DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CRISTIAN DAVID SOLANO VINCHIRA

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CRISTIAN DAVID SOLANO VINCHIRA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

Tabla de Contenido

Lista de Tablas

Tabla de ilustraciones

Glosario

AS: Un Sistema Autónomo (en inglés, Autonomous System: AS) se define como “un grupo de redes IP que poseen una política de rutas propia e independiente”. Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. Un número de AS o ASN se asigna a cada AS, el que lo identifica de manera única a sus redes dentro de Internet.

BGP: es el protocolo de encaminamiento EGP más utilizado en Internet. La versión 1 de este protocolo (RFC 1105) apareció en 1989 para sustituir a EGP. ... BGP es un protocolo que funciona sobre TCP por el puerto 179. BGP permite el encamZinamiento de los paquetes IP que se intercambian entre los distintos AS.

DTP: DTP (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet. Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE.

Interface loopback: una interfaz loopback es aquella interfaz virtual mas no física que sirve para tener latente el protocolo de enrutamiento como OSPF, el cual, al no detectar interfaces activas en el dispositivo después de cierto tiempo

Interface troncal: Un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red. Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet.

Router: es como su propio nombre indica, y fácilmente se puede traducir, un enrutador o encaminador que nos sirve para interconectar redes de ordenadores y que actualmente implementan puertas de acceso a internet como son los router para ADSL, los de Cable o 3G

Switch: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet

VLAN: (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch

VTP: Protocolo VTP. Virtual Trunking Protocol (VTP) es un protocolo propietario de CISCO. VTP sirve para centralizar en un solo switch la administración de todas las VLANs. En una red física suele haber varios switches interconectados que admiten varias VLANs

Resumen

La idea fundamental de este trabajo es realizar las practica principalmente del protocolo de enrutamieno de exteriores BGP el cual es el encargado de enrutar la data en Internet entre diferentes sistemas Autonomos e ISP´S, los protocolos de enrutamiento dinamico como lo es BGP nos permite compartir de manera dinamica los segmentos directamente conectados a los enrutadores haciendo que el proceso de creacion de las tabla de enrutamiento sea altamente escalable, ademas de colocar en practica el protocolo VTP el cual es de gran ayuda para gestionar las VLAN de manera centralizada entendiendo los riegos y la vulnerabilidades que posee, esta actividad se realizara enteramente sobre switches de la compañía CISCO los temas aca expuestos son parte de la curricula de la certificacion CCNP R&S para los examenes CCNP Route y CCNP Switch.

Abstract

The fundamental idea of this work is to carry out the practices mainly of the external routing protocol BGP which is in charge of routing the data on the Internet between different Autonomous systems and ISP´S, dynamic routing protocols such as BGP allows us to share dynamically the segments directly connected to the routers making the routing table creation process highly scalable, in addition to putting into practice the VTP protocol which is of great help in managing VLANs in a centralized way, understanding the risks and The vulnerabilities it has, this activity will be carried out entirely on switches from the CISCO company. The topics presented here are part of the CCNP R&S certification curriculum for the CCNP Route and CCNP Switch exams.

Introduccion

El objetivo principal del curso fue explicar de manera detallada toda la curricula o blueprint de los exámenes de certificación de Cisco Systems CCNP Switch y CCNP Route, allí se nos explica aplicaciones reales de la teoria en casos que podriamos encontrar en redes enterprise.

En este presente trabajo se muestras las evidencias de las prácticas de los escenarios 1 configuración básica de BGP y escenario 2 configuraciones del protocolo VTP, junto a las evidencias fotográficas e scrips usados para completar la actividad de manera exitosa.

