


Figura 9 Comando show vlan brief en switch SW-BB

3. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Tabla 5 Escenario 2

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

X= número de cada PC particular

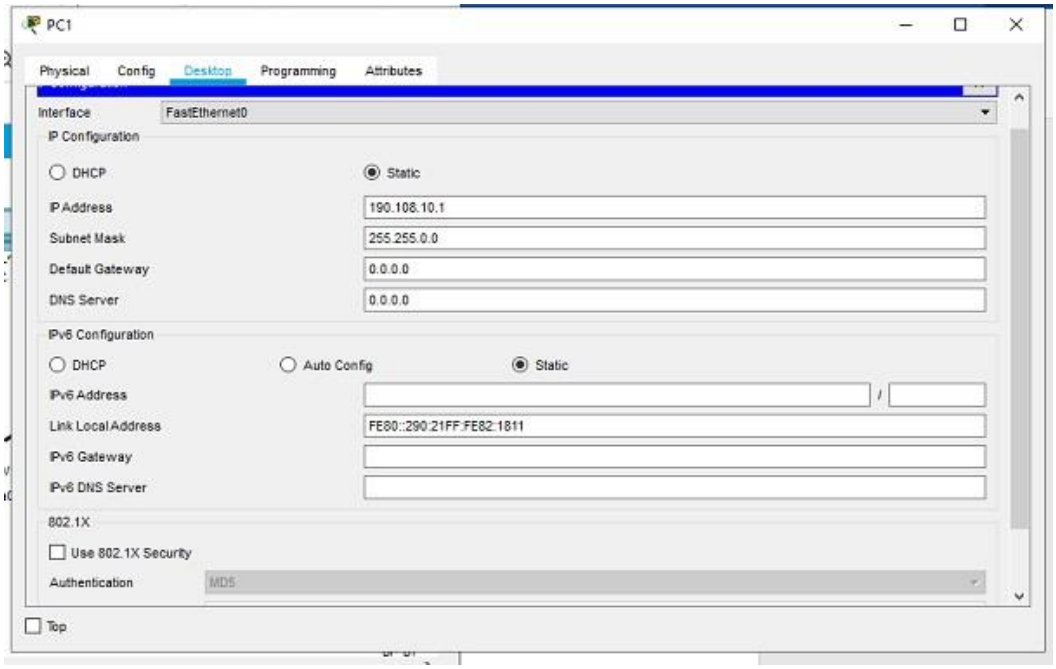


Figura 10 Configuración de PC 1

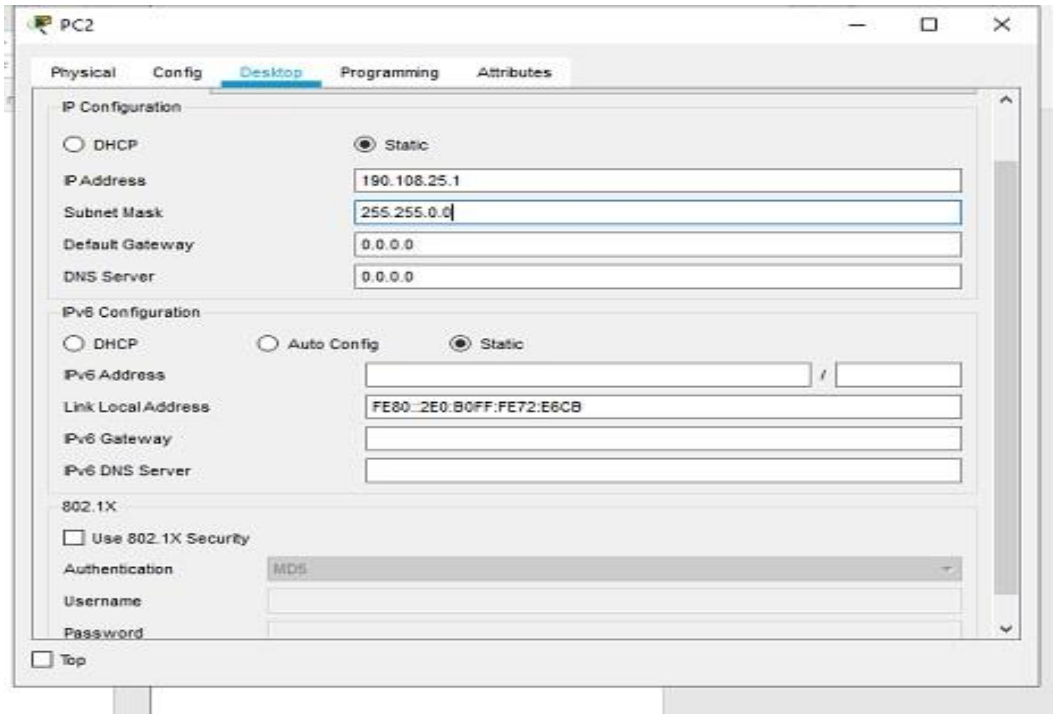


Figura 11 Configuración de PC 2

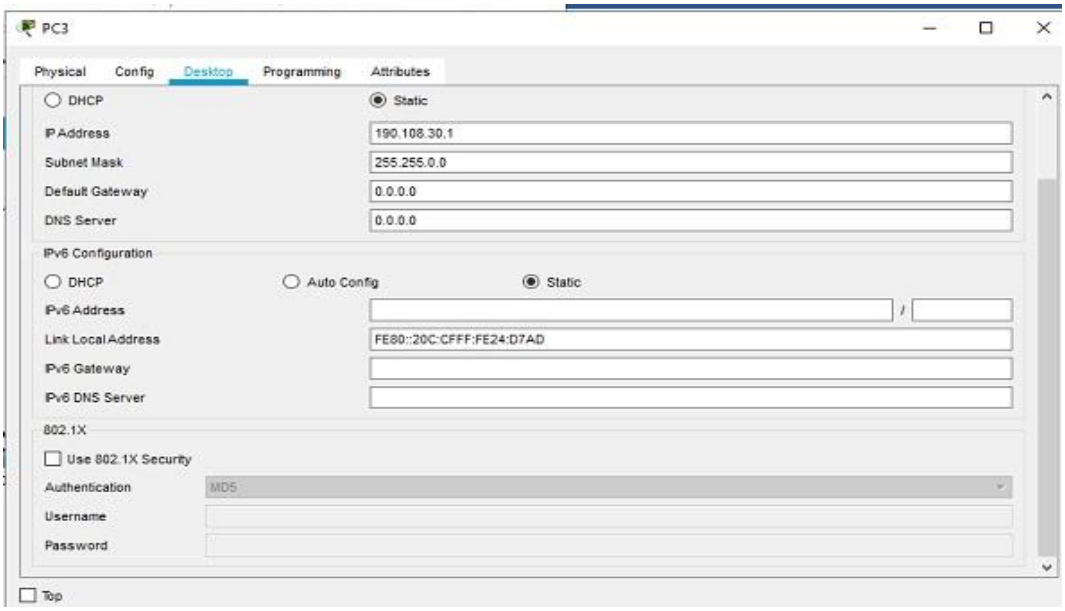


Figura 12 Configuración de PC 3

4. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

SW-AA:

```
SW-AA>en
SW-AA#conf t
SW-AA(config)#int f0/10
SW-AA(config-if)#switchport access vlan 10
```

SW-BB:

```
SW-BB>en
SW-BB#conf t
SW-BB(config)#int f0/10
SW-BB(config-if)#switchport access vlan 10
```

SW-CC:

```
SW-CC>en
SW-CC#conf t
SW-CC(config)#int f0/10
SW-CC(config-if)#switchport access vlan 10
```

5. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

SW-AA:
SW-AA>en
SW-AA#conf t
SW-AA(config-if)#int f0/15
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#int f0/20
SW-AA(config-if)#switchport access vlan 30

SW-BB:
SW-BB>en
SW-BB#conf t
SW-BB(config-if)#int f0/15
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#int f0/20
SW-BB(config-if)#switchport access vlan 30

SW-CC:
SW-CC>en
SW-CC#conf t
SW-CC(config-if)#int f0/15
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#int f0/20
SW-CC(config-if)#switchport access vlan 30

D. Configurar las direcciones IP en los Switches

1. En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 6 Configuración de las direcciones IP en los Switches

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

SW-AA:

```
SW-AA>en
SW-AA#conf t
SW-AA(config)#vlan 99
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#int vlan 99
SW-AA(config-if)#

SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#no shut
```

SW-BB:

```
SW-BB>en
SW-BB#conf t
SW-BB(config)#vlan 99
SW-BB(config-vlan)#int vlan 99
SW-BB(config-if)#

SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#no shut
```

SW-CC:

```
SW-CC>en
SW-CC#conf t
SW-CC(config)#vlan 99
SW-CC(config)#int vlan 99
SW-CC(config-if)#
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#no shut
```

E. Verificar la conectividad Extremo a Extremo

1. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.
2. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.
3. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

Solución 1:

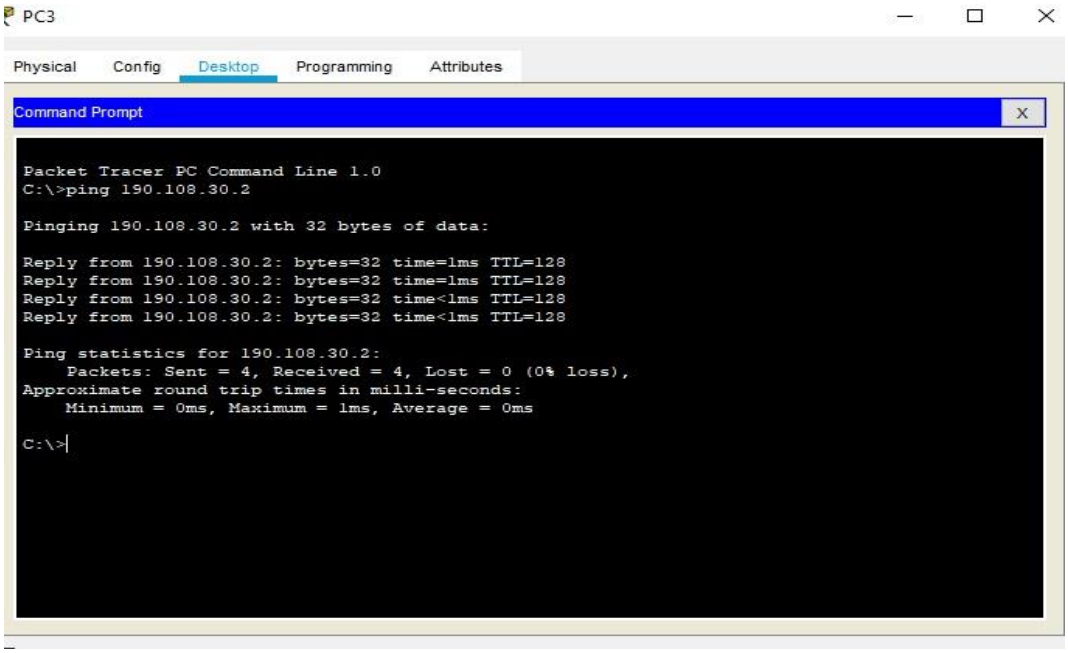
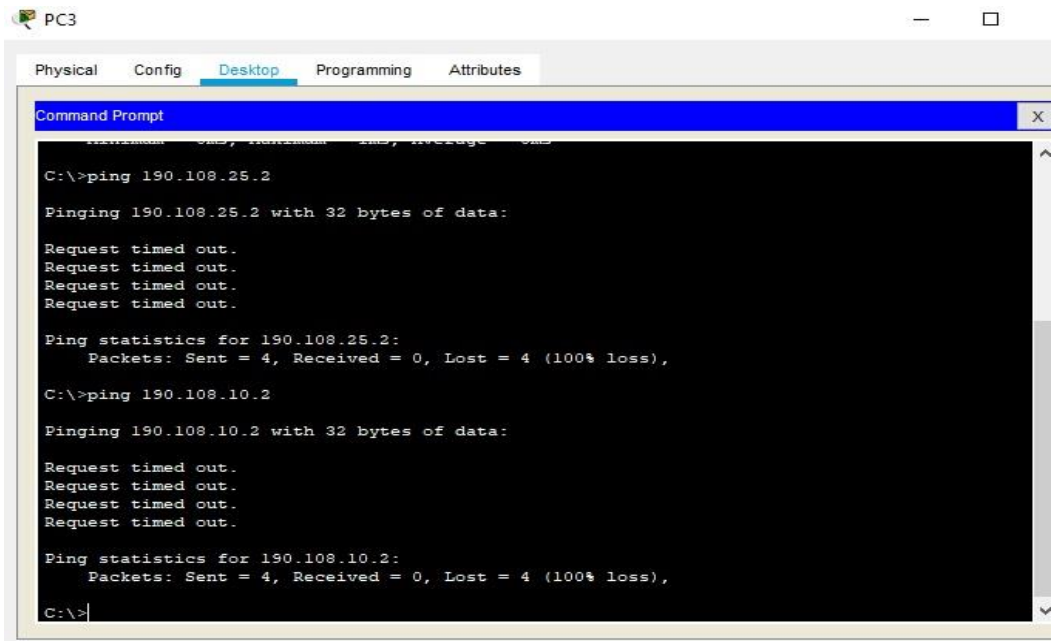


Figura 13 Aplicando ping entre PCs



Se observa que entre los pc de las mismas vlan se obtuvo conexión, pero entre los pc de diferentes vlan no hubo conexión, esto se debe q que se configuro el switch solamente con conexión entre vlan.

Solución 2:

Figura 14 Aplicando ping entre Switches

Se observa que entre los switch si existe conexión, ya que pertenecen a la misma vlan 99.

Solución 3:

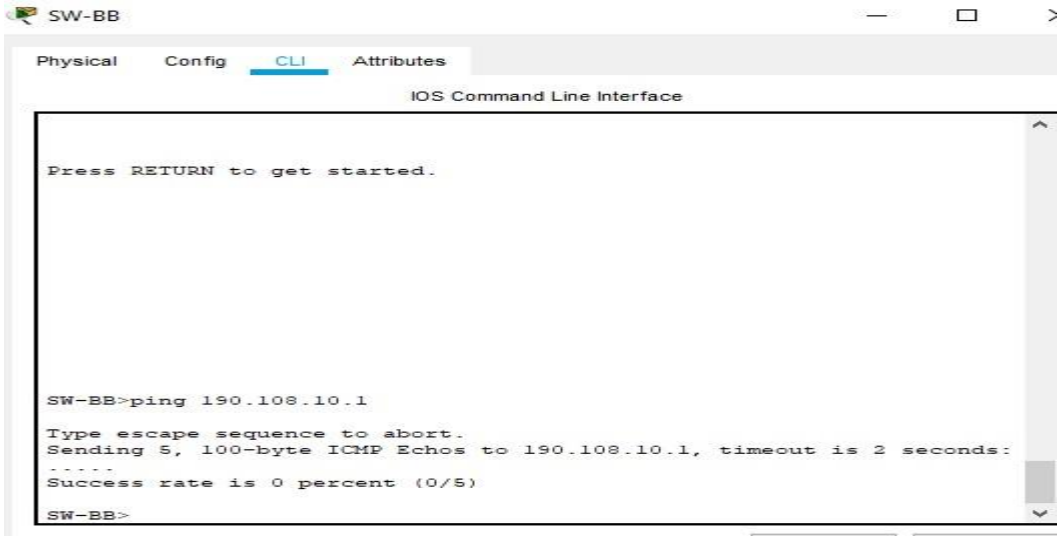


Figura 15 Aplicando ping entre Switches y PCs

Vemos que no se puede realizar ping desde los switch hacia los pcs debido a que los pcs y los switch tienen diferente vlan.

CONCLUSIONES

Con la práctica hecha en esta esta actividad evaluativa, se consiguió recordar temas abordados durante el curso del diplomado y de igual forma los temas vistos en cursos anteriores, donde se pudo realizar diferentes tipos de configuraciones aplicadas a los equipos de capa 2 y capa 3; y así realizar el diferente direccionamiento entre dispositivos. También se aplicó la configuración de interfaces virtuales realizando y validando su conectividad entre los diferentes enlaces.

En la realización de este trabajo, se logró poner en práctica mediante unos escenarios propuestos diferentes protocolos de enrutamiento, como por ejemplo en el primer escenario se hace la configuración entre routers vecinos con el protocolo de Gateway exterior (BGP), para permitir el intercambio de información de ruteo entre sí.

En el desarrollo del segundo escenario se llevó a cabo la configuración de switches mediante el protocolo VTP, el cual sirvió para centralizar en un solo switch la administración de todas las VLANs, configurando éstas de forma manual en cada switch. De igual manera de se llevó a cabo la configuración del protocolo de enrutamiento DTP, para poder habilitar de forma automática los switches y dar un buen direccionamiento entre los dispositivos, fortaleciendo los niveles básicos de seguridad.

.

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de: http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

UNAD (2015). Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg