

PRUEBA DE HABILIDADES PRÁCTICAS

ANDRES FERNANDO GÓMEZ URBANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
POPAYAN CAUCA
MAYO 2019

PRUEBA DE HABILIDADES PRÁCTICAS

ANDRES FERNANDO GÓMEZ URBANO

DIPLOMADO DE PROFUNDIZACION CISCO CCNP

GERARDO GRANADOS ACUÑA
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
POPAYAN CAUCA
MAYO 2019

CONTENIDO

	Pág.
GLOSARIO	7
RESÚMEN	9
INTRODUCCIÓN	10
1. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES	11
1.1 ESCENARIO 1	11
1.2 ESCENARIO 2	17
1.3 ESCENARIO 3	24
2. CONCLUSIONES	35
REFERENCIAS BIBLIOGRÁFICAS	36

LISTA DE ILUSTRACIONES

	Pág.
ILUSTRACIÓN 1. ESCENARIO 1	11
ILUSTRACIÓN 2 TABLA DE ENRUTAMIENTO R3	14
ILUSTRACIÓN 3 VERIFICACIÓN DE RUTAS EN R1	15
ILUSTRACIÓN 4 VERIFICACIÓN DE RUTAS EN R5	16
ILUSTRACIÓN 5 ESCENARIO 2	17
ILUSTRACIÓN 6 SHOW IP ROUTE R1	20
ILUSTRACIÓN 7 SHOW IP ROUTE R2	20
ILUSTRACIÓN 8 SHOW IP ROUTE R3	22
ILUSTRACIÓN 9 SHOW IP ROUTE R4	23
ILUSTRACIÓN 10 ESCENARIO 3	24
ILUSTRACIÓN 11 VERIFICACIÓN CONFIGURACIÓN VTP SWT 1	25
ILUSTRACIÓN 12 VERIFICACIÓN CONFIGURACIÓN VTP SWT 2	26
ILUSTRACIÓN 13 VERIFICACIÓN CONFIGURACIÓN VTP SWT 3	26
ILUSTRACIÓN 14 VERIFICACIÓN ENLACE TRONCAL SWT 1	27
ILUSTRACIÓN 15 VERIFICACIÓN ENLACE TRONCAL SWT 2	27
ILUSTRACIÓN 16 VERIFICACIÓN ENLACE TRONCAL ESTÁTICO SWT 1	28
ILUSTRACIÓN 17 VERIFICACIÓN CONFIGURACIÓN VLAN EN SWT 1	29
ILUSTRACIÓN 18 VERIFICACIÓN CONFIGURACIÓN VLAN EN SWT 2	30
ILUSTRACIÓN 19 VERIFICACIÓN CONFIGURACIÓN VLA EN SWT 3	30
ILUSTRACIÓN 20 VERIFICACIÓN CONEXIÓN DE PC A PC	33

ILUSTRACIÓN 21 VERIFICACIÓN CONEXIÓN SWITCH A SWITCH	33
ILUSTRACIÓN 22 VERIFICACIÓN CONEXIÓN SWITCH A PC	34

LISTA DE TABLAS

	Pág.
TABLA 1 INTERFACES ESCENARIO 2	17
TABLA 2 ASIGNACIÓN DE PUERTOS A LAS VLAN	31
TABLA 3 CONFIGURAR LAS DIRECCIONES IP DE LOS SWITCHES	32

GLOSARIO

CCNP: (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía .3 Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

DOMINIO: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

ETHERNET: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

FIREWALL: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

HOST: Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas. Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

INTERFACE: Interfaz o interface es el punto de conexión ya sea dos componentes de hardware, dos programas o entre un usuario y un programa.

IP PRIVADO: Las IPs privadas sirven para proveer conectividad entre equipos internos sin que se pueda acceder directamente a Internet (se debería definir un NAT). Los routers descartan los paquetes con direccionamiento privado desde la interfaz outsider (salvo problema de seguridad) por lo que como mucho podríamos lanzar paquetes pero nunca podría contestar ya que no se podría saber cómo “volver”.

IPV6: Con el crecimiento exponencial de las computadoras, el sistema de direcciones IP, IPv4, se va a quedar sin direcciones IP. Entra en acción IPv6, también llamado IPng (IP Next Generation - IP de Nueva Generación); es la siguiente versión planificada para el sistema de direcciones IP.

PROTOCOLO: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

ROUTER: Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.

SWITCH: Un switch o conmutador es un dispositivo de interconexión de redes informáticas. En computación y en informática de redes, un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.

RESÚMEN

El informe se realiza con el fin de dar a conocer los pasos correspondientes a la configuración de tres escenarios los cuales hacen parte de la prueba de habilidades prácticas del diplomado de profundización cisco CCNP.

Además de describir los pasos de las configuraciones también se agregan imágenes que corresponde a los comandos empleados y resultados obtenidos en cada uno de los escenarios.

INTRODUCCIÓN

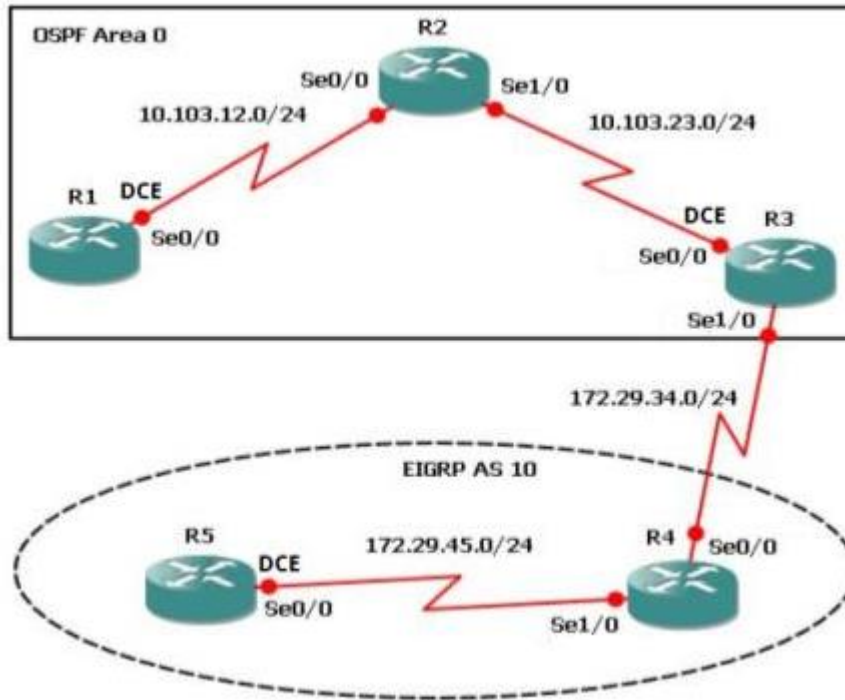
El diplomado de CCNP está diseñado para personas que desean dar continuidad a su preparación académica y seguir adquiriendo habilidades de gestión de redes orientadas hacia el mundo profesional y empresarial. CCNP ayuda a las personas a desarrollar las habilidades necesarias para complementar con éxito títulos universitarios afines con las TIC, además continuar su preparación para la certificación Cisco CCIE. Brinda una gran experiencia de aprendizaje con una carga tanto teórica como práctica que abarca habilidades avanzadas de Routing, Switching.

Teniendo en cuenta la definición de que es CCNP se da a conocer y entender con qué finalidad se realizó el presente trabajo, dicha finalidad es la de brindar solución a varios escenarios de configuraciones correspondientes al diplomado de CCNP las cuales se desarrollaran en el programa de simulación packet tracer.

1. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1.1 Escenario 1

Ilustración 1. Escenario 1



Paso1: Se aplica las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama y se Configuran las interfaces con las direcciones que se muestran en la topología de red. Se aplica la siguiente configuración inicial en cada uno de los routers, R1, R2, R3, R4 Y R5.

Ejemplo de configuración R1

```
Router#configure terminal
```

```
Router(config)#hostname R1
```

```
R1(config)#interface serial1/0
```

```
R1(config-if)#ip address 10.103.12.1 255.255.255.0
```

```
R1(config-if)#clock rate 64000
```

```
R1(config-if)#no shutdown
```

```
R1#wr
```

Paso2: Crear cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configurar esas interfaces para participar en el área 0 de OSPF.

```
R1(config)# interface Loopback1
```

```
R1(config-if)# ip address 10.1.0.3 255.255.252.0
```

```
R1(config-if)# interface Loopback2
```

```
R1(config-if)# ip address 10.2.0.3 255.255.252.0
```

```
R1(config-if)# interface Loopback3
```

```
R1(config-if)# ip address 10.3.0.3 255.255.252.0
```

```
R1(config-if)# interface Loopback4
```

```
R1(config-if)# ip address 10.4.0.4 255.255.252.0
```

```
R1(config-if)#exit
```

```
R1(config)# router ospf 1
```

```
R1(config-router)# network 10.1.0.0 0.0.3.255 area 0
```

```
R1(config-router)# network 10.2.0.0 0.0.3.255 area 0
```

```
R1(config-router)# network 10.3.0.0 0.0.3.255 area 0
```

```
R1(config-router)# network 10.4.0.0 0.0.3.255 area 0
```

Paso3: Crear cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configurar esas interfaces para participar en el Sistema Autónomo EIGRP 10.

```
R5(config)# interface Loopback1
```

```
R5(config-if)# ip address 172.5.0.3 255.255.252.0
```

```
R5(config-if)# interface Loopback2
```

```
R5(config-if)# ip address 172.6.0.3 255.255.252.0
```

```
R5(config-if)# interface Loopback3
```

```
R5(config-if)# ip address 172.7.0.3 255.255.252.0
```

```
R5(config-if)# interface Loopback4
```

```
R5(config-if)# ip address 172.8.0.3 255.255.252.0
```

```
R5(config-if)# exit
```

```
R5(config)# router eigrp 10
```

```
R5(config-router)# network 172.5.0.0 0.0.3.255
```

```
R5(config-router)# network 172.6.0.0 0.0.3.255
```

```
R5(config-router)# network 172.7.0.0 0.0.3.255
```

```
R5(config-router)# network 172.8.0.0 0.0.3.255
```

Paso4: Analizar la tabla de enrutamiento de R3 y verificar que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando show ip route.

Ilustración 2 Tabla de enrutamiento R3

```
R3#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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

    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       10.1.0.3/32 [110/129] via 10.103.23.1, 00:08:34, Serial0/0/0
O       10.2.0.3/32 [110/129] via 10.103.23.1, 00:08:24, Serial0/0/0
O       10.3.0.3/32 [110/129] via 10.103.23.1, 00:08:24, Serial0/0/0
O       10.4.0.4/32 [110/129] via 10.103.23.1, 00:08:24, Serial0/0/0
O       10.103.12.0/24 [110/128] via 10.103.23.1, 00:34:52, Serial0/0/0
C       10.103.23.0/24 is directly connected, Serial0/0/0
L       10.103.23.2/32 is directly connected, Serial0/0/0
    172.29.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.29.34.0/24 is directly connected, Serial0/0/1
L       172.29.34.1/32 is directly connected, Serial0/0/1

R3#
```

Paso5: Configurar R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuir las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

```
R3(config)# router eigrp 10
```

```
R3(config-router)# redistribute ospf 1 metric 50000 20 255 255 1500
```

```
R3(config-router)# exit
```

```
R3(config)# router ospf 1
```

```
R3(config-router)# redistribute eigrp 10 subnets
```

Paso6: Verificar en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando show ip route.

Ilustración 3 Verificación de rutas en R1

```
R1#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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

    10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
C       10.1.0.0/22 is directly connected, Loopback1
L       10.1.0.3/32 is directly connected, Loopback1
C       10.2.0.0/22 is directly connected, Loopback2
L       10.2.0.3/32 is directly connected, Loopback2
C       10.3.0.0/22 is directly connected, Loopback3
L       10.3.0.3/32 is directly connected, Loopback3
C       10.4.0.0/22 is directly connected, Loopback4
L       10.4.0.4/32 is directly connected, Loopback4
C       10.103.12.0/24 is directly connected, Serial10/0/0
L       10.103.12.1/32 is directly connected, Serial10/0/0
O       10.103.23.0/24 [110/128] via 10.103.12.2, 00:51:20, Serial10/0/0

R1#
```

Ilustración 4 Verificación de rutas en R5

```
R5#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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

    172.5.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.5.0.0/22 is directly connected, Loopback1
L       172.5.0.3/32 is directly connected, Loopback1
    172.6.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.6.0.0/22 is directly connected, Loopback2
L       172.6.0.3/32 is directly connected, Loopback2
    172.7.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.7.0.0/22 is directly connected, Loopback3
L       172.7.0.3/32 is directly connected, Loopback3
    172.8.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.8.0.0/22 is directly connected, Loopback4
L       172.8.0.3/32 is directly connected, Loopback4
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.29.34.0/24 [90/2681856] via 172.29.45.2, 00:53:04, Serial0/0/0
C       172.29.45.0/24 is directly connected, Serial0/0/0
L       172.29.45.1/32 is directly connected, Serial0/0/0

R5#
```