Escenario # 1

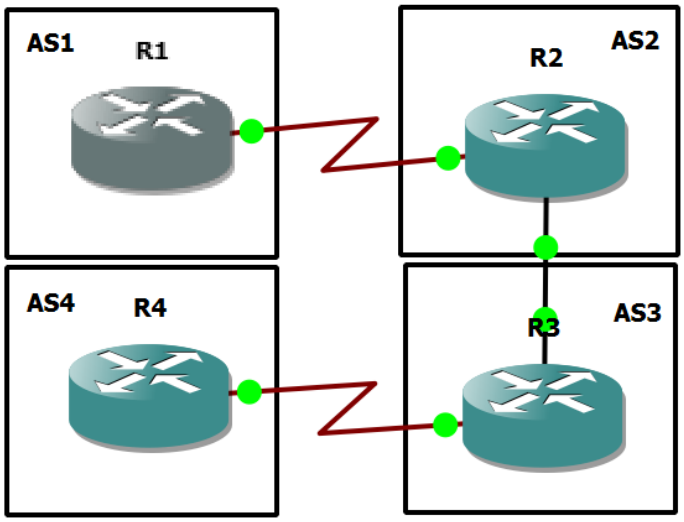

Figura 1: Escenario 1

Información para configuración de los Routers

R1

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

R2

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 1: Direccionamientos R1 y R2

R3

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

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

Tabla 2: Direccionamientos R3 y R4

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.**

interface lo0
ip add 1.1.1.1 255.0.0.0
interface lo1
ip add 11.1.0.1 255.255.0.0
interface s1/0
ip add 192.168.12.1 255.255.255.0
no shut
router bgp 100
network 1.0.0.0 mask 255.0.0.0
network 11.1.0.0 mask 255.255.0.0
network 192.168.12.0 mask 255.255.255.0
neighbor 192.168.12.2 remote-as 200
bgp router-id 22.22.22.22

```
router bgp 100
 no synchronization
 bgp router-id 22.22.22.22
 bgp log-neighbor-changes
 network 1.0.0.0
 network 11.1.0.0 mask 255.255.0.0
 network 192.168.12.0
 neighbor 192.168.12.2 remote-as 200
 no auto-summary
```

Figura 2: Configuración BGP R1

interface lo0
ip add 2.2.2.2 255.0.0.0
interface lo1
ip add 12.1.0.1 255.255.0.0
interface s1/0
ip add 192.168.12.2 255.255.255.0
no shut
interface fast 2/0
ip add 192.168.23.2 255.255.255.0
router bgp 200
network 2.0.0.0 mask 255.0.0.0
network 12.1.0.0 mask 255.255.0.0
network 192.168.12.0 mask 255.255.255.0
neighbor 192.168.12.2 remote-as 100
neighbor 192.168.23.3 remote-as 300
bgp router-id 33.33.33.33

```
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 2.0.0.0
 network 12.1.0.0 mask 255.255.0.0
 network 192.168.12.0
 network 192.168.23.0
 neighbor 192.168.12.1 remote-as 100
 neighbor 192.168.23.3 remote-as 300
 no auto-summary
```

Figura 3: Configuración BGP 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.**

   interface lo0
   ip add 3.3.3.3 255.0.0.0
   interface lo1
   ip add 13.1.0.1 255.255.0.0
   interface fast 2/0
   no switchport
   no shut
   ip add 192.168.23.3 255.255.255.0
   interface s1/0
   no shut
   ip add 192.1.34.3 255.255.255.0
   no shut
   router bgp 300
   network 3.0.0.0 mask 255.0.0.0
   network 13.1.0.0 mask 255.255.0.0

network 192.168.23.0 mask 255.255.255.0
neighbor 192.168.23.2 remote-as 200
neighbor 192.168.34.4 remote-as 400
bgp router-id 44.44.44.44

```
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 network 3.0.0.0
 network 13.1.0.0 mask 255.255.0.0
 network 192.168.23.0
 network 192.168.34.0
 neighbor 192.168.23.2 remote-as 200
 neighbor 192.168.34.4 remote-as 400
 no auto-summary
```

Figura 4: Configuración BGP 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.**

```
interface lo0
ip add 4.4.4.4 255.0.0.0
interface lo1
ip add 14.1.0.1 255.255.0.0
interface s1/0
no shut
ip add 192.168.34.4 255.255.255.0
router bgp 400
network 4.0.0.0 mask 255.0.0.0
network 14.1.0.0 mask 255.255.0.0
network 192.168.34.0 mask 255.255.255.0
neighbor 192.168.34.3 remote-as 300
bgp router-id 44.44.44.44
```

TABLAS DE ENRUTAMIENTO

```
R2#sh 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    192.168.12.0/24 is directly connected, Serial1/0
B    1.0.0.0/8 [20/0] via 192.168.12.1, 00:14:37
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.168.23.3, 00:14:06
B    4.0.0.0/8 [20/0] via 192.168.23.3, 00:00:27
C    192.168.23.0/24 is directly connected, FastEthernet2/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.168.12.1, 00:14:37
B    192.168.34.0/24 [20/0] via 192.168.23.3, 00:14:37
     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 192.168.23.3, 00:14:08
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.168.23.3, 00:00:28
```

Figura 5: Tabla enrutamiento R2

```
R1#SH 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    192.168.12.0/24 is directly connected, Serial1/0
C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.168.12.2, 00:15:04
B    3.0.0.0/8 [20/0] via 192.168.12.2, 00:14:34
B    4.0.0.0/8 [20/0] via 192.168.12.2, 00:00:55
B    192.168.23.0/24 [20/0] via 192.168.12.2, 00:15:04
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
B    192.168.34.0/24 [20/0] via 192.168.12.2, 00:15:04
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.168.12.2, 00:15:06
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.168.12.2, 00:14:36
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.168.12.2, 00:00:56
```

Figura 6: Tabla enrutamiento R1

```
R3#SH 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    192.168.12.0/24 [20/0] via 192.168.23.2, 00:15:23
B    1.0.0.0/8 [20/0] via 192.168.23.2, 00:15:23
B    2.0.0.0/8 [20/0] via 192.168.23.2, 00:15:23
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.168.34.4, 00:01:14
C    192.168.23.0/24 is directly connected, FastEthernet2/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.168.23.2, 00:15:23
C    192.168.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.168.23.2, 00:15:24
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.168.34.4, 00:01:15
```

Figura 7: Tabla enrutamiento R3

```
R4#SH 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    192.168.12.0/24 [20/0] via 192.168.34.3, 00:02:21
B    1.0.0.0/8 [20/0] via 192.168.34.3, 00:02:21
B    2.0.0.0/8 [20/0] via 192.168.34.3, 00:02:21
B    3.0.0.0/8 [20/0] via 192.168.34.3, 00:02:21
C    4.0.0.0/8 is directly connected, Loopback0
B    192.168.23.0/24 [20/0] via 192.168.34.3, 00:02:21
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.168.34.3, 00:02:21
C    192.168.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.168.34.3, 00:02:22
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.168.34.3, 00:02:22
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
```

Figura 8: Tabla enrutamiento R4

Escenario # 2

A. Configurar VTP

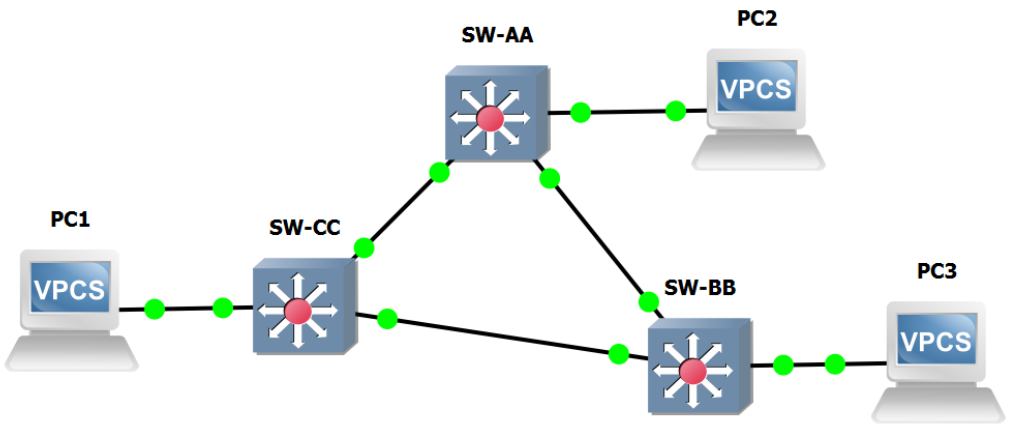

Figura 9: Escenario 2

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.

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

vtp mode server
vtp domain CCNP
vtp version 2
vtp password cisco

```
SW_AA(config)#hostname SW_AA
SW_AA(config)#vtp mode server
Device mode already VTP Server for VLANS.
SW_AA(config)#vtp domain CCNP
Domain name already set to CCNP.
SW_AA(config)#vtp password cisco
Password already set to cisco
SW_AA(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0ce9.ceb7.8000
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)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
SW_AA(config)#
SW_AA(config)#
```

Figura 10: Configuración VTP SW_AA

vtp mode client
vtp domain CCNP
vtp version 2
vtp password cisco

```
SW_BB(config)#hostname SW_BB
SW_BB(config)#vtp mode client
Device mode already VTP Client for VLANS.
SW_BB(config)#vtp domain CCNP
Domain name already set to CCNP.
SW_BB(config)#vtp password cisco
Password already set to cisco
SW_BB(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0ce9.cec4.8000
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                    0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
SW_BB(config)#
```

Figura 11: Configuración VTP SW_BB

vtp mode client
vtp domain CCNP
vtp version 2
vtp password cisco

```
Switch(config)#hostname SW_CC
SW_CC(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW_CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW_CC(config)#vtp password cisco
Setting device VTP password to cisco
SW_CC(config)#do show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0ce9.ce88.8000
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 0
MD5 digest                      : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                                  0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99

SW_CC(config)#
*May 15 15:38:04.493: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNP.
```

Figura 12: Configuración VTP SW_CC

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***.

interface g0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport mode dynamic desirable

```
SW_AA(config-if)#interface g0/0
SW_AA(config-if)#switchport trunk encapsulation dot1q
SW_AA(config-if)#switchport mode trunk
SW_AA(config-if)#switchport mode dynamic desirable
SW_AA(config-if)#
```

Figura 13: Configuración interface trunk SW_AA

interface g0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport mode dynamic desirable

```
SW_BB(config)#interface g0/0
SW_BB(config-if)#switchport trunk encapsulation dot1q
SW_BB(config-if)#switchport mode trunk
SW_BB(config-if)#switchport mode dynamic desirable
```

Figura 14: Configuración interface trunk SW_BB

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

```
SW_AA#sh interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1
```

Figura 15: Estado trunk

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

interface g0/0
switchport trunk encapsulation dot1q
switchport mode trunk
no negotiation auto

```
SW_AA(config)#interface g0/0
SW_AA(config-if)#switchport mode trunk
SW_AA(config-if)#no negotiation auto
```

Figura 16: Configuración interface trunk SW_AA

interface g0/0
switchport mode trunk
no negotiation auto

```
SW_BB(config-if)#interface g0/0
SW_BB(config-if)#switchport mode trunk
SW_BB(config-if)#no negotiation auto
```

Figura 17: Configuración interface trunk SW_BB

6. 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

interface g0/0
switchport mode trunk
no negotiation auto

```
SW_BB(config-if)#interface g0/0
SW_BB(config-if)#switchport mode trunk
SW_BB(config-if)#no negotiation auto
```

Figura 18: Configuración interface trunk SW_BB

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

```
SW_BB#sh interfaces tr

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       none
```

Figura 19: Estado interface trunk SW

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

interface g0/3
no negotiation auto
switchport trunk encapsulation dot1q
switchport mode trunk

```
SW_BB(config-if)#interface g0/3
SW_BB(config-if)#no negotiation auto
SW_BB(config-if)#switchport mode trunk
SW_BB(config-if)#switchport trunk encap dot1q
```

Figura 20: Configuración trunk SW_BB

interface g0/3
no negotiation auto
switchport trunk encapsulation dot1q
switchport mode trunk

```
SW_CC(config-if)#interface g0/3
SW_CC(config-if)#no negotiation auto
SW_CC(config-if)#switchport mode trunk
SW_CC(config-if)#switchport trunk encap dot1q
```

