DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ALEXANDER REYES GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ALEXANDER REYES GONZÁLEZ

Diplomado de opción de grado para optar el
título de INGENIERO ELECTRÓNICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTÁ, 22 de mayo de 2020

DEDICATORIA

A Angélica, mi esposa. Su apoyo constante e incondicional, sus oportunas palabras de motivación y su compañía en cada pequeño logro me mantuvieron en pie durante los momentos difíciles y colmaron de sentido cada momento vivido durante este proceso.

A Eyleen, mi hija y a Sebastián, mi hijo. Mi fuente inagotable de esperanza y de fuerza; por quienes quise convertir esta experiencia en un testimonio de disciplina, esfuerzo, dedicación y fe.

Este título profesional es una meta lograda, pero mi propósito y fin siempre serán ustedes.

LOS AMO.

CONTENIDO

Pág.

LISTA DE IMÁGENES

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ANFITRIÓN (HOST): Un sistema de computadoras en red (véase Estación de trabajo). También un sistema de computadoras que proporciona servicio a usuarios (véase Servidor).

AUTENTICACIÓN**:** En el contexto de seguridad de una red, se trata de un método sistemático para confirmar la identidad de una identidad. Por ejemplo, en una transacción Web segura entre un cliente y un servidor, se usa un procedimiento de autenticación para establecer una prueba de identidad entre los dos nodos.

CLIENTE**:** Un dispositivo de red que requiere recursos de un servidor.

CONMUTADOR **(**SWITCH**):** Un dispositivo de red que filtra o envía datos con base en información específica. Un conmutador de capa 2 (por ejemplo, un conmutador Ethernet) filtra o envía bloques de un nodo a otro usando direcciones de nivel MAC (esto es, hardware); un conmutador de capa 3 filtra o envía paquetes con base en direcciones de red, y un conmutador de capa 4 (o superior) filtra o envía mensajes con base en protocolos específicos de aplicación. Las velocidades de envío son usualmente hechas a velocidad de alambre y por medio de conexiones “privadas” (esto es, ningún otro nodo “ve” el tráfico). Los conmutadores subdividen las redes Ethernet/802.3 en múltiples dominios de colisión.

DIRECCIÓN IPV4**:** Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

DIRECCIÓN IPV6**:** Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2^{128} vs. 2^{32}). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación “punto”), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

ENRUTADOR**:** Un dispositivo de capa 3 responsable de determinar la trayectoria apropiada que un paquete toma para alcanzar su destino. Llamado comúnmente gateway.

ENRUTAMIENTO**:** Una función de nivel 3 que dirige los paquetes de datos de la fuente a su destino.

ESTACIÓN DE TRABAJO: Un sistema de computadora que tiene su propio sistema operativo y está conectada a una red. Una estación de trabajo puede ser una computadora personal como una Macintosh o una PC con base Intel, una estación de trabajo de gráficas como las fabricadas por Sun Microsystems, una superminicomputadora como la AS/400 de IBM, una supermicrocomputadora como la Alpha de DEC o una unidad central como la ES-9000 de IBM. Se llama también anfitrión, servidor, computadora de escritorio (desktop), o cliente.

GATEWAY**:** Una aplicación de software que convierte entre protocolos de aplicación diferentes. El anfitrión en que este software reside se llama máquina gateway. Históricamente, este término también se refiere a un emulador en la comunidad IP.

PING**:** Un programa UNIX y Microsoft NT usado para probar el camino de comunicación entre nodos fuente y destino. ping es una aplicación con base en ICMP y es un acrónimo de “packet Internet groper.”

PROTOCOLO DE ENRUTAMIENTO DE GATEWAY INTERIOR (IGRP): Un protocolo de enrutamiento desarrollado por Cisco para tratar algunos de los problemas asociados con ruteo en grandes redes heterogéneas.

PROTOCOLO DE GATEWAY EXTERIOR (EGP): Cualquier protocolo de enrutamiento Internet entre dominios usado para intercambiar información de enrutamiento con otros sistemas autónomos. Se refiere también a un EGP específico definido en RFC 904. Otro EGP es el Protocolo de Gateway de Frontera (BGP), definido en RFC 1105 y RFC 1771. Tanto EGP como BGP son parte del grupo de protocolos TCP/IP. Sin embargo, de los dos, BGP ha evolucionado a un protocolo robusto de enrutamiento Internet y el término “protocolo de gateway de frontera” se usa en favor del término “protocolo de gateway exterior”.

PROTOCOLO DE GATEWAY INTERIOR (IGP): Cualquier protocolo Internet de intradominio usado para intercambiar información de enrutamiento dentro de un sistema autónomo. Ejemplos incluyen RIP, R1P-2, OSPF, IGRP, y IGRP ampliado (EIGRP).

PROTOCOLO DE INFORMACIÓN DEL ENRUTAMIENTO (RIP): Un algoritmo vector distancia que determina la mejor ruta usando una métrica de saltos. RIP fue alguna vez el estándar defacto para enrutamiento IP.

PROTOCOLO DE RESERVACIÓN DE RECURSOS (RSVP): Un Protocolo de nivel 3 desarrollado por IETF para proporcionar un mecanismo para el control de latencia de red para aplicaciones específicas. Esto se hace priorizando datos y asignando suficiente ancho de banda para la transmisión de datos. El RSPV se puede pensar como un protocolo QoS con base en un IP.

PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN **(**ARP**):** Un protocolo Internet que une una dirección IP de nodo a su correspondiente dirección de subcapa MAC (hardware).

SERVIDOR**:** Un dispositivo de red que proporciona recursos a máquinas clientes. Ejemplos incluyen servidores de impresión, servidores de correo, servidores de archivo y servidores de Web. Los servidores son compartidos por más de un usuario; los clientes tienen un solo usuario.

SISTEMA AUTÓNOMO **(**AS**):** Una colección de redes controladas por una sola autoridad administrativa que comparte una estrategia común de enrutamiento. Los enrutadores que conectan redes dentro de un AS se confían entre sí e intercambian información de enrutamiento usando un protocolo de enrutamiento previamente acordado. También conocido como dominio de enrutamiento o área de protocolo.

RESUMEN

La Universidad Nacional Abierta y a Distancia – UNAD en coordinación con la empresa CISCO, orienta procesos de aprendizaje relacionados con el diseño, implementación y administración de redes de comunicaciones. Hace parte de esta oferta académica el diplomado denominado “Curso de profundización CCNP”, al cual pueden acceder los estudiantes de Ingeniería Electrónica como opción de grado. Para este fin, es necesario presentar la prueba de habilidades relacionada con la configuración de funciones de enrutamiento y conmutación, a través de las cuales se da solución a dos escenarios problema, cuya descripción se suministra en este documento. Para el primero, se da aplicación al concepto de vecindad, en el sentido de configurar routers para intercambio de datos entre dispositivos que hacen parte de sistemas autónomos diferentes, lo que se complementa con el establecimiento de rutas estáticas para facilitar las actividades de administración. Para el segundo caso, se centraliza la administración de las redes virtuales locales – VLANs, a través del protocolo VTP, al tiempo que se configura el protocolo de enlaces dinámicos troncales – DTP, con el cual se automatiza la asignación de etiquetas a las tramas que circulan entre las VLANs de la red.

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

ABSTRACT

The Universidad Nacional Abierta y a Distancia – UNAD by means of coordination with CISCO Enterprise, provides guidance on learning processes related to networking design, implementation and management. The academic programs availability includes the CP CCNP ROUTE and CP CCNP SWITCH courses, which can be taken by Electronic Engineering students to comply with graduation requirements. For this purpose, it is necessary to present a hand-on-skill exam that deals with routing and switching to solving two problem scenarios, which description is provided herein. In the first place, peering is stablished through neighbor routers from different autonomous systems, and the establishment of static routes for the ease of management activities. Secondly, local virtual networks - VLANs management is centralized using VTP, as Dynamic Trunking Protocol – DTP is set in order to automate tag assignment on traveling frames between VLANs within the network.

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

INTRODUCCIÓN

El mundo actual se mueve en función de la disponibilidad de información oportuna y de calidad. De esta condición se deriva la necesidad de contar con los medios apropiados para su gestión, toda vez que la integridad y precisión de los datos son elementos habilitantes de la toma de decisiones, la identificación de problemas y el diseño de estrategias de negocio pertinentes y eficaces. En este sentido, la participación de profesionales con formación tecnológica orientada a la administración de redes de comunicación para el intercambio de datos, adquiere gran importancia al considerar la complejidad que representa su diseño, instalación y administración.

En virtud de lo expuesto previamente, la Universidad Nacional Abierta y a Distancia – UNAD incluyó en su oferta académica el diplomado denominado "Curso de Profundización CISCO CCNP", con el cual da la oportunidad a estudiantes de ingeniería de adquirir competencias específicas en conmutación y enrutamiento. Para el primer caso, el módulo CCNP SWITCH brinda orientación respecto a la implementación y monitoreo de las funciones de conmutación, la implementación de redes locales virtuales (VLAN), la optimización de la disponibilidad y redundancia de los dispositivos y la configuración de funciones de seguridad. En el segundo caso, el módulo CCNP ROUTE facilita las herramientas para el diseño de enrutamiento avanzado, la automatización de las decisiones sobre asignación de rutas, la implementación de protocolos para interoperabilidad con redes IP, la configuración de enrutamiento para comunicación con proveedores de servicios de Internet (ISP) y la comunicación entre sucursales y estaciones móviles.

Estas competencias son el resultado de la interacción de los estudiantes de ingeniería con las herramientas de simulación disponibles para el desarrollo del curso: Packet Tracer, GNS3 y el laboratorio remoto SMARTLAB; las cuales facilitaron, a través de la sintaxis particular de cada función, una transición efectiva entre la teoría y la práctica; condición que se valida con la solución propuesta en este documento respecto a los escenarios relacionados con funciones de enrutamiento y conmutación de una red de comunicaciones.

1. ENRUTAMIENTO

Las actividades de enrutamiento (routing) orientadas al óptimo funcionamiento de una red se centran en el intercambio de información respecto a las rutas preferentes que facilitan la comunicación entre diferentes dispositivos y a través de segmentos específicos de la red. Esto se logra mediante configuraciones de los routers para el aprendizaje y actualización de tablas de direcciones, lo que facilita una adaptación dinámica ante posibles cambios. En algunos casos se requiere que el intercambio de datos se realice con proveedores de servicios de Internet, lo que sugiere una comunicación con elementos externos a la organización, en cuyo caso el diseño de algoritmos específicos termina en la existencia de **protocolos** para el logro de este fin particular.

Uno de los protocolos típicos para el intercambio de información (respecto a rutas) entre diferentes sistemas autónomos es el conocido como Protocolo de Puerta de Frontera (Border Gateway Protocol - BGP). Este protocolo permite el reconocimiento de la existencia de diferentes sistemas autónomos a partir de la relación que se declara entre un dispositivo de la red y la identificación numérica del sistema autónomo. Es así que, diferentes números indican diferentes sistemas autónomos.

Un router que ha sido configurado como BGP adquiere la posibilidad de aprender rutas anunciadas por otros routers, a condición de contar con el establecimiento de sesiones de intercambio de información de rutas denominadas “vecinos”, lo que lo habilita también para alcanzar otras redes que son anunciadas por otros routers.

Lo expuesto anteriormente, sirve de base para la solución al primer escenario ya que la topología indicada en la Imagen 1, muestra la existencia de cuatro sistemas autónomos, a partir de los cuales se debe establecer una relación de vecindad mediante routers conectados directamente. Al encontrarse en diferentes sistemas autónomos, se recurre a la versión de protocolo externo de BGP (EBGP).

Una de las maneras de lograr que la dirección IP declarada en la configuración de vecinos pueda ser alcanzada sin el uso de un protocolo adicional (como el Protocolo de Puerta Interior – IGP), es la configuración de una ruta estática a esa IP, lo cual hace parte de la solución a este primer escenario.

En términos generales, la configuración de routers BGP se basa en la existencia de diferentes sistemas autónomos, el establecimiento de vecindad, y la conexión directa de los dispositivos, lo cual se evidencia en el siguiente desarrollo.