1.2 Escenario 2

Ilustración 5 Escenario 2

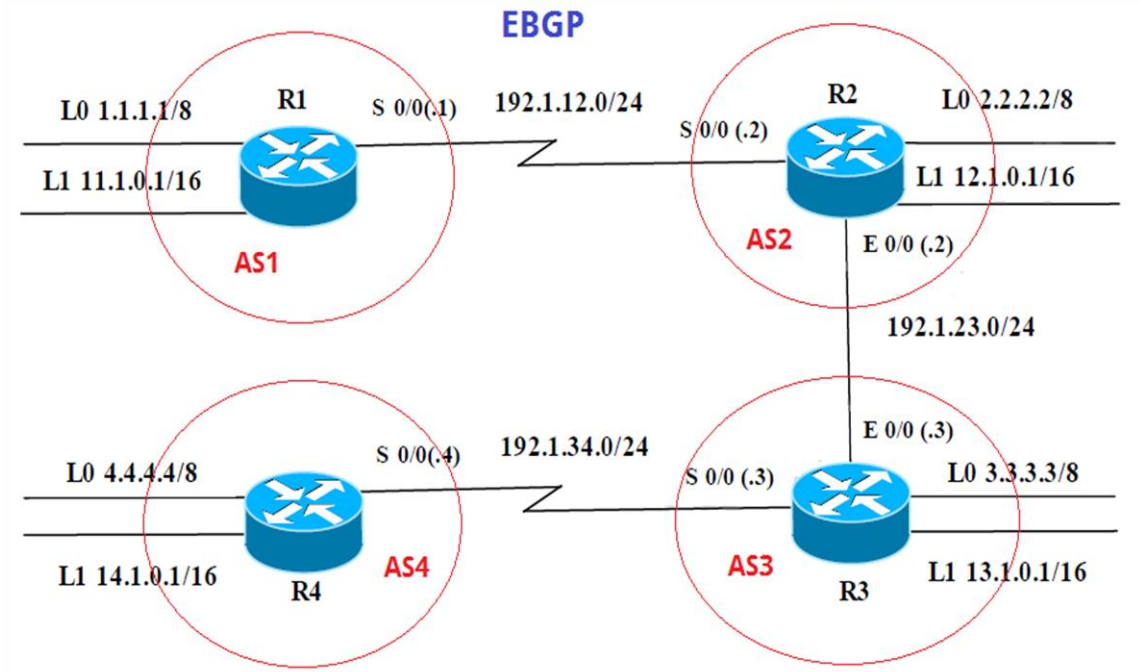


Tabla 1 Interfaces Escenario 2

R	Interfaz	Dirección IP	Máscara
1	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

R	Interfaz	Dirección IP	Máscara
2	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 (Continuación)

R 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	

R 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	

Paso1: Configurar las interfaces de todos los router de acuerdo a la tabla de direccionamiento

Ejemplo de configuración en R1

```
R1(config)# interface Loopback1
```

```
R1(config-if)# ip address 1.1.1.1 255.0.0.0
```

```
R1(config-if)# interface Loopback1
```

```
R1(config-if)# ip address 11.1.0.1 255.255.0.0
```

```
R1(config-if)# interface Serial0/0/0
```

```
R1(config-if)# ip address 192.1.12.1 255.255.255.0
```

Paso2: Configurar una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anunciar las direcciones de Loopback en BGP. Codificar los ID para los routers BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2.

Configuración R1

```
R1(config)# router bgp 1
```

```
R1(config-router)# bgp router-id 11.11.11.11
```

```
R1(config-router)# neighbor 192.1.12.2 remote-as 2
```

```
R1(config-router)# network 1.0.0.0
```

```
R1(config-router)# network 11.1.0.0 mask 255.255.0.0
```

```
R1(config-router)# network 192.1.12.0
```

Configuración R2

```
R2(config)# router bgp 2
```

```
R2(config-router)# bgp router-id 22.22.22.22
```

```
R2(config-router)# neighbor 192.1.12.1 remote-as 1
```

```
R2(config-router)# neighbor 192.1.23.3 remote-as 3
```

```
R2(config-router)# network 2.0.0.0
```

```
R2(config-router)# network 12.1.0.0 mask 255.255.0.0
```

```
R2(config-router)# network 192.1.12.0
```

```
R2(config-router)# network 192.1.23.0
```