Figura 21: Configuración trunk SW_CC

C. Agregar VLANs y asignar puertos.

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

vlan 10
name COMPRAS
vlan 25
name PERSONAL
vlan 30
name PLANTA
vlan 99
name ADMON

```
SW_AA(config-vlan)#vlan 10
SW_AA(config-vlan)#name COMPRAS
SW_AA(config-vlan)#vlan 25
SW_AA(config-vlan)#name PERSONAL
SW_AA(config-vlan)#vlan 30
SW_AA(config-vlan)#name PLANTA
SW_AA(config-vlan)#vlan 99
SW_AA(config-vlan)#name ADMON
```

Figura 22: Configuración VLAN SW_AA

10. Verifique que las VLANs han sido agregadas correctamente.

```
SW_AA#sh vlan
*May 15 15:53:21.843: %SYS-5-CONFIG_I: Configured from console by consolebrief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi1/0
                                                Gi1/1, Gi1/2, Gi1/3, Gi2/0
                                                Gi2/1, Gi2/2, Gi2/3, Gi3/0
                                                Gi3/1, Gi3/2, Gi3/3
10   COMPRAS                          active
25   PERSONAL                         active
30   PLANTA                           active
99   ADMON                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW_AA#
```

Figura 23: Show vlan sobre SW_AA

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

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

Tabla 3: Asignación VLAN interfaces acceso

interface gigabitethernet2/0
switchport mode access
switchport access vlan 10

interface gigabitethernet2/1
switchport mode access
switchport access vlan 25

interface gigabitethernet2/2
switchport mode access
switchport access vlan 30

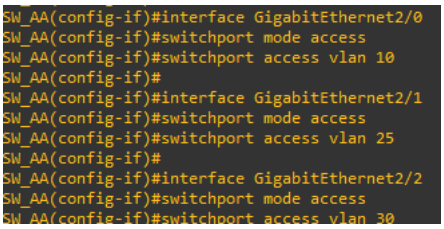

Figura 24: Configuración puertos de acceso SW_AA

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

interface gigabitethernet2/0
switchport mode access
switchport access vlan 10

interface gigabitethernet2/1
switchport mode access
switchport access vlan 25

interface gigabitethernet2/2
switchport mode access
switchport access vlan 30

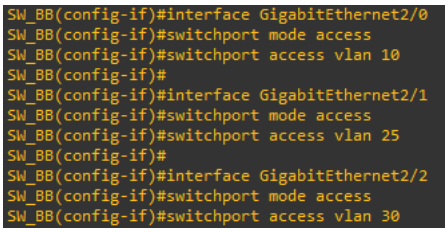

Figura 25: Configuración puertos de acceso SW_BB

interface gigabitethernet2/0
switchport mode access
switchport access vlan 10

interface gigabitethernet2/1
switchport mode access
switchport access vlan 25

interface gigabitethernet2/2
switchport mode access
switchport access vlan 30

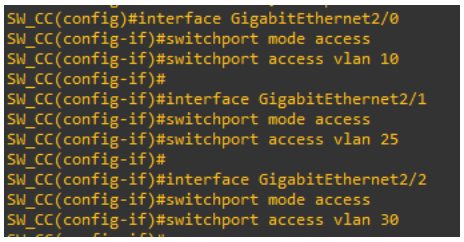

Figura 26: Configuración puertos de acceso SW_CC

13. 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.

interface gigabitethernet2/0
switchport mode access
switchport access vlan 10

interface gigabitethernet2/1
switchport mode access
switchport access vlan 25

interface gigabitethernet2/2
switchport mode access
switchport access vlan 30

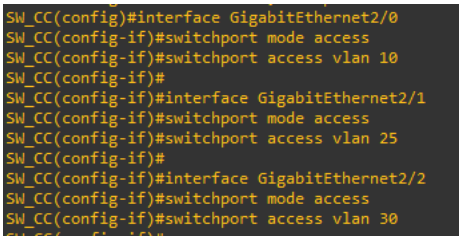

Figura 27: Configuración puertos de acceso SW_CC

D. Configurar las direcciones IP en los Switches.

14. 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.

interface vlan 99
ip add 190.108.99.1 255.255.255.0
no shut

```
SW_AA(config)#vlan 99
SW_AA(config-vlan)#name ADMINISTRACION
SW_AA(config-vlan)#interface vlan 99
SW_AA(config-if)#ip add 190.108.99.1 255.255.255.0
SW_AA(config-if)#
*May 15 16:02:41.468: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
```

