

EVALUACIÓN FINAL
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

IVÁN FELIPE SARMIENTO GARCÍA
Para optar al título de
Ingeniero Electrónico

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERÍA ELECTRÓNICA RESOLUCIÓN 13155
DIPLOMADO CISCO CCNP
CHOCONTÁ-CUNDINAMARCA
2019

EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS CCNP

IVÁN FELIPE SARMIENTO GARCÍA

Diplomado de profundización cisco CCNP prueba de
Habilidades prácticas

Gerardo Granados Acuña
Magíster en Telemática e Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
INGENIERÍA ELECTRÓNICA RESOLUCIÓN 13155
DIPLOMADO CISCO CCNP
CHOCONTÁ-CUNDINAMARCA
2019

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Chocontá-Cundinamarca,06 de julio de 2019

CONTENIDO

	pág.
INTRODUCCIÓN	10
1. DESARROLLO DE CADA UNO DE LOS ESCENARIOS PROPUESTOS	11
1.1. Descripción de escenarios propuestos para la prueba de habilidades	11
1.1.1 Escenario 1	11
1.1.2. Escenario 2	25
1.1.3Escenario 3	40
CONCLUSIONES	76
Referencias Bibliográficas	77

LISTA DE TABLAS

	pág.
Tabla 1. Interfaces de Loopback	18
Tabla 2. Interfaces de Loopback	19
Tabla 3. Configuración de routers	27
Tabla 4. De configuración de direcciones ip y VLANs	52
Tabla 5. Configuración	53
Tabla 6. direcciones IP en los Switches	57

LISTA DE ILUSTRACIONES

	pág.
Ilustración 1 Topología Escenario 1	11
Ilustración 2 Topología Escenario 1 Packet Tracer	11
Ilustración 3.Evidencia tabla de enrutamiento de R3	21
Ilustración 4.Evidencia del comando show ip route	21
Ilustración 5.Evidencia del comando SHOW R	23
Ilustración 6.Evidencia del comando show ip route en R1 y R5	24
Ilustración 7.Evidencia de la topología	24
Ilustración 8.Escnario 2 topología	25
Ilustración 9. Escenario 2 topología Packet Tracer	25
Ilustración 10 .Evidencia del comando show ip route	32
Ilustración 11.Evidencia del comando show ip bgp neighbors	33
Ilustración 12.Evidencia del comando show ip bgp	33
Ilustración 13.Evidencia del comando show ip route	35
Ilustración 14.Evidencia del comando show ip bgp neighbors	35
Ilustración 15.Evidencia del comando show ip bgp	36
Ilustración 16.Evidencia del comando show ip route	38
Ilustración 17.Evidencia del comando show ip bgp neighbors	38
Ilustración 18.Evidencia del comando show ip bgp	39
Ilustración 19.Topología Escenario 3	40
Ilustración 20.Topología Escenario 3 Packet Tracer	40
Ilustración 21.Evidencia show vtp status SWT2	45
Ilustración 22.Evidencia show vtp status SWT1 y SWT3	46
Ilustración 23.Evidencia del comando show interfaces trunk	47
Ilustración 24.Evidencia show interface f0/1 switchport	47
Ilustración 25.Evidencia del comando show interfaces trunk	48
Ilustración 26.Evidencia de configuración	49
Ilustración 27.Evidencia de los comandos show vlan brief	51
Ilustración 28.Evidencia de los comandos show vlan brief	51
Ilustración 29.Evidencia de direcciones ip de los pcs del SWT1	54
Ilustración 30.Evidencia de direcciones ip de los pcs del SWT2	54
Ilustración 31.Evidencia direcciones ip de los pcs del SWT3	55
Ilustración 32.Evidencia de comando wr	58
Ilustración 33.Evidencia de pings	59
Ilustración 34.Evidencia de pings	60
Ilustración 35.Evidencia de pings	61
Ilustración 36.Evidencia de pings	62
Ilustración 37.Evidencia de pings	63
Ilustración 38.Evidencia de pings	64
Ilustración 39.Evidencia de pings	65
Ilustración 40.Evidencia de pings	66
Ilustración 41.Evidencia de pings	67
Ilustración 42.Evidencia de pings exitosos	68

Ilustración 43.Evidencia de pings fallidos	69
Ilustración 44.Evidencia Ping desde el SWT1	70
Ilustración 45.Evidencia de Ping desde el SWT2	71
Ilustración 46.Evidencia de Ping desde el SWT3	71
Ilustración 47.Evidencia de Ping desde el SWT1 a todas las pc	72
Ilustración 48.Evidencia de Ping desde el SWT2 a todas las pc	73
Ilustración 49.Evidencia de Ping desde el SWT3 a todas las pc	74
Ilustración 50.Evidencia de ping que tendrá éxito	75
Ilustración 51.Evidencia de Pings correctos	75

GLOSARIO

CCNP: Es un curso que se desarrolla de manera virtual, el cual permite adquirir habilidades para construcción y configuración de redes, consiste en evaluaciones sobre diferentes capítulos también comprende actividades de simulación, y una evaluación final que evalúan los conocimientos adquiridos que es de forma virtual junto con una evaluación practica que consiste en resolver algunos problemas planteados, para obtener el certificado hay poseer una calificación igual o superior de 3.5 /5.0.

CISCO PACKET TRACER: Programa utilizado para la simulación de redes, de forma didáctica y educativa. Este permite la configuración de redes con una gran cantidad de comandos utilizados en las redes físicas actualmente, de tal forma que el usuario puede adquirir estas habilidades y utilizarlas en su vida profesional.

COMANDOS: Son palabras o códigos que permiten realizar algún tipo de configuración a la red.

EIGRP: Protocolo diseñado para usar el de vector distancia para lograr la comunicación.

OSPF: Protocolo que consiste en realizar una comunicación mediante La ruta más corta y obtener beneficios para la comunicación.

PROTOCOLOS DE RED: Son los procedimientos que se encuentran definidos o estandarizados para el uso y configuración adecuada de una red con el fin de que funcione de la mejor manera posible dependiendo de su topología, cantidad de dispositivos en la red y de las necesidades de funcionamiento de la red.

TOPOLOGÍA DE RED: Son las estructuras que están compuestas por los dispositivos de la red, para este trabajo conformadas routers y switches. Existen varios tipos: bus, estrella, anillo, árbol, malla, hibrida son algunas de las más importantes las cuales se seleccionan para construir una red de acuerdo a las necesidades de está.

VTP: Es un Protocolo de enlace troncal VLAN.

RESUMEN

El trabajo contiene información de dos módulos: CCNP R&S route y CCNP R&S switch, las temáticas de estos módulos se representan mediante la solución de tres escenarios, simulando en el programa Cisco Packet Tracer versión 7.2.1.

Se evidencia el uso de comandos ping, traceroute, show ip route para observar las correctas configuraciones realizadas y su conectividad, dentro de la actividad se resaltan las temáticas más importantes las unidades del curso: Unidad 1 - Protocolos de Enrutamiento Avanzado, Unidad 2 - Implementación de soluciones soportadas en enrutamiento avanzado, esas dos temáticas pertenecen a CCNP R&S route y Unidad 3 - Configuración de sistemas de red soportados en VLANs Unidad 4 - Administración, Seguridad y Escalabilidad en redes conmutadas son de CCNP R&S switch.

Estos escenarios se enfocan en configuración y simulaciones los protocolos OSPF Área 0, EIGRP AS10 en primer escenario, en el segundo el protocolo EIGRP y en el escenario final se configura VTP.

Mediante las simulaciones de cada uno de los escenarios se practican los comandos de la configuración de cada uno de los protocolos mencionados anteriormente y se practica configuraciones iniciales como lo son colocar el nombre a cada dispositivo en modo de configuración global con el comando Router(config)#HOSTNAME, mediante un texto a modo de instructivo se evidencia cada uno de los pasos realizados de forma ordenada y se da a conocer cada uno de los comandos con su respectiva función dentro del proceso, de esta forma se entiende claramente cada configuración y el lector podrá adquirir los conocimientos presentados.

Palabras clave: CCNP R&S route, CCNP R&S switch, Cisco Packet Tracer, ping, traceroute, show ip route, OSPF, EIGRP, EIGRP, VTP, protocolos, HOSTNAME, Protocolos de Enrutamiento Avanzado, Administración, Seguridad, Escalabilidad.

INTRODUCCIÓN

El presente documento da a conocer las temáticas más relevantes que se aprenden en el diplomado de profundización cisco CCNP, en la actualidad es importante tener buena comunicación ágil y de calidad ,el curso consta de dos módulos: CCNP R&S route y CCNP R&S switch.

Cada uno de estos módulos comprende dos unidades: Unidad 1 - Protocolos de Enrutamiento Avanzado, Unidad 2 - Implementación de soluciones soportadas en enrutamiento avanzado, esas dos temáticas pertenecen a CCNP R&S route y Unidad 3 - Configuración de sistemas de red soportados en VLANs Unidad 4 - Administración, Seguridad y Escalabilidad en redes conmutadas pertenecen a CCNP R&S switch, importantes para la construcción de buenas redes cisco.

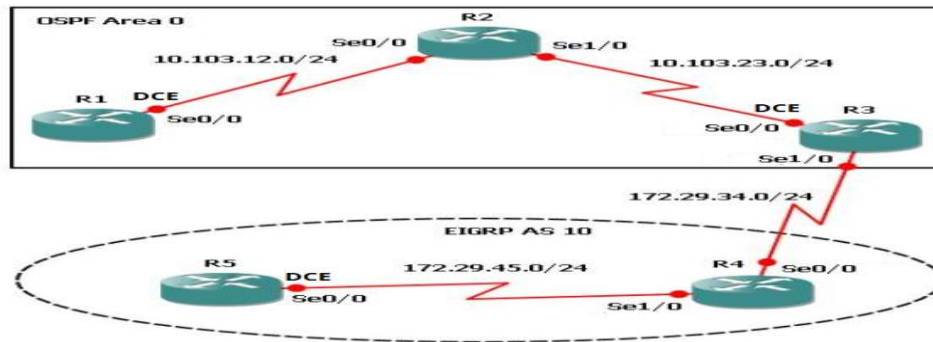
Dentro de este trabajo se encuentran resueltos tres escenarios planteados por la universidad con el fin de, permitirme evidenciar los conocimientos adquiridos sobre route y switch durante el desarrollo del diplomado de profundización se encuentra su configuración características más destacadas ventajas, e implementación en el programa Cisco Packet Tracer versión 7.2.1.

1. DESARROLLO DE CADA UNO DE LOS ESCENARIOS PROPUESTOS

1.1. Descripción de escenarios propuestos para la prueba de habilidades

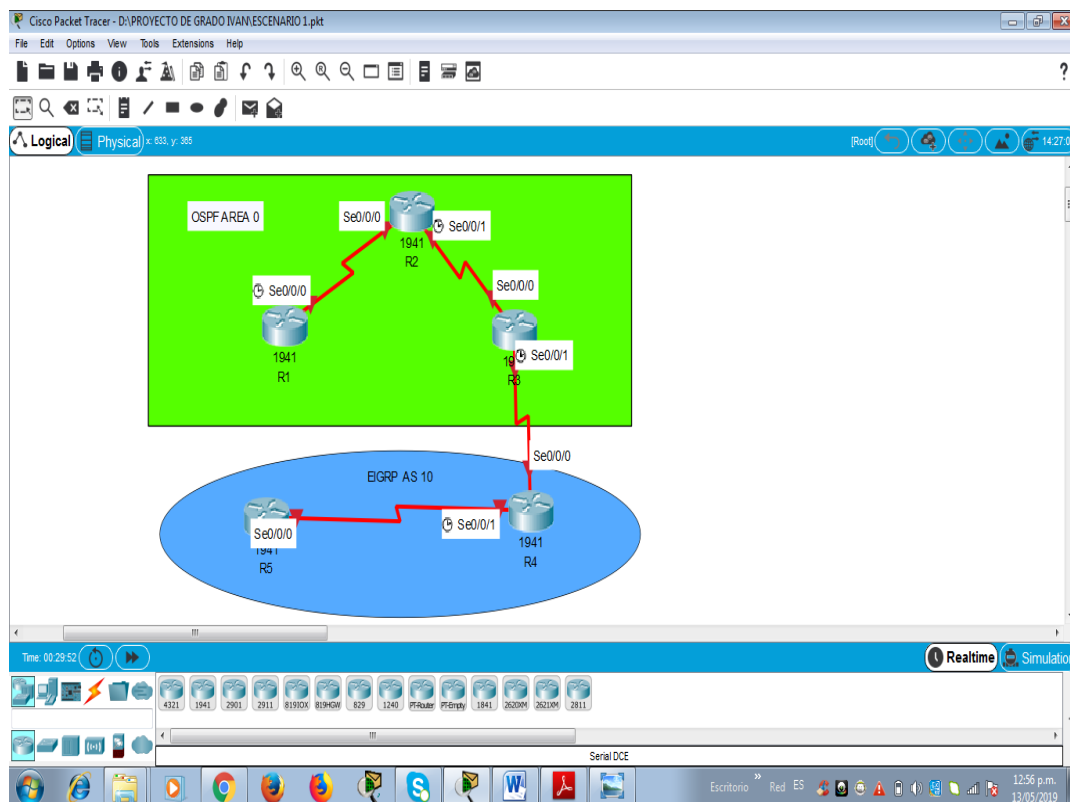
1.1.1 Escenario 1

Ilustración 1 Topología Escenario 1



Fuente 1. Universidad Nacional Abierta y a Distancia (UNAD).

Ilustración 2 Topología Escenario 1 Packet Tracer



Fuente 2: El Autor.

1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Desarrollo:

A continuación, se muestran las configuraciones iniciales de los cinco routers nombrados cada uno con el respetivo nombre dado en el ejercicio:

ROUTER 1 R1

```
Router>
```

```
Router>en
```

```
Router#CONFIG T
```

```
Router(config)#HOSTNAME R1
```

```
R1(config)# no ip domain-lookup
```

```
R1(config)# line con 0
```

```
R1(config-line)# logging synchronous
```

```
R1(config-line)# exec-timeout 0 0
```

```
R1(config-line)#EXIT
```

```
R1(config)#
```

ROUTER 2 R1

```
Router>
```

```
Router>en
```

```
Router#CONFIG T
```

```
Router(config)#HOSTNAME R2
```

```
R2(config)# no ip domain-lookup
```

```
R2(config)# line con 0
```

```
R2(config-line)# logging synchronous
```

```
R2(config-line)# exec-timeout 0 0
```

```
R2(config-line)#EXIT
```

```
R2(config)#
```

ROUTER 3 R3

```
Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R3
R3(config)# no ip domain-lookup
R3(config)# line con 0
R3(config-line)# logging synchronous
R3(config-line)# exec-timeout 0 0
R3(config-line)#EXIT
R3(config)#
```

ROUTER 4 R4

```
Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R4
R4(config)# no ip domain-lookup
R4(config)# line con 0
R4(config-line)# logging synchronous
R4(config-line)# exec-timeout 0 0
R4(config-line)#EXIT
R4(config)#
```

ROUTER 5 R5

```
Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R5
R5(config)# no ip domain-lookup
R5(config)# line con 0
R5(config-line)# logging synchronous
```

```
R5(config-line)# exec-timeout 0 0
```

```
R5(config-line)#EXIT
```

```
R5(config)#
```

Se procede a configurar los protocolos de enrutamiento para los cinco routers según el diagrama, se debe seleccionar el valor del rango eigrp el cual indican en el ejercicio que es el numero 10 se agregan las redes directamente conectadas a cada router con su respectivo wildcard en este caso como todas las redes tienen mascara de subred de /24 su wildcard es 0.0.0.255 también se desactiva el resumen automático.

CONFIGURACIÓN EIGRP AS 10 ROUTER 5 R5

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

```
R5(config-router)# no auto-summary
```

```
R5(config-router)# network 172.29.45.0 0.0.0.255
```

CONFIGURACIÓN EIGRP AS 10 ROUTER 4 R4

```
R4(config)#router eigrp 10
```

```
R4(config-router)# no auto-summary
```

```
R4(config-router)#network 172.29.45.0 0.0.0.255
```

```
R4(config-router)#network 172.29.34.0 0.0.0.255
```

CONFIGURACIÓN EIGRP AS 10 ROUTER 3 R3

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

```
R3(config-router)# no auto-summary
```

```
R3(config-router)#network 172.29.34.0 0.0.0.255
```

Se elige el número de rango de OSPF y se agregan las redes directamente conectadas al router con la wildcard que le corresponde además se agrega el área a la que pertenece, también se crea el ID de enrutador de OSPF en los routers que utilizaran ese protocolo.

CONFIGURACIÓN OSPF AREA 0 ROUTER 1 R1

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.103.12.0 0.0.0.255 area 0
R1(config-router)# exit
```

CONFIGURACIÓN OSPF AREA 0 ROUTER 2 R2

```
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.103.12.0 0.0.0.255 area 0
R2(config-router)# network 10.103.23.0 0.0.0.255 area 0
R2(config-router)# exit
```

CONFIGURACIÓN OSPF AREA 0 ROUTER 3 R3

```
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 172.29.34.0 0.0.0.255 area 0
R3(config-router)# network 10.103.23.0 0.0.0.255 area 0
R3(config-router)# exit
```

Configuración de interfaces según el diagrama, se agrega la descripción, se establece la frecuencia de reloj, el ancho de banda se asigna la dirección ip con su respectiva mascara de subred y se enciende la interface.

ROUTER 1 R1

```
R1(config)# interface Serial 0/0/0
R1(config-if)# description R1-->R2
R1(config-if)# clock rate 64000
R1(config-if)# bandwidth 64
R1(config-if)# ip address 10.103.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

ROUTER 2 R2

```
R2(config)# interface Serial 0/0/0
R2(config-if)# description R2-->R1
```

```
R2(config-if)# bandwidth 64
R2(config-if)# ip address 10.103.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

```
R2(config)# interface Serial 0/0/1
R2(config-if)# description R2-->R3
R2(config-if)# clock rate 64000
R2(config-if)# bandwidth 64
R2(config-if)# ip address 10.103.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

ROUTER 3 R3

```
R3(config)# interface Serial 0/0/0
R3(config-if)# description R3-->R2
R3(config-if)# bandwidth 64
R3(config-if)# ip address 10.103.23.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
```

```
R3(config)# interface Serial 0/0/1
R3(config-if)# description R3-->R4
R3(config-if)# clock rate 64000
R3(config-if)# bandwidth 64
R3(config-if)# ip address 172.29.34.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
```


ROUTER 4 R4

```
R4(config)# interface Serial 0/0/0
R4(config-if)# description R4-->R3
R4(config-if)# bandwidth 64
R4(config-if)# ip address 172.29.34.4 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# exit
```

```
R4(config)# interface Serial 0/0/1
R4(config-if)# description R4-->R5
R4(config-if)# clock rate 64000
R4(config-if)# bandwidth 64
R4(config-if)# ip address 172.29.45.4 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# exit
```

ROUTER 5 R5

```
R5(config)# interface Serial 0/0/0
R5(config-if)# description R5-->R4
R5(config-if)# bandwidth 64
R5(config-if)# ip address 172.29.45.5 255.255.255.0
R5(config-if)# no shutdown
R5(config-if)# exit
```

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

Desarrollo:

Tabla 1. Interfaces de Loopback

INTERFACE	IP ADDRESS/MASK
Loopback12	10.1.12.1/22 255.255.252.0
Loopback22	10.1.22.1/22 255.255.252.0
Loopback33	10.1.33.1/22 255.255.252.0
Loopback44	10.1.44.1/22 255.255.252.0

Fuente 52: El Autor.

Se diseñaron las cuatro interfaces de Loopback en R1 con las direcciones que se muestran en la tabla creada y su respectiva mascara de subred, también se agregaron esas direcciones al área OSPF 0 con los siguientes comandos:

```
R1(config)# interface Loopback12
R1(config-if)# ip address 10.1.12.1 255.255.252.0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
```

```
R1(config)# interface Loopback22
R1(config-if)# ip address 10.1.22.1 255.255.252.0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
```

```
R1(config)# interface Loopback33
R1(config-if)# ip address 10.1.33.1 255.255.252.0
R1(config-if)# ip ospf network point-to-point
```

```

R1(config-if)# exit
R1(config)# interface Loopback44
R1(config-if)# ip address 10.1.44.1 255.255.252.0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit

```

Se agregan las redes al área 0 OSPF con su respectivo Wildcard

CONFIGURACIÓN OSPF AREA 0 ROUTER 1 R1

```

R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.12.0 0.0.3.255 area 0
R1(config-router)# network 10.1.22.0 0.0.3.255 area 0
R1(config-router)# network 10.1.33.0 0.0.3.255 area 0
R1(config-router)# network 10.1.44.0 0.0.3.255 area 0
R1(config-router)# exit

```

3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

Desarrollo:

Tabla 2. Interfaces de Loopback

INTERFACE	IP ADDRESS/MASK
Loopback1	172.5.1.1/22 255.255.252.0
Loopback3	172.5.3.3/22 255.255.252.0
Loopback5	172.5.5.5/22 255.255.252.0

Loopback7	172.5.7.7/22 255.255.252.0
-----------	-------------------------------

Fuente 53: El Autor.

Se crean las cuatro interfaces de Loopback en R5 con las direcciones que se muestran en la tabla diseñada y su respectiva mascara de subred, también agregamos esas direcciones al protocolo EIGRP 10 con los siguientes comandos:

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

```
R5(config-if)# ip address 172.5.1.1 255.255.252.0
```

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

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

```
R5(config-if)# ip address 172.5.3.3 255.255.252.0
```

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

```
R5(config)# interface Loopback5
```

```
R5(config-if)# ip address 172.5.5.5 255.255.252.0
```

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

```
R5(config)# interface Loopback7
```

```
R5(config-if)# ip address 172.5.7.7 255.255.252.0
```

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

Se agregan las redes al protocolo EIGRP 10 con su respectivo Wildcard

CONFIGURACIÓN EIGRP 10 ROUTER 5 R5

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

```
R5(config-router)# no auto-summary
```

```
R5(config-router)#network 172.5.1.0 0.0.3.255
```

```
R5(config-router)#network 172.5.3.0 0.0.3.255
```

```
R5(config-router)#network 172.5.5.0 0.0.3.255
```

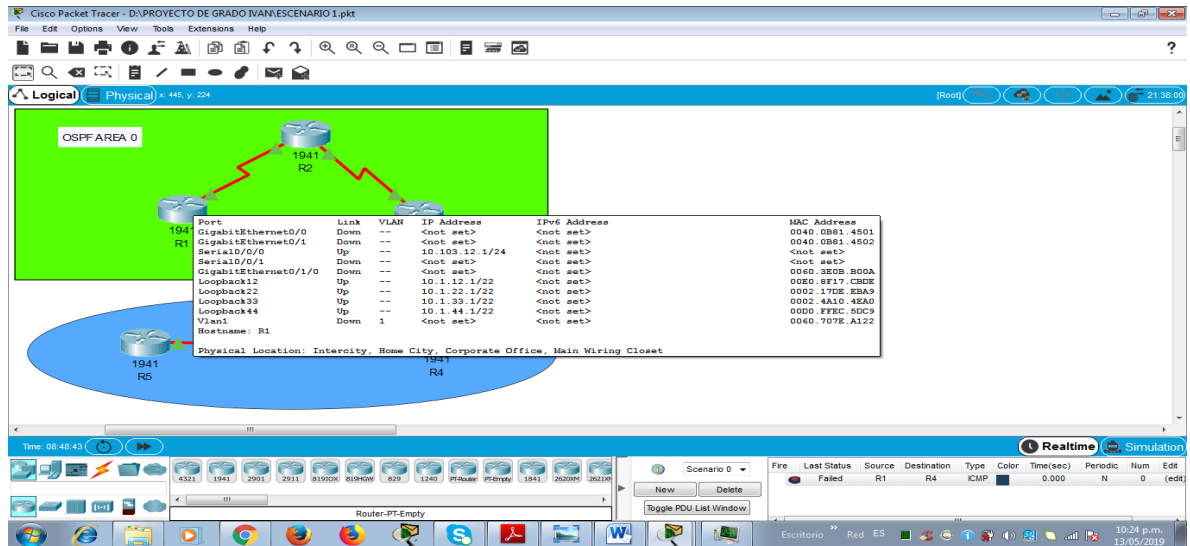
```
R5(config-router)#network 172.5.7.0 0.0.3.255
```

R5(config-router)#exit

R5(config)#

4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando show ip route.

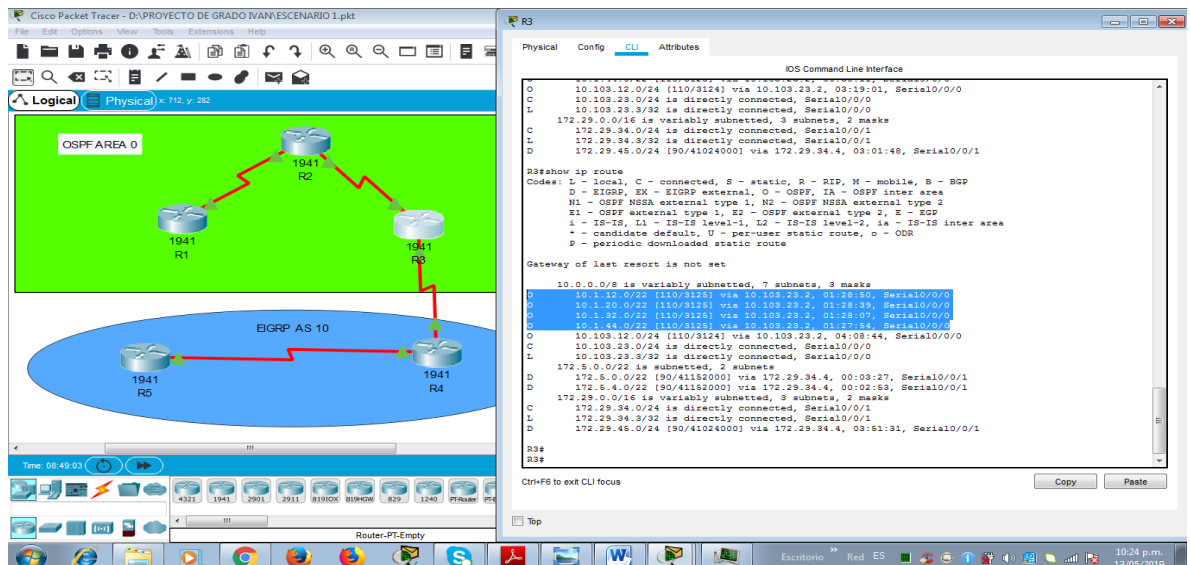
Ilustración 3.Evidencia tabla de enrutamiento de R3



Fuente 3: El Autor.

Se puede observar en la imagen en R1 que se crearon las Loopback 12,22,33 y 44 con sus respectivas máscaras de subred /22 y se encuentran en estado activas (up).

Ilustración 4.Evidencia del comando show ip route



Fuente 4: El Autor.

En la imagen se analiza el resultado del comando `show ip route` en R3 donde se observa que está aprendiendo las nuevas interfaces de Loopback y utilizando para comunicarse las direcciones ip creadas con las Loopback, también se puede visualizar que están utilizando el protocolo OSPF que se configuro el cual esta simbolizado por la letra O en la tabla.

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

Desarrollo:

A continuación, se muestra los comandos para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 en R3:

```
R3(config)# router ospf 1
R3(config)# redistribute eigrp 10 metric 50000 subnets
R3(config-router)#EXIT
R3(config)#
R3#
```

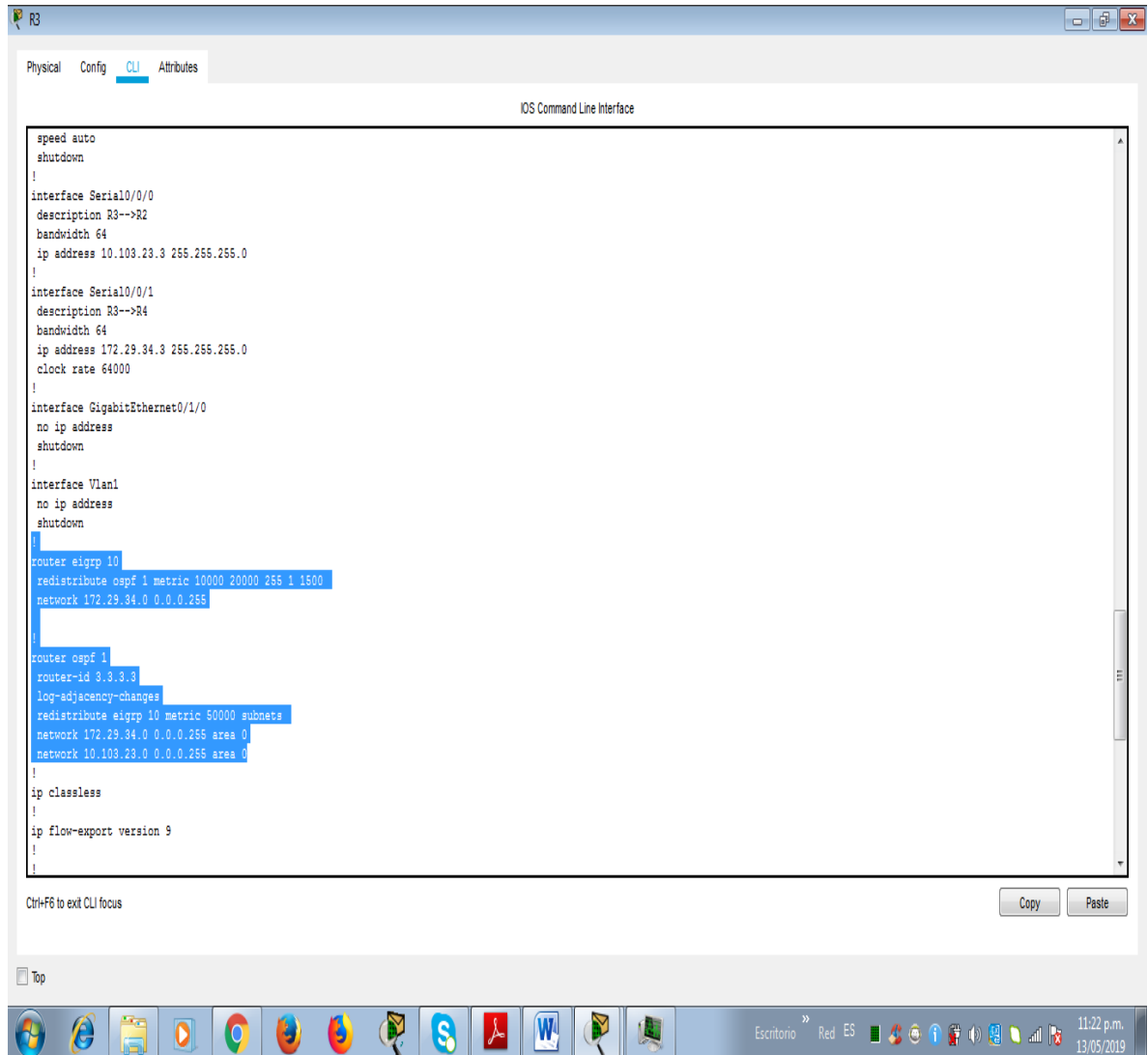
De igual manera se redistribuye las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo con los siguientes comandos:

```
R3(config)# router eigrp 10
R3(config-router)# redistribute ospf 1 metric 10000 20000 255 1 1500
R3(config-router)# exit
```

Con el siguiente comando se observan las configuraciones realizadas

```
R3#SHOW R
```

Ilustración 5.Evidencia del comando SHOW R



```
speed auto
shutdown
!
interface Serial10/0/0
description R3-->R2
bandwidth 64
ip address 10.103.23.3 255.255.255.0
!
interface Serial10/0/1
description R3-->R4
bandwidth 64
ip address 172.29.34.3 255.255.255.0
clock rate 64000
!
interface GigabitEthernet0/1/0
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 10
 redistribute ospf 1 metric 10000 20000 255 1 1500
 network 172.29.34.0 0.0.0.255
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 redistribute eigrp 10 metric 50000 subnets
 network 172.29.34.0 0.0.0.255 area 0
 network 10.103.23.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
```

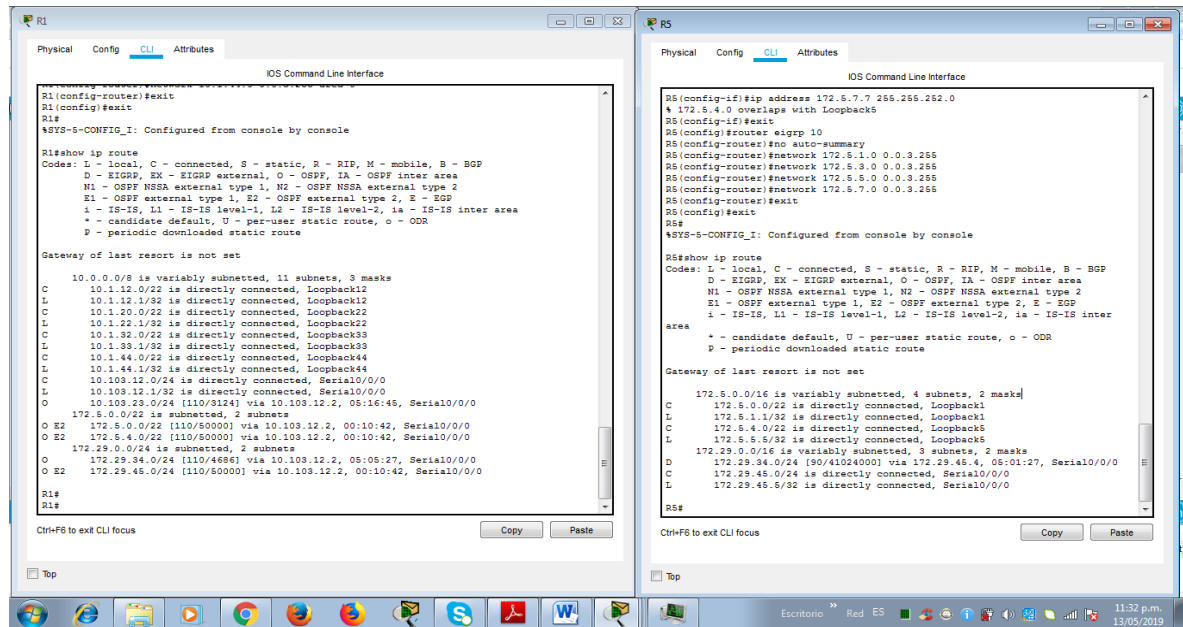
Fuente 5: El Autor.

Se observa que la redistribución del protocolo OSPF 1 y EIGRP 10, se encuentra activas y con los parámetro solicitados como: las rutas EIGRP en OSPF usando el costo de 50000 y las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

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

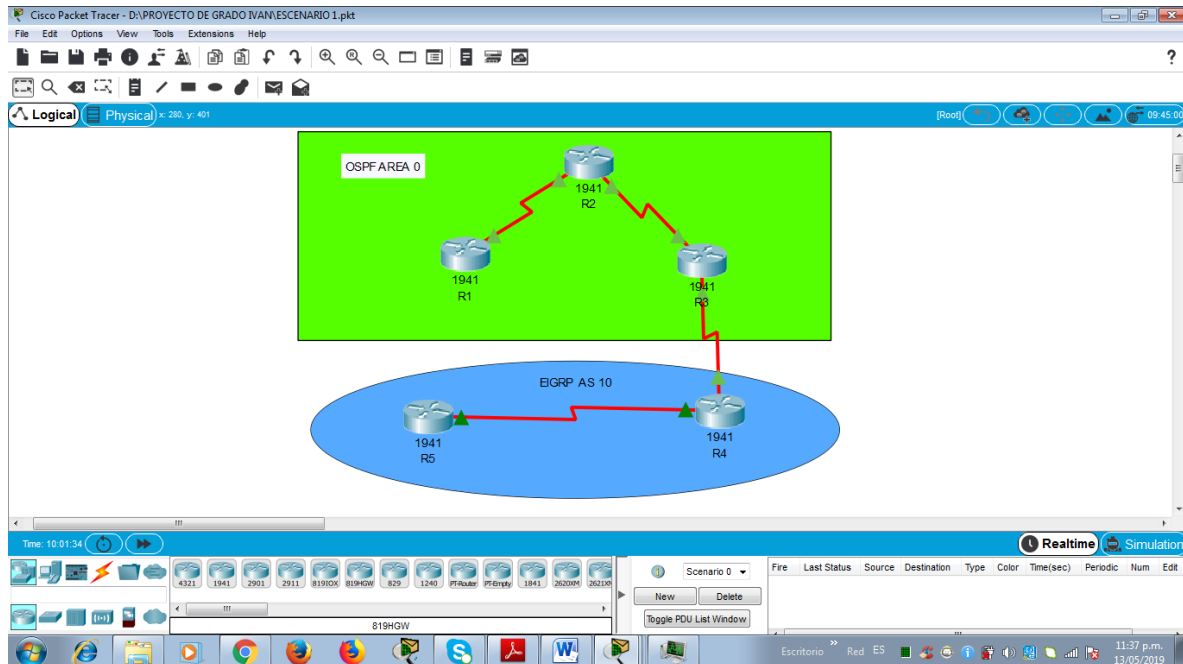
Desarrollo:

Ilustración 6. Evidencia del comando show ip route en R1 y R5



Fuente 6: El Autor.

Ilustración 7. Evidencia de la topología

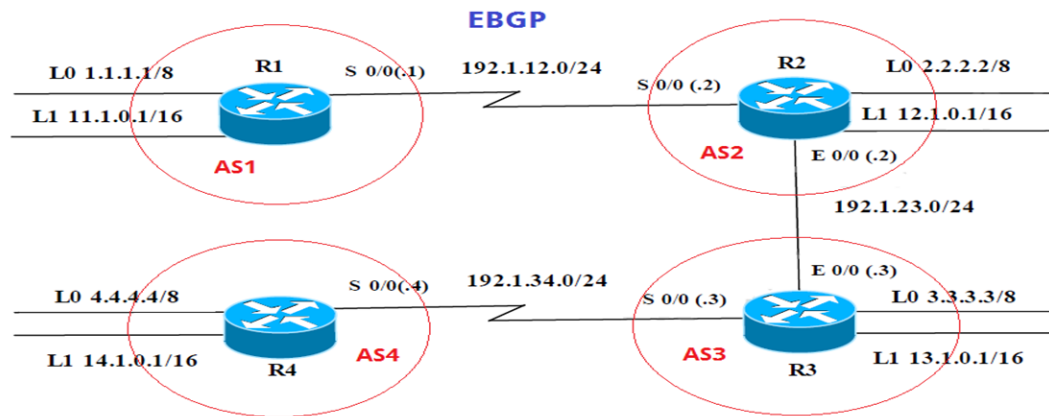


Fuente 7: El Autor.

Las direcciones ip del sistema autónomo opuesto existen en la tabla de enrutamiento de cada sistema.

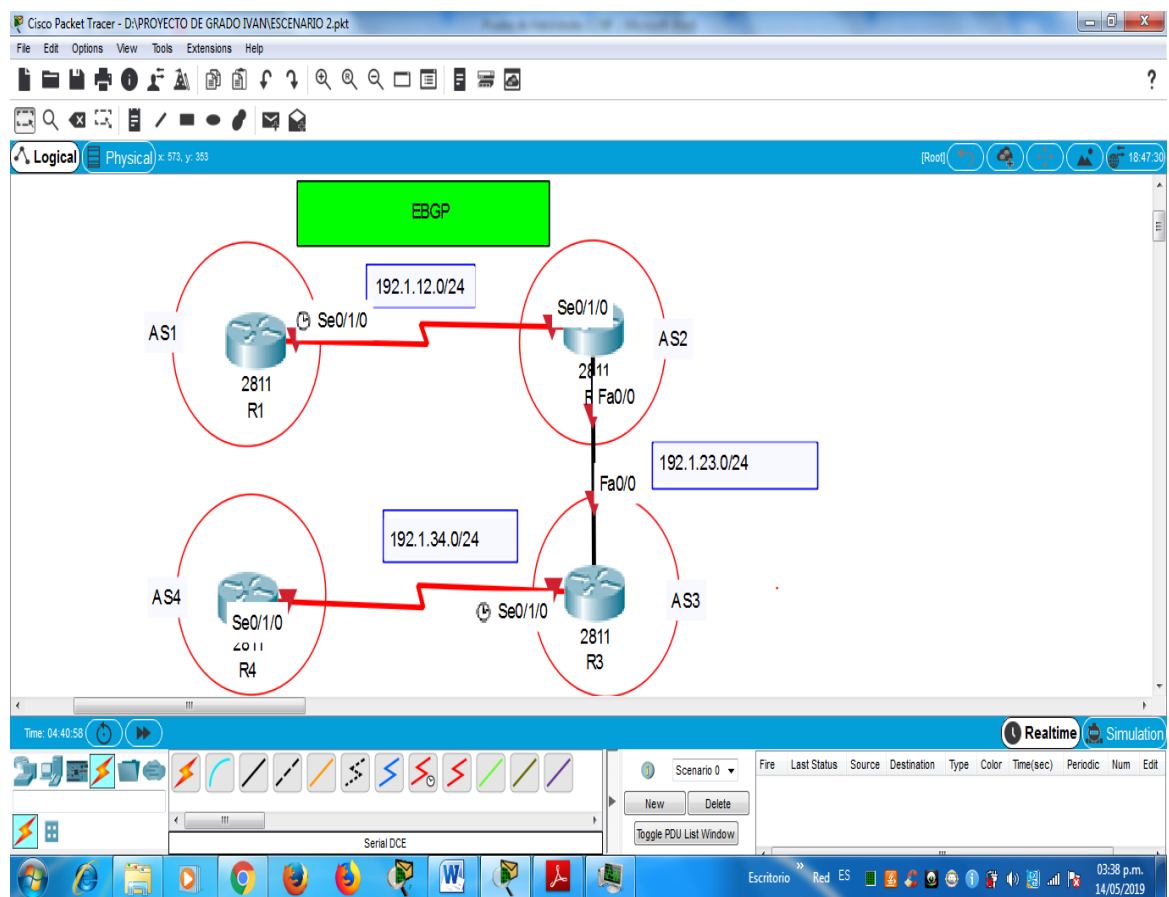
1.1.2. Escenario 2

Ilustración 8. Escenario 2 topología



Fuente 8. Universidad Nacional Abierta y a Distancia (UNAD).

Ilustración 9. Escenario 2 topología Packet Tracer



Fuente 9: El Autor.

Los siguientes son los comandos que permiten darle las configuraciones iniciales a los cuatro routers y su respectivo nombre:

ROUTER 1 R1

```
Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R1
R1(config)# no ip domain-lookup
R1(config)# line con 0
R1(config-line)# logging synchronous
R1(config-line)# exec-timeout 0 0
R1(config-line)#EXIT
R1(config)#
```

ROUTER 2 R2

```
Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R2
R2(config)# no ip domain-lookup
R2(config)# line con 0
R2(config-line)# logging synchronous
R2(config-line)# exec-timeout 0 0
R2(config-line)#EXIT
R2(config)#
```

ROUTER 3 R3

```
Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R3
```

```

R3(config)# no ip domain-lookup
R3(config)# line con 0
R3(config-line)# logging synchronous
R3(config-line)# exec-timeout 0 0
R3(config-line)#EXIT
R3(config)#

```

ROUTER 4 R4

```

Router>
Router>en
Router#CONFIG T
Router(config)#HOSTNAME R4
R4(config)# no ip domain-lookup
R4(config)# line con 0
R4(config-line)# logging synchronous
R4(config-line)# exec-timeout 0 0
R4(config-line)#EXIT
R4(config)#

```

Información para configuración de los Routers

Tabla 3.Configuración de 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 0/1/0	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 0/1/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

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 0/1/0	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 0/1/0	192.1.34.4	255.255.255.0

Fuente 53. Universidad Nacional Abierta y A Distancia (UNAD).

Configuración de interfaces según el diagrama, se agrega la descripción, se establece la frecuencia de reloj, el ancho de banda se asigna la dirección ip con su respectiva máscara de subred y se enciende la interface.

ROUTER 1 R1

```
R1(config)# interface Serial 0/1/0
R1(config-if)# description R1-->R2
R1(config-if)# clock rate 64000
R1(config-if)# bandwidth 64
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

ROUTER 2 R2

```
R2(config)# interface Serial 0/1/0
R2(config-if)# description R2-->R1
R2(config-if)# bandwidth 64
R2(config-if)# ip address 192.1.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

```
R2(config)# interface fa0/0
R2(config-if)# description R2-->R3
R2(config-if)# bandwidth 64
R2(config-if)# ip address 192.1.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

ROUTER 3 R3

```
R3(config)# interface Serial 0/1/0
R3(config-if)# description R3-->R4
R3(config-if)# bandwidth 64
R3(config-if)# ip address 192.1.34.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
```

```
R3(config)# interface fa0/0
R3(config-if)# description R3-->R2
R3(config-if)# ip address 192.1.23.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
```

ROUTER 4 R4

```
R4(config)# interface Serial 0/1/0
R4(config-if)# description R4-->R3
R4(config-if)# clock rate 64000
R4(config-if)# bandwidth 64
R4(config-if)# ip address 192.1.34.4 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# exit
```

con los siguientes comandos se hace la configuración de las Loopback con sus respectivas direcciones y máscaras de subred dadas en la tabla de todos los routers:

ROUTER 1 R1

```
R1(config)# interface Loopback0
R1(config-if)# ip address 1.1.1.1 255.0.0.0 R1(config-if)# exit
R1(config)# interface Loopback1
R1(config-if)# ip address 11.1.0.1 255.255.0.0
R1(config-if)# exit
```

ROUTER 2 R2

```
R2(config)# interface Loopback0
R2(config-if)# ip address 2.2.2.2 255.0.0.0 R2(config-if)# exit

R2(config)# interface Loopback1
R2(config-if)# ip address 12.1.0.1 255.255.0.0
R2(config-if)# exit
```

ROUTER 3 R3

```
R3(config)# interface Loopback0
R3(config-if)# ip address 3.3.3.3 255.0.0.0 R3(config-if)# exit

R3(config)# interface Loopback1
R3(config-if)# ip address 13.1.0.1 255.255.0.0
R3(config-if)# exit
```

ROUTER 4 R4

```
R4(config)# interface Loopback0
```

```
R4(config-if)# ip address 4.4.4.4 255.0.0.0 R4(config-if)# exit
```

```
R4(config)# interface Loopback1
```

```
R4(config-if)# ip address 14.1.0.1 255.255.0.0
```

```
R4(config-if)# exit
```

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 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Desarrollo: Con los siguientes comandos se procede a realizar la configuración de vecino BGP entre R1 y R2 con los respectivos AS que indica el diagrama dado, también se anunciarán las direcciones de Loopback en BGP, también se asigna el ID para los routers:

```
R1#conf t
```

```
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 192.1.12.0 mask 255.255.255.0
```

```
R1(config-router)# neighbor 2.2.2.2 remote-as 2
```

```
R1(config-router)# neighbor 2.2.2.2 update-source Loopback0(Comando no soportado por Packet Tracer )
```

```
R1(config-router)# neighbor 12.1.0.1 remote-as 2
```

```
R1(config-router)# neighbor 12.1.0.1 update-source Loopback1(Comando no soportado por Packet Tracer )
```

```
R2#conf t
```

```
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)#network 192.1.12.0 mask 255.255.255.0
```

R2(config-router)# neighbor 1.1.1.1 remote-as 1

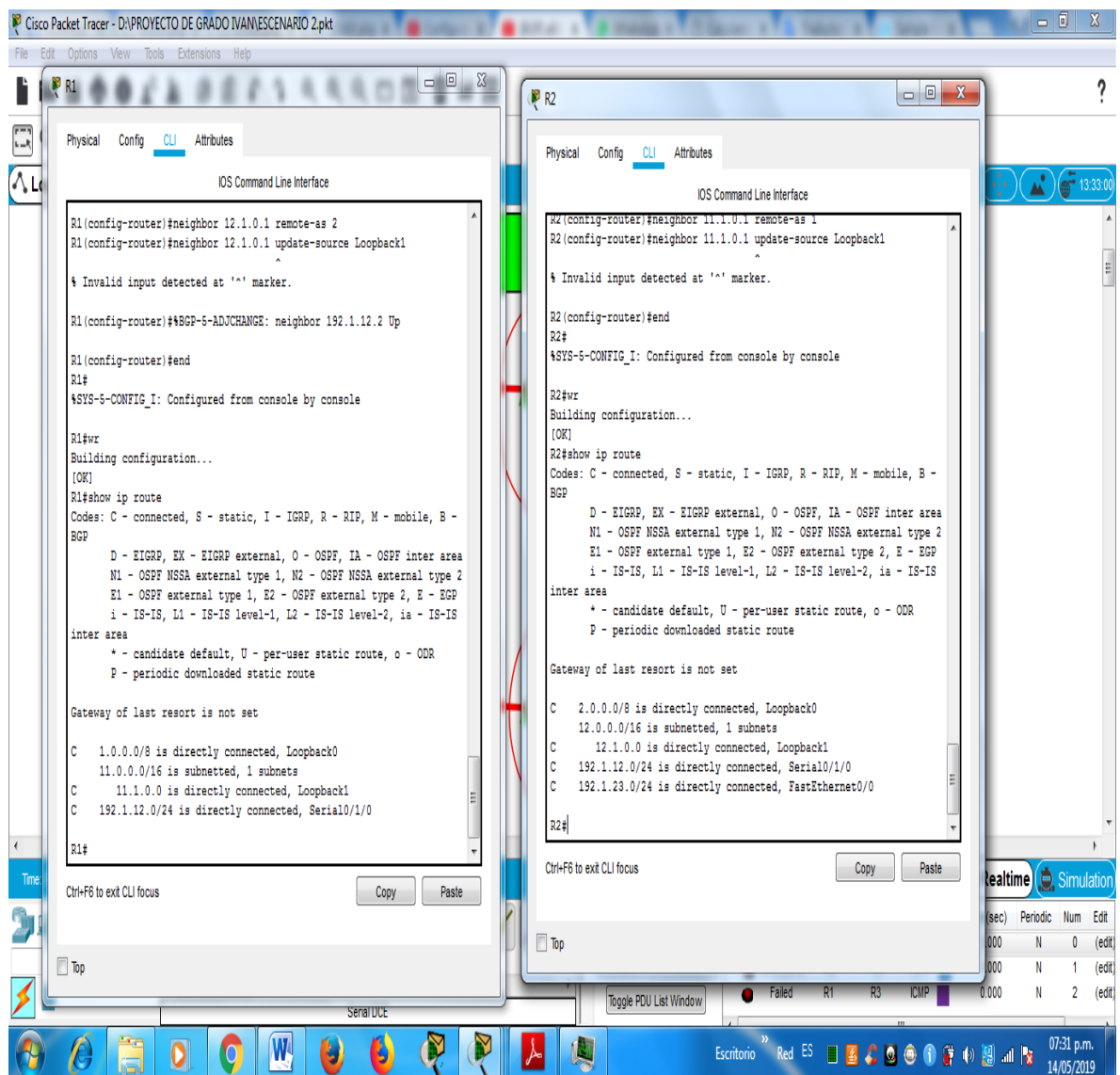
R2(config-router)# neighbor 1.1.1.1 update-source Loopback0(Comando no soportado por Packet Tracer)

R2(config-router)# neighbor 11.1.0.1 remote-as 1

R2(config-router)# neighbor 11.1.0.1 update-source Loopback1(Comando no soportado por Packet Tracer)

show ip route

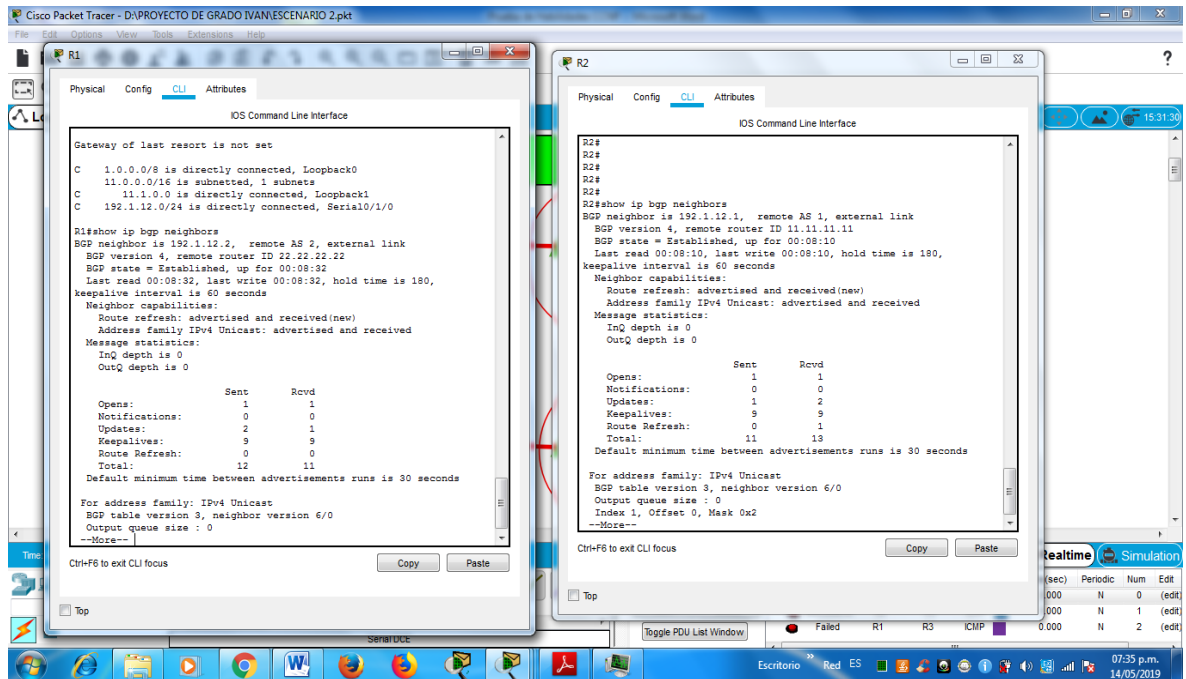
Ilustración 10 .Evidencia del comando show ip route



Fuente 10: El Autor.

show ip bgp neighbors

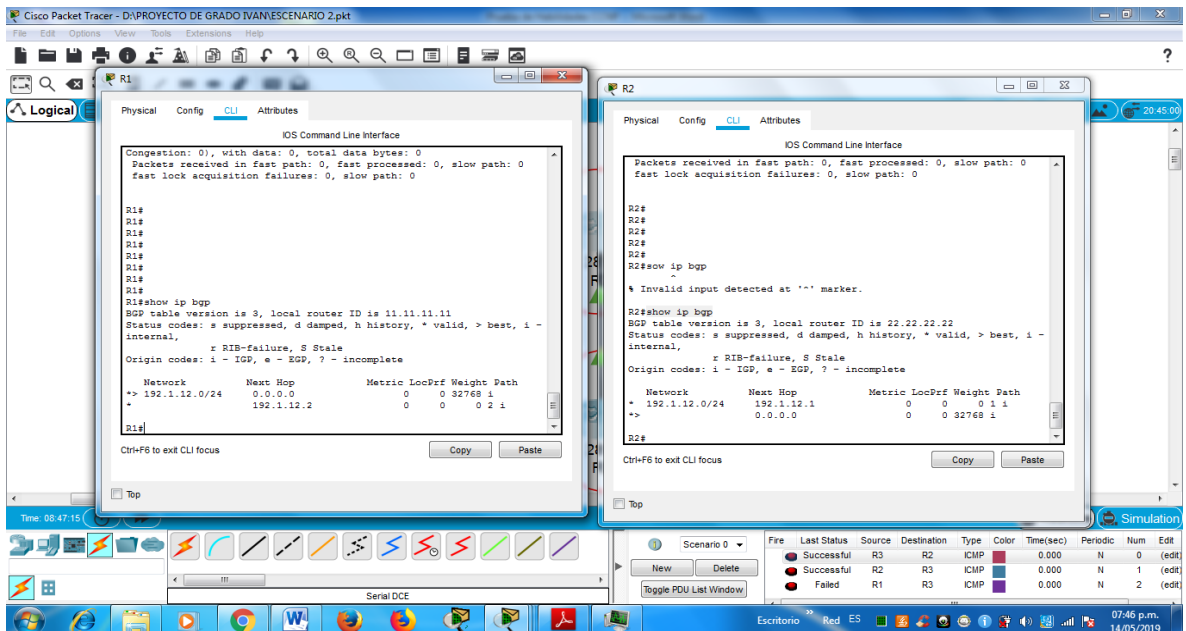
Ilustración 11.Evidencia del comando show ip bgp neighbors



Fuente 11: El Autor.

show ip bgp

Ilustración 12.Evidencia del comando show ip bgp



Fuente 12: El Autor.

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 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

Desarrollo: Con los siguientes comandos se procede a realizar la configuración de vecino BGP entre R2 y R3 con los respectivos AS que indica el diagrama dado, también se anunciarán las direcciones de Loopback en BGP, también se asigna el ID para los routers:

```
R2#conf t
```

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

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

```
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
```

```
R2(config-router)# neighbor 3.3.3.3 remote-as 3
```

```
R2(config-router)# neighbor 3.3.3.3 update-source Loopback0(Comando no soportado por Packet Tracer )
```

```
R2(config-router)# neighbor 13.1.0.1 remote-as 3
```

```
R2(config-router)# neighbor 13.1.0.1 update-source Loopback1(Comando no soportado por Packet Tracer )
```

```
R3#conf t
```

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

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

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

```
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
```

```
R3(config-router)# neighbor 2.2.2.2 remote-as 2
```

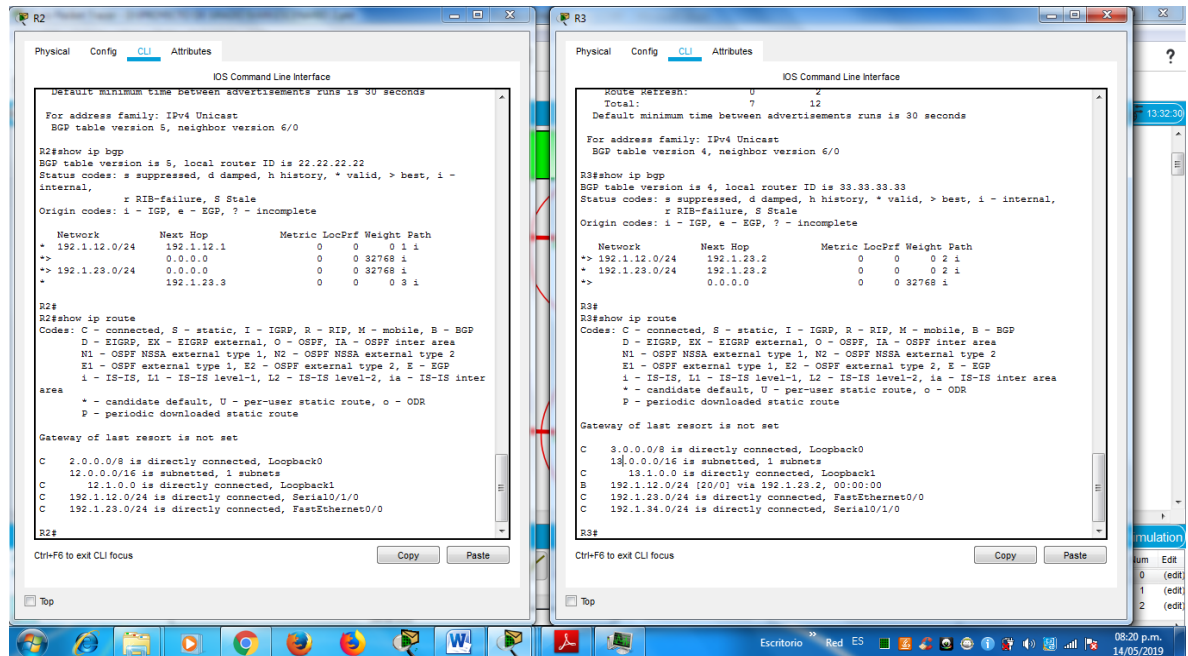
```
R3(config-router)# neighbor 2.2.2.2 update-source Loopback0(Comando no soportado por Packet Tracer )
```

```
R3(config-router)# neighbor 12.1.0.1 remote-as 2
```

```
R3(config-router)# neighbor 12.1.0.1 update-source Loopback1(Comando no soportado por Packet Tracer )
```

show ip route

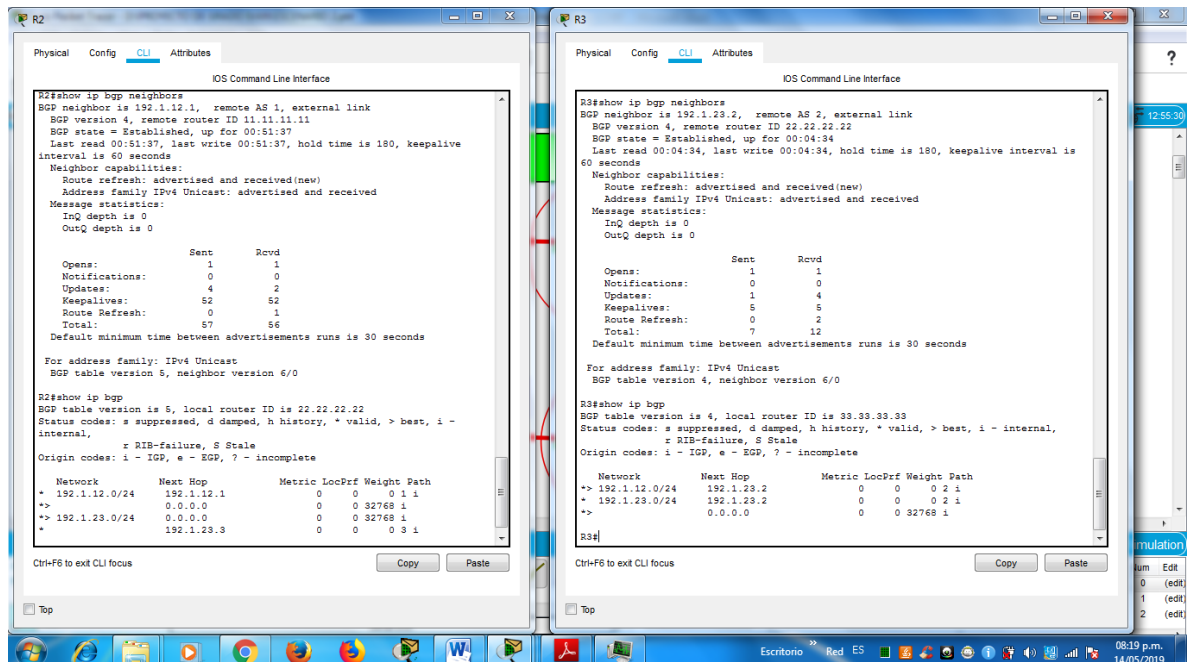
Ilustración 13.Evidencia del comando show ip route



Fuente 13: El Autor.

show ip bgp neighbors

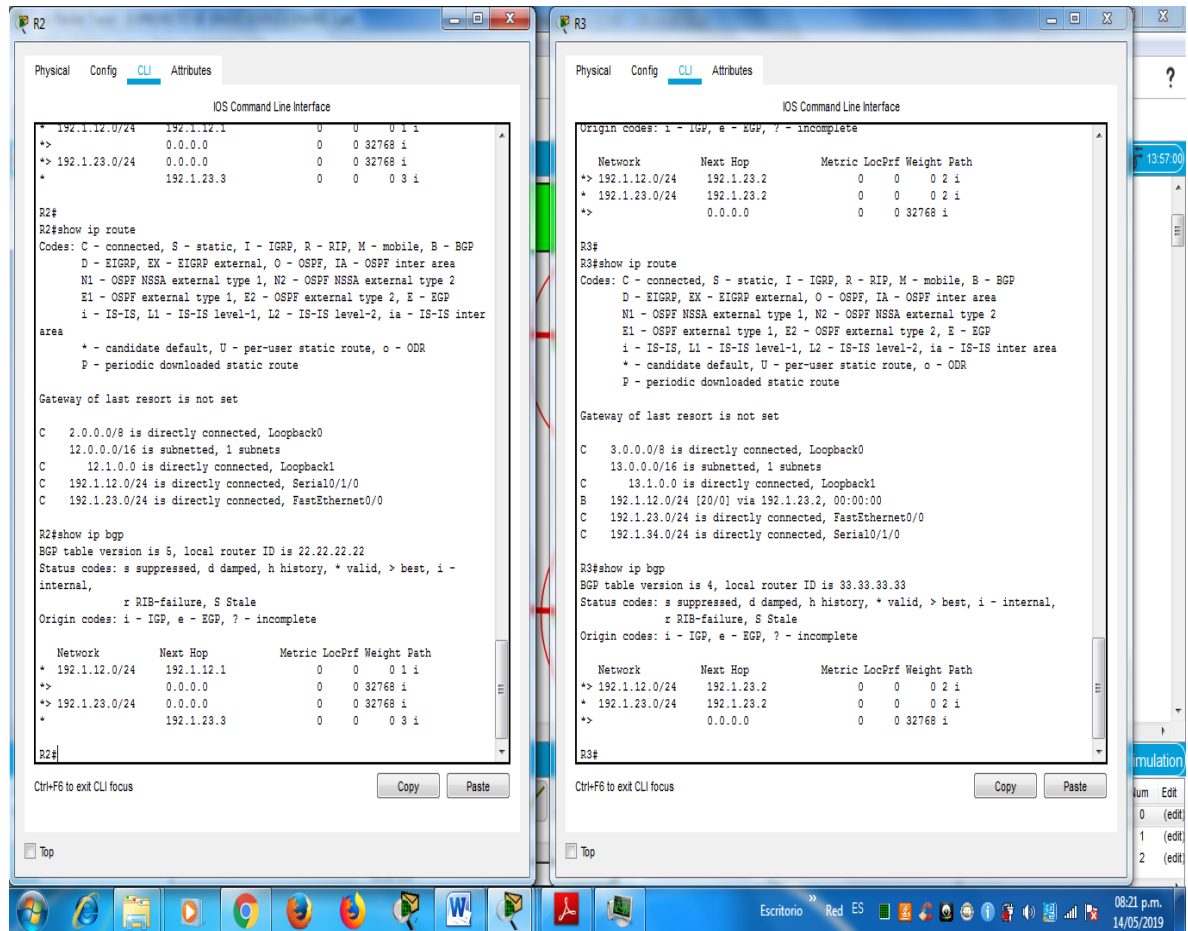
Ilustración 14.Evidencia del comando show ip bgp neighbors



Fuente 14: El Autor.

show ip bgp

Ilustración 15.Evidencia del comando show ip bgp



Fuente 15: El Autor.

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 44.44.44.44. 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.

Desarrollo: Con los siguientes comandos se procede a realizar la configuración de vecino BGP entre R3 y R4 con los respectivos AS que indica el diagrama dado, también se anunciarán las direcciones de Loopback 0 en BGP, también se asigna el ID para los routers:

```
R3#conf t
R3(config)# router bgp 3
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
```

```
R3(config-router)# neighbor 4.4.4.4 remote-as 4
R3(config-router)# neighbor 4.4.4.4 update-source Loopback0(Comando no
soportado por Packet Tracer )
```

```
R3(config-router)# neighbor 14.1.0.1 remote-as 4
R3(config-router)# neighbor 14.1.0.1 update-source Loopback1(Comando no
soportado por Packet Tracer )
```

```
R4#conf t
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 192.1.34.0 mask 255.255.255.0
```

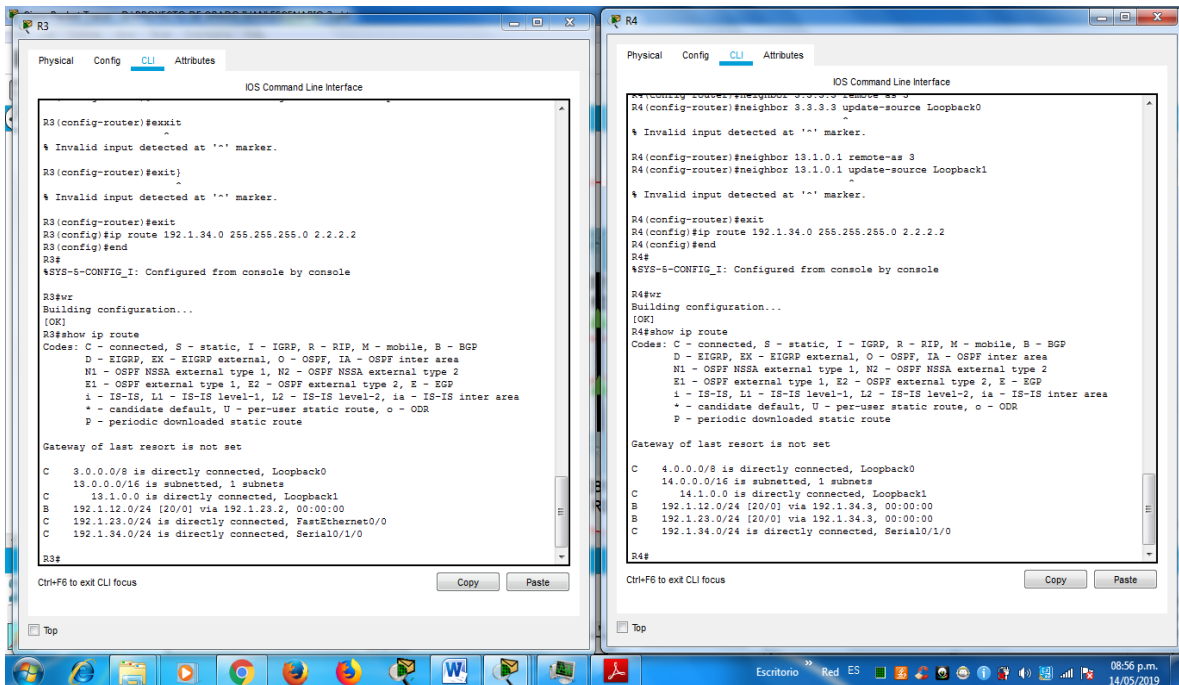
```
R4(config-router)# neighbor 3.3.3.3 remote-as 3
R4(config-router)# neighbor 3.3.3.3 update-source Loopback0(Comando no
soportado por Packet Tracer )
R4(config-router)# neighbor 13.1.0.1 remote-as 3
R4(config-router)# neighbor 13.1.0.1 update-source Loopback1(Comando no
soportado por Packet Tracer)
```

Comandos para configurar las rutas estáticas

```
R3 (config) # ip route 192.1.34.0 255.255.255.0 2.2.2.2
R4 (config) # ip route 192.1.34.0 255.255.255.0 2.2.2.2
```

show ip route

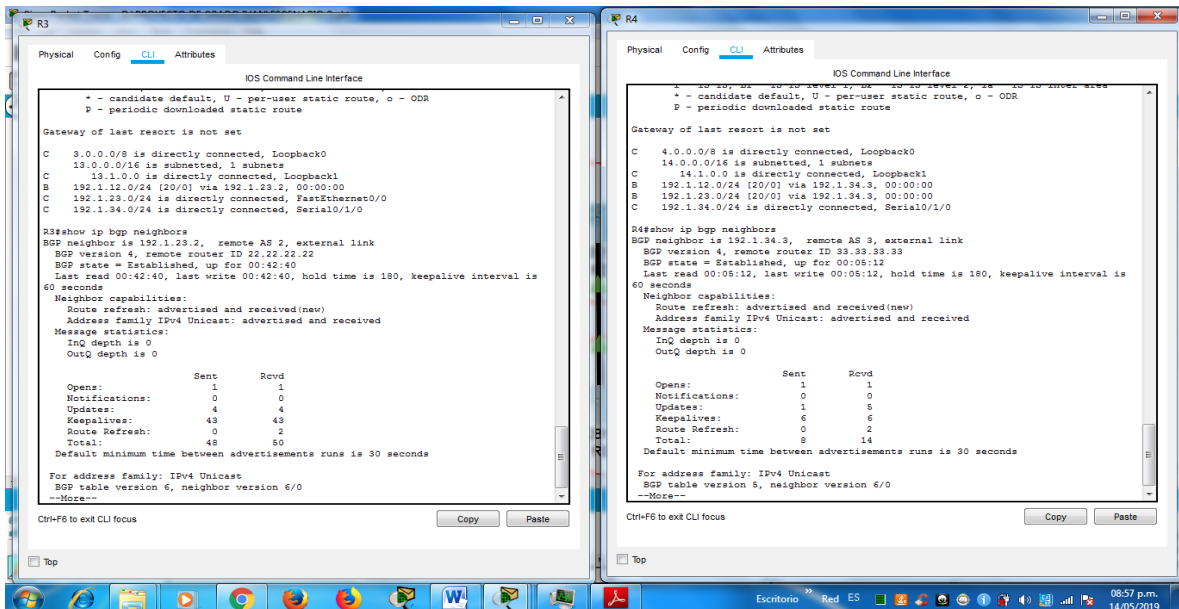
Ilustración 16.Evidencia del comando show ip route



Fuente 16: El Autor.

show ip bgp neighbors

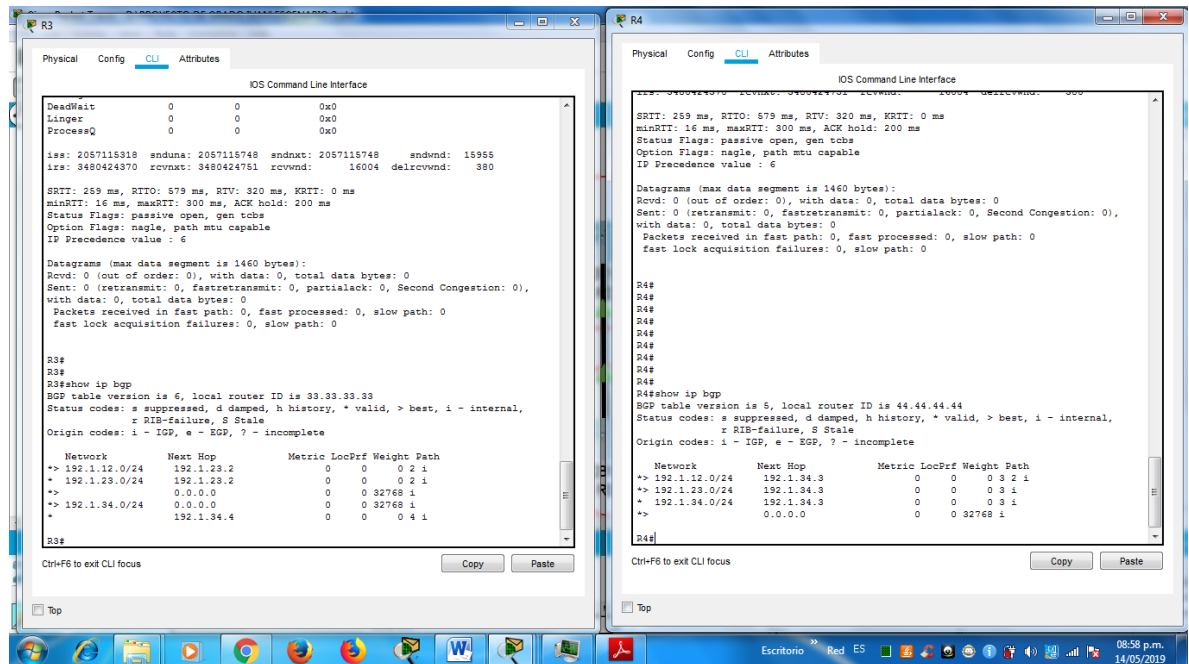
Ilustración 17.Evidencia del comando show ip bgp neighbors



Fuente 17: El Autor.

show ip bgp

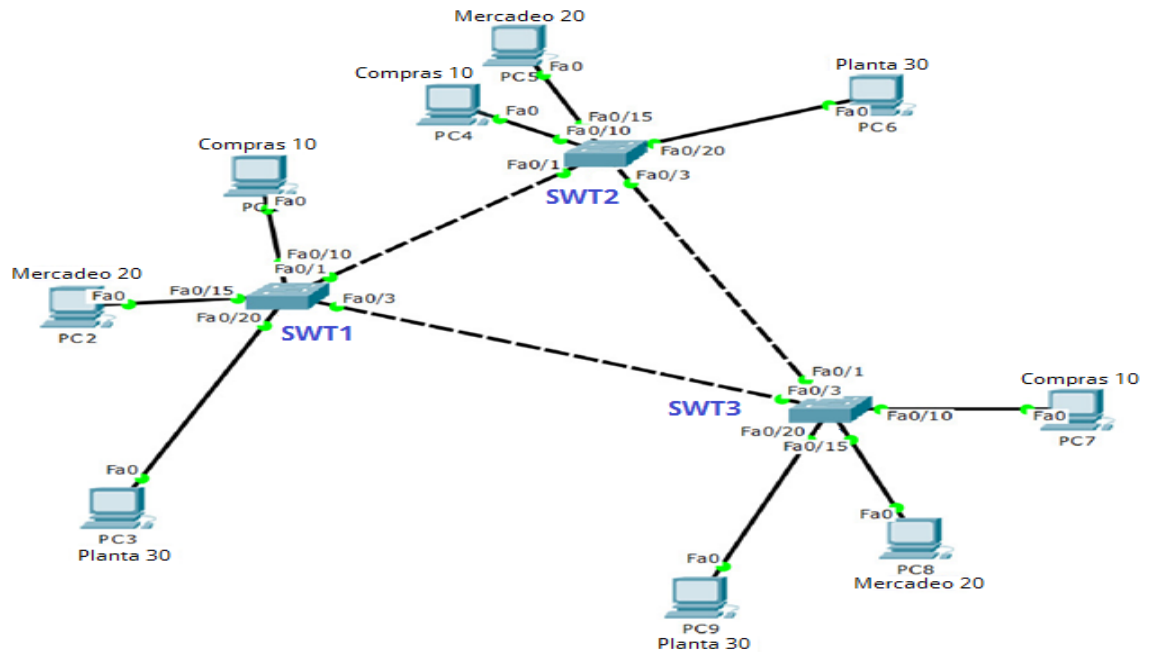
Ilustración 18.Evidencia del comando show ip bgp



Fuente 18: El Autor.

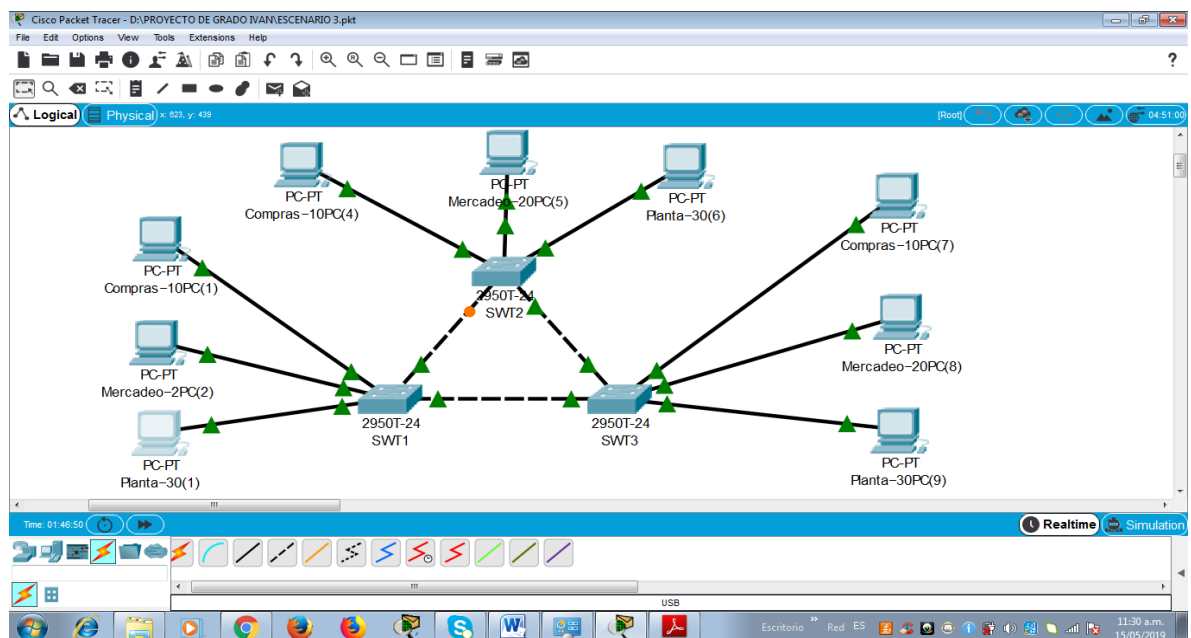
1.1.3 Escenario 3

Ilustración 19. Topología Escenario 3



Fuente 19. Universidad Nacional Abierta y a Distancia (UNAD).

Ilustración 20. Topología Escenario 3 Packet Tracer



Fuente 20: El Autor.

Configuraciones iniciales

SWITCH 1 SWT1

```
en
config t
hostname SWT1
ip domain-name CCNP.NET
no ip domain lookup
interface range f0/1-24 , g0/1-2
shutdown
exit
vtp mode transparent
line con 0
no exec-timeout
logging synchronous
exit
```

SWITCH 2 SWT2

```
en
config t
hostname SWT2
ip domain-name CCNP.NET
no ip domain lookup
interface range f0/1-24 , g0/1-2
shutdown
exit
vtp mode transparent
line con 0
no exec-timeout
logging synchronous
exit
```

SWITCH 3 SWT3

```
en
```

```
config t
hostname SWT3
ip domain-name CCNP.NET
no ip domain lookup
interface range f0/1-24 , g0/1-2
shutdown
exit
vtp mode transparent
line con 0
no exec-timeout
logging synchronous
exit
```

Configuración de interfaces que se utilizan con los siguientes comandos se encenderán:

SWITCH 1 SWT1

```
en
config t
interface range f0/1
no shutdown
exit
interface range f0/3
no shutdown
exit
interface range f0/10
no shutdown
exit
interface range f0/15
no shutdown
exit
interface range f0/20
no shutdown
exit
```

SWITCH 2 SWT2

```
en
config t
interface range f0/1
no shutdown
exit
interface range f0/3
no shutdown
exit
interface range f0/10
no shutdown
exit
interface range f0/15
no shutdown
exit
interface range f0/20
no shutdown
exit
```

SWITCH 3 SWT3

```
en
config t
interface range f0/1
no shutdown
exit
interface range f0/3
no shutdown
exit
interface range f0/10
no shutdown
exit
interface range f0/15
```

```
no shutdown
exit
interface range f0/20
no shutdown
exit
```

A. Configurar VTP

1. 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.

Desarrollo:

A continuación, se darán los comandos para configurar vtp en SWT2 y se configurara en modo servidor se nombrará el dominio como CCNP y se asignara la contraseña indicada por el ejercicio:

```
SWT2(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT2(config)#vtp version 2
SWT2(config)#vtp mode server
Setting device to VTP SERVER mode.
SWT2(config)#vtp password cisco
Setting device VLAN database password to cisco
```

De igual manera se configurarán los switches SWT1 y SWT3 para utilizar VTP como clientes dentro de un dominio VPT llamado CCNP con su contraseña usando los siguientes comandos:

```
SWT1#config t
SWT1(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT1(config)#vtp version 2
```

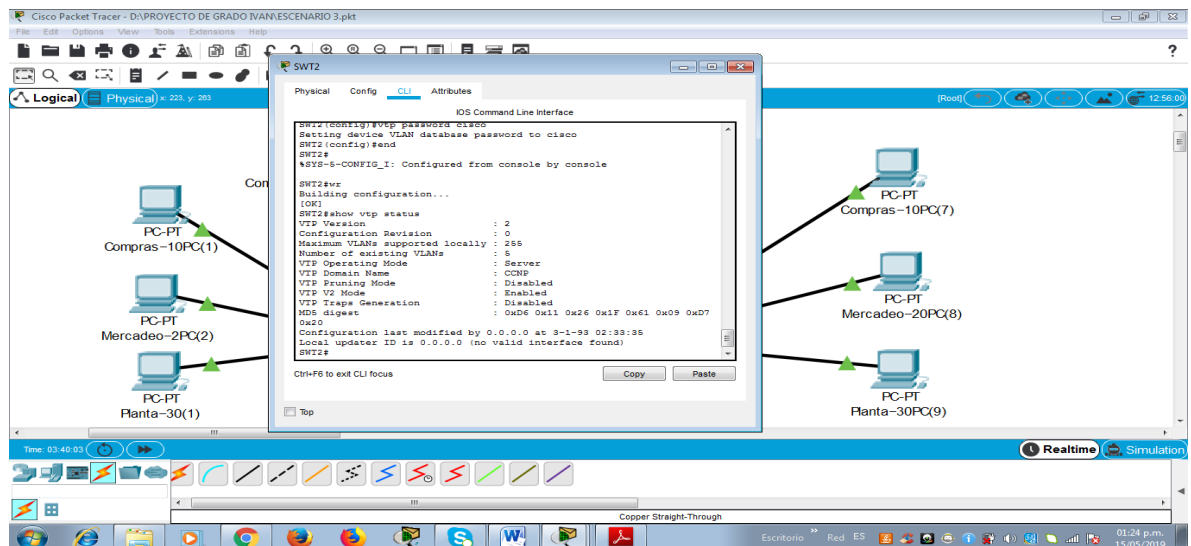
```
SWT1(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWT1(config)#vtp password cisco
Setting device VLAN database password to cisco
SWT1(config)#exit
```

```
SWT3#config t
SWT3(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT3(config)#vtp version 2
SWT3(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWT3(config)#vtp password cisco
Setting device VLAN database password to cisco
SWT3(config)#exit
```

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

show vtp status SWT2

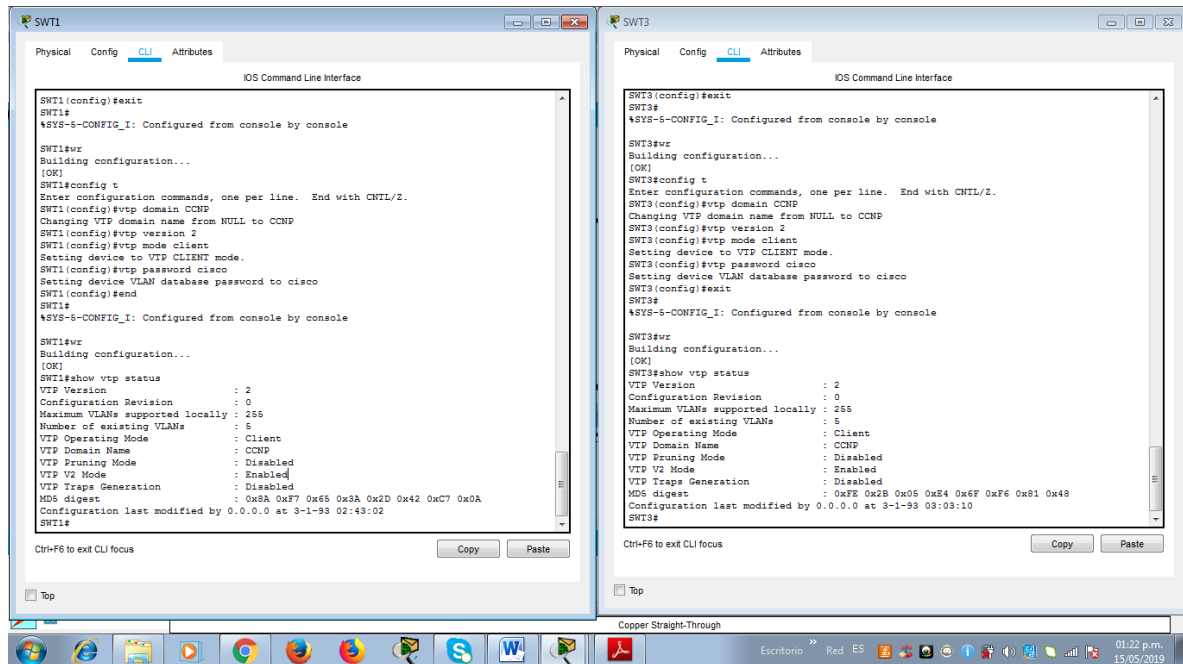
Ilustración 21.Evidencia show vtp status SWT2



Fuente 21: El Autor.

show vtp status SWT1 y SWT3

Ilustración 22.Evidencia show vtp status SWT1 y SWT3



Fuente.22: El Autor.

B. Configurar DTP (Dynamic Trunking Protocol)

1. Configure 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.

Desarrollo: comandos para realizar la configuración de un enlace troncal ("trunk"):

```
SWT1#config t
```

```
SWT1(config)#interface fa0/1
```

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

```
SWT1(config-if)#switchport mode dynamic auto
```

```
SWT1(config-if)#exit
```

```
SWT2(config)#interface f0/1
```

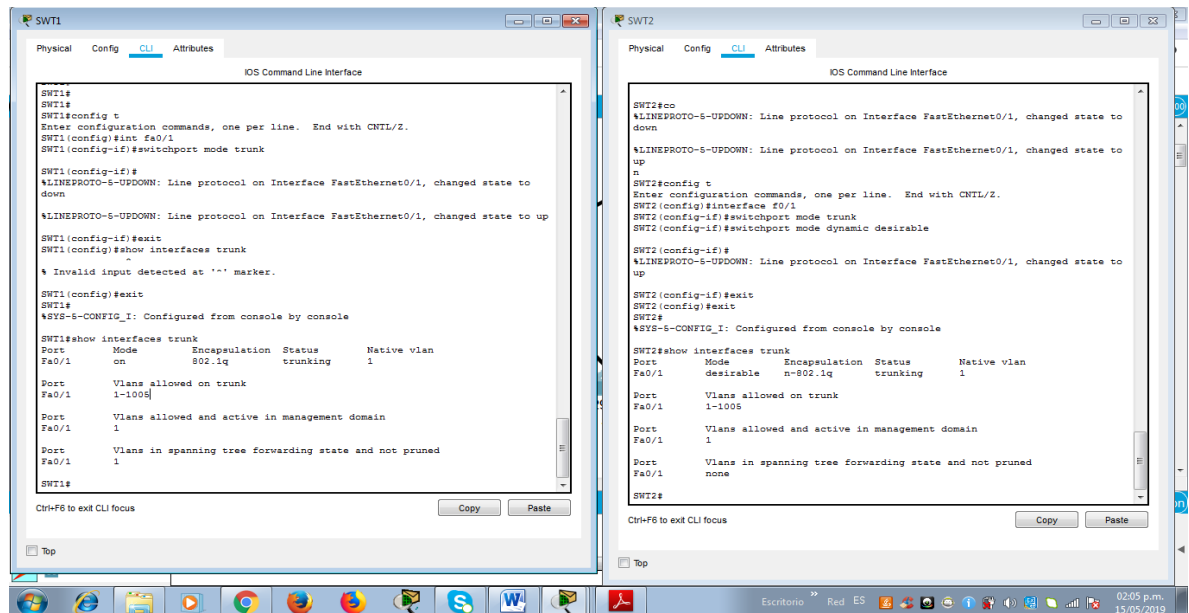
```
SWT2(config-if)#switchport mode trunk
```

```
SWT2(config-if)#switchport mode dynamic desirable
```

```
SWT1(config-if)#exit
```

2. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.

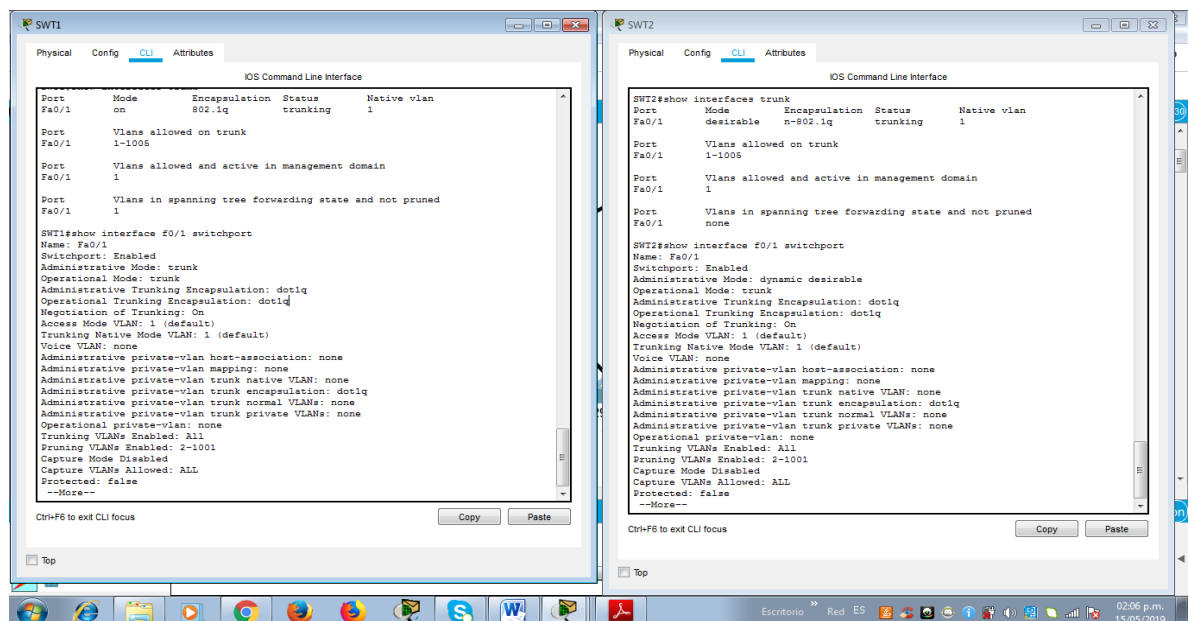
Ilustración 23. Evidencia del comando show interfaces trunk



Fuente 23: El Autor.

show interface f0/1 switchport

Ilustración 24. Evidencia show interface f0/1 switchport



Fuente 24: El Autor.

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

Desarrollo: configuración de un enlace "trunk" estático en SWT1 y SWT3 con los siguientes comandos:

```
SWT1#config t
```

```
SWT1(config)#interface fa0/3
```

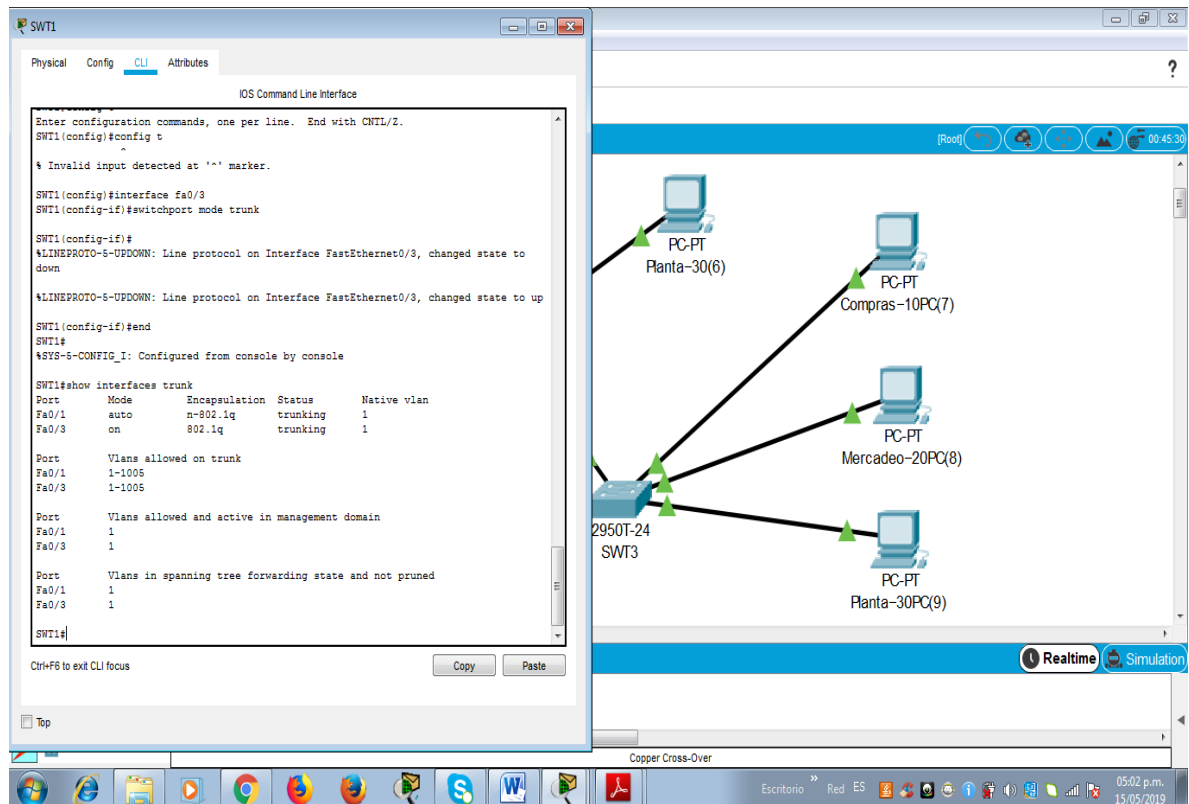
```
SWT1(config-if)#switchport mode trunk
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
```

- Verifique el enlace "trunk" el comando `show interfaces trunk` en SWT1.

Ilustración 25.Evidencia del comando `show interfaces trunk`



Fuente 25: El Autor.

5. Configure un enlace "trunk" permanente entre SWT2 y SWT3.

Desarrollo: a continuación, se muestran los comandos para configurar un enlace "trunk" permanente entre SWT2 y SWT3:

```
SWT2#config t
```

```
SWT2(config)#interface fa0/3
```

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

```
SWT2(config-if) #end
```

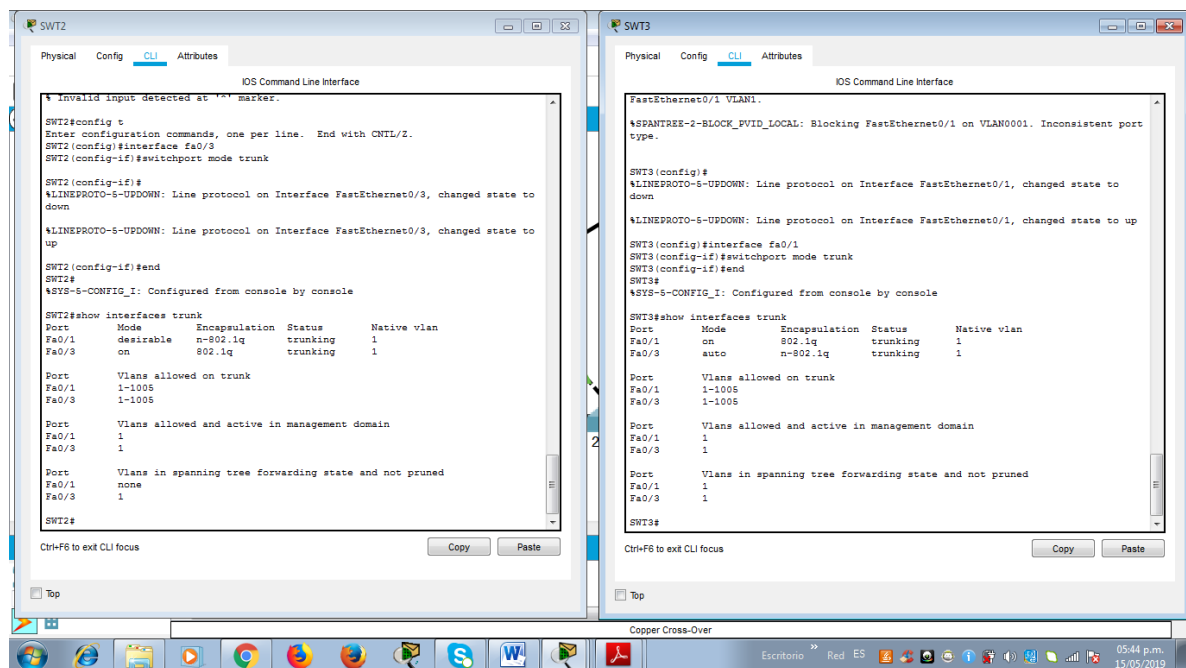
```
SWT3#config t
```

```
SWT3(config)#interface fa0/1
```

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

```
SWT3(config-if) #end
```

Ilustración 26.Evidencia de configuración



Fuente 26: El Autor.

C. Agregar VLANs y asignar puertos.

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

Desarrollo:

Se crea en STW1 la VLAN 10 con los siguientes comandos:

```
SWT1>enable
```

```
SWT1#conf terminal
```

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

```
SWT1(config)#vlan 10
```

VTP VLAN configuration not allowed when device is in CLIENT mode.

```
SWT1(config)# exit
```

```
SWT1#
```

Con los siguientes comandos en STW2 se crean las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99)

```
SWT2# config t
```

```
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
```

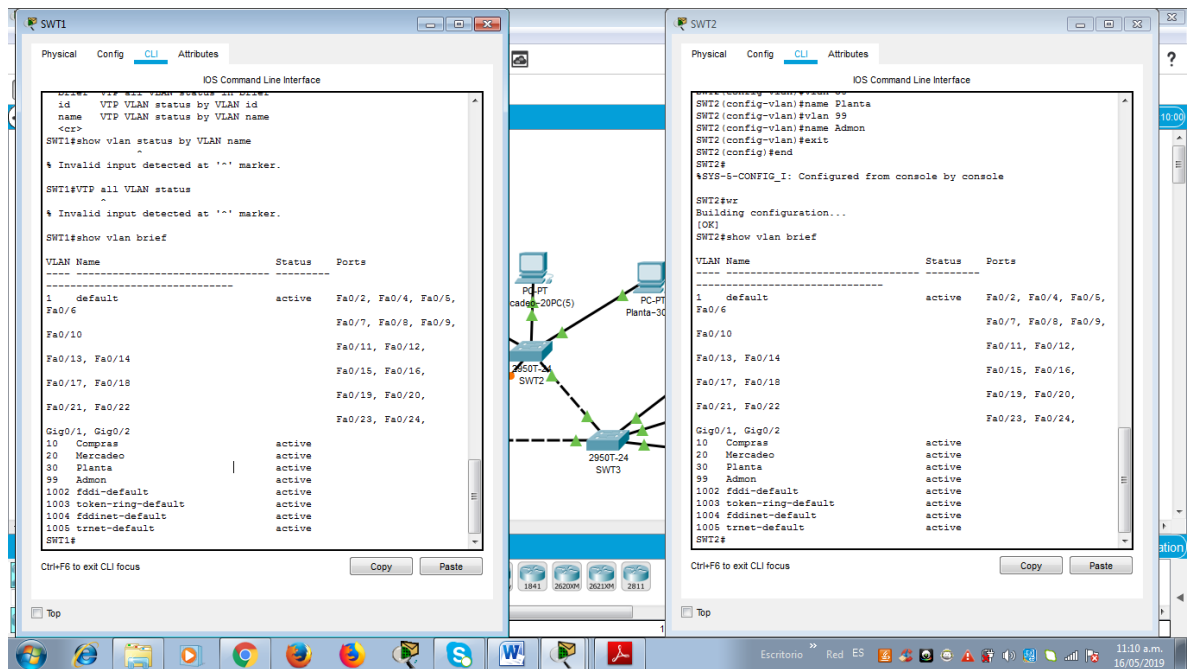
```
SWT2(config-vlan)#exit
```

```
SWT2(config)#
```

2. Verifique que las VLANs han sido agregadas correctamente.

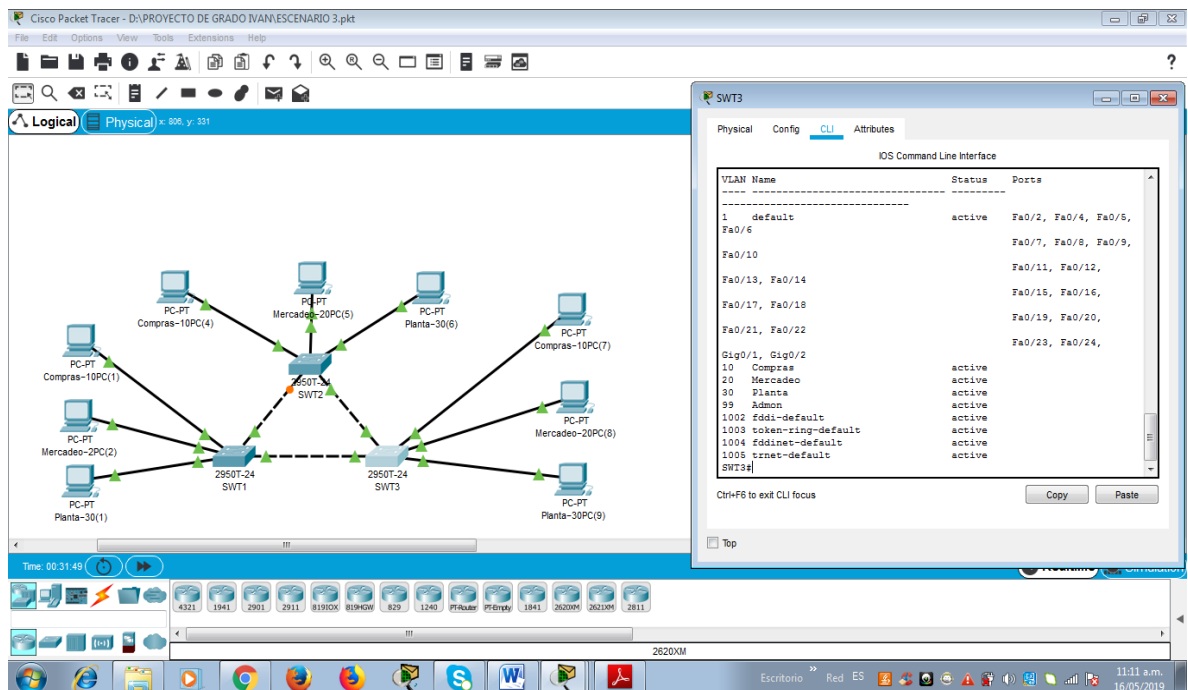
Con el comando show vlan brief se revisa las vlans creadas en los switch

Ilustración 27. Evidencia de los comandos show vlan brief



Fuente 27: El Autor.

Ilustración 28. Evidencia de los comandos show vlan brief



Fuente 28: El Autor.

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

Tabla 4. De configuración de direcciones ip y VLANS

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

Fuente 54. Universidad Nacional Abierta y a Distancia (UNAD).

4. Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.

Desarrollo:

Con estos comandos se asocia la respectiva interfaz con la vlan10 en cada swich:

SWITCH 1 SWT1

```
SWT1#conf t
SWT1(config)#interface f0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#exit
SWT1(config)#
```

SWITCH 2 SWT2

```
SWT2#conf t
SWT2(config)#interface f0/10
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 10
```

SWT2(config-if)#exit

SWT2(config)#

SWITCH 3SWT3

SWT1# conf t

SWT3(config)#interface f0/10

SWT3(config-if)#switchport mode access

SWT3(config-if)#switchport access vlan 10

SWT3(config-if)#exit

SWT3(config)#

A continuación se muestra la configuración de las direcciones IP de todos los pc:

Tabla 5. Configuración

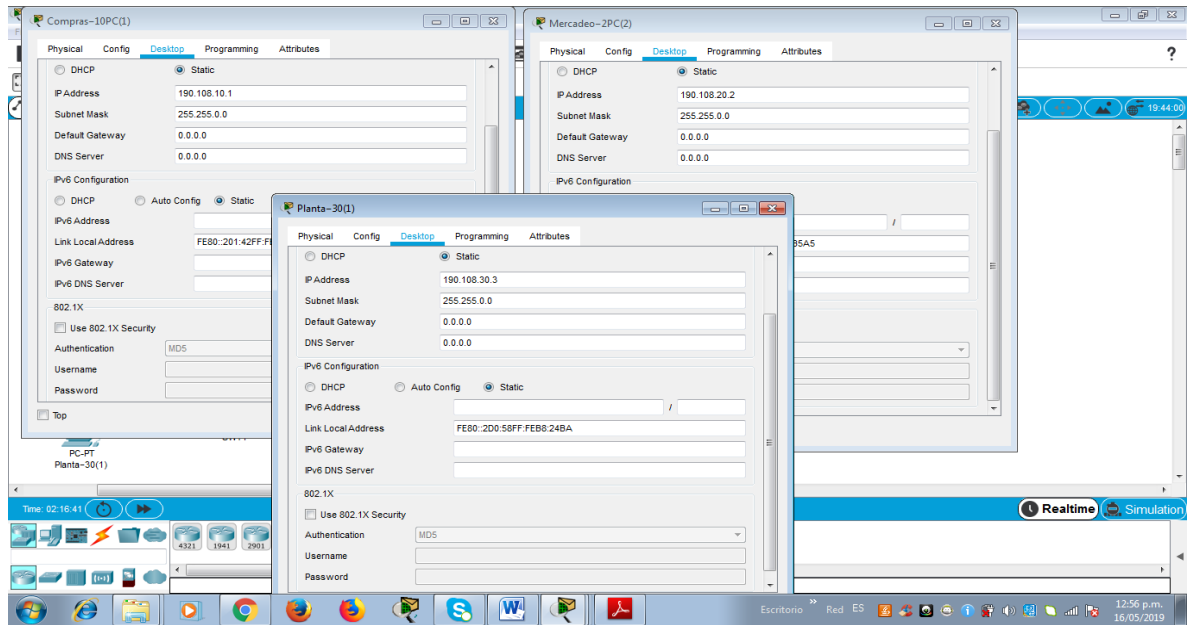
	Interfaz	VLAN	Direcciones IP de los PCs
SWT1	F0/10	VLAN 10	190.108.10.1 / 24
	F0/15	VLAN 20	190.108.20.2 /24
	F0/20	VLAN 30	190.108.30.3 /24
SWT2	F0/10	VLAN 10	190.108.10.4/ 24
	F0/15	VLAN 20	190.108.20.5 /24
	F0/20	VLAN 30	190.108.30.6 /24
SWT3	F0/10	VLAN 10	190.108.10.7 / 24
	F0/15	VLAN 20	190.108.20.8 /24
	F0/20	VLAN 30	190.108.30.9 /24

X = número de cada PC particular

Fuente 55. Universidad Nacional Abierta y a Distancia (UNAD).

DIRECCIONES IP DE LOS PCS DEL SWT1

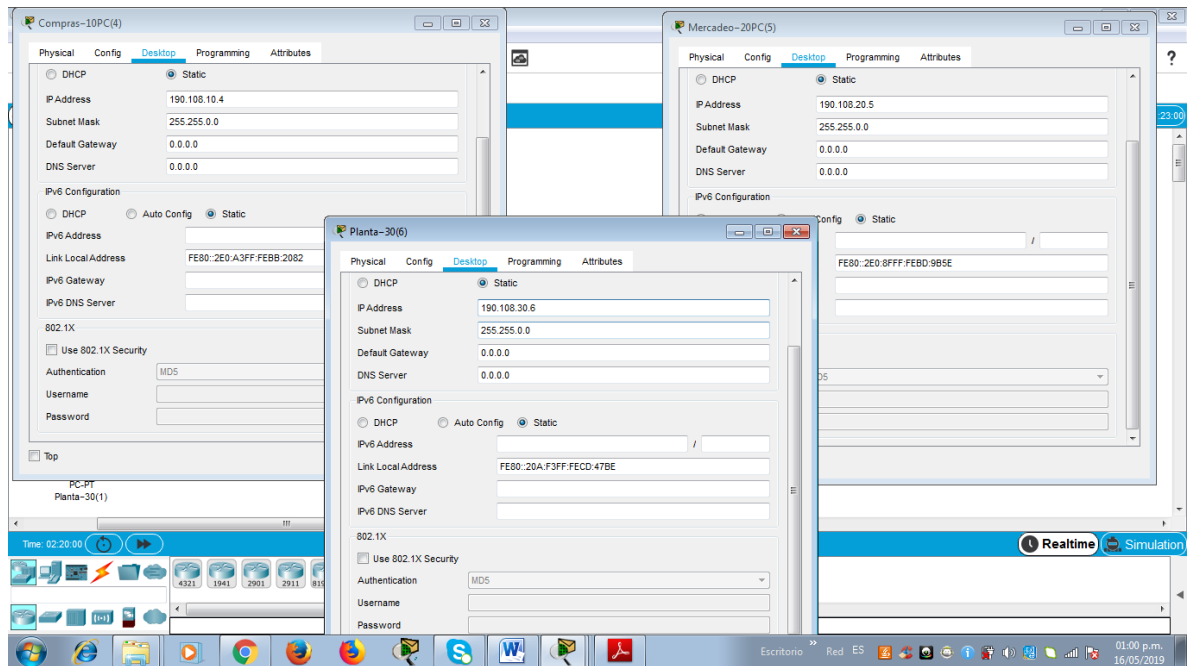
Ilustración 29.Evidencia de direcciones ip de los pcs del SWT1



Fuente 29: El Autor.

DIRECCIONES IP DE LOS PCS DEL SWT2

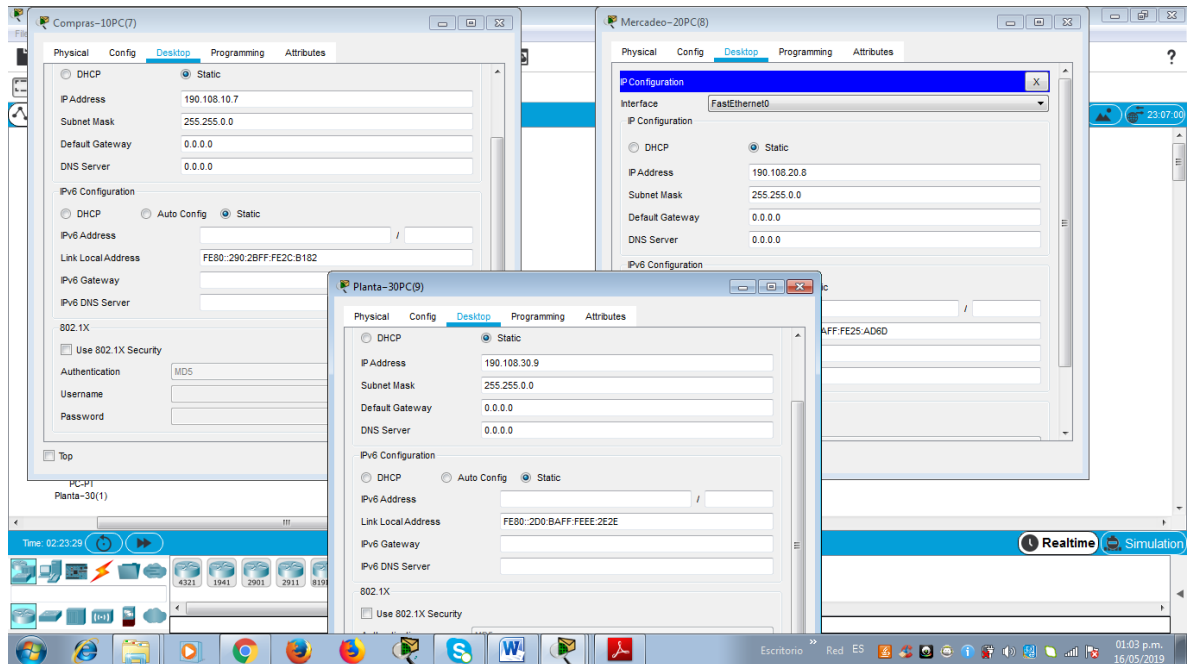
Ilustración 30.Evidencia de direcciones ip de los pcs del SWT2



Fuente 30: El Autor.

DIRECCIONES IP DE LOS PCS DEL SWT3

Ilustración 31. Evidencia direcciones ip de los pcs del SWT3



Fuente 31: El Autor.

5. 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.

Desarrollo:

Con estos comandos se asocia las respectivas interfaces o puertos con la vlan20 y vlan30 en cada switch:

SWITCH 1 SWT1

```
SWT1#conf t
```

```
SWT1(config)#interface f0/15
```

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

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

```
SWT1(config-if)#exit
```

```
SWT1(config)#
```

```
SWT1#conf t
SWT1(config)#interface f0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
SWT1(config-if)#exit
SWT1(config)#
```

SWITCH 2 SWT2

```
SWT2#conf t
SWT2(config)#interface f0/15
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#exit
SWT2(config)#
```

```
SWT2#conf t
SWT2(config)#interface f0/20
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 30
SWT2(config-if)#exit
SWT2(config)#
```

SWITCH 3SWT3

```
SWT3# conf t
SWT3(config)#interface f0/15
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 20
SWT3(config-if)#exit
SWT3(config)#
SWT3# conf t
SWT3(config)#interface f0/20
```



```
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 30
SWT3(config-if)#exit
SWT3(config)#
```

D. Configurar las direcciones IP en los Switches.

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

Tabla 6. direcciones IP en 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

Fuente 56. Universidad Nacional Abierta y a Distancia (UNAD).

Desarrollo:

Comandos para asignación de direccion IP al SVI (Switch Virtual Interface) de cada Switch según la tabla dada y se activaran las interfaces los comandos son:

SWITCH 1 SWT1

```
SWT1# conf t
SWT1(config)#interface vlan 99
SWT1(config-if)# ip address 190.108.99.1 255.255.255.0
SWT1(config-if)# no shutdown
```

SWITCH 2 SWT2

```
SWT2# conf t
SWT2(config)#interface vlan 99
SWT2(config-if)# ip address 190.108.99.2 255.255.255.0
SWT2(config-if)# no shutdown
```

SWITCH 3 SWT3

SWT3# conf t

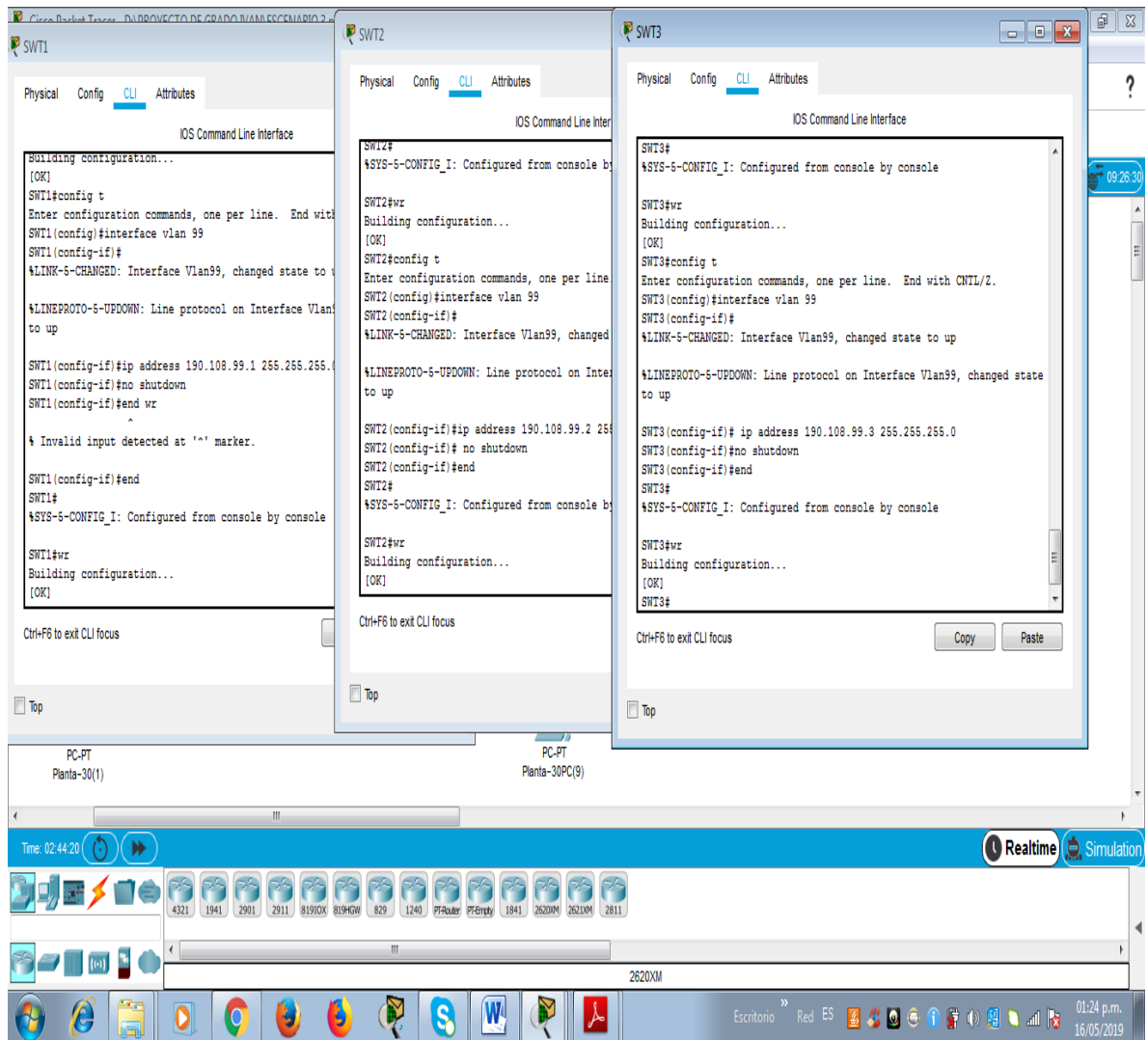
SWT3(config)#interface vlan 99

SWT3(config-if)# ip address 190.108.99.3 255.255.255.0

SWT3(config-if)# no shutdown

Finamente con el comando wr se guardan las configuraciones hechas en los Switches para que estas configuraciones permanezcan aun cuando los apaguen y los vuelvan a encender.

Ilustración 32.Evidencia de comando wr



Fuente 32: El Autor.

E. Verificar la conectividad Extremo a Extremo

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

Desarrollo:

Pings desde la PC Compras-10PC(1)

ping 190.108.20.2 fallo

ping 190.108.30.3 fallo

ping 190.108.10.4 exitoso

ping 190.108.20.5 fallo

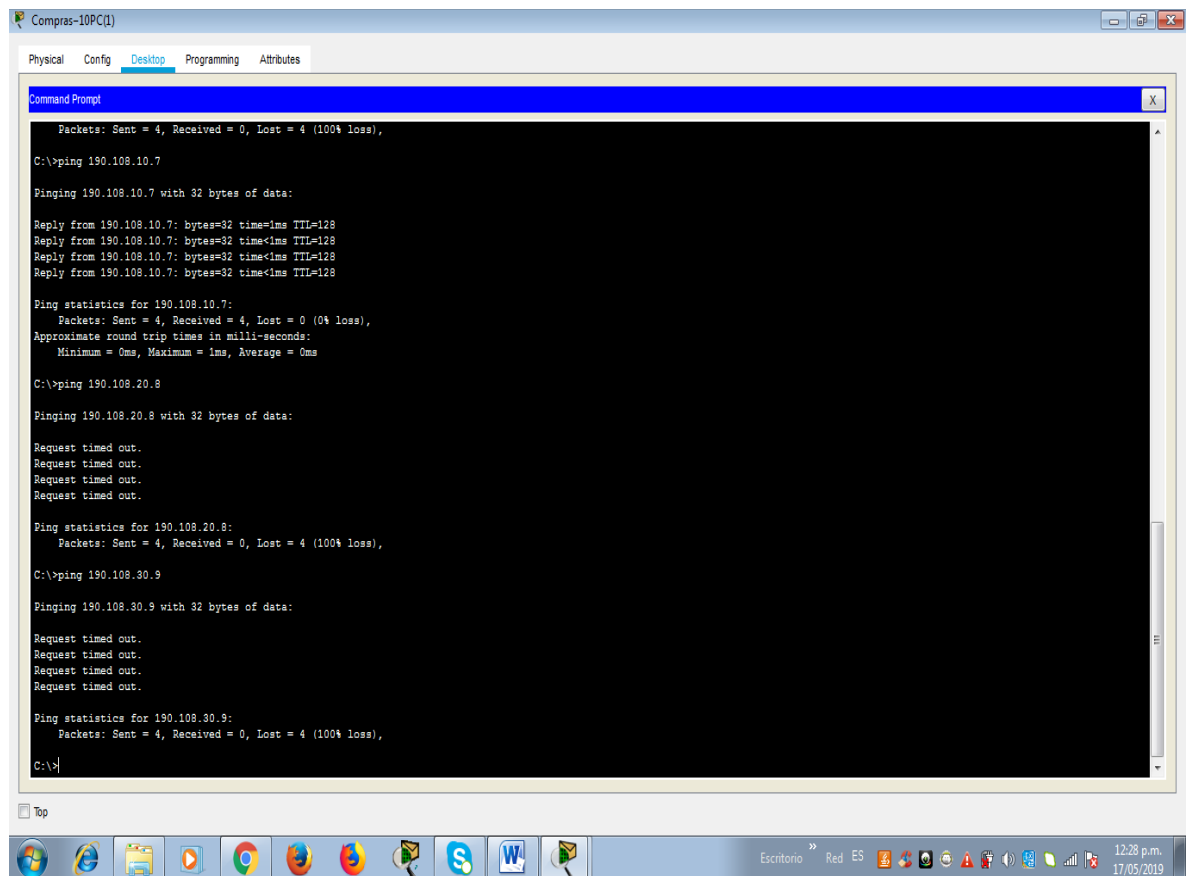
ping 190.108.30.6 fallo

ping 190.108.10.7 exitoso

ping 190.108.20.8 fallo

ping 190.108.30.9 fallo

Ilustración 33.Evidencia de pings



Fuente 33: El Autor.

Pings desde la PC Mercadeo-20PC(2)

ping 190.108.10.1 fallo

ping 190.108.30.3 fallo

ping 190.108.10.4 fallo

ping 190.108.20.5 exitoso

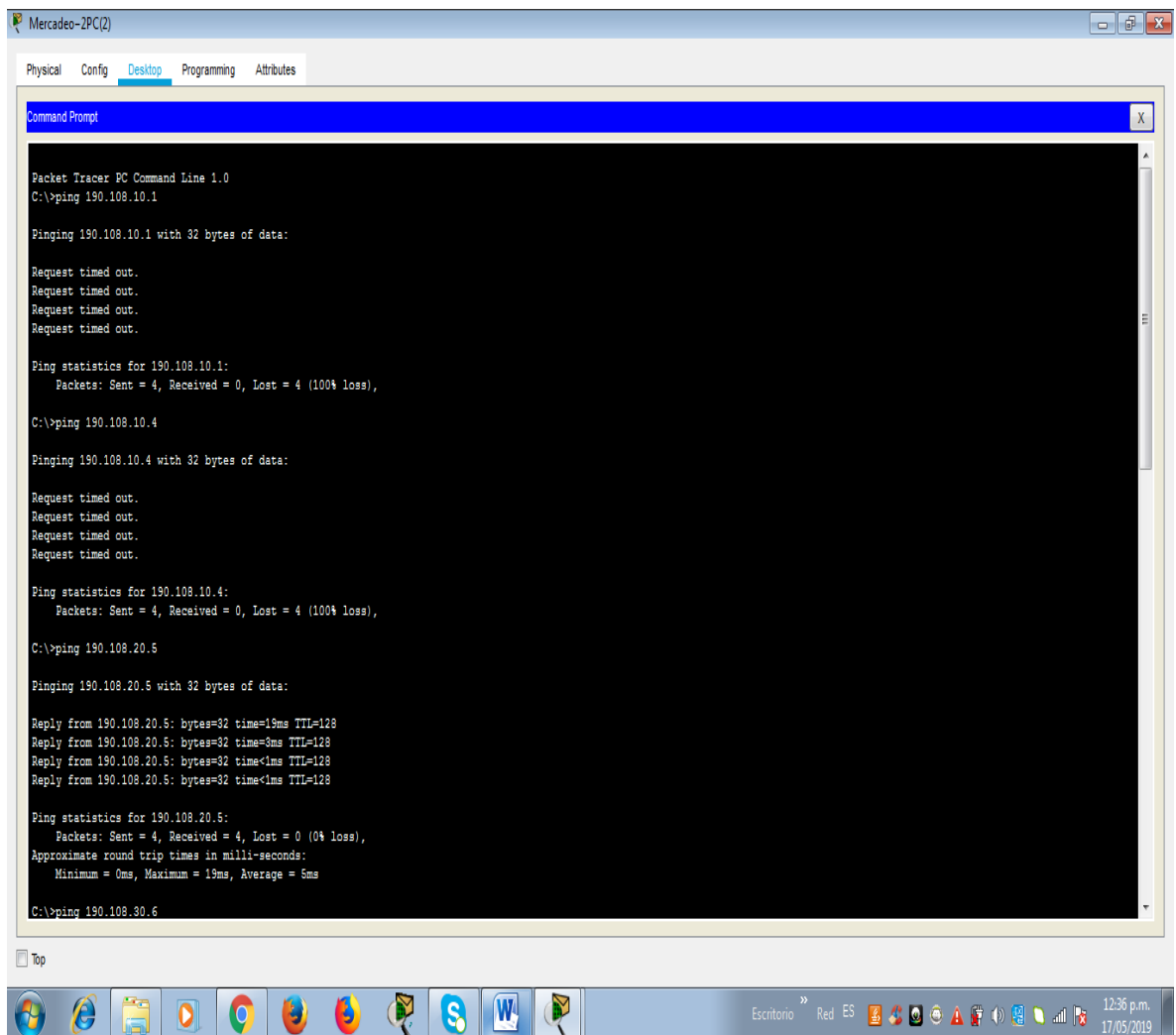
ping 190.108.30.6 fallo

ping 190.108.10.7 fallo

ping 190.108.20.8 exitoso

ping 190.108.30.9 fallo

Ilustración 34.Evidencia de pings



The screenshot shows a Packet Tracer PC Command Line window for a device named 'Mercadeo-20PC(2)'. The window displays the results of several ping commands. The first three pings (to 190.108.10.1, 190.108.10.4, and 190.108.30.6) all fail with 'Request timed out.' and 'Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)'. The fourth ping (to 190.108.20.5) is successful, showing 'Reply from 190.108.20.5: bytes=32 time=19ms TTL=128' and 'Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)'. The fifth ping (to 190.108.30.6) fails with 'Request timed out.' and 'Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)'. The window also shows the approximate round trip times in milliseconds for the successful ping to 190.108.20.5: Minimum = 0ms, Maximum = 19ms, Average = 5ms.

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.1

Pinging 190.108.10.1 with 32 bytes of data:

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

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

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

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.5

Pinging 190.108.20.5 with 32 bytes of data:

Reply from 190.108.20.5: bytes=32 time=19ms TTL=128
Reply from 190.108.20.5: bytes=32 time=3ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 5ms

C:\>ping 190.108.30.6

Pinging 190.108.30.6 with 32 bytes of data:

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

Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fuente 34: El Autor.

Pings desde la PC Planta-30PC(3)

ping 190.108.10.1 fallo

ping 190.108.20.2 fallo

ping 190.108.10.4 fallo

ping 190.108.20.5 fallo

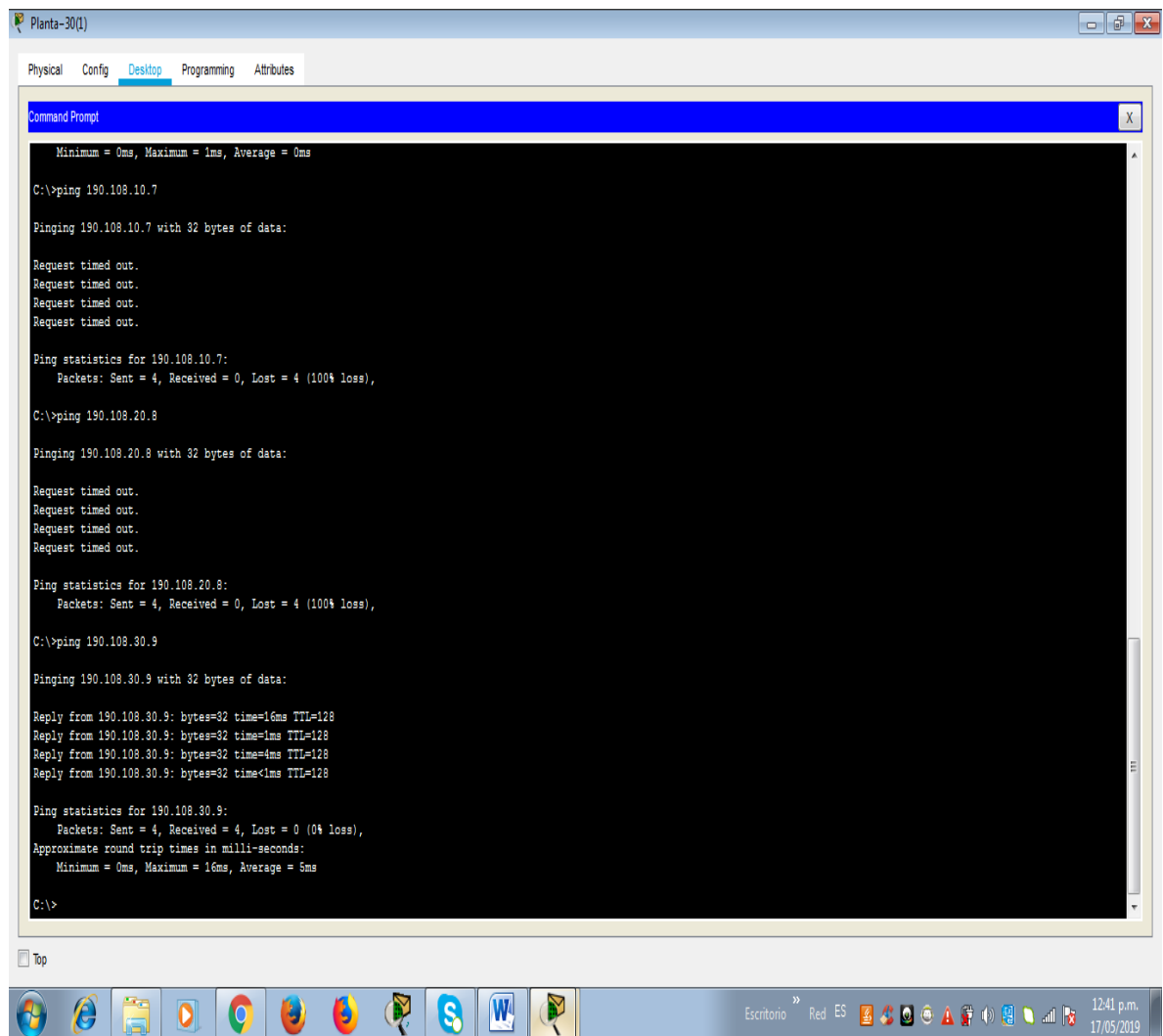
ping 190.108.30.6 exitoso

ping 190.108.10.7 fallo

ping 190.108.20.8 fallo

ping 190.108.30.9 exitoso

Ilustración 35.Evidencia de pings



```
Planta-30(1)
Physical Config Desktop Programming Attributes

Command Prompt
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

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

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>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),

C:\>ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

Reply from 190.108.30.9: bytes=32 time=16ms TTL=128
Reply from 190.108.30.9: bytes=32 time=1ms TTL=128
Reply from 190.108.30.9: bytes=32 time=4ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 5ms

C:\>
```

Fuente 35: El Autor.

Pings desde la PC Compras-10PC(4)

ping 190.108.10.1 exitoso

ping 190.108.20.2 fallo

ping 190.108.30.3 fallo

ping 190.108.20.5 fallo

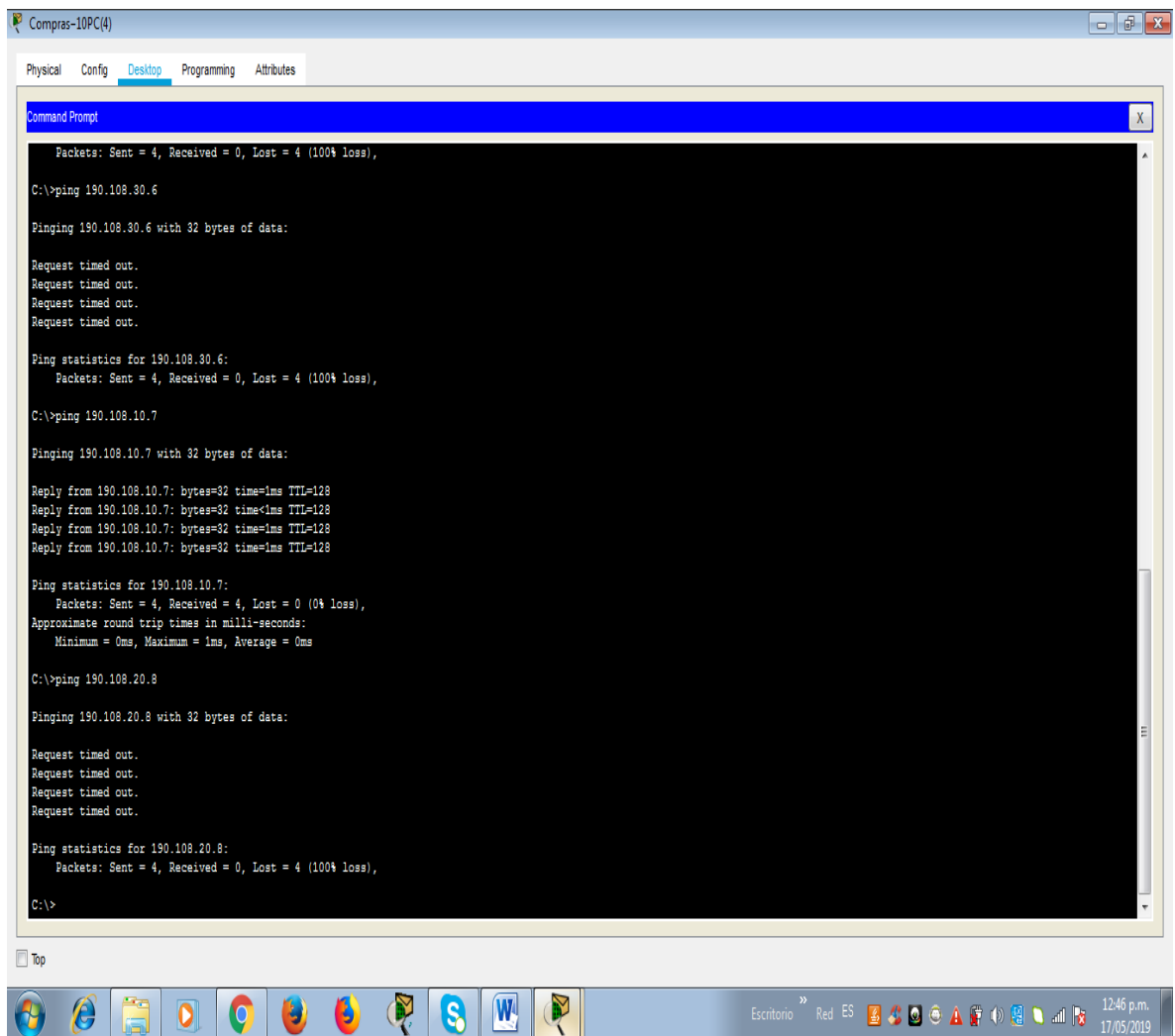
ping 190.108.30.6 fallo

ping 190.108.10.7 exitoso

ping 190.108.20.8 fallo

ping 190.108.30.9 fallo

Ilustración 36.Evidencia de pings



```
Compras-10PC(4)
Physical Config Desktop Programming Attributes

Command Prompt

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.6

Pinging 190.108.30.6 with 32 bytes of data:

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

Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

Reply from 190.108.10.7: bytes=32 time=1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>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),

C:\>
```

Fuente 36: El Autor.

Pings desde la PC Mercadeo-20PC(5)

ping 190.108.10.1 fallo

ping 190.108.20.2 exitoso

ping 190.108.30.3 fallo

ping 190.108.10.4 fallo

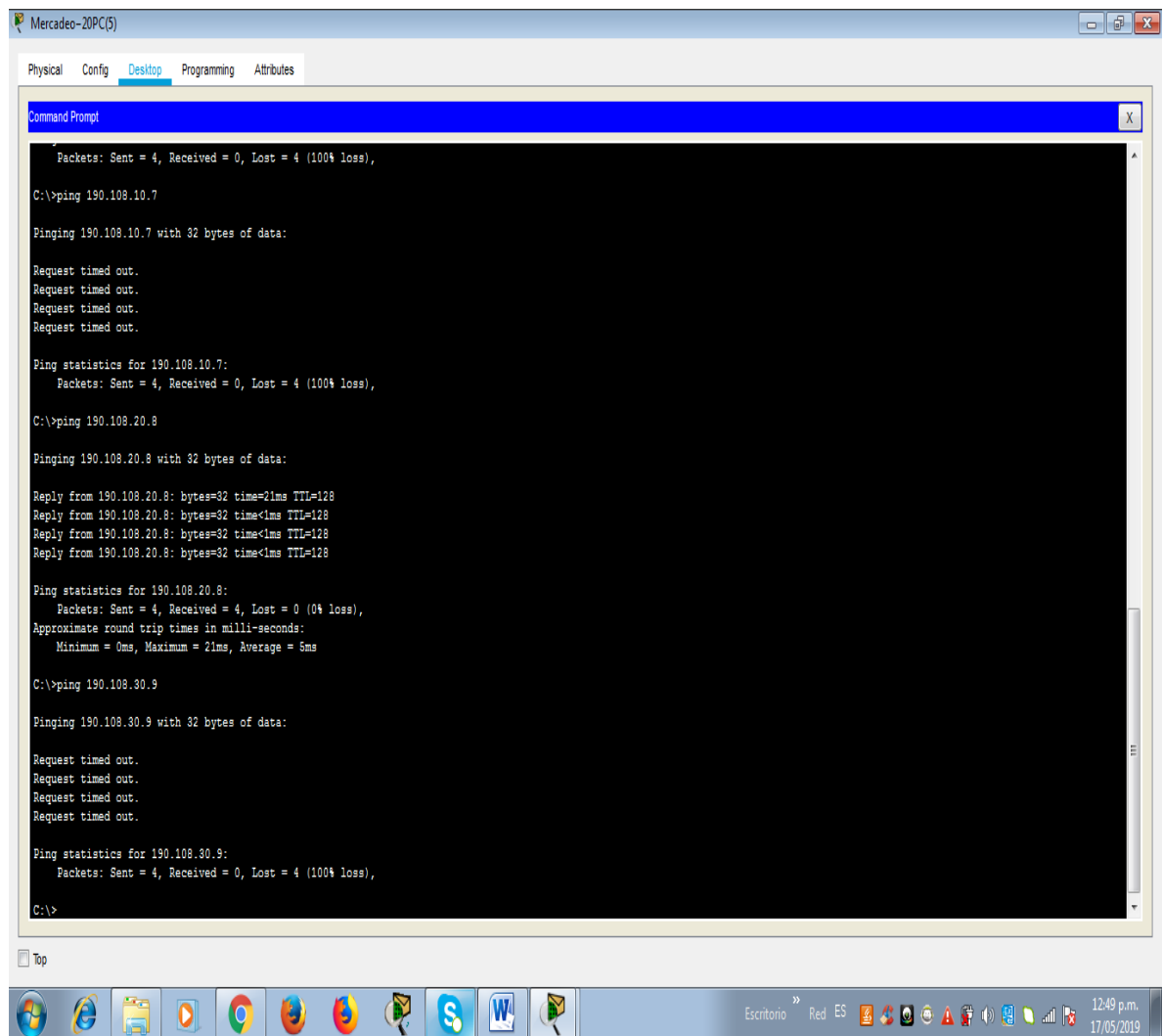
ping 190.108.30.6 fallo

ping 190.108.10.7 fallo

ping 190.108.20.8 exitoso

ping 190.108.30.9 fallo

Ilustración 37.Evidencia de pings



```

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

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

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.8

Pinging 190.108.20.8 with 32 bytes of data:

Reply from 190.108.20.8: bytes=32 time=21ms TTL=128
Reply from 190.108.20.8: bytes=32 time<1ms TTL=128
Reply from 190.108.20.8: bytes=32 time<1ms TTL=128
Reply from 190.108.20.8: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 21ms, Average = 5ms

C:\>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),

C:\>
```

Fuente 37: El Autor.

Pings desde la PC Planta-30PC(6)

ping 190.108.10.1 fallo

ping 190.108.20.2 fallo

ping 190.108.30.3 exitoso

ping 190.108.10.4 fallo

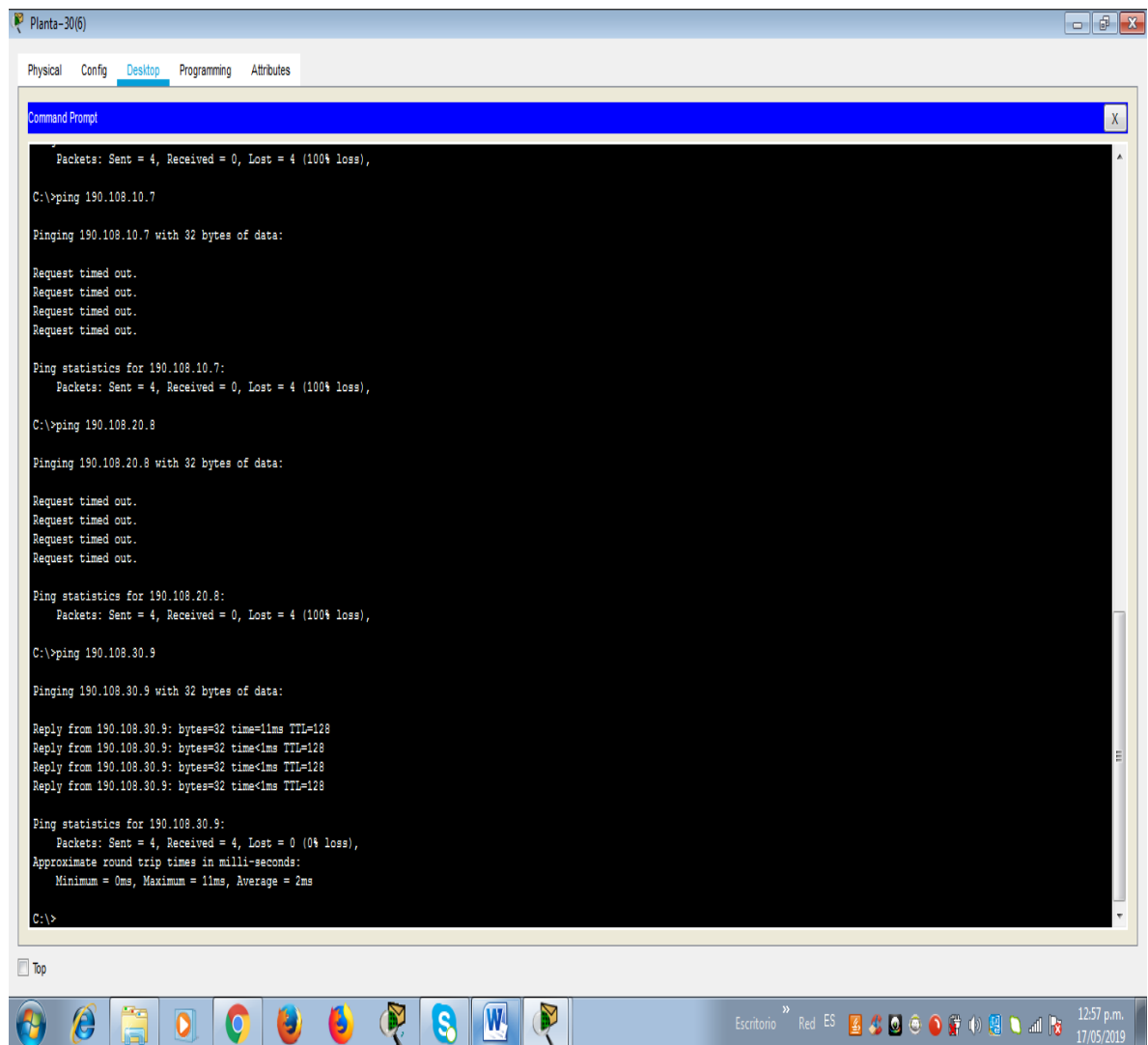
ping 190.108.20.5 fallo

ping 190.108.10.7 fallo

ping 190.108.20.8 fallo

ping 190.108.30.9 exitoso

Ilustración 38.Evidencia de pings



The screenshot shows a Windows desktop environment. At the top, a window titled 'Planta-30(6)' is open, displaying tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, showing a 'Command Prompt' window. The Command Prompt displays the following text:

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\>ping 190.108.10.7  
Pinging 190.108.10.7 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Ping statistics for 190.108.10.7:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\>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),  
C:\>ping 190.108.30.9  
Pinging 190.108.30.9 with 32 bytes of data:  
Reply from 190.108.30.9: bytes=32 time=11ms TTL=128  
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128  
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128  
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128  
Ping statistics for 190.108.30.9:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 11ms, Average = 2ms  
C:\>
```

The desktop taskbar at the bottom shows various application icons, including Internet Explorer, Google Chrome, and Microsoft Word. The system tray on the right indicates the time as 12:57 p.m. on 17/05/2019.

Fuente 38: El Autor.

Pings desde la PC Compras-10PC(7)

ping 190.108.10.1 exitoso

ping 190.108.20.2 fallo

ping 190.108.30.3 fallo

ping 190.108.10.4 exitoso

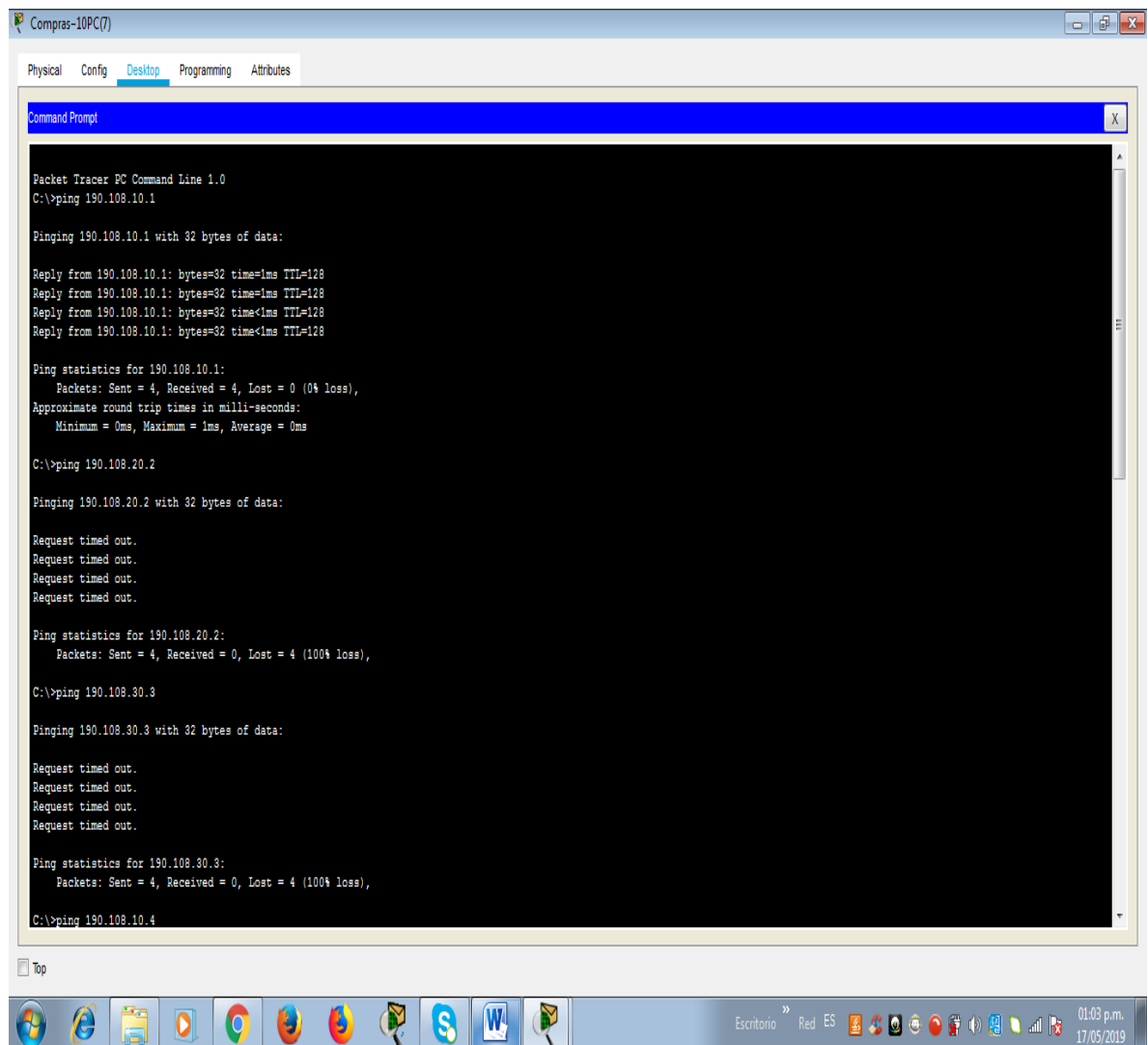
ping 190.108.20.5 fallo

ping 190.108.30.6 fallo

ping 190.108.20.8 fallo

ping 190.108.30.9 fallo

Ilustración 39.Evidencia de pings



Fuente 39: El Autor.

Pings desde la PC Mercadeo-20PC(8)

ping 190.108.10.1 falla

ping 190.108.20.2 exitoso

ping 190.108.30.3 fallo

ping 190.108.10.4 fallo

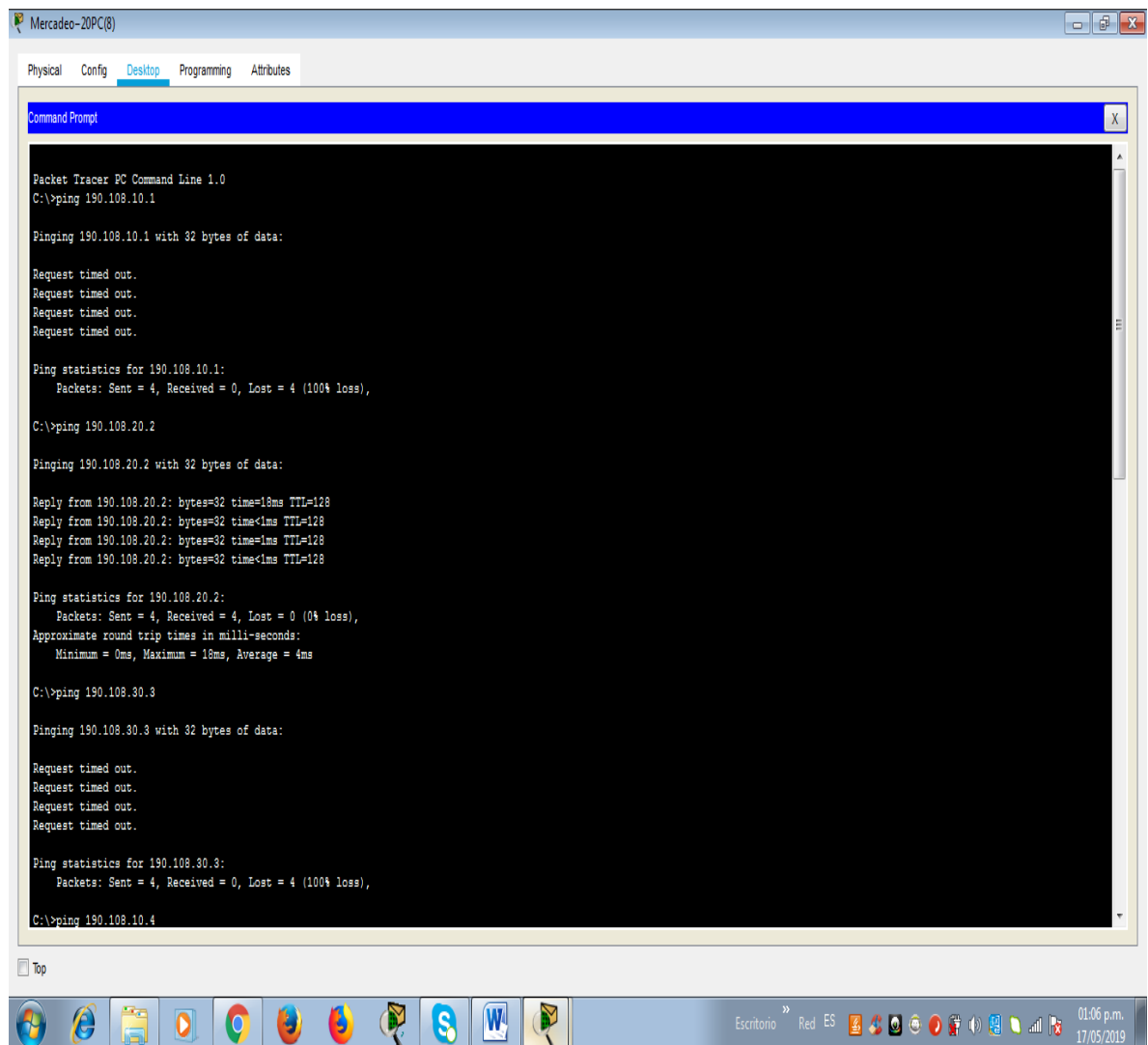
ping 190.108.20.5 exitoso

ping 190.108.30.6 fallo

ping 190.108.10.7 fallo

ping 190.108.30.9 fallo

Ilustración 40.Evidencia de pings



The screenshot shows a Packet Tracer PC Command Line window titled 'Mercadeo-20PC(8)'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. Inside the window is a 'Command Prompt' window with the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.1

Pinging 190.108.10.1 with 32 bytes of data:

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

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:

Reply from 190.108.20.2: bytes=32 time=18ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

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

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.4
```

The taskbar at the bottom shows various application icons and the system clock indicating 01:06 p.m. on 17/05/2019.

Fuente 40: El Autor.

Pings desde la PC Planta-30PC(9)

ping 190.108.10.1 fallo

ping 190.108.20.2 fallo

ping 190.108.30.3 exitoso

ping 190.108.10.4 fallo

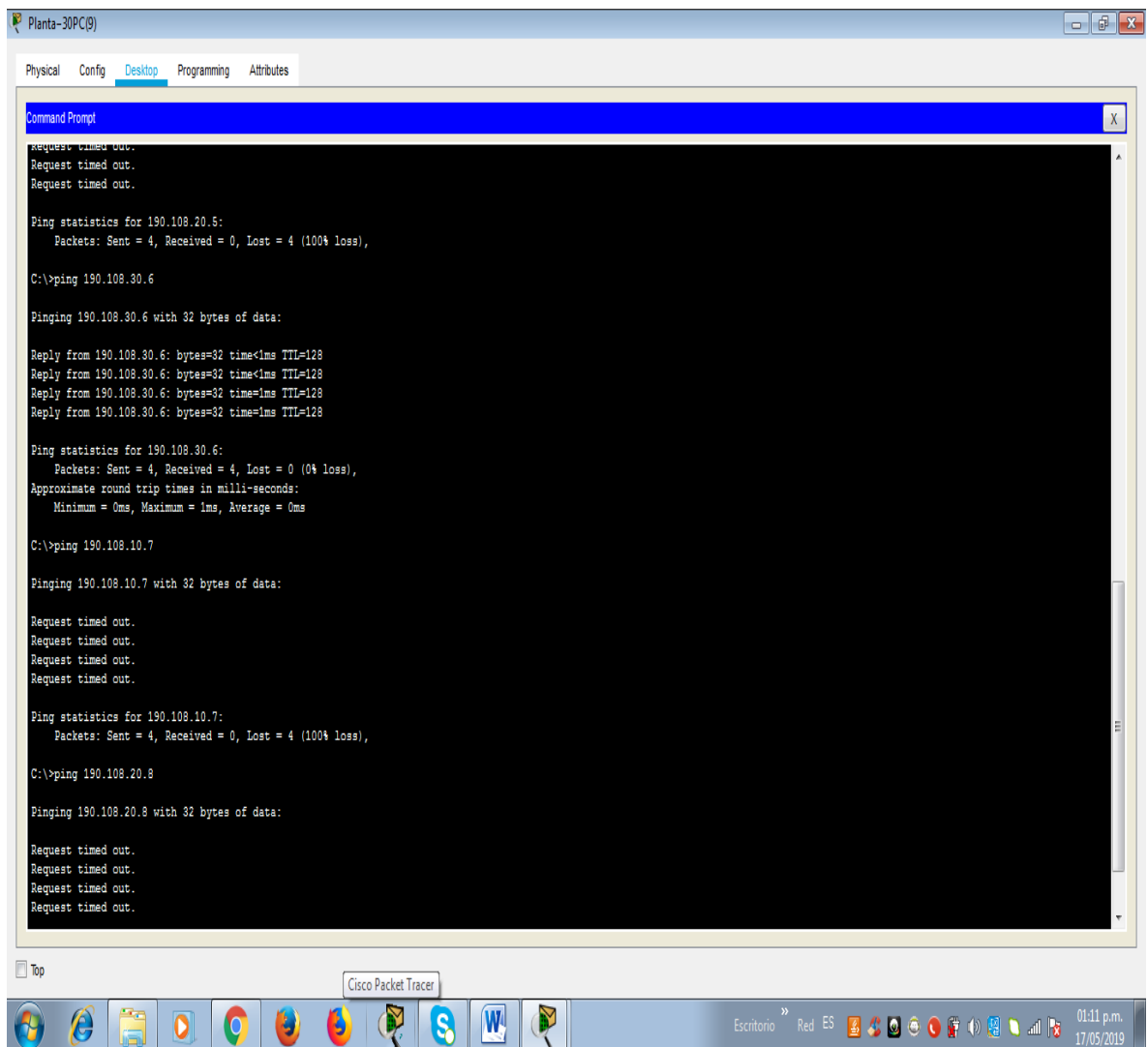
ping 190.108.20.5 fallo

ping 190.108.30.6 exitoso

ping 190.108.10.7 fallo

ping 190.108.20.8 fallo

Ilustración 41.Evidencia de pings

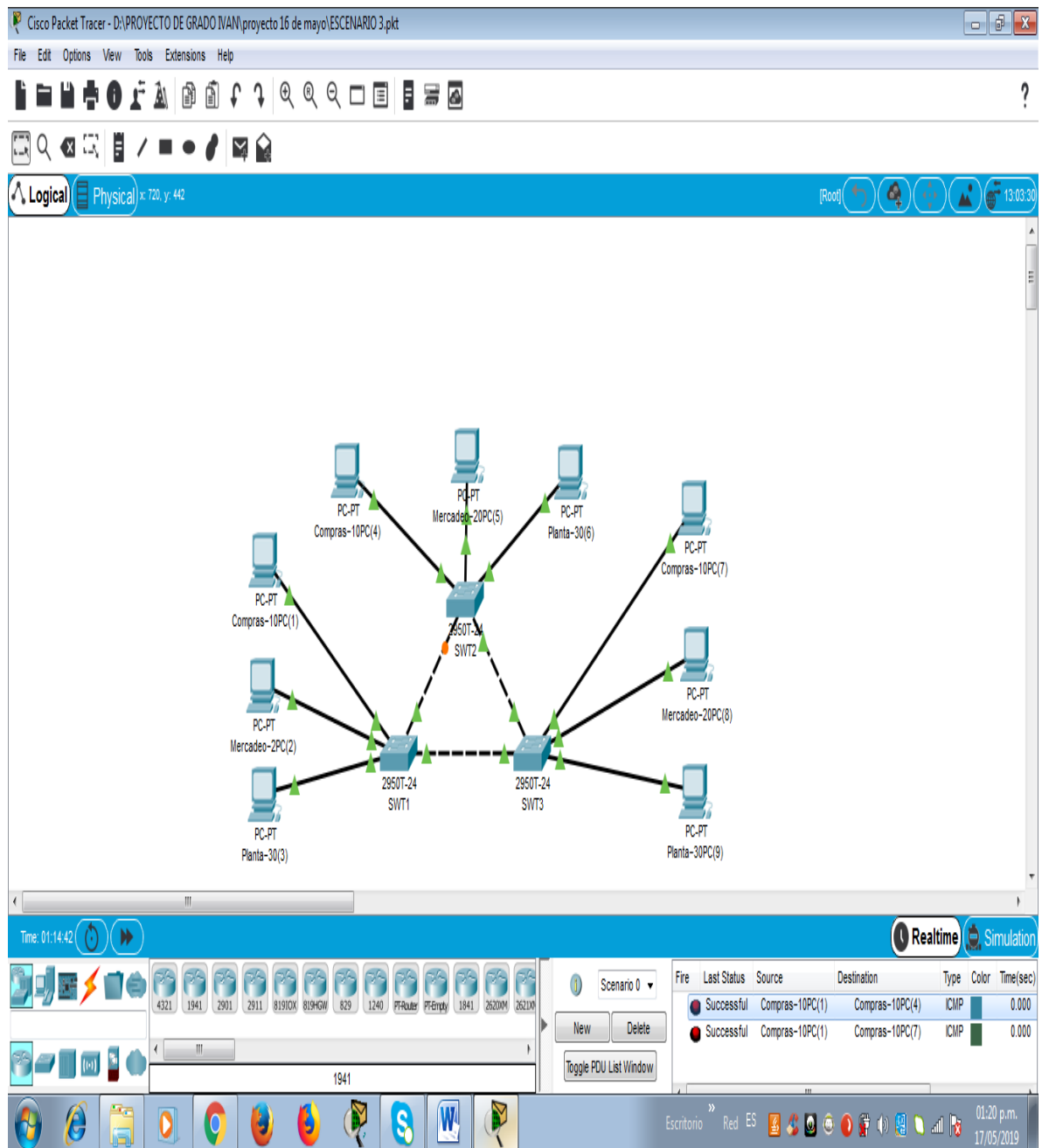


Fuente 41: El Autor.

Solo 6 pings tuvieron éxito ya que existen tres vlans diferentes la 10,20 y 30 nueve computadores y tres están conectados a la vlan 10 , tres a la vlan 20 y tres a la vlan 30 por lo que al hacer ping solo tuvieron éxito los que están conectados a la misma vlan y fallaron todos los demás pings .

Ejemplo de pings exitosos entre la vlan 10 de compras:

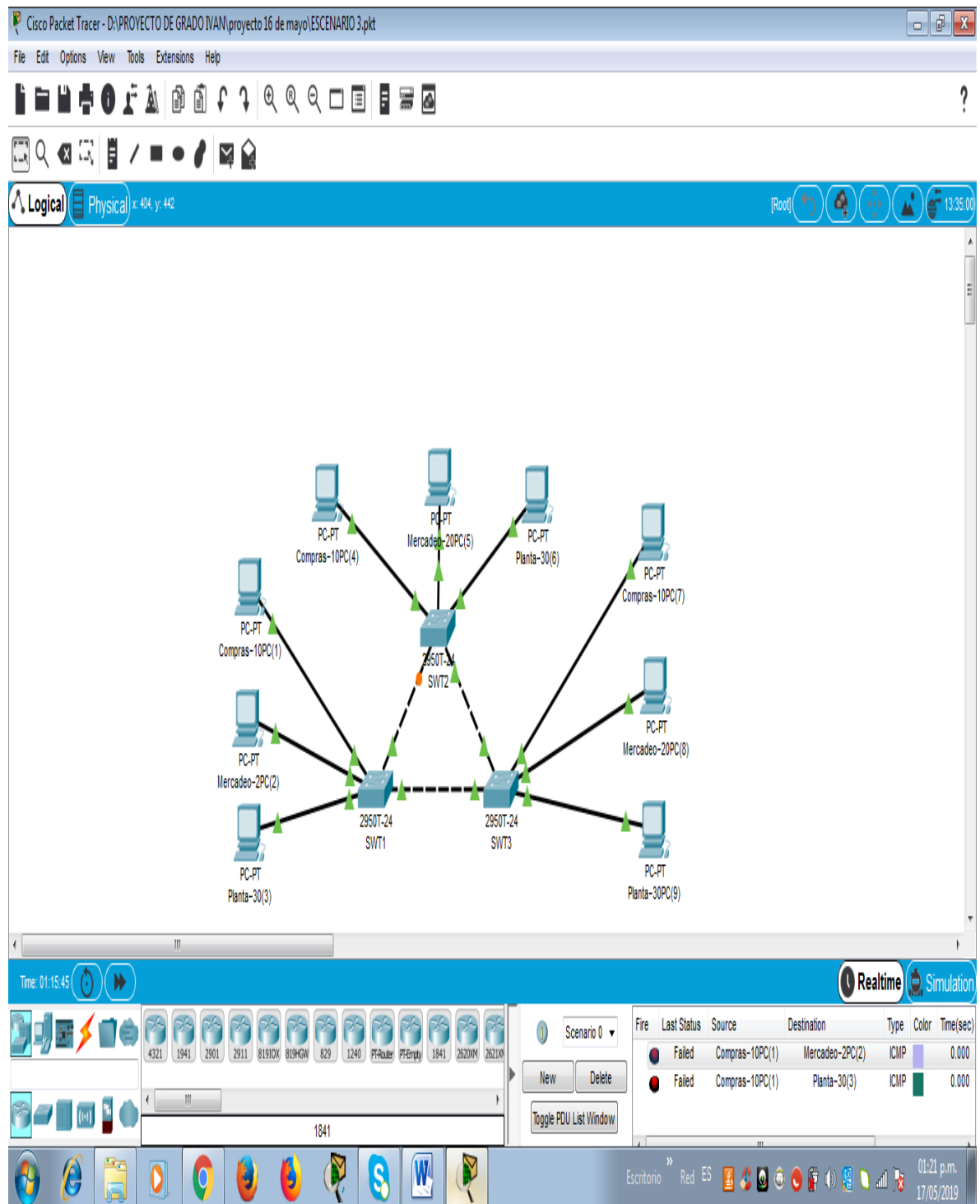
Ilustración 42.Evidencia de pings exitosos



Fuente 42: El Autor.

Ejemplo de ping fallido entre la vlan 10 de compras y la vlan 20 y 30:

Ilustración 43.Evidencia de pings fallidos



Fuente 43: El Autor.

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

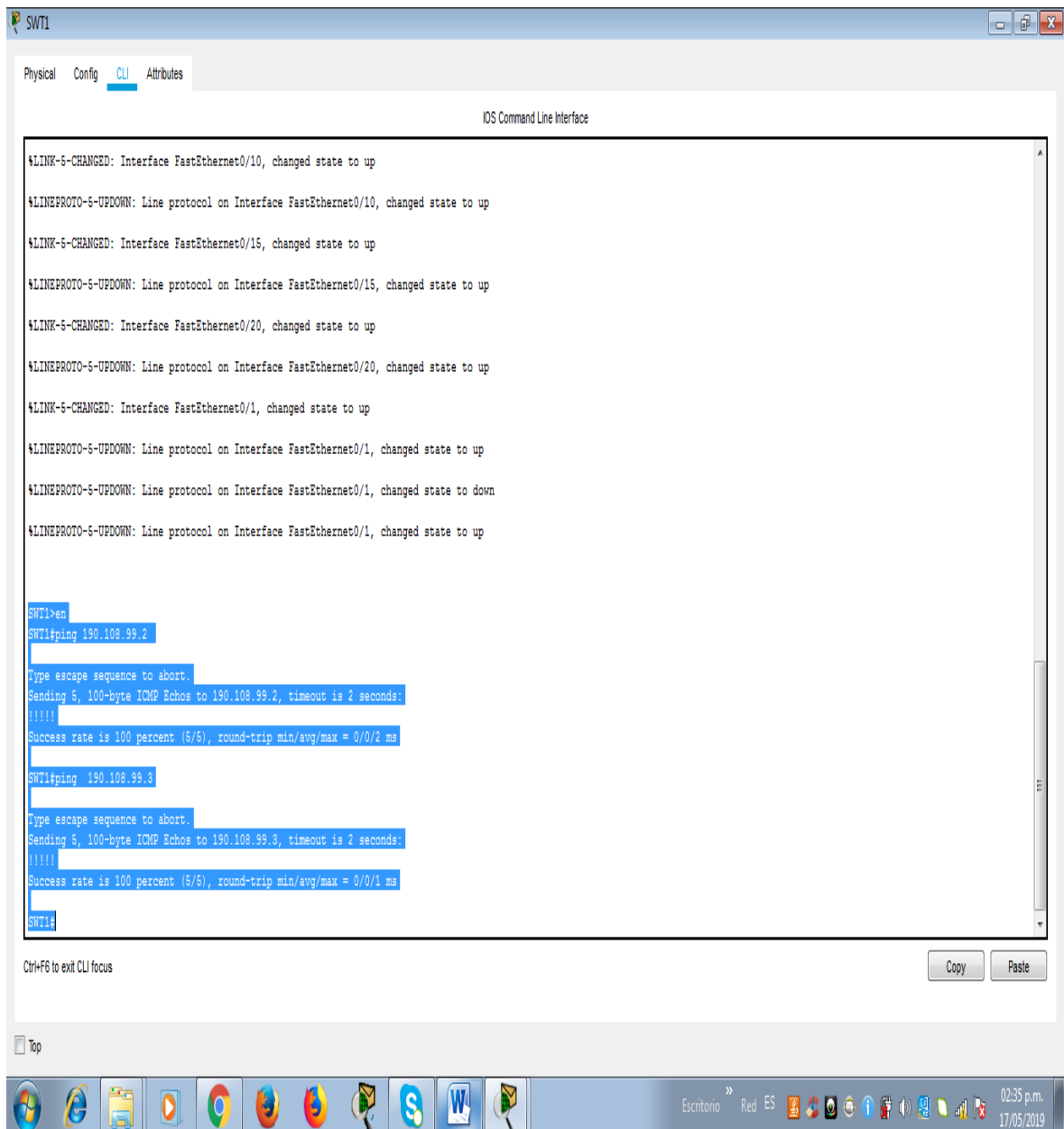
Desarrollo:

Ping desde el SWT1

ping 190.108.99.2

ping 190.108.99.3

Ilustración 44.Evidencia Ping desde el SWT1



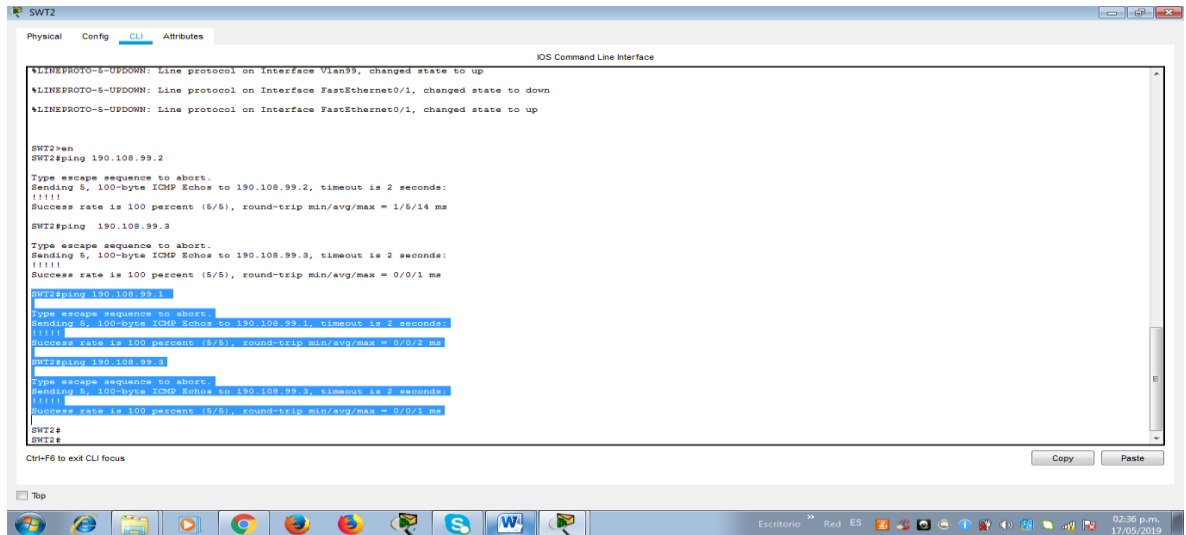
Fuente 44: El Autor.

Ping desde el SWT2

ping 190.108.99.1

ping 190.108.99.3

Ilustración 45.Evidencia de Ping desde el SWT2



```
SWT2
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

SWT2>en
SWT2#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 = 1/5/14 ms

SWT2#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

SWT2#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 = 0/0/1 ms

SWT2#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

SWT2#
SWT2#
```

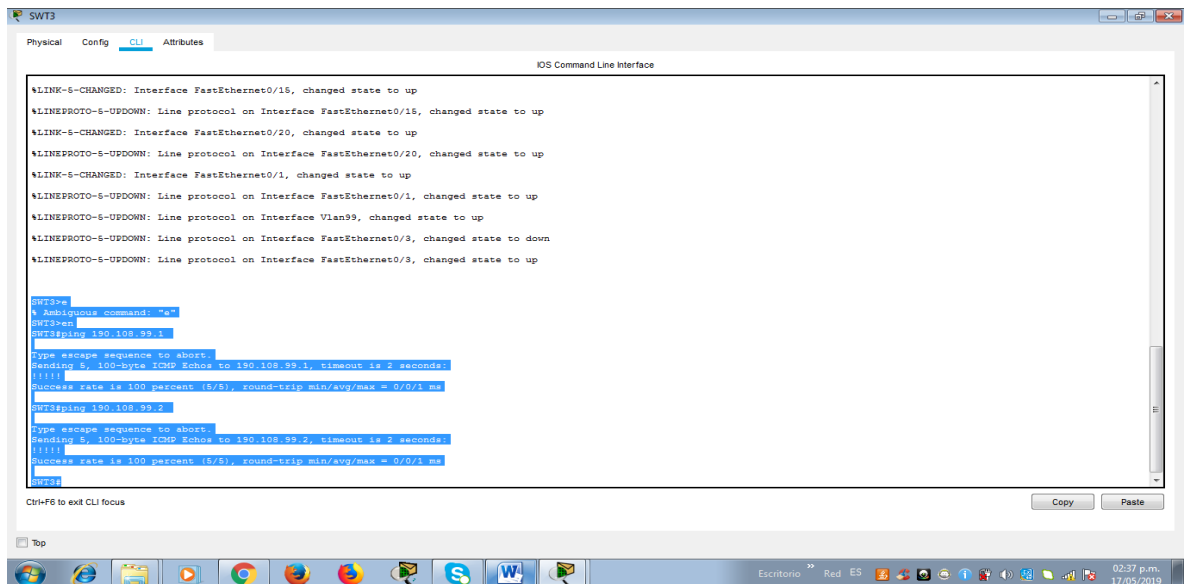
Fuente 45: El Autor.

Ping desde el SWT3

ping 190.108.99.1

ping 190.108.99.2

Ilustración 46.Evidencia de Ping desde el SWT3



```
SWT3
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

SWT3>en
SWT3>
SWT3>en
SWT3#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 = 0/0/1 ms

SWT3#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

SWT3#
```

Fuente 46: El Autor.

Son exitosos todos los pings ejecutados desde un Switch a los demás, debido a que están todos comunicados mediante la vlan 99 Admon (99) y poseen su respectiva dirección ip adecuada, y la configuración de los Switches está en modo Trunking Protocol, estático, permanente y dinámico.

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

Ping desde el SWT1 a todas las pc

ping 190.108.10.1

ping 190.108.20.2

ping 190.108.30.3

ping 190.108.10.4

ping 190.108.20.5

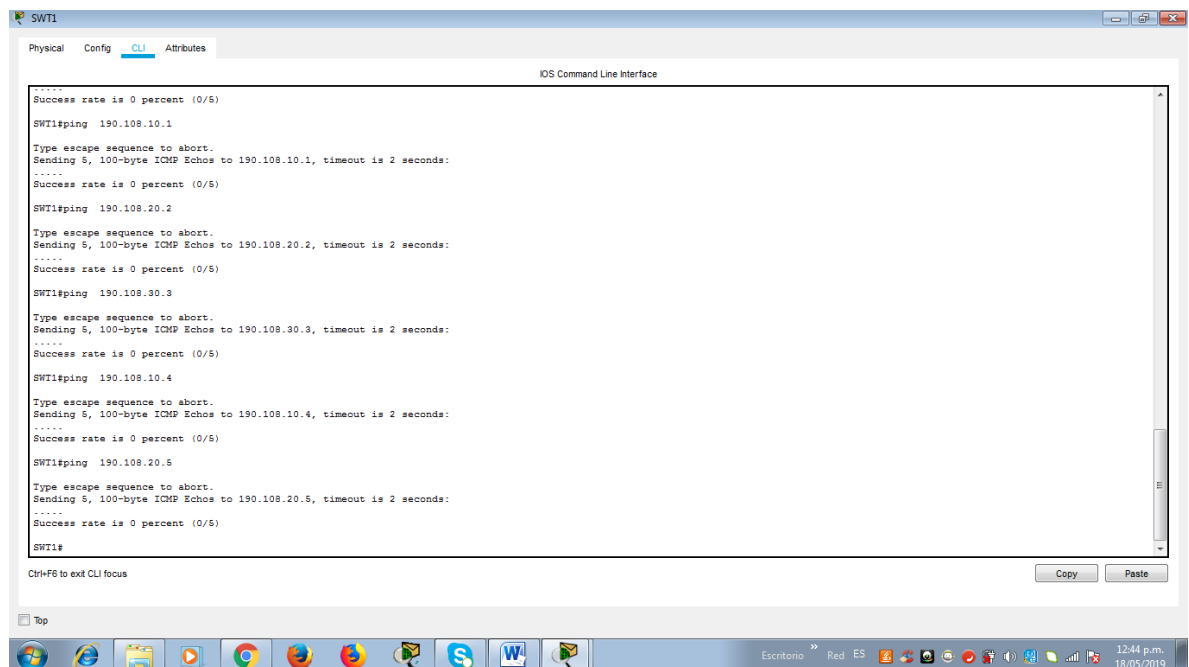
ping 190.108.30.6

ping 190.108.10.7

ping 190.108.20.8

ping 190.108.30.9

Ilustración 47. Evidencia de Ping desde el SWT1 a todas las pc



Fuente 47: El Autor.

Ping desde el SWT2 a todos los pcs

ping 190.108.10.1

ping 190.108.20.2

ping 190.108.30.3

ping 190.108.10.4

ping 190.108.20.5

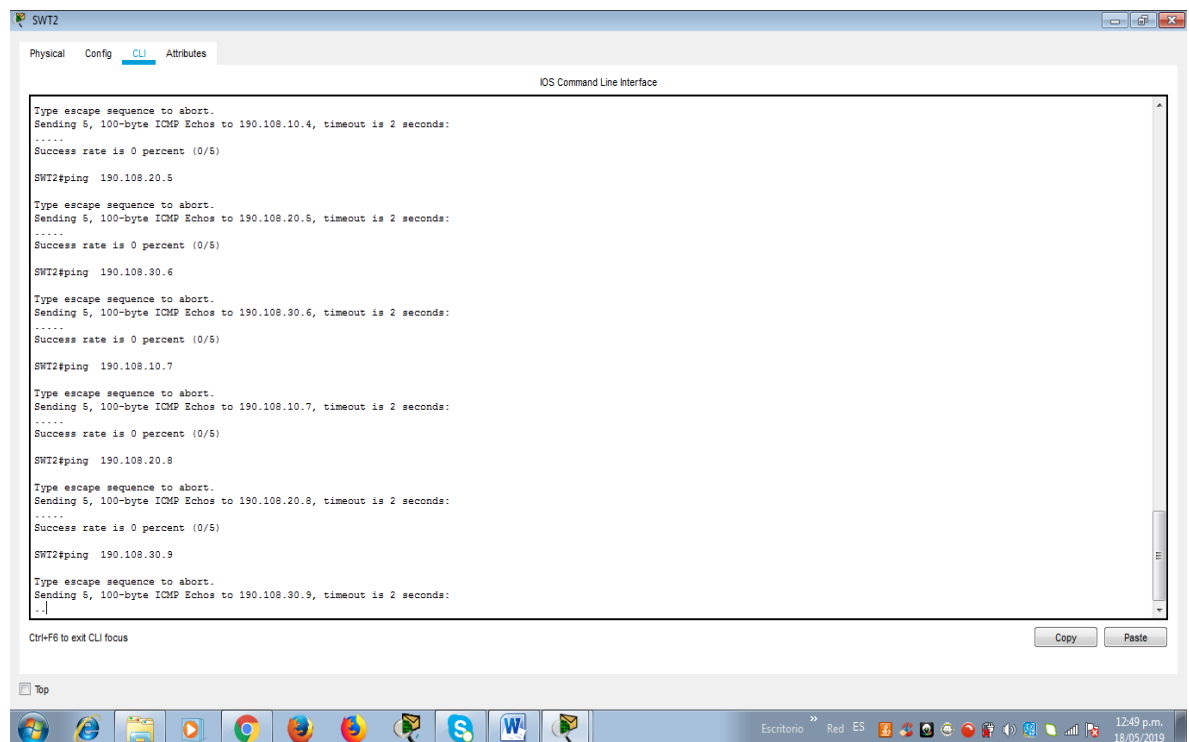
ping 190.108.30.6

ping 190.108.10.7

ping 190.108.20.8

ping 190.108.30.9

Ilustración 48.Evidencia de Ping desde el SWT2 a todos los pcs



Fuente 48: El Autor.

Ping desde el SWT3 a todas las pcs

ping 190.108.10.1

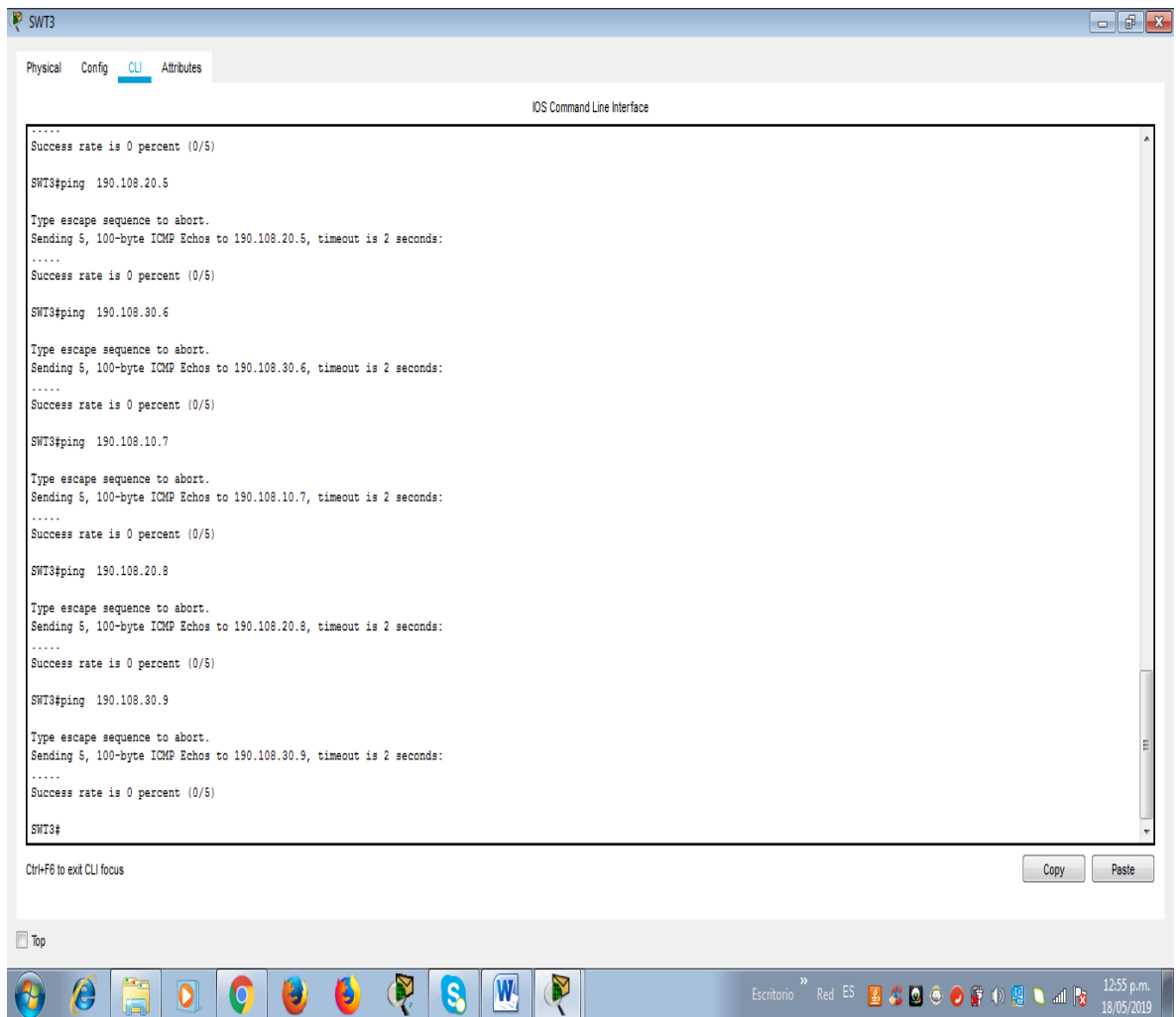
ping 190.108.20.2

ping 190.108.30.3

ping 190.108.10.4

ping 190.108.20.5
ping 190.108.30.6
ping 190.108.10.7
ping 190.108.20.8
ping 190.108.30.9

Ilustración 49.Evidencia de Ping desde el SWT3 a todas las pcs



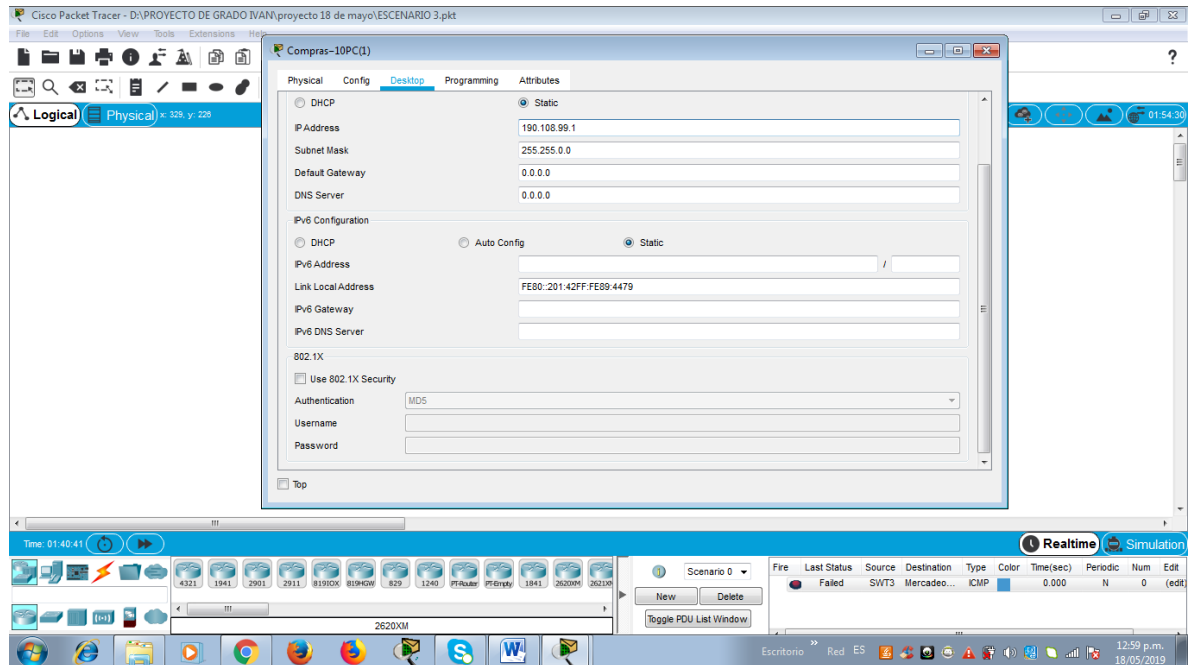
```
SWT3
Physical Config CLI Attributes
IOS Command Line Interface
.....
Success rate is 0 percent (0/5)
SWT3#ping 190.108.20.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SWT3#ping 190.108.30.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SWT3#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)
SWT3#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)
SWT3#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)
SWT3#
```

Fuente 49: El Autor.

Ningún ping tuvo éxito debido a que se encuentran en vlans diferentes los Switches están en la están en la vlan 99 y los pc están en la vlan 10,20 y 30 respectivamente por eso no hay comunicación.

Como ejemplo se puede mostrar que si se cambia cualquier pc a la vlan 99 el ping tendrá éxito:

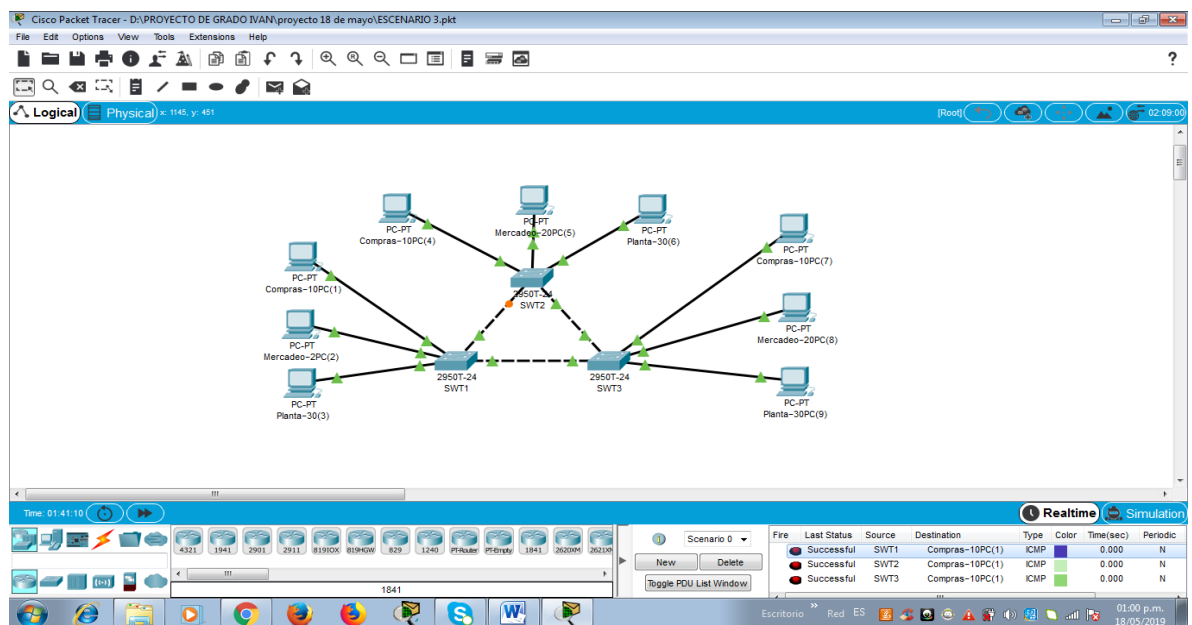
Ilustración 50.Evidencia de ping que tendrá éxito



Fuente 50: El Autor.

Pings correctos hacia el pc 1 desde todos los Switches

Ilustración 51.Evidencia de Pings correctos



Fuente 51: El Autor.

CONCLUSIONES

Con el desarrollo de la presente actividad se puede demostrar los conocimientos que se aprenden sobre CCNP R&S route y CCNP R&S switch, logrando resolver tres ejercicios propuestos sobre redes los cuales estaban diseñados para demostrar los conocimientos adquiridos en las construcciones de redes y su correcta implementación.

De tal forma se plasmo esos conocimientos dando a conocer la programación adecuando tanto de los routers como de los switches mediante los comandos indicados para resolverlos escenarios y enfocado en resolver los ejercicios de tal manera que cumplieran con los requerimientos solicitados.

Finalmente se evidencio con algunos comandos como comandos ping, traceroute, show ip route, entre otros que permiten evidenciar las configuraciones realizadas y observar si hay o no hay comunicación entre los dispositivos, estos conocimientos son fundamentales para aplicarlos en la vida profesional y construir redes que tengan escalabilidad, sean rápidas, de bajo costo y alta seguridad para evitar robos de información confidenciales de empresas.

Referencias Bibliográficas

FROOM, R., Frahim, E. CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019 Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

FROOM, R., Frahim, E. CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

FROOM, R., Frahim, E. CISCO Press (Ed). Campus Network Security. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). First Hop Redundancy Protocols. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). High Availability. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). Network Management. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide

CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>.

FROOM, R., Frahim, E. CISCO Press (Ed). Switching Features and Technologies. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>.

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. [En línea] . (2015). [Citado 11 se mayo del 2019] . Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). [Citado 11 se mayo del 2019] . Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>.

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>.

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Implementing Routing Facilities for Branch Offices and Mobile Workers. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Implementing IPv6 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Manipulating Routing Updates. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.(2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>.

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). OSPF Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015).[Citado 11 se mayo del 2019] . Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>.

TEARE, D., Vachon B., Graziani, R. CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. (2015). [Citado 11 se mayo del 2019]. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>