Ilustración 6 Show ip route R1

```
R1#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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

    1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/8 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
B       2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
B       3.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
    11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.1.0.0/16 is directly connected, Loopback1
L       11.1.0.1/32 is directly connected, Loopback1
    12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
    13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.1/32 is directly connected, Serial0/0/0
B       192.1.23.0/24 [20/0] via 192.1.12.2, 00:00:00
B       192.1.34.0/24 [20/0] via 192.1.12.2, 00:00:00

R1#
```

Ilustración 7 Show ip route R2

```
R2#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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       1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       2.0.0.0/8 is directly connected, Loopback0
L       2.2.2.2/32 is directly connected, Loopback0
B       3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
    11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       12.1.0.0/16 is directly connected, Loopback1
L       12.1.0.1/32 is directly connected, Loopback1
    13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.2/32 is directly connected, Serial0/0/0
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.23.0/24 is directly connected, GigabitEthernet0/0
L       192.1.23.2/32 is directly connected, GigabitEthernet0/0
B       192.1.34.0/24 [20/0] via 192.1.23.3, 00:00:00

R2#
```

Paso 3: Configurar 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. Codificar el ID del router R3 como 33.33.33.33.

```
R3(config)# router bgp 3
```

```
R3(config-router)# bgp router-id 33.33.33.33
```

```
R3(config-router)# neighbor 192.1.34.4 remote-as 4
```

```
R3(config-router)# neighbor 192.1.23.2 remote-as 2
```

```
R3(config-router)# network 3.0.0.0
```

```
R3(config-router)# network 13.1.0.0 mask 255.255.0.0
```

```
R3(config-router)# network 192.1.34.0
```

```
R3(config-router)# network 192.1.23.0
```

Ilustración 8 Show ip route R3

```
R3#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
     3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    3.0.0.0/8 is directly connected, Loopback0
L    3.3.3.3/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.0.0/16 is directly connected, Loopback1
L    13.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/0/0
L    192.1.34.3/32 is directly connected, Serial0/0/0

R3#
```

Paso 4: Configurar una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anunciar las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 44.44.44.44. Establecer las relaciones de vecino con base en las direcciones de Loopback 0. Crear rutas estáticas para alcanzar la Loopback 0 del otro router. No anunciarr la Loopback 0 en BGP. Anuncir la red Loopback de R4 en BGP.

```
R4(config)# router bgp 4
```

```
R4(config-router)# bgp router-id 44.44.44.44
```

```
R4(config-router)# neighbor 192.1.34.3 remote-as 3
```

```
R4(config-router)# network 4.0.0.0
```

```
R4(config-router)# network 14.1.0.0 mask 255.255.0.0
```

```
R4(config-router)# network 192.1.34.0
```

Ilustración 9 Show ip route R4

```
R4#sh ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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

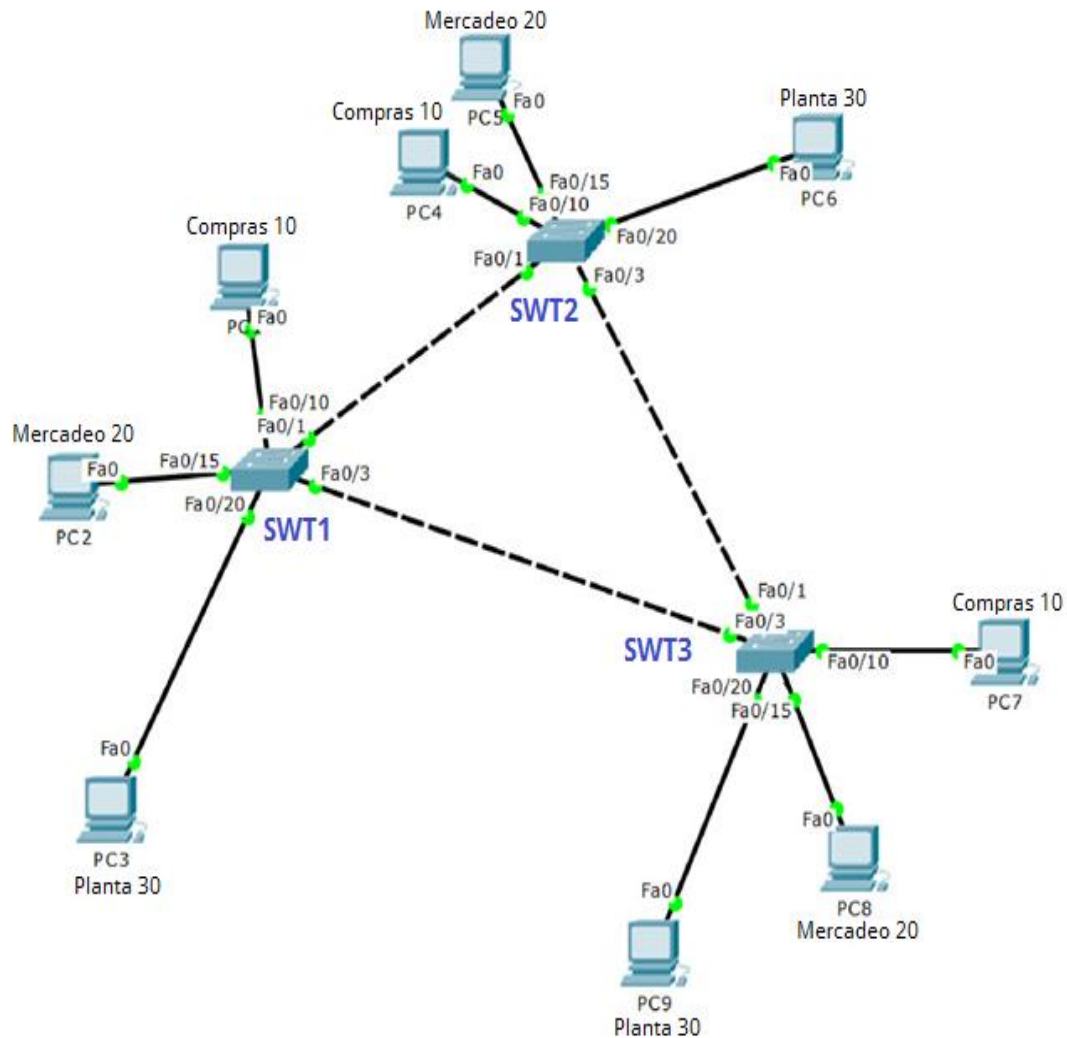
Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
     4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.34.3, 00:00:00
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:00:00
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/0/0
L    192.1.34.4/32 is directly connected, Serial0/0/0

R4#
```

1.3 Escenario 3

Ilustración 10 Escenario 3



Parte 1-Configurar VTP

Paso1: Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SWT2 se configurará como el servidor. Los switches SWT1 y SWT3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Ejemplo de configuración VTP modo cliente

SWT1(config)#vtp mode client

SWT1(config)#vtp domain CCNP

SWT1(config)#vtp password cisco

Ejemplo de configuración SWT2 como servidor

SWT2(config)#vtp mode server

SWT2(config)#vtp domain CCNP

SWT2(config)#vtp password cisco

Paso2: Verificar las configuraciones mediante el comando show vtp status.

Ilustración 11 Verificación configuración VTP SWT 1

```
SWT1#sh 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
SWT1#
```

Ilustración 12 Verificación configuración VTP SWT 2

```
SWT2#sh 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)
SWT2#
```

Ilustración 13 Verificación configuración VTP SWT 3

```
SWT3#wr
Building configuration...
[OK]
SWT3#sh 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
SWT3#
```

Parte2-Configurar DTP (Dynamic Trunking Protocol)

Paso1: Configurar un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

```
SWT1(config)# interface FastEthernet0/1
```

SWT1(config-if)# switchport mode dynamic desirable

Paso2: Verificar el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.

Ilustración 14 Verificación enlace troncal SWT 1

```
SWT1#sh interface 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

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

SWT1#
```

Ilustración 15 Verificación enlace troncal SWT 2

```
SWT2#sh int 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

SWT2#
```

Paso3: Entre SWT1 y SWT3 configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SWT1

SWT1(config)# interface FastEthernet0/3

SWT1(config-if)# switchport mode trunk

Paso4: Verifique el enlace "trunk" el comando show interfaces trunk en SWT1.

Ilustración 16 Verificación enlace troncal estático SWT 1

```
SWT1#sh interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable 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     none
Fa0/3     1

SWT1#
```

Paso5: Configurar un enlace "trunk" permanente entre SWT2 y SWT3.

```
SWT2(config)# interface FastEthernet0/3
```

```
SWT2(config-if)# switchport mode trunk
```

```
SWT3(config)# interface FastEthernet0/1
```

```
SWT3(config-if)# switchport mode trunk
```

Parte3-Agregar VLANs y asignar puertos.

Paso1: En STW1 agregar la VLAN 10. En STW2 agregue las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99)

```
SWT2(config)#vlan 10
```

```
SWT2(config-vlan)#name Compras
```

```
SWT2(config-vlan)#vlan 20
```

```
SWT2(config-vlan)#name Mercadeo
```

```
SWT2(config-vlan)#vlan 30
```

```
SWT2(config-vlan)#name Planta
```

```
SWT2(config-vlan)#vlan 99
```

```
SWT2(config-vlan)#name Admon
```

Paso2: Verifique que las VLANs han sido agregadas correctamente.

Ilustración 17 Verificación configuración VLAN en SWT 1

```
SWT1#sh vlan br
```

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, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SWT1#
```

Ilustración 18 Verificación configuración VLAN en SWT 2

```
SWT2#sh vlan br
```

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, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SWT2#
```

Ilustración 19 Verificación configuración VLA en SWT 3

```
SWT3#sh vlan br
```

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, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
SWT3#
```

Paso4: Asociar los puertos a las VLAN y configurar las direcciones IP de acuerdo con la siguiente tabla.

Tabla 2 Asignación de puertos a las VLAN

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

X = número de cada PC particular

Paso5: Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

Ejemplo de configuración SWT1

```
SWT1(config)# interface FastEthernet0/10
```

```
SWT1(config-if)# switchport mode access
```

```
SWT1(config-if)# switchport access vlan 10
```

```
SWT1(config-if)# interface FastEthernet0/15
```

```
SWT1(config-if)# switchport mode access
```

```
SWT1(config-if)# switchport access vlan 20
```

```
SWT1(config-if)# interface FastEthernet0/20
```

```
SWT1(config-if)# switchport mode access
```

```
SWT1(config-if)# switchport access vlan 30
```

Parte4-Configurar las direcciones IP en los Switches.

Paso1: En cada uno de los Switches asignar una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 3 Configurar las direcciones IP de los switches

Equipo	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

```
SWT1(config)# interface Vlan99
```

```
SWT1(config-if)# ip address 190.108.99.1 255.255.255.0
```

```
SWT2(config)# interface Vlan99
```

```
SWT2(config-if)# ip address 190.108.99.2 255.255.255.0
```

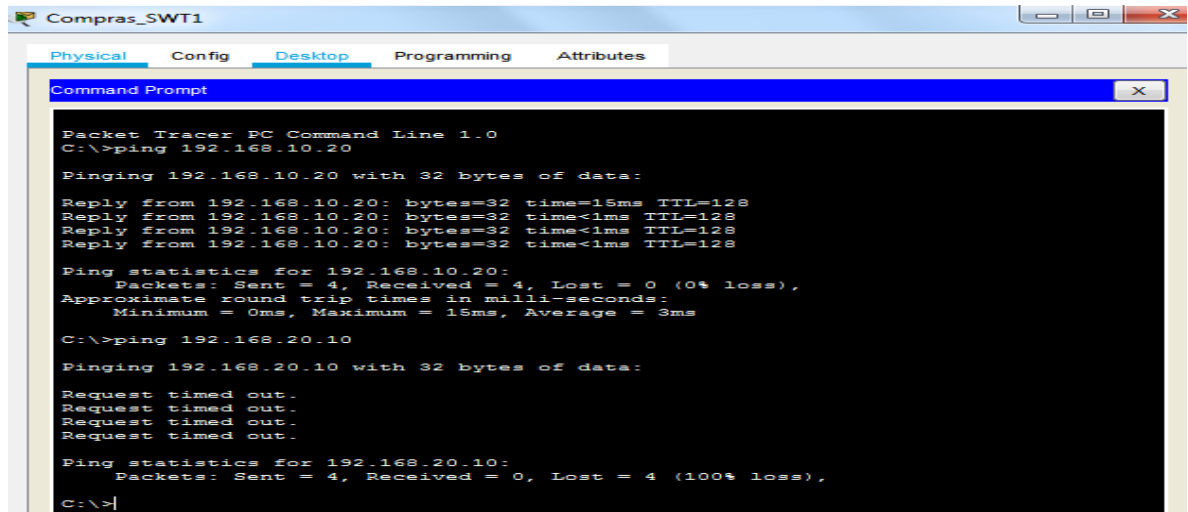
```
SWT3(config)# interface Vlan99
```

```
SWT3(config-if)# ip address 190.108.99.3 255.255.255.0
```


Paso2: 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.

Ilustración 20 Verificación conexión de PC a PC

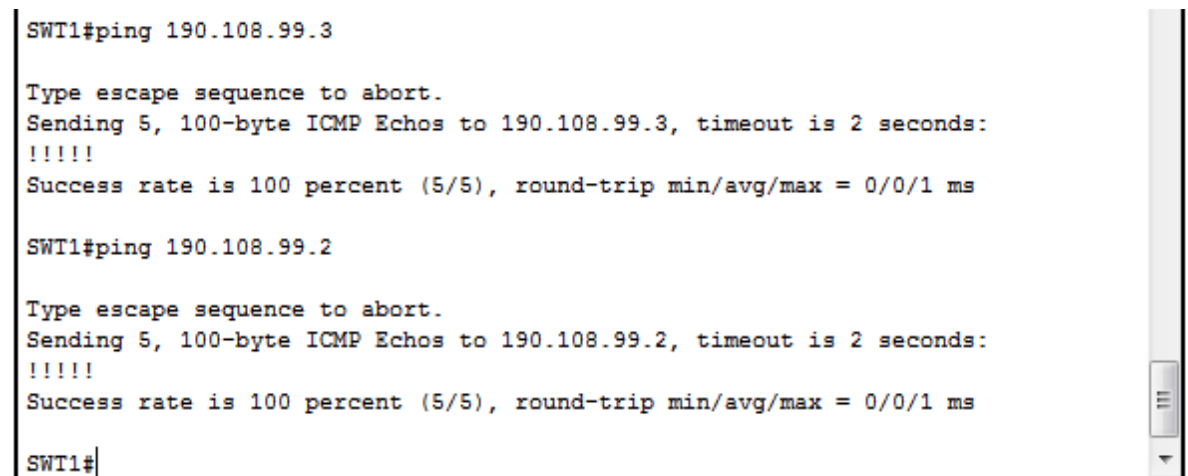


```
Compras_SWT1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.20
Pinging 192.168.10.20 with 32 bytes of data:
Reply from 192.168.10.20: bytes=32 time=15ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 3ms
C:\>ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>|
```

El ping tiene éxito a los pc de la misma VLAN pero no tiene conexión a los PC de otras VLAN porque no se ha configurado enrutamiento inter VLAN

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

Ilustración 21 Verificación conexión switch a switch



```
SWT1#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 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SWT1#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 = 0/0/1 ms

SWT1#
```

El ping tiene éxito entre los switches porque hay configuración de enlaces troncales

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

Ilustración 22 Verificación conexión switch a PC

```
SWT3#ping 192.168.10.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.30, timeout is 2 seconds:
-----
Success rate is 0 percent (0/5)

SWT3#ping 192.168.20.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.30, timeout is 2 seconds:
-----
Success rate is 0 percent (0/5)

SWT3#ping 192.168.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.10, timeout is 2 seconds:
-----
Success rate is 0 percent (0/5)

SWT3#
```

El ping a los PC desde el switch no tiene éxito porque no hay enrutamiento inter VLAN por tanto no hay comunicación entre los switches y los PC.

2. CONCLUSIONES

CCNP provee el conocimiento y las habilidades necesarias para la implementación y el mantenimiento de una infraestructura de red integrada de servicios y aplicaciones. CCNP se ha diseñado para reflejar las habilidades y las responsabilidades laborales asociadas a los roles profesionales de ingeniero de redes, ingeniero de sistemas, ingeniero de soporte de redes, administrador de redes, asesor de redes e integrador de sistemas Ingeniero de telecomunicaciones y demás profesiones afines.

La presente certificación además, ofrece una experiencia de aprendizaje con una gran carga académica tanto teórica como práctica con laboratorios reales dentro del aula, que abarca habilidades avanzadas de routing, switching y solución de problemas, por consiguiente CCNP es el escalón que deben subir los alumnos de CCNA los cuales deseen ampliar sus habilidades y prepararse para una carrera profesional afín.

REFERENCIAS BIBLIOGRÁFICAS

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de [http://www.birminghamcharter.com/ourpages/auto/2012/3/22/41980164/CCNA %20Electronic%20Book%206th%20edition.pdf](http://www.birminghamcharter.com/ourpages/auto/2012/3/22/41980164/CCNA%20Electronic%20Book%206th%20edition.pdf)

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de <http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/Cisco-ICND2.pdf>

UNAD (2015). SwitchCISCO Security Management [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IlyVeVJCCezJ2QE5c>