Figura 28: Configuración SVI Administración SW_AA

interface vlan 99
ip add 190.108.99.2 255.255.255.0
no shut

```
SW_BB(config-if)#interface vlan 99
SW_BB(config-if)#ip add 190.108.99.2 255.255.255.0
```

Figura 29: Configuración VLAN Administración SW_BB

interface vlan 99
ip add 190.108.99.3 255.255.255.0
no shut

```
SW_CC(config-if)#interface vlan 99
SW_CC(config-if)#ip add 190.108.99.3 255.255.255.0
SW_CC(config-if)#
*May 15 16:03:20.806: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
```

Figura 30: Configuración SVI Administración SW_CC

E. Verificar la conectividad Extremo a Extremo

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

```
SW_CC#sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0ce9.ceb7.c101    DYNAMIC     Gi0/1
   1    0ce9.cec4.fe03    DYNAMIC     Gi0/3
  10    0050.7966.6800    DYNAMIC     Gi2/0
  10    0050.7966.6801    DYNAMIC     Gi0/3
  99    0ce9.ceb7.8063    DYNAMIC     Gi0/3
  99    0ce9.cec4.8063    DYNAMIC     Gi0/3
```

Figura 31: Pruebas SW conectividad

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

```
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 80 percent (4/5), round-trip min/avg/max = 19/22/27 ms
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 80 percent (4/5), round-trip min/avg/max = 16/18/22 ms
SW_AA#
```

Figura 32: Pruebas conectividad SW_AA

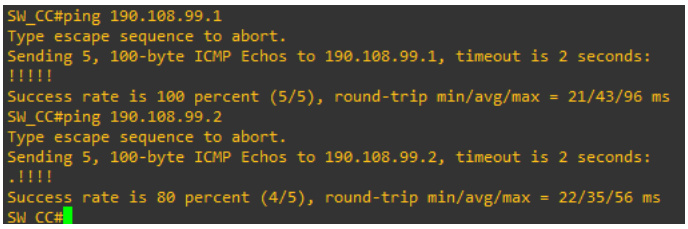

Figura 33: Pruebas conectividad SW_CC

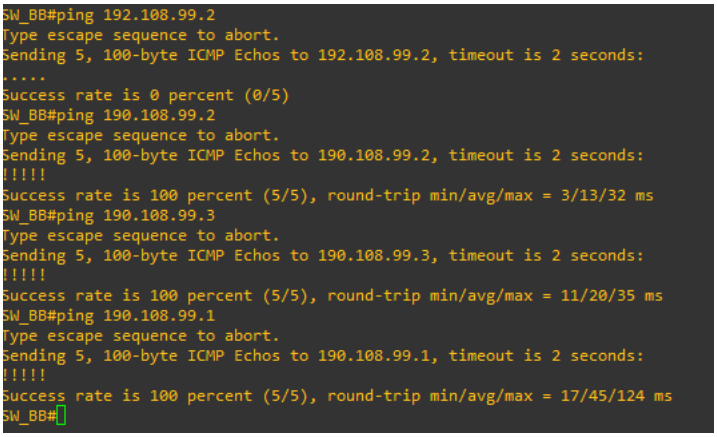

Figura 34: Pruebas conectividad SW_BB

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

No tiene éxito debido a que los SW están configurados en Layer 2 para la vlan de los PC por lo cual no tiene manera de realizar enrutamiento entre las vlan ya que no hay SVI creadas.

Conclusiones

- El protocolo VTP presenta varias vulnerabilidades bastante graves en su versión 1 y 2, hay que tener conciencia de ellos y hay que tener bastante cuidado al ingresar un nuevo SW a una topología existente en donde se encuentre usando este protocolo

- BGP provee una gran flexibilidad en su implementación, además de tener una escalabilidad muy alta y fiabilidad.

- El protocolo DTP abre una brecha de seguridad ya que permite la negociación de interface troncales, es recomendable desactivarlo, configurar la interface manualmente y deshabilitar la negociación.

Bibliografía

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

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2

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

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

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl