

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

OSCAR DAVID VELASQUEZ ANZOLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA
TELECOMUNICACIONES BOGOTA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

OSCAR DAVID VELASQUEZ ANZOLA

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 BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA
TELECOMUNICACIONES BOGOTA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 22 de mayo de 2020

CONTENIDO

CONTENIDO	4
LISTA DE FIGURAS	5
LISTA DE TABLAS	6
GLOSARIO	7
RESUMEN	8
ABSTRACT	8
INTRODUCCIÓN	9
DESARROLLO	10
ESCENARIO 1	10
1. Configure una relación de vecino BGP entre R1 y R2	11
2. Configure una relación de vecino BGP entre R2 y R3.	13
3. Configure una relación de vecino BGP entre R3 y R4	14
ESCENARIO 2	17
A. Configurar VTP	17
B. Configurar DTP (Dynamic Trunking Protocol).....	19
C. Agregar VLANs y asignar puertos.	21
D. Configurar las direcciones IP en los Switches	25
E. Verificar la conectividad Extremo a Extremo	26
CONCLUSIONES	31
BIBLIOGRAFÍA	32

LISTA DE FIGURAS

Figura 1 – Escenario1	10
Figura 2 – Configuración r1 bgp entre r1 y r2.....	12
Figura 3 – Configuración r2 bgp entre r1 y r2.....	12
Figura 4 – Configuración r2 bgp entre r2 y r3.....	14
Figura 5 – Configuración r3 entre r2 y r3.....	14
Figura 6 – Configuración r3 bgp entre r3 y r4.....	16
Figura 7 – Configuración r4 entre r3 y r4.....	17
Figura 8 – Escenario 2	17
Figura 9 – Configuración vtp sw-aa.....	18
Figura 10 – Configuración vtp sw-bb.....	18
Figura 11 – Configuración vtp sw-cc.....	19
Figura 12 – Show interfaces trunk dynamic sw-aa.....	19
Figura 13 – Show interfaces trunk sw-bb.....	20
Figura 14 – Show interfaces trunk estatico sw-aa.....	20
Figura 15 – Show interfaces trunk permanente sw-bb.....	21
Figura 16 – Show interfaces trunk permanente sw-cc.....	21
Figura 17 – Configuración vlan sw-aa.....	22
Figura 18 – Configuración vlan sw-aa.....	22
Figura 19 – Configuración vlan sw-bb.....	23
Figura 20 – Configuración vlan sw-cc.....	23
Figura 21 – Ping de pc1 a pc3.....	26
Figura 22 – Ping de pc1 a pc4.....	27
Figura 23 – Ping de pc5 a pc8 y pc9.....	27
Figura 24 – Ping de pc9 a pc2 y pc3.....	28
Figura 25 – Ping de sw-aa a swbb y swcc.....	28
Figura 26 – Ping de sw-bb a swaa y swcc.....	29
Figura 27 – Ping de sw-cc a swbb y swaa.....	29
Figura 28 – Ping de sw-aa a pc1-pc2 y pc3.....	29
Figura 29 – Ping de sw-cc a pc7-pc8 y pc3.....	30

LISTA DE TABLAS

Tabla 1 – Configuración routers r1 y r2.....	10
Tabla 2 – Configuración routers r3 y r4.....	11
Tabla 3 – Puertos vlan.....	23
Tabla 4 – Direcciones ip en switch.....	25

GLOSARIO

BGP: protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos.

CONSOLA: método que permite a las personas dar instrucciones por medio de código a los diferentes dispositivos.

DTP: (Dynamic Trunking Protocol) protocolo creado por Cisco Systems, opera entre switches Cisco, automatiza la configuración de trunking.

EBGP: sesiones externas de BGP, envía información de routing entre ASs

EIGRP: protocolo de Enrutamiento de Puerta de enlace Interior mejorado.

INTERFACE LOOPBACK: interfaz de red virtual, utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

OSPF: protocolo de red para enrutamiento jerárquico, usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

ROUTER: producto de hardware que permite interconectar redes de datos, se encarga de establecer la mejor ruta.

SISTEMA AUTÓNOMO: grupo de redes IP que poseen una política de rutas propia e independiente.

SWITCH: dispositivo de interconexión de equipos a nivel local.

TOPOLOGÍA DE RED: mapa físico o lógico de una red para intercambiar datos.

VLAN: (Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

VTP: VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco.

RESUMEN

Proporcionar solución a dos (2) escenarios propuestos del diplomado de Cisco CCNP, que corresponden a configuración de routes y switches, acompañado de los respectivos procesos de documentación de la solución, los cuales pertenecen al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de protocolos Bgp, Vtp, Dtp, Vlan y el uso de comandos como ping, traceroute, show ip route, entre otros.

Para realizar los procesos de configuración y simulación se emplearan las herramientas: Packet Tracer y GNS3.

Palabras Clave: CISCO, CCNP, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA.

ABSTRACT

Provide solution to two (2) proposed scenarios of the Cisco CCNP, which corresponds to configuration of routes and switches, accompanied by the respective documentation processes of the solution, which belong to the configuration record of each of the devices, the detailed step-by-step description of each of the stages carried out during its development, the registration of connectivity verification processes through the use of Bgp, Vtp, Dtp, Vlan protocols and the use of commands such as ping, traceroute, show ip route, among others.

To carry out the configuration and simulation processes, the tools: Packet Tracer and GNS3 will be used.

Keywords: SWITCHING, ROUTING, NETWORKS, ELECTRONICS.

INTRODUCCIÓN

El presente trabajo de opción de grado para optar el título de ingeniero de telecomunicaciones tiene como principal objetivo identificar, el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado.

Se proporcionará solución a dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, los cuales corresponden al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Para el escenario 1 es necesario configurar una relación de vecino BGP entre diferentes routes y anunciar direcciones Loopback.

Para el escenario 2 es necesario configurar los protocolos VTP, DTP (Dynamic Trunking Protocol), agregar VLANs y asignar puertos, Configurar las direcciones IP en los Switches, verificar la conectividad extremo a extremo

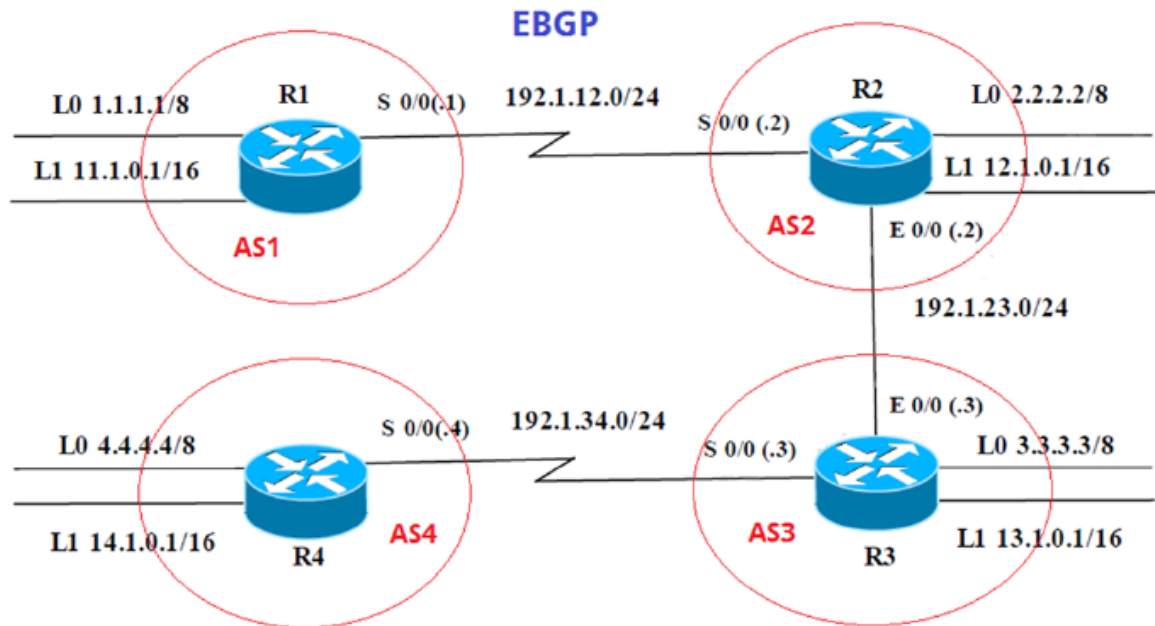
Los procesos de configuración y simulación de los escenarios se realizaran mediante herramientas: Packet Tracer y GNS3.

Con la solución de este trabajo se demuestra los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

DESARROLLO

ESCENARIO 1

FIGURA 1 – ESCENARIO1



Información para configuración de los Routers

TABLA 1 – CONFIGURACIÓN RUTERS R1 Y R2

	Interfaz	Dirección IP	Máscara
R1	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
R2	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 2 – CONFIGURACIÓN ROUTERS R1 Y R2

	Interfaz	Dirección IP	Máscara
R3	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
R4	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

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.

```

R1#configure terminal
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 1

```

```

R2#configure terminal
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0

```

```

R2(config-if)#interface serial 1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface fastEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 2

```

FIGURA 2 – CONFIGURACIÓN R1 BGP ENTRE R1 Y R2

```

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial1/0
C    1.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
R1# FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0035 0104 0002 00B4 2121 2121 1802 0601 0400 0100 0102 0280 0002 0
202 0002 0641 0400 0000 02

```

FIGURA 3 – CONFIGURACIÓN R2 BGP ENTRE R1 Y R2

```

R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial1/0
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:34
C    192.1.23.0/24 is directly connected, FastEthernet0/0
B    192.1.34.0/24 [20/0] via 192.1.23.3, 00:00:34
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:00:34
R2#
*May 15 21:08:20.359: %BGP-3-NOTIFICATION: received from neighbor 192.1.12.1 2/2 (peer in wrong AS) 2 bytes 00

```

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#configure terminal
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

```
R3#configure terminal
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface fastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

FIGURA 4 – CONFIGURACIÓN R2 BGP ENTRE R2 Y R3

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial1/0
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:06:26
C    192.1.23.0/24 is directly connected, FastEthernet0/0
B    192.1.34.0/24 [20/0] via 192.1.23.3, 00:06:26
     12.0.0.0/16 is subnetted, 1 subnets
C         12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B         13.1.0.0 [20/0] via 192.1.23.3, 00:06:26
R2#
```

FIGURA 5 – CONFIGURACIÓN R3 ENTRE R2 Y R3

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:04:21
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:04:21
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.23.2, 00:04:21
     13.0.0.0/16 is subnetted, 1 subnets
C         13.1.0.0 is directly connected, Loopback1
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.

```
R3#configure terminal
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 3
```

```
R4#configure terminal
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 4
```

FIGURA 6 – CONFIGURACIÓN R3 BGP ENTRE R3 y R4

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:11:02
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:11:02
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:11:02
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3# FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0035 0104 0004 00B4 4242 4242 1802 0601 0400 0100 0102 0280 0002 0
202 0002 0641 0400 0000 04
```

FIGURA 7 – CONFIGURACIÓN R4 ENTRE R3 y R4

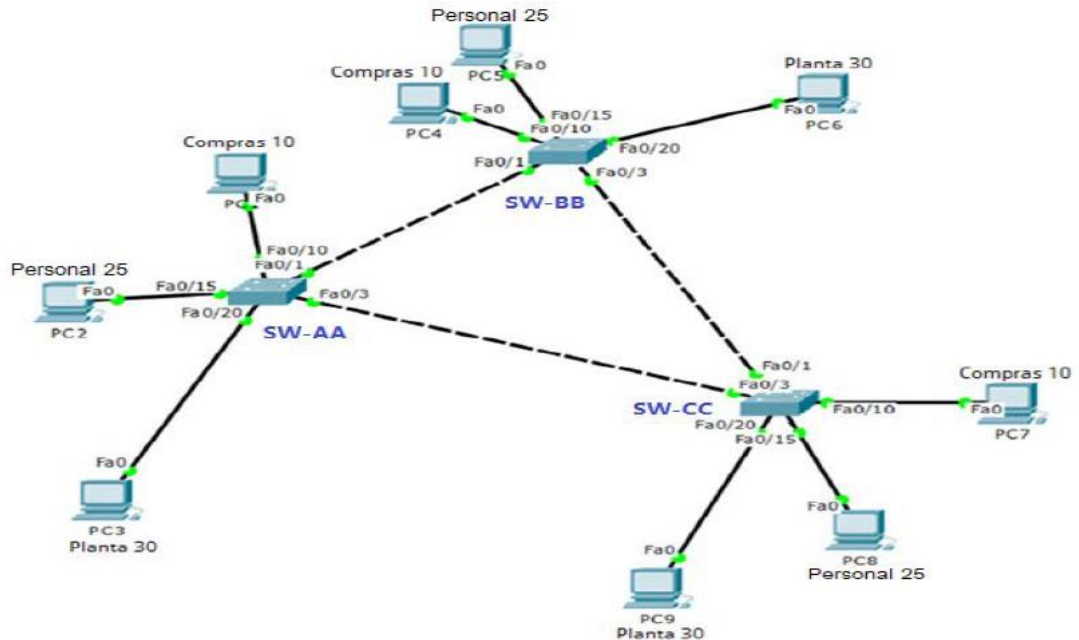
```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

S    3.0.0.0/8 [1/0] via 192.1.34.3
C    4.0.0.0/8 is directly connected, Loopback0
C    192.1.34.0/24 is directly connected, Serial1/0
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
R4#
*May 15 21:20:08.831: %BGP-3-NOTIFICATION: sent to neighbor 192.1.34.3 2/2 (peer in wrong AS) 2 bytes 0003
R4# FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0035 0104 0003 00B4 2C2C 2C2C 1802 0601 0400 0100 0102 0280 0002 0
202 0002 0641 0400 0000 03
```


ESCENARIO 2

FIGURA 8 – 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 VTP llamado CCNP y usando la contraseña cisco.

```
SW-AA(config) #vtp mode client
setting device to vtp client mode.
SW-AA (config) #vtp domain ccnp
changing vtp domain name from null to ccnp
SW-AA (config) #vtp password cisco
setting device vlan database password to cisco
```

```
SW-BB# configure terminal
SW-BB (config) #vtp mode server
Setting device to VTP SERVER mode.
SW-BB (config) #vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB (config) #vtp password cisco
Setting device VLAN database password to cisco
```

```

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

```

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

FIGURA 9 – CONFIGURACIÓN VTP SW-AA

```

SW-AA#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Client
VTP Domain Name           : CCNP
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xB1 0x62 0xD1 0x85 0xDB 0x68 0x6B 0x06
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

```

FIGURA 10 – CONFIGURACIÓN VTP SW-BB

```

SW-BB#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           : CCNP
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

```

FIGURA 11 – CONFIGURACIÓN VTP SW-CC

```
SW-CC#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

B. Configurar DTP (Dynamic Trunking Protocol)

3. 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-BB#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW-BB(config)#interface fa0/1
```

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

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

FIGURA 12 – SHOW INTERFACES TRUNK DYNAMIC SW-AA

```
SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto     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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
```

FIGURA 13 – SHOW INTERFACES TRUNK SW-BB

```
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
```

5. 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#configure terminal
SW-AA(config)#int fa0/3
SW-AA(config-if)#switchport mode trunk
```

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

FIGURA 14 – SHOW INTERFACES TRUNK ESTATICO SW-AA

```
SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-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
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1
```

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

```
SW-BB#configure terminal
SW-BB(config)#int f0/3
SW-BB(config-if)#switchport mode trunk
```

FIGURA 15 – SHOW INTERFACES TRUNK PERMANENTE SW-BB

```
SW-BB#show interfaces 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         1,10,25,30,99
Fa0/3         1,10,25,30,99

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,25,30,99
Fa0/3         none
```

FIGURA 16 – SHOW INTERFACES TRUNK PERMANENTE SW-CC

```
SW-CC#show interfaces trunk
Port          Mode          Encapsulation  Status        Native vlan
Fa0/1         on            802.1q         trunking      1
Fa0/3         auto          n-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
Fa0/3         1

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         none
Fa0/3         1
```

C. Agregar VLANs y asignar puertos.

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

```
SW-AA#conf t
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode
```

FIGURA 17 – CONFIGURACIÓN VLAN SW-AA

```
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

SW-BB#conf t

Enter configuration commands, one per line. End with CNTL/Z.

```
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name admon
SW-BB(config-vlan)#exit
```

9. Verifique que las VLANs han sido agregadas correctamente.

FIGURA 18 – CONFIGURACIÓN VLAN SW-AA

```
SW-AA#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10	compras	active	
25	personal	active	
30	planta	active	
99	admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

FIGURA 19 – CONFIGURACIÓN VLAN SW-BB

SW-BB#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10 compras	active	
25 personal	active	
30 planta	active	
99 admon	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

FIGURA 20 – CONFIGURACIÓN VLAN SW-CC

SW-CC>enable
SW-CC#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig1/1, Gig1/2
10 compras	active	
25 personal	active	
30 planta	active	
99 admon	active	

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

TABLA 3 – PUERTOS VLAN

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

11. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.
12. 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(config)#int fa 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#int fa 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#int fa 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

```
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#int fa 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#int fa 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#int fa 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
```

```
SW-CC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#int fa 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#int fa 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
```



```

SW-CC(config-if)#exit
SW-CC(config)#int fa 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

```

```

PC1: ip address 190.108.10.1 255.255.255.0
PC2: ip address 190.108.20.2 255.255.255.0
PC3: ip address 190.108.30.3 255.255.255.0
PC4: ip address 190.108.10.4 255.255.255.0
PC5: ip address 190.108.20.5 255.255.255.0
PC6: ip address 190.108.30.6 255.255.255.0
PC7: ip address 190.108.10.7 255.255.255.0
PC8: ip address 190.108.20.8 255.255.255.0
PC9: ip address 190.108.30.9 255.255.255.0

```

D. Configurar las direcciones IP en los Switches.

13. 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 4 – DIRECCIONES IP EN SWITCH

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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#

```

```

SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface vlan 99
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up

```

```
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

```
SW-CC#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
SW-CC(config)#interface vlan 99
```

```
SW-CC(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed  
state to up
```

```
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

E. Verificar la conectividad Extremo a Extremo

14. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

FIGURA 21. PING DE PC1 A PC3

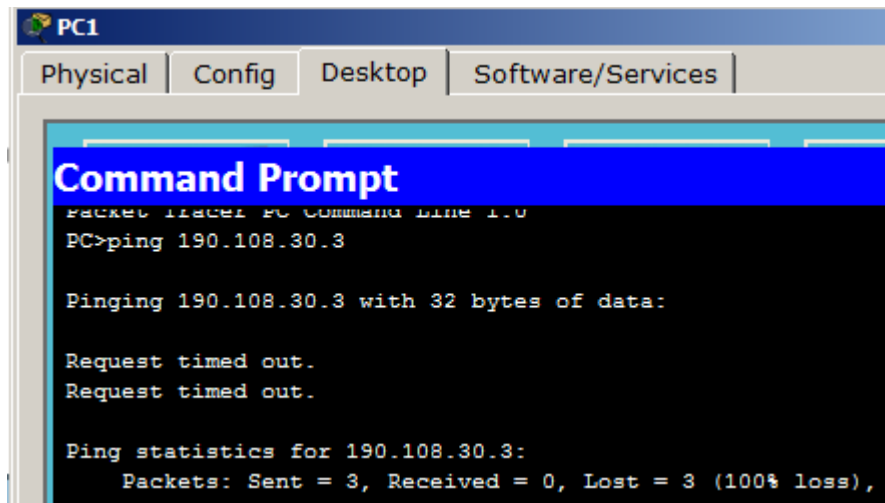
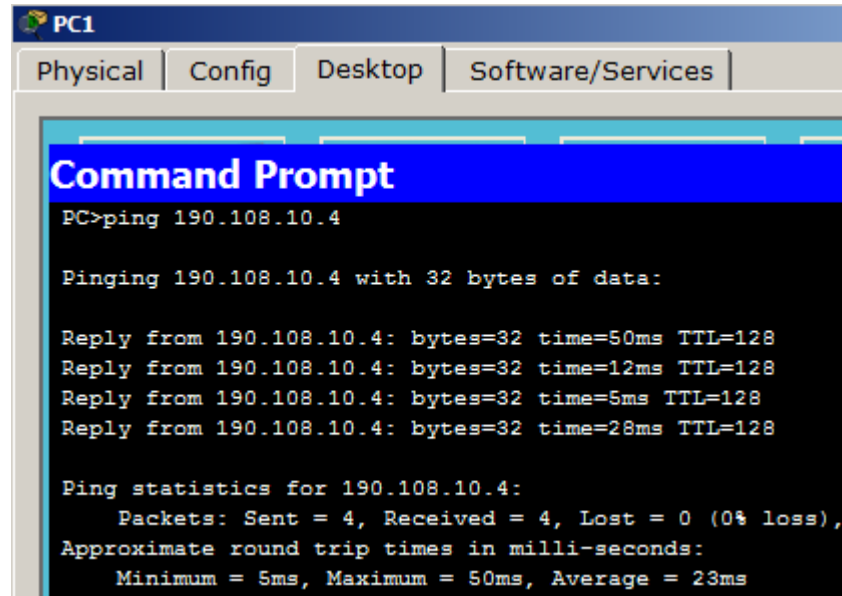


FIGURA 22 PING DE PC1 A PC4



```
PC1
Physical Config Desktop Software/Services

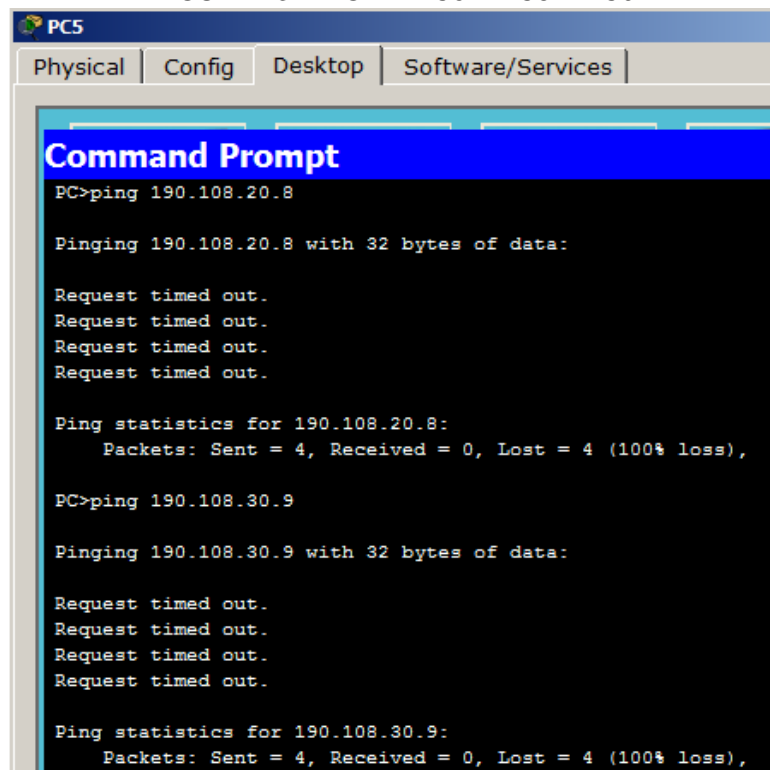
Command Prompt
PC>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

Reply from 190.108.10.4: bytes=32 time=50ms TTL=128
Reply from 190.108.10.4: bytes=32 time=12ms TTL=128
Reply from 190.108.10.4: bytes=32 time=5ms TTL=128
Reply from 190.108.10.4: bytes=32 time=28ms TTL=128

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 50ms, Average = 23ms
```

FIGURA 23 PING DE PC5 A PC8 Y PC9



```
PC5
Physical Config Desktop Software/Services

Command Prompt
PC>ping 190.108.20.8

Pinging 190.108.20.8 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

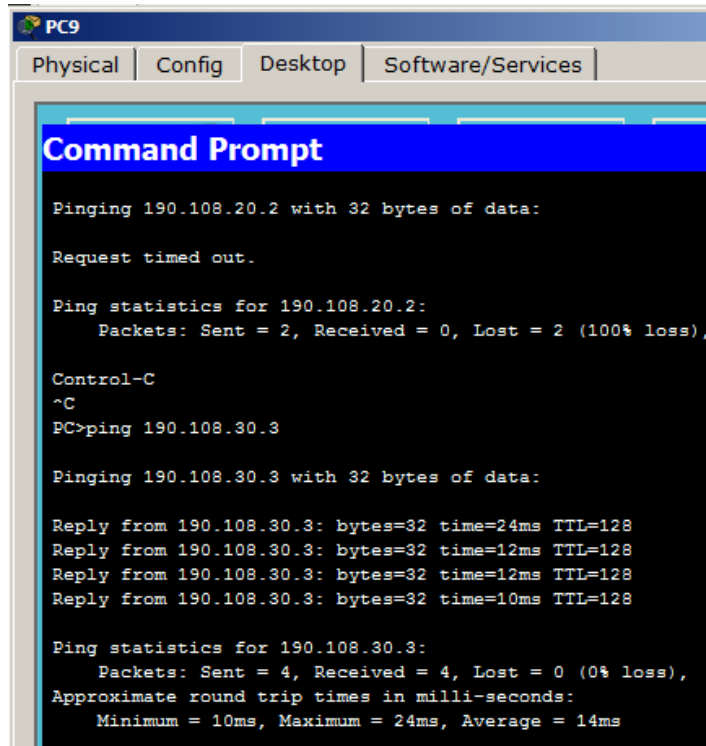
PC>ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

FIGURA 24 PING DE PC9 A PC2 Y PC3



```
PC9
Physical Config Desktop Software/Services
Command Prompt

Pinging 190.108.20.2 with 32 bytes of data:

Request timed out.

Ping statistics for 190.108.20.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
PC>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

Reply from 190.108.30.3: bytes=32 time=24ms TTL=128
Reply from 190.108.30.3: bytes=32 time=12ms TTL=128
Reply from 190.108.30.3: bytes=32 time=12ms TTL=128
Reply from 190.108.30.3: bytes=32 time=10ms TTL=128

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 24ms, Average = 14ms
```

El ping realizado entre los PCs pertenecientes a diferentes Vlan no tuvo éxito, los pings realizados a PCs que perteneces a la misma Vlan, si tuvieron éxito. El error en los PCs pertenecientes a diferentes Vlan se presenta ya que cada PC pertenece a un segmento de red diferente.

15. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

FIGURA 25 PING DE SW-AA A SWBB Y SWCC

```
SW-AA#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 4/4/4 ms

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

FIGURA 26 PING DE SW-BB A SWAA Y SWCC

```
SW-BB#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms

SW-BB#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

FIGURA 27 PING DE SW-CC A SWBB Y SWAA

```
SW-CC#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/10 ms

SW-CC#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

16. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

FIGURA 28 PING DE SW-AA A PC1-PC2 Y PC3

```
SW-AA#ping 192.108.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 192.108.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 192.108.30.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

FIGURA 29 PING DE SW-CC A PC7-PC8 Y PC3

```
SW-CC>ping 190.108.10.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC>ping 190.108.20.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC>ping 190.108.30.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

CONCLUSIONES

Se aplicaron las preparaciones para realizar el enrutamiento EBGP el cual es uno de protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos.

Se designaron los conocimientos para realizar el enrutamiento EBGP el cual es uno de protocolo mediante el cual se intercambia información de partida o ruteo entre sistemas autónomos.

Se emplearon los conocimientos para realizar el enrutamiento EBGP el cual es uno de protocolo mediante el cual se intercambia información de orientación o ruteo entre sistemas autónomos.

Con las herramientas como GNS3, Packet Tracer se realizó el desarrollo de los escenarios propuestos como parte de la evaluación final del curso, se logra aplicar los conocimientos teóricos y las habilidades prácticas construidas a través del curso.

BIBLIOGRAFÍA

Casos Prácticos de BGP. (30 de Octubre de 2008). Obtenido de Cisco:
https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

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>

Temática: High Availability

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

Temática: First Hop Redundancy Protocols

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). OSPF Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>