Imagen 1. Topología de red para EBGP

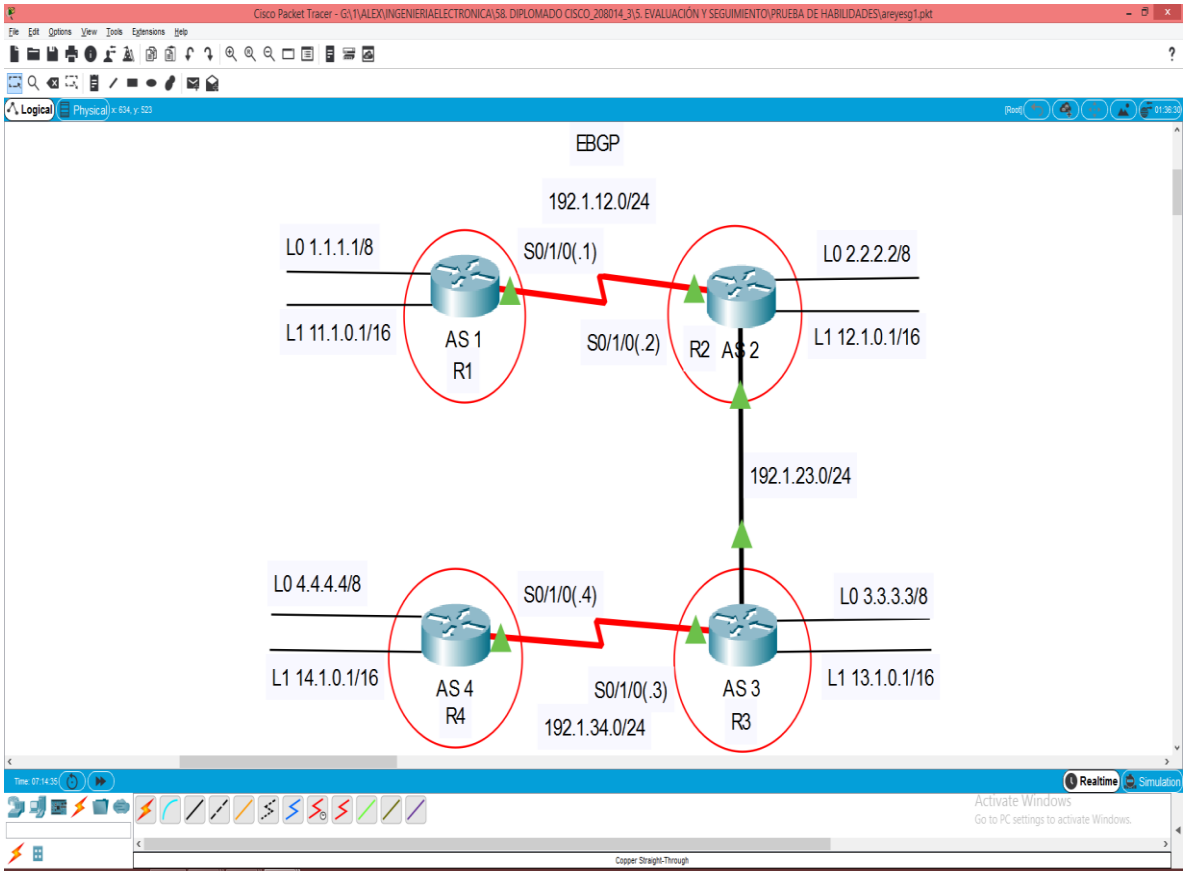


Tabla 1. Información para la configuración de los routers

ROUTER	INTERFAZ	DIRECCIÓN IP	MÁSCARA
R1	Loopback 0	1.1.1.1	255.0.0.0
R1	Loopback 1	11.1.0.1	255.255.0.0
R1	S 0/0	192.1.12.1	255.255.255.0
R2	Loopback 0	2.2.2.2	255.0.0.0
R2	Loopback 1	12.1.0.1	255.255.0.0
R2	S 0/0	192.1.12.2	255.255.255.0
R2	E 0/0	192.1.23.2	255.255.255.0
R3	Loopback 0	3.3.3.3	255.0.0.0
R3	Loopback 1	13.1.0.1	255.255.0.0
R3	S 0/0	192.1.34.3	255.255.255.0
R3	E 0/0	192.1.23.3	255.255.255.0
R4	Loopback 0	4.4.4.4	255.0.0.0
R4	Loopback 1	14.1.0.1	255.255.0.0
R4	S 0/0	192.1.34.4	255.255.255.0

1.1CONFIGURACIÓN DE BGP

La configuración de este protocolo se basa en disponibilidad de datos sobre la identificación de los sistemas autónomos (números), las direcciones IP de los routers vecinos y las redes que deben ser anunciadas. En este sentido, el proceso para la configuración de BGP a partir de la Imagen 1 y Tabla 1, es el siguiente:

1.1.1 Configuración de una relación de vecino BGP entre R1 y R2.

a. Configuración básica R1

Router(config)> **enable**
Router(config)> **conf t**
Router(config)> **hostname R1**
R1(config)# **no ip domain-lookup**
R1(config)# **line con 0**
R1(config-line)# **logging synchronous**
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**
R1 (config)# **interface Serial0/1/0**
R1 (config-if)# **ip address 192.1.12.1 255.255.255.0**
R1 (config-if)# **clock rate 128000**
R1 (config-if)# **no shutdown**
R1 (config-if)# **end**
R1# **copy running-config startup-config**

b. Configuración básica R2

Router(config)> **enable**
Router(config)> **conf t**
Router(config)> **hostname R2**
R2(config)# **no ip domain-lookup**
R2(config)# **line con 0**
R2(config-line)# **logging synchronous**
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**

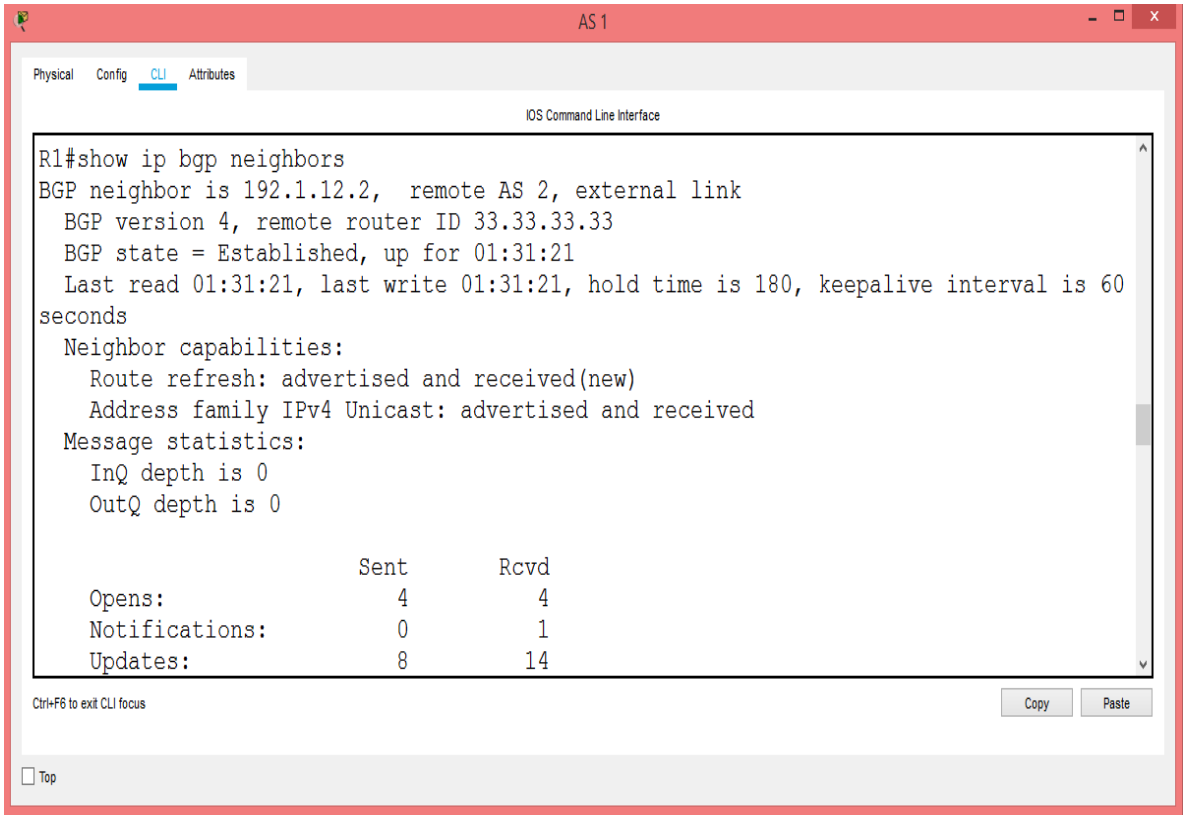
R2 (config-if)# **ip address 12.1.0.1 255.255.0.0**
R2 (config-if)# **exit**
R2 (config)# **interface Serial0/1/0**
R2 (config-if)# **ip address 192.1.12.2 255.255.255.0**
R2 (config-if)# **clock rate 128000**
R2 (config-if)# **no shutdown**
R2 (config)# **interface GigabitEthernet0/1**
R2 (config-if)# **ip address 192.1.23.2 255.255.255.0**
R2 (config-if)# **no shutdown**
R2 (config-if)# **end**
R2# **copy running-config startup-config**

c. Activación de la sesión BGP y definición de vecinos

Configuración R1 en AS1 y R2 en AS2

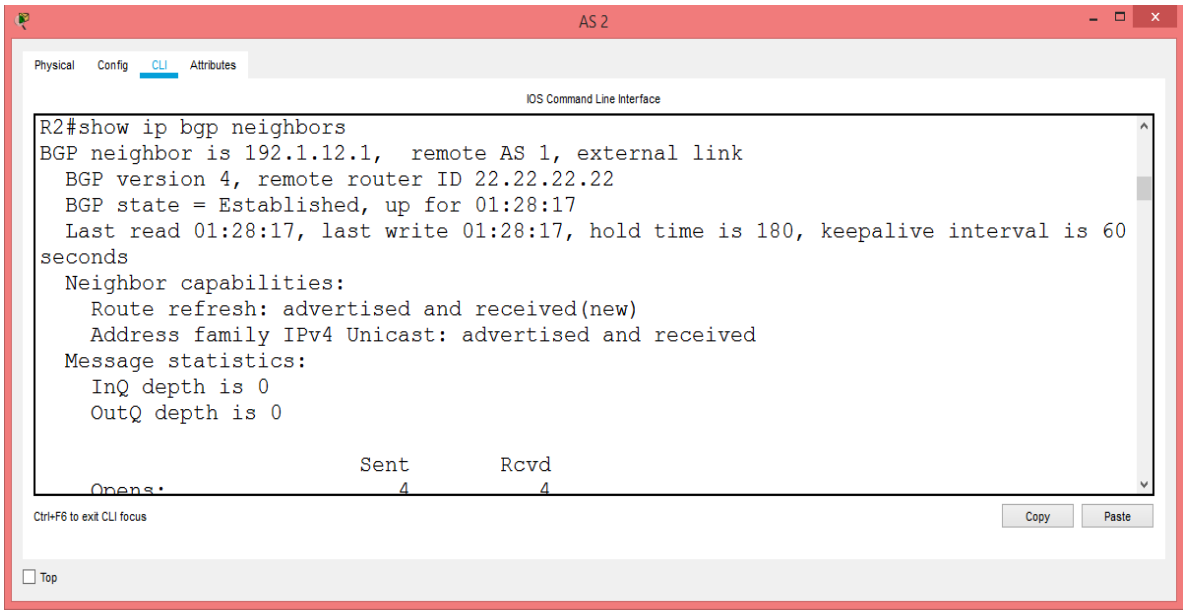
R1(config)# **router bgp 1**
R1(config-router)# **neighbor 192.1.12.2 remote-as 2**
R1(config-router)# **exit**

Imagen 2. Verificación de vecindad para R1-R2



R2(config)# **router bgp 2**
R2(config-router)# **neighbor 192.1.12.1 remote-as 1**
R2(config-router)# **exit**

Imagen 3. Verificación de vecindad para R2-R1



d. Anuncio de direcciones Loopback en BGP

R1(config)# **router bgp 1**
R1(config-router)# **network 1.1.1.1 mask 255.0.0.0**
R1(config-router)# **network 11.1.0.1 mask 255.255.0.0**
R1(config-router)# **exit**

R2(config)# **router bgp 2**
R2(config-router)# **network 2.2.2.2 mask 255.0.0.0**
R2(config-router)# **network 12.1.0.1 mask 255.255.0.0**
R2(config-router)# **exit**

e. Codificación de ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2

R1(config)# **router bgp 1**
R1(config-router)# **bgp router-id 22.22.22.22**

R2(config)# **router bgp 2**
R2(config-router)# **bgp router-id 33.33.33.33**

f. Salida del comando **show ip route**

Imagen 4. Salida comando show ip route para R1-R2

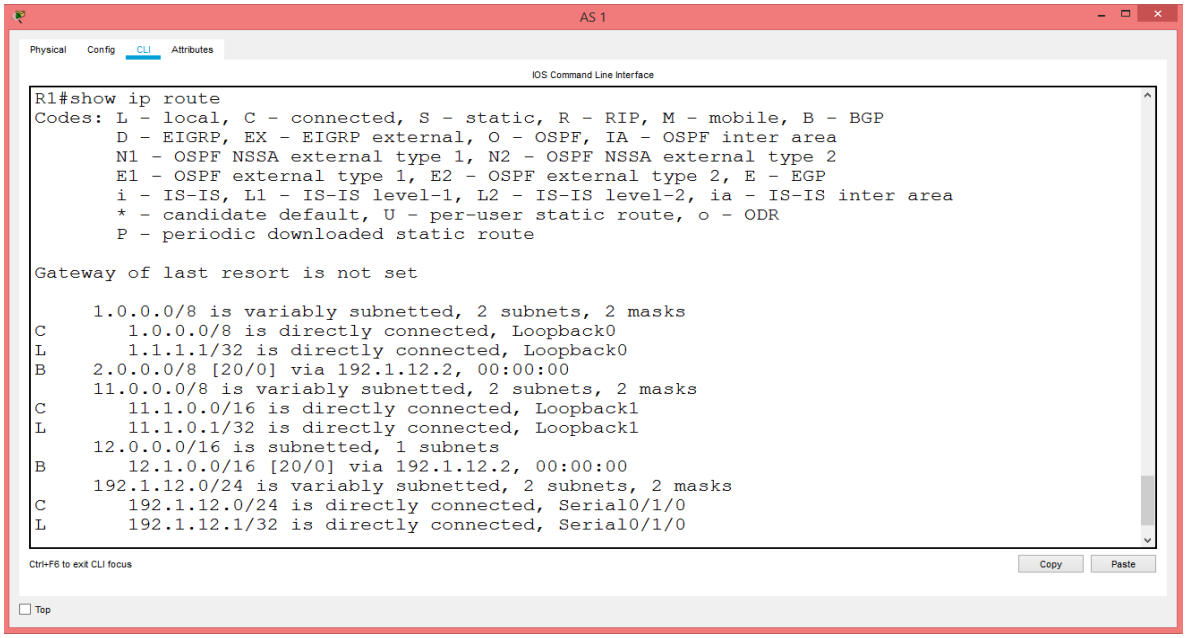
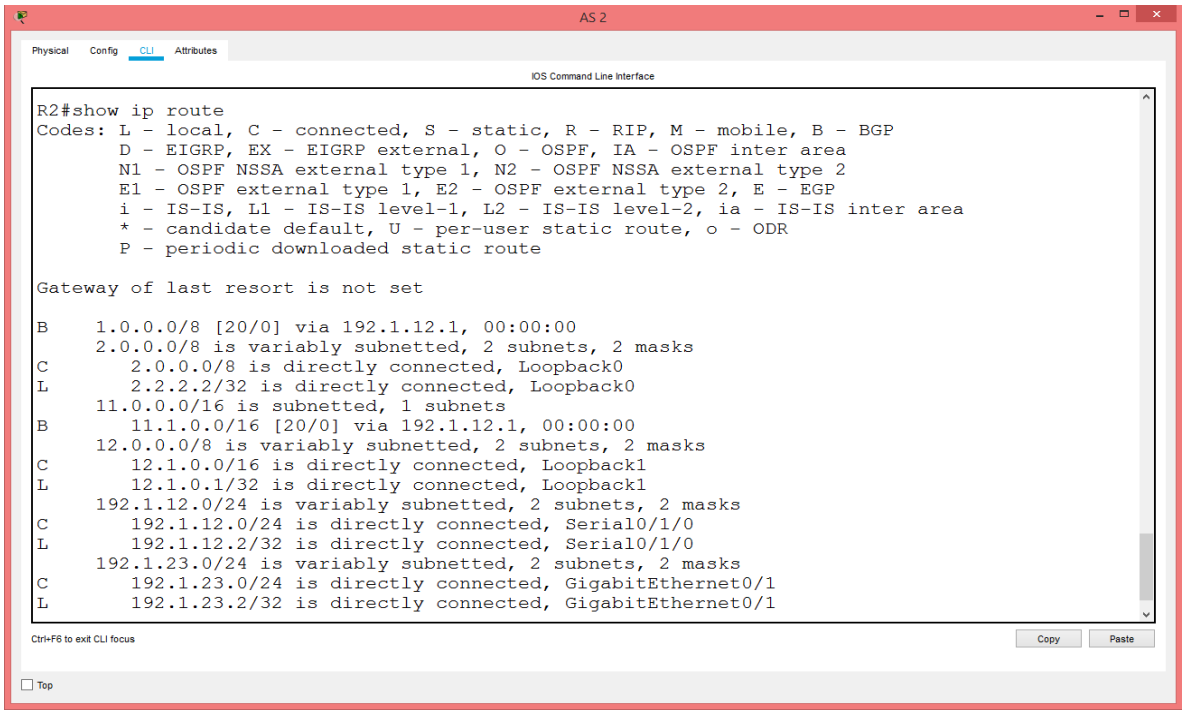


Imagen 5. Salida comando show ip route para R2-R1



1.1.2 Configuración de una relación de vecino BGP entre R2 y R3.

a. R2 configurado previamente en AS2
b. Configuración básica R3

```
Router(config)> enable
Router(config)> conf t
Router(config)> hostname R3
R3(config)# no ip domain-lookup
R3 (config)# line con 0
R3 (config-line)# logging synchronous
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
R3 (config)# interface Serial0/1/0
R3 (config-if)# ip address 192.1.34.3 255.255.255.0
R3 (config-if)# clock rate 128000
R3 (config-if)# no shutdown
R3 (config)# interface GigabitEthernet0/1
R3 (config-if)# ip address 192.1.23.3 255.255.255.0
R3 (config-if)# end
R3# copy running-config startup-config
```

c. Configuración R3 en AS3

```
R3(config)# router bgp 3
R3(config-router)# neighbor 192.1.23.2 remote-as 2
R3(config-router)# exit
```

d. Configuración vecindad de R2

```
R2(config)# router bgp 2
R2(config-router)# neighbor 192.1.23.3 remote-as 3
R2(config-router)# exit
```

e. Anuncio de las direcciones de Loopback de R3 en BGP

```
R3(config)# router bgp 3
R3(config-router)# network 3.3.3.3 mask 255.0.0.0
R3(config-router)# network 13.1.0.1 mask 255.255.0.0
R3(config-router)# exit
```

Imagen 6. Verificación de vecindad para R3-R2

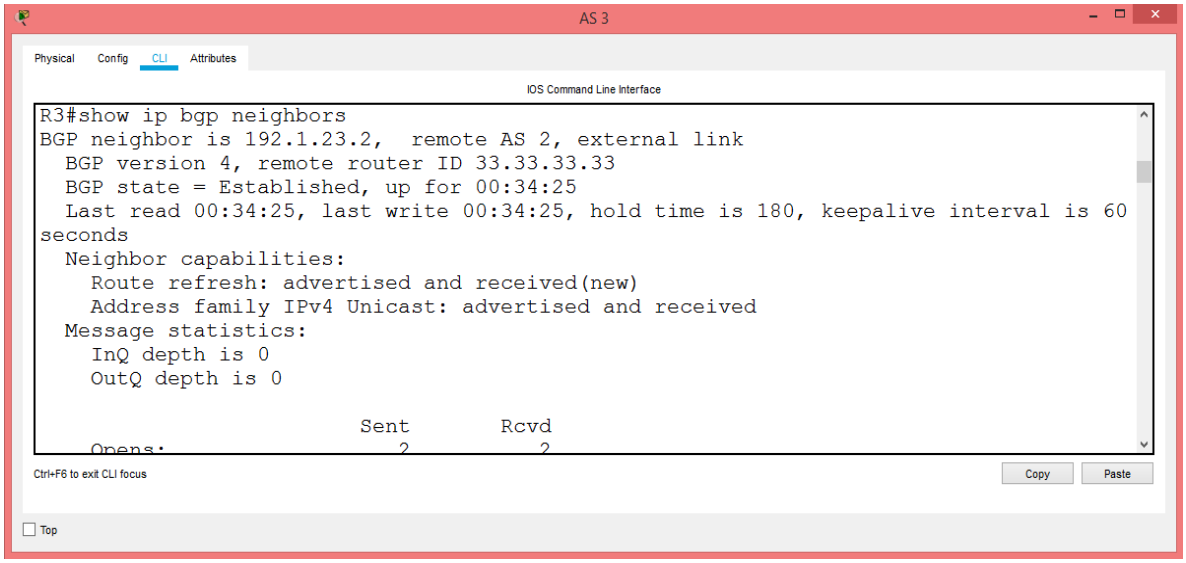
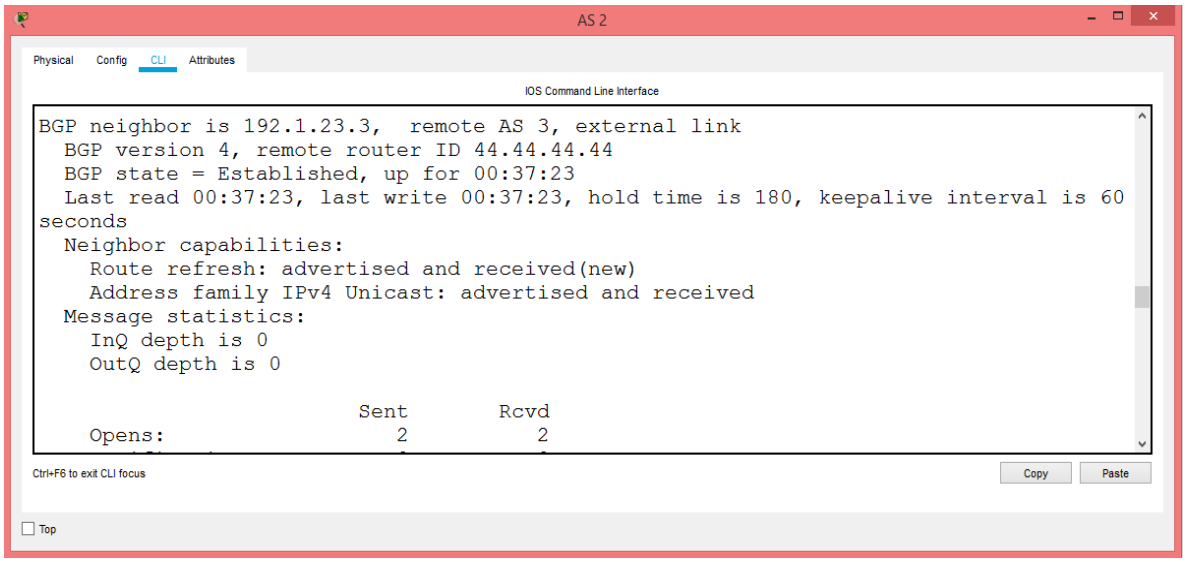


Imagen 7. Verificación de vecindad para R2-R3

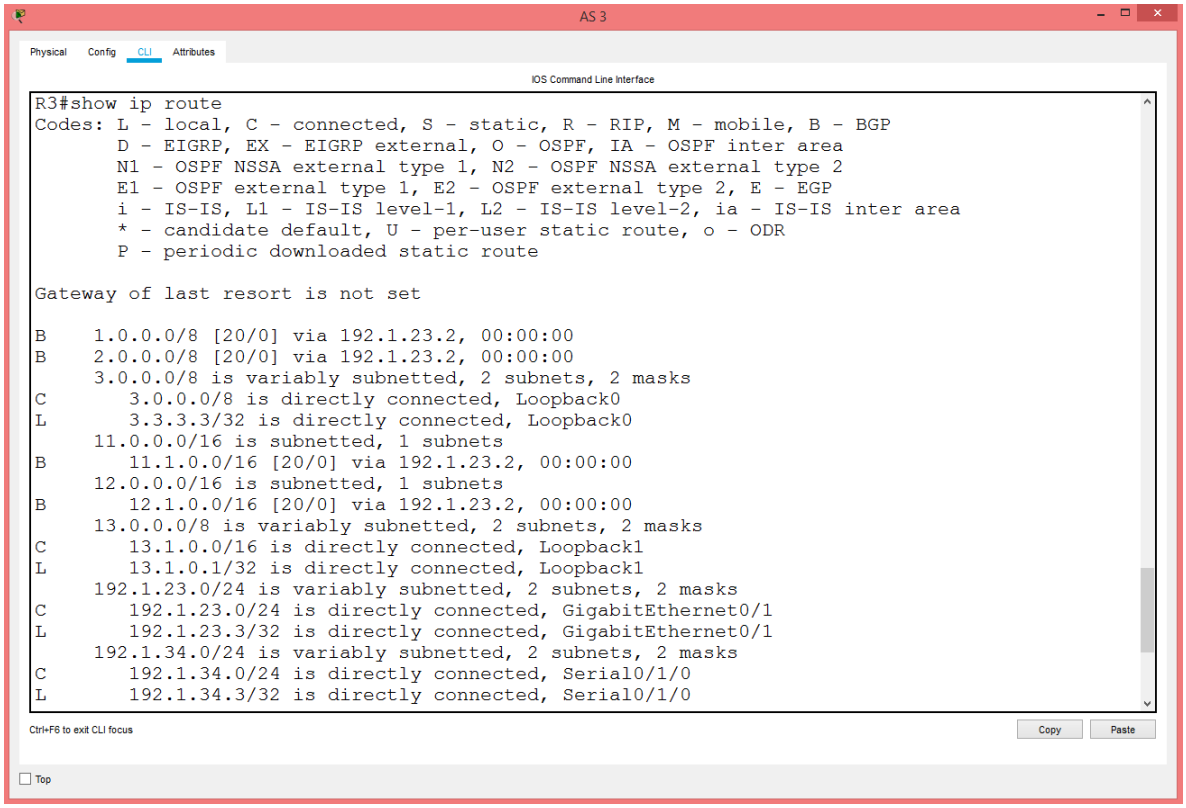


f. Codificación d ID del router R3 como 44.44.44.44.

R3(config)# **router bgp 3**
R3(config-router)# **bgp router-id 44.44.44.44**

g. Salida del comando **show ip route**

Imagen 8. Salida comando show ip route para R3-R2



1.1.3 Configuración de relación de vecino BGP entre R3 y R4.

a. R3 configurado previamente en AS3
b. Configuración básica R4

Router(config)> **enable**
Router(config)> **conf t**
Router(config)> **hostname R4**
R4(config)# **no ip domain-lookup**
R4 (config)# **line con 0**
R4 (config-line)# **logging synchronous**
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**
R4 (config)# **interface Serial0/1/0**
R4 (config-if)# **ip address 192.1.34.4 255.255.255.0**

R4 (config-if)# **clock rate 128000**
R4 (config-if)# **no shutdown**
R4 (config-if)# **end**
R4# **copy running-config startup-config**

c. Configuración R4 en AS4

R4(config)# **router bgp 4**
R4(config-router)# **neighbor 192.1.34.3 remote-as 3**
R4(config-router)# **exit**

d. Configuración vecindad de R3

R3(config)# **router bgp 3**
R3(config-router)# **neighbor 192.1.34.4 remote-as 4**
R3(config-router)# **exit**

e. Anuncio de las direcciones de Loopback de R4 en BGP

R4(config)# **router bgp 4**
R4(config-router)# **network 4.4.4.4 mask 255.0.0.0**
R4(config-router)# **network 14.1.0.1 mask 255.255.0.0**
R4(config-router)# **exit**

f. Codificación del ID del router R4 como 66.66.66.66.

R4(config)# **router bgp 4**
R4(config-router)# **bgp router-id 66.66.66.66**

g. Establecimiento de relaciones de vecino con base en las direcciones de Loopback 0.

R4(config)# **router bgp 4**
R4(config-router)# **neighbor 3.3.3.3 remote-as 3**
R4(config-router)# **exit**

R3(config)# **router bgp 3**
R3(config-router)# **neighbor 4.4.4.4 remote-as 4**
R3(config-router)# **exit**

Imagen 9. Verificación de vecindad para R4-R3

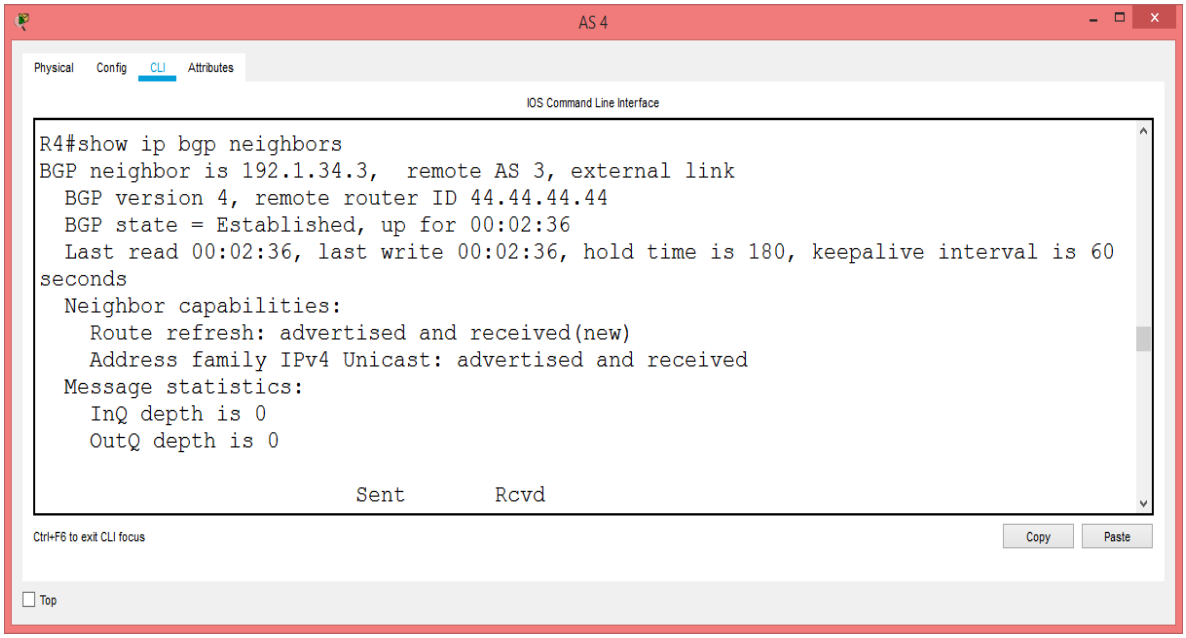


Imagen 10. Verificación de vecindad para R3-R4

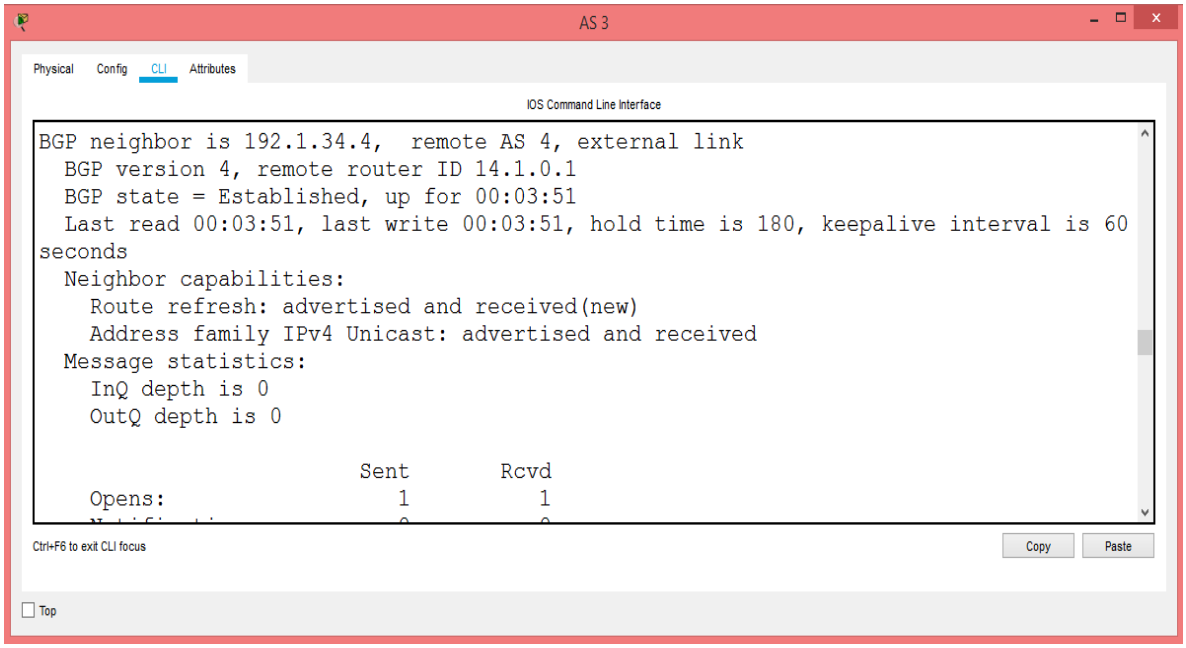


Imagen 11. Verificación de vecindad L0 para R4-R3

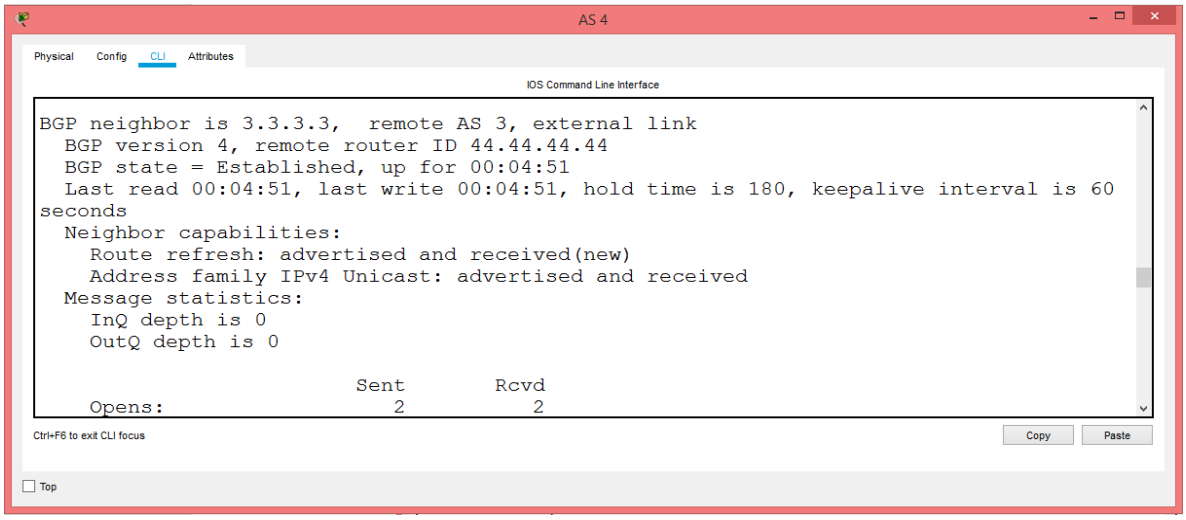
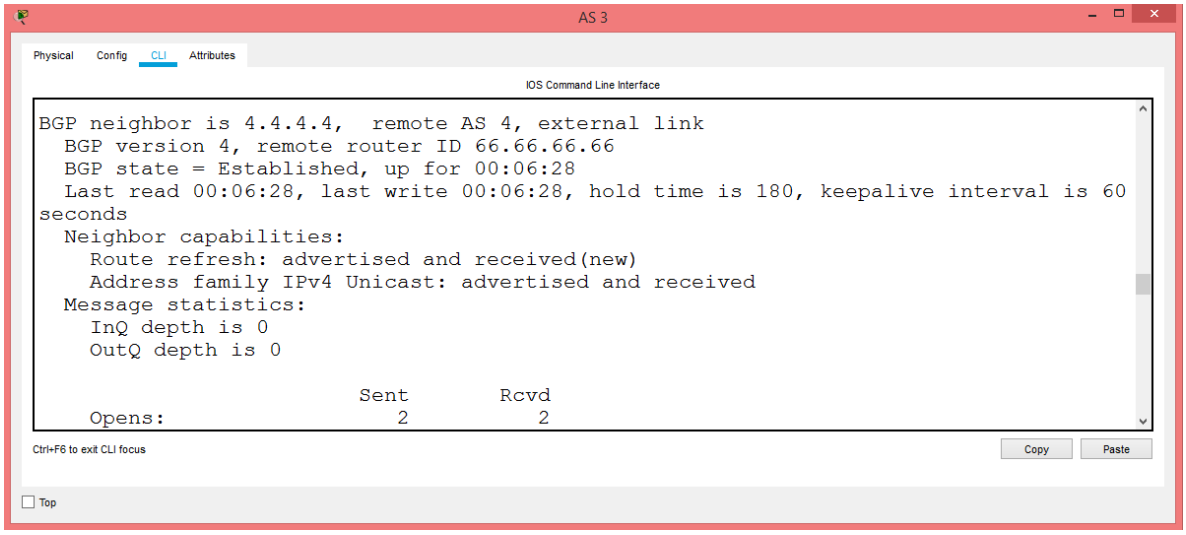


Imagen 12. Verificación de vecindad L0 para R3-R4



h. Creación de rutas estáticas para alcanzar la Loopback 0 del otro router

R4(config)# **ip route 192.1.23.0 255.255.255.0 192.1.34.3**

R3(config)# **ip route 192.1.34.0 255.255.255.0 192.1.34.4**

i. Anuncio de la red Loopback de R4 en BGP.

R4(config)# **router bgp 4**
R4(config-router)# **network 192.1.34.0 mask 255.255.255.0**
R4(config-router)# **exit**

Nota: No se anuncia la Loopback 0 en BGP.

j. Salida del comando **show ip route**

Imagen 13. Salida comando show ip route para R4-R3

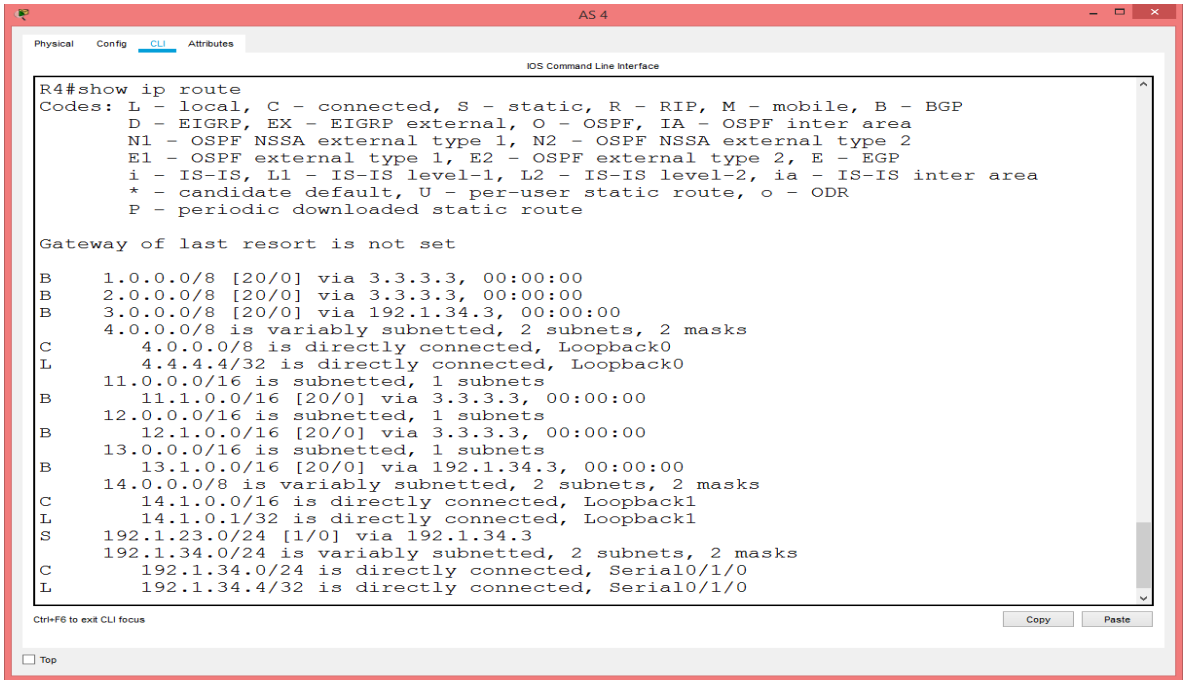


Imagen 14. Ping de R4 a L0 en R3

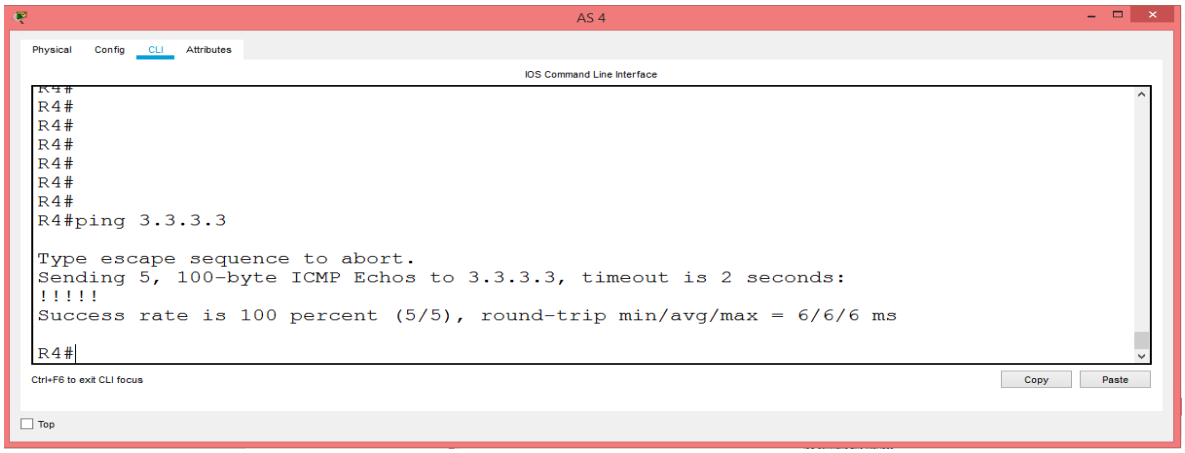


Imagen 15. Ping de R3 a L0 en R4

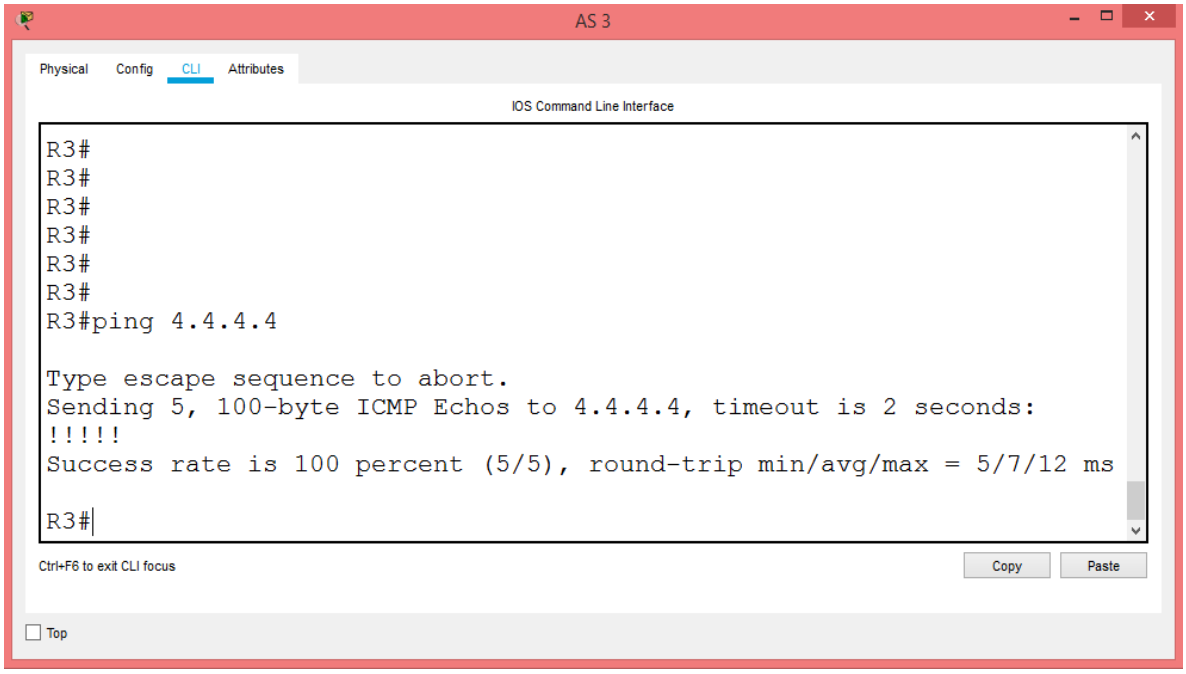


Imagen 16. Salida comando show ip bgp para R1

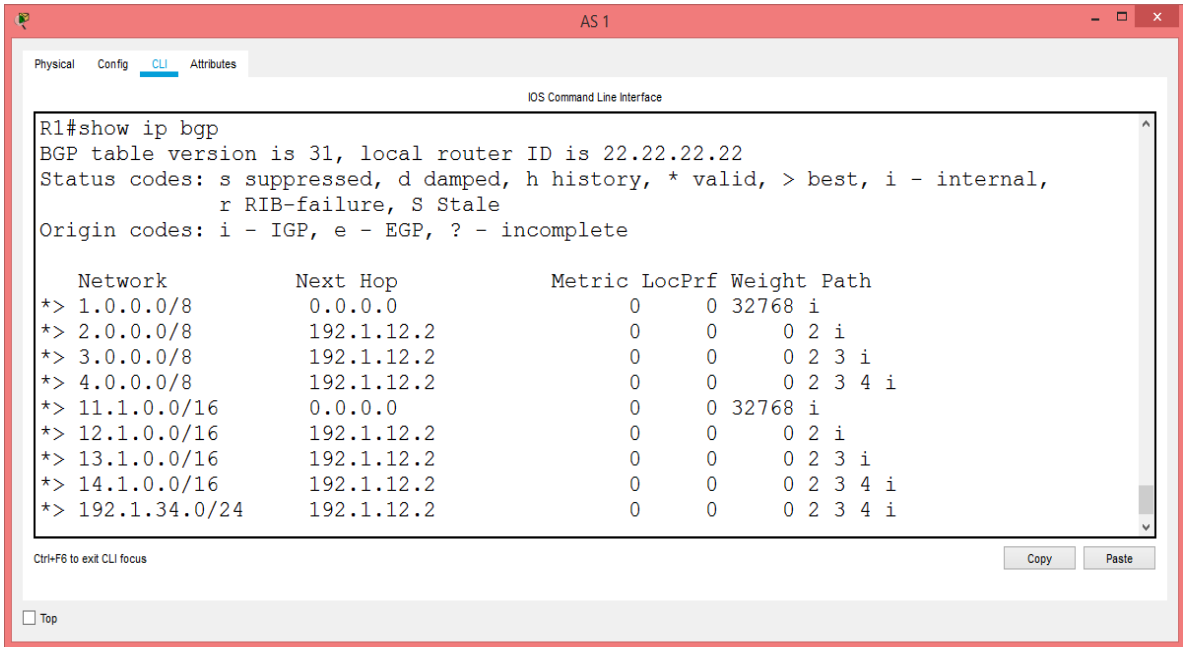


Imagen 17. Salida comando show ip bgp para R2

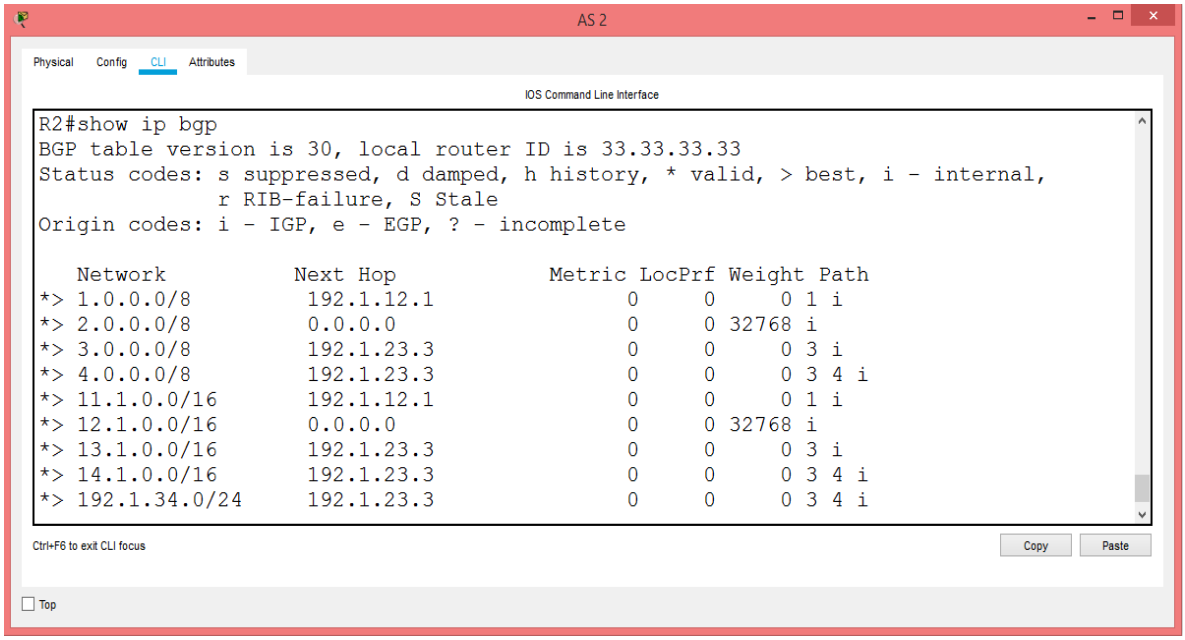


Imagen 18. Salida comando show ip bgp para R3

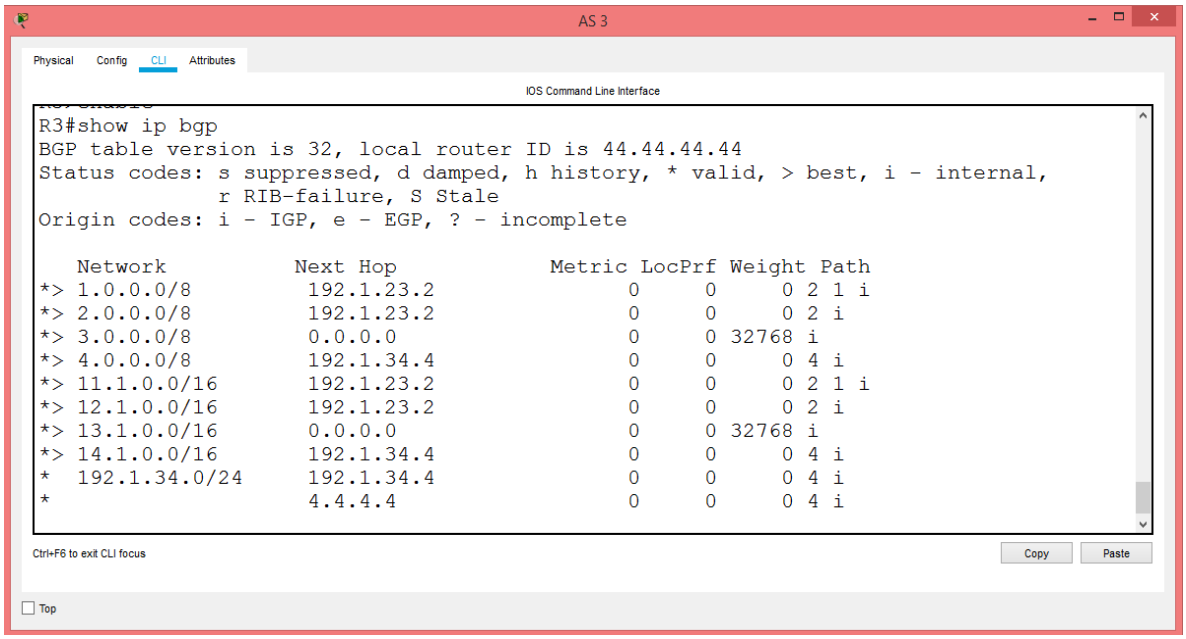


Imagen 19. Salida comando show ip bgp para R4

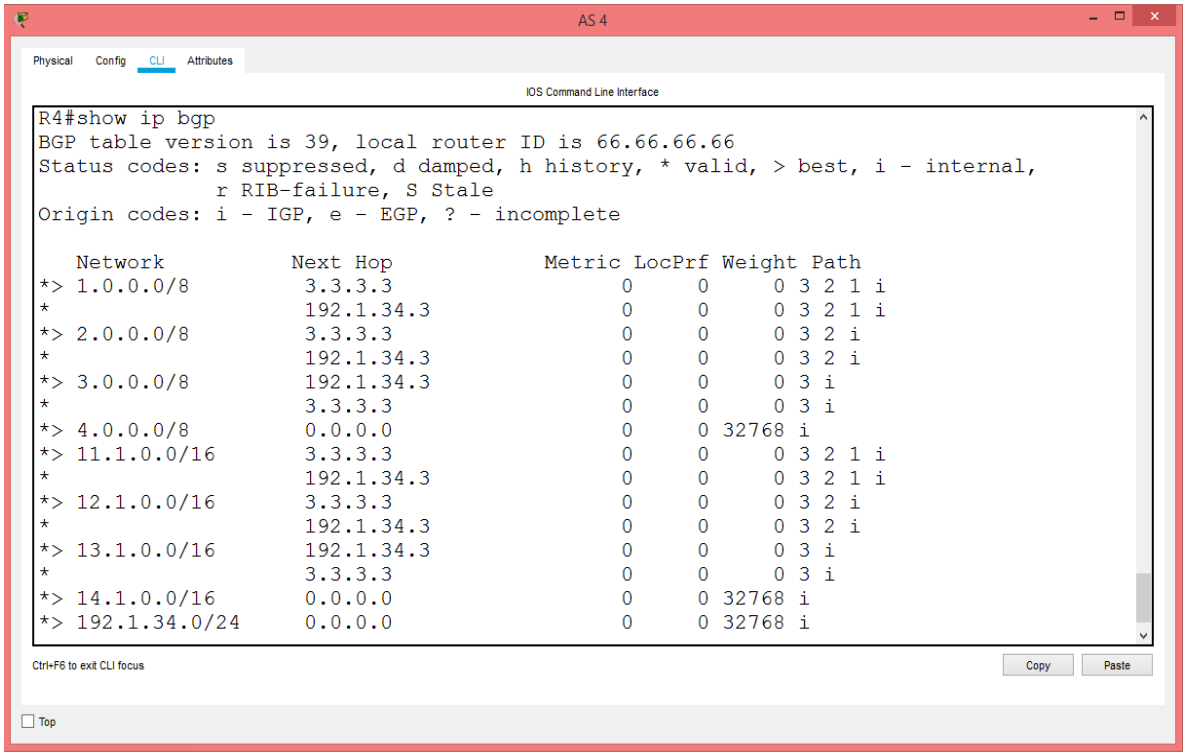


Imagen 20. Salida comando show ip bgp summary para R1

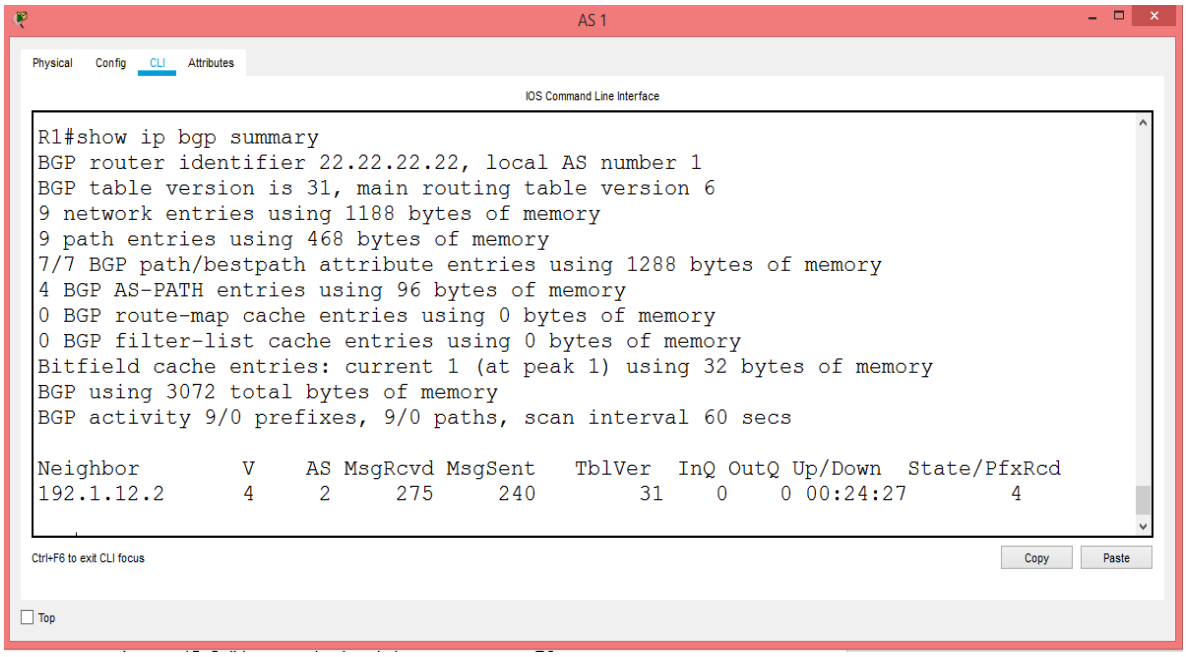


Imagen 21. Salida comando show ip bgp summary para R2

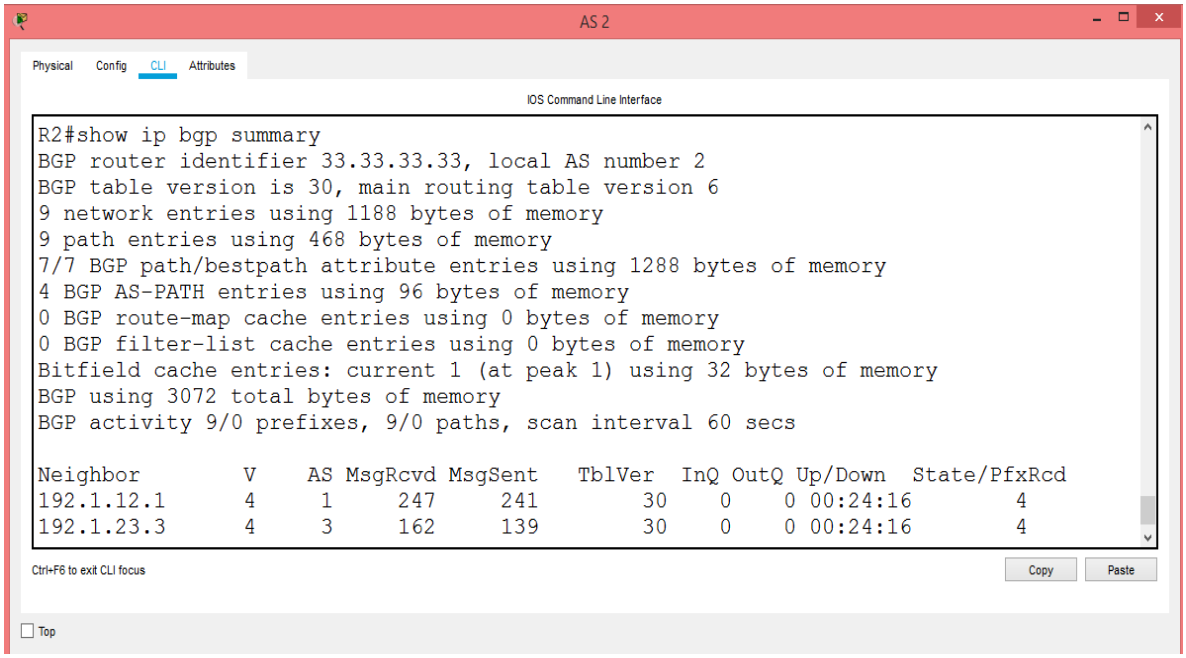


Imagen 22. Salida comando show ip bgp summary para R3

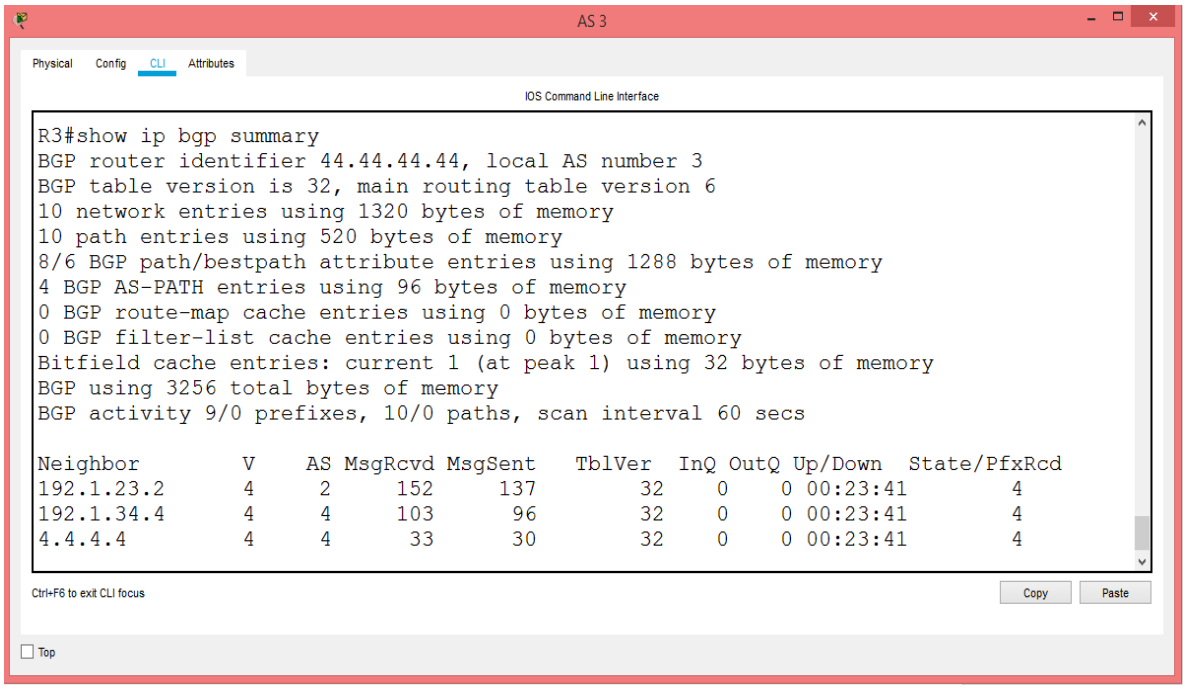
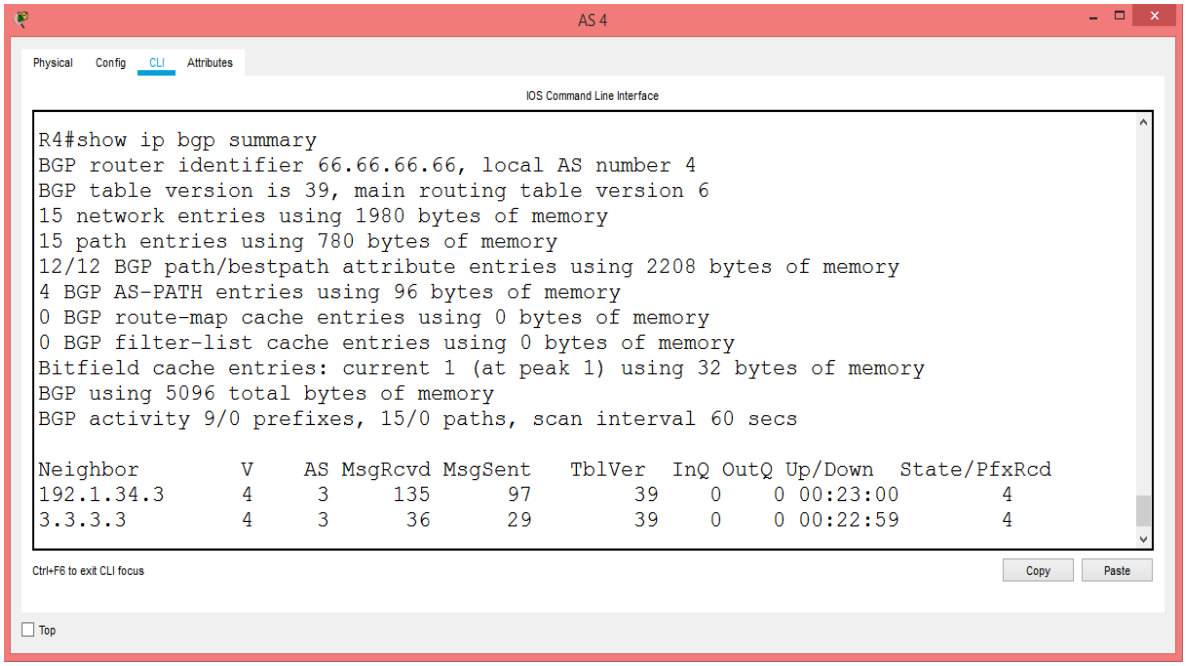


Imagen 23. Salida comando show ip bgp summary para R4



2. CONMUTACIÓN

El principio de la conmutación se basa en la posibilidad de varios dispositivos para conectarse a la misma red, pero cada uno con un ancho de banda específico; lo que conduce a un mayor rendimiento. No obstante, los dispositivos modernos de conmutación pueden ofrecer servicios de enrutamiento, permitir la redundancia y facilitar la condición de convergencia.

La acción de un switch puede representar la decisión de envío de información a través de un puerto determinado, o grupo de puertos denominado Red Virtual de Área Local (VLAN), la cual involucra una configuración lógica que permite la selección de puertos para envío / recepción de información. Contrario al enrutamiento, la conmutación a través de switches impide la migración de tramas a puertos de otros grupos, confinando el intercambio de datos entre dispositivos de la misma VLAN, lo que se conoce como **difusión en el mismo dominio**.

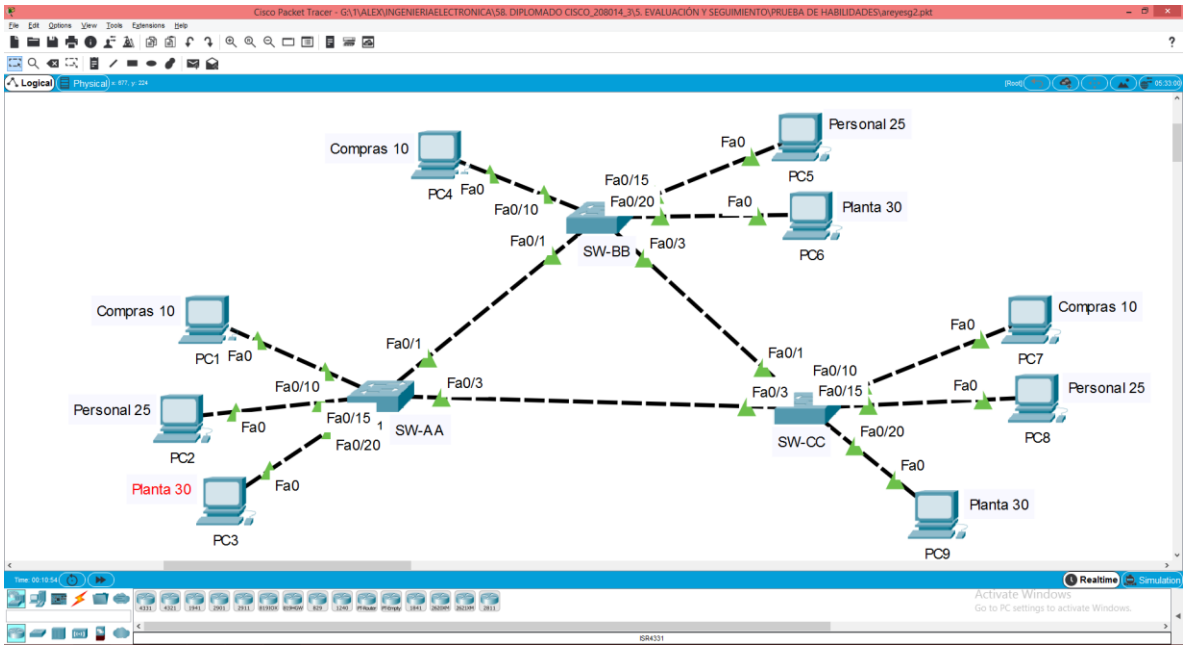
En algunos casos se requiere que las VLAN funcionen de manera independiente a través de varios switches (configuración end-to-end), lo que facilita el aprovechamiento de ventajas como la segmentación de difusiones en dominios de capa 2. Esta configuración se conoce como “troncal”, donde cada puerto configurado con esta condición puede recibir y enviar información para diferentes VLANs, lo que se logra asignando una “etiqueta” a las tramas para identificar las VLANs de origen / destino. Para este fin se requiere de la configuración troncal física punto a punto entre dos dispositivos.

El link destinado a compartir información entre VLANs ubicadas a través de diferentes switches, puede darse de manera dinámica (Dynamic Trunk Protocol) para negociar el estado del enlace y seleccionar el protocolo adecuado. El estado puede ser de enlace permanente con o sin modo troncal a través de negociación, o dinámico para convertir un puerto en troncal, obedeciendo a la configuración del vecino.

Con el fin de gestionar las VLAN de una red, en cuanto a creación, eliminación, identificación y distribución sincronizada de las bases de datos a través de una red soportada en switches, a la vez que se minimizan los errores de configuración, se utiliza el denominado Protocolo Troncal de VLAN – VTP. Este protocolo ofrece tres opciones de configuración: servidor, cliente y transparente. El primero permite opciones extendidas de gestión de VLANs en comparación de los otros dos, particularmente la creación y eliminación.

Tanto DTP como VTP son utilizados para dar solución al segundo escenario, cuyo desarrollo se describe a continuación.

Imagen 24. Topología de red para VLANs



La topología indicada en la Imagen 24, muestra la existencia de tres VLANs a saber: 10 (Compras), 25 (Personal) y 30 (Planta). Se observan tres switches a los cuales se encuentran conectados directamente tres PCs, cada uno de ellos asociado a una VLAN diferente. Se requiere establecer comunicación entre PCs pertenecientes a cada VLAN, por tal razón se acude a la configuración de enlaces troncales entre los switches mediante DTP, realizando previamente la configuración para gestión de la red activando VTP en modo servidor para el switch BB y en modo cliente para los switches AA y CC. El procedimiento es el siguiente:

2.1 CONFIGURACIÓN DE VTP

a. Configuración básica de switches

Switch> **enable**
Switch)# **conf t**
Switch (config)# **hostname SW-AA**

Switch> **enable**
Switch)# **conf t**
Switch (config)# **hostname SW-BB**

Switch> **enable**
Switch)# **conf t**
Switch (config)# **hostname SW-CC**

b. Configuración del switch SW-BB como el servidor

SW-BB(config)# **vtp domain CCNP**
SW-BB (config)# **vtp version 2**
SW-BB (config)# **vtp mode server**
SW-BB (config)# **vtp password cisco**

c. Configuración de los switches SW-AA y SW-CC como clientes

SW-AA(config)# **vtp domain CCNP**
SW-AA (config)# **vtp version 2**
SW-AA (config)# **vtp mode client**
SW-AA (config)# **vtp password cisco**

SW-CC(config)# **vtp domain CCNP**
SW-CC (config)# **vtp version 2**
SW-CC (config)# **vtp mode client**
SW-CC (config)# **vtp password cisco**

d. Salida del comando **show vtp status**

Imagen 25. Salida del comando show vtp status para SW-AA

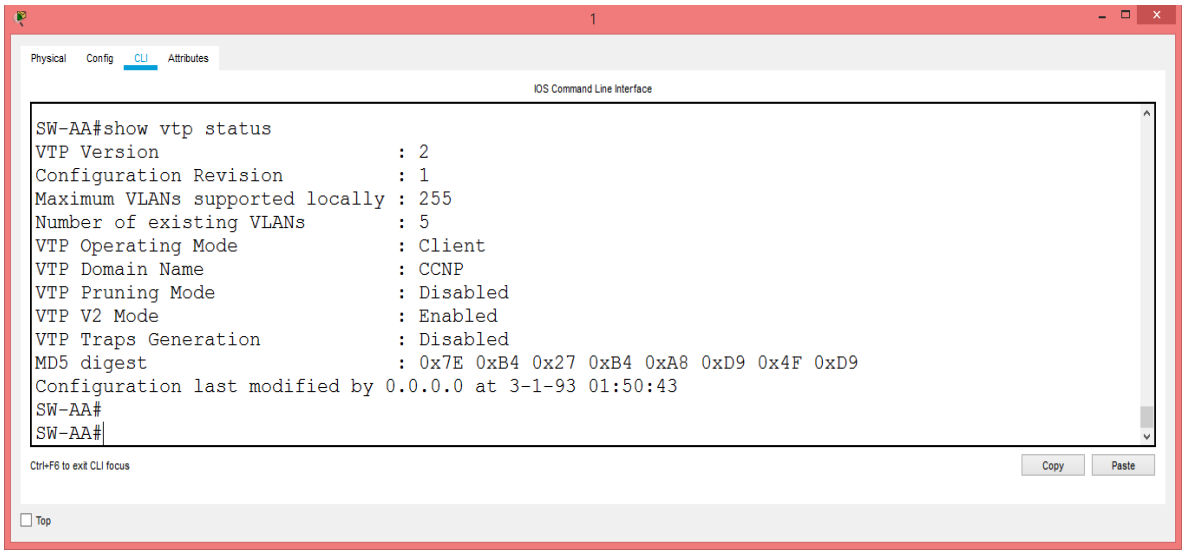


Imagen 26. Salida del comando show vtp status para SW-BB

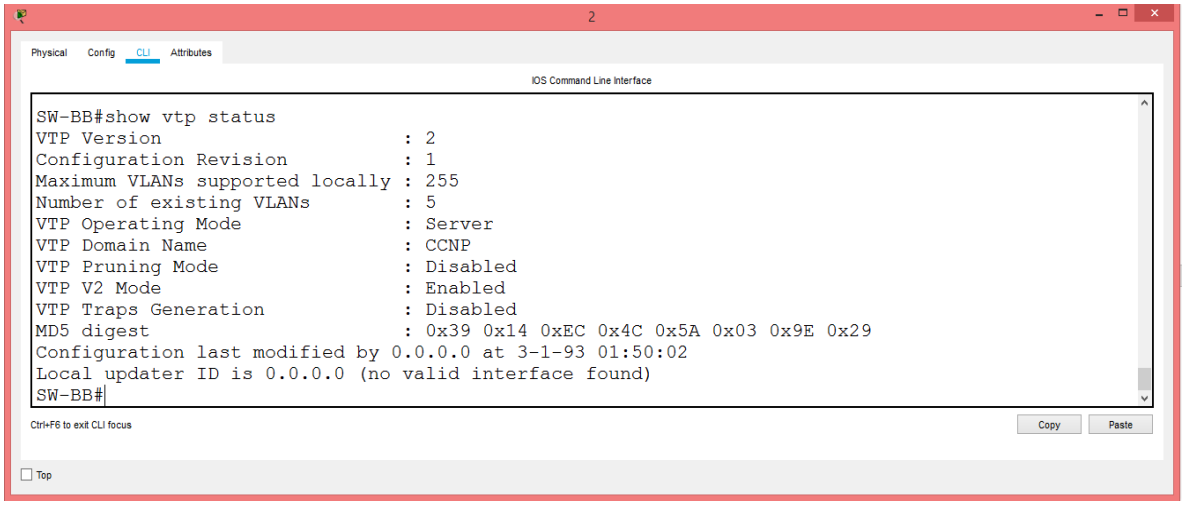
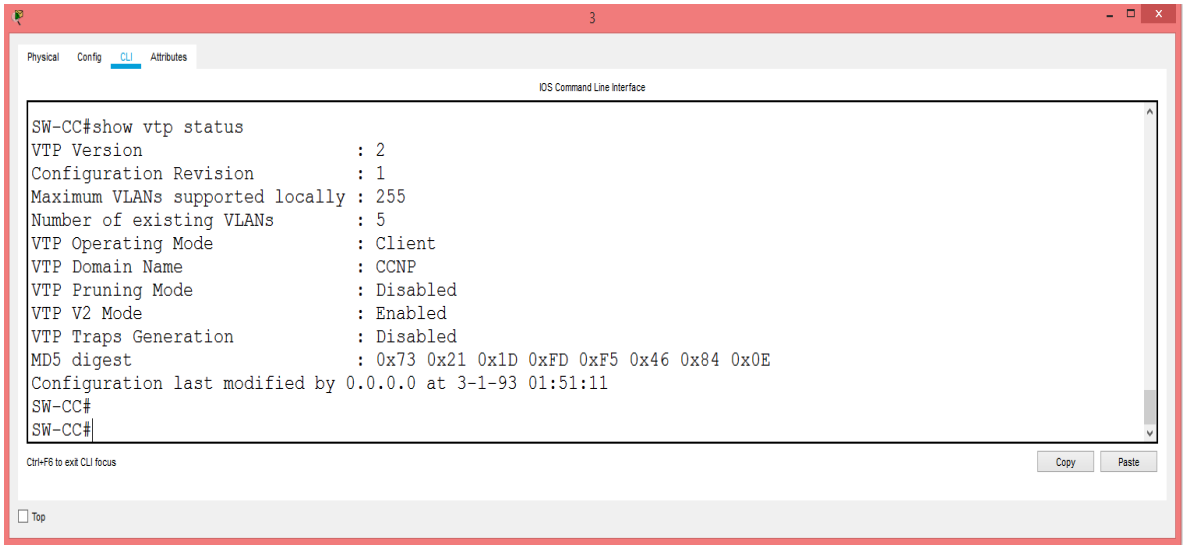


Imagen 27. Salida del comando show vtp status para SW-CC



2.2 CONFIGURACIÓN DE DTP (DYNAMIC TRUNKING PROTOCOL)

a. Configuración de enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace se configura como dynamic desirable.

SW-AA(config)# **interface FastEthernet0/1**
SW-AA(config-if)# **switchport mode trunk**
SW-AA(config-if)# **switchport mode dynamic desirable**

SW-BB(config)# **interface FastEthernet0/1**
SW-BB(config-if)# **switchport mode trunk**

b. Verificación del enlace "trunk" entre SW-AA y SW-BB usando el comando **show interfaces trunk**.

Imagen 28. Salida del comando show interfaces trunk para SW-AA

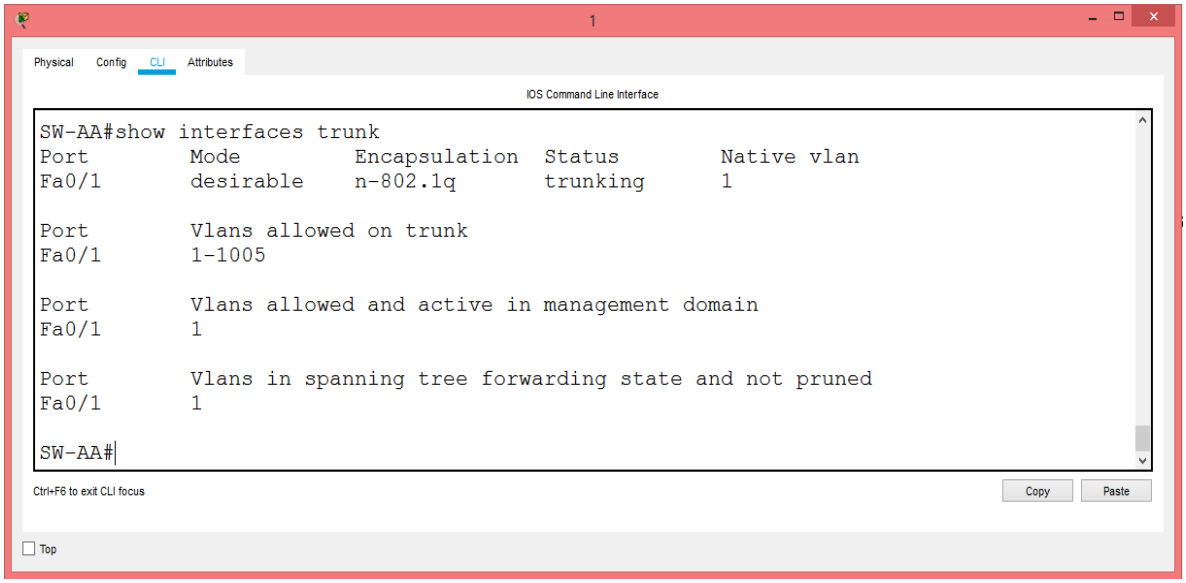
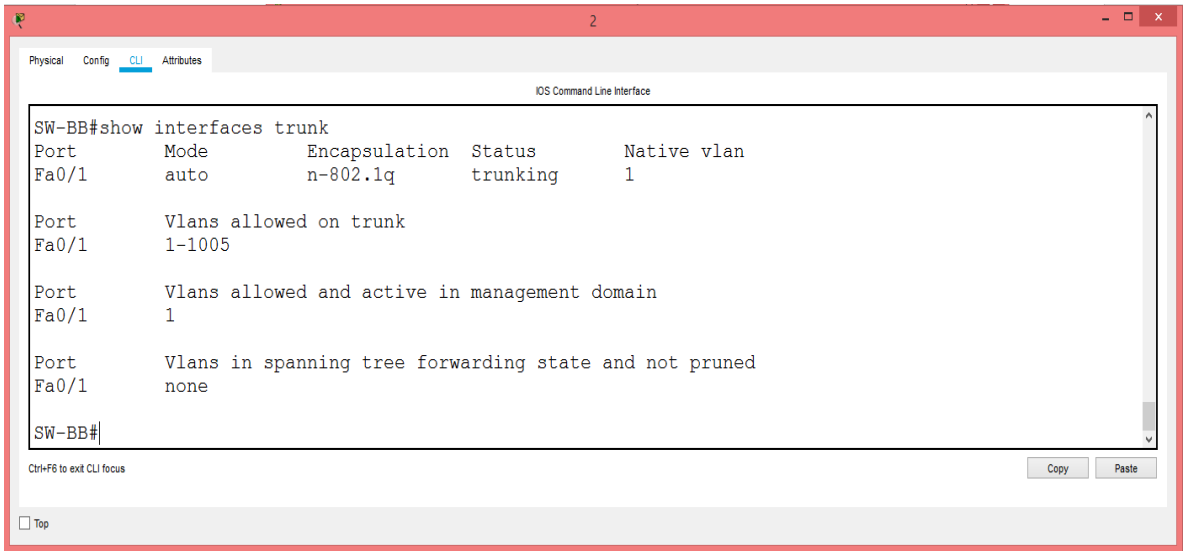


Imagen 29. Salida del comando show interfaces trunk para SW-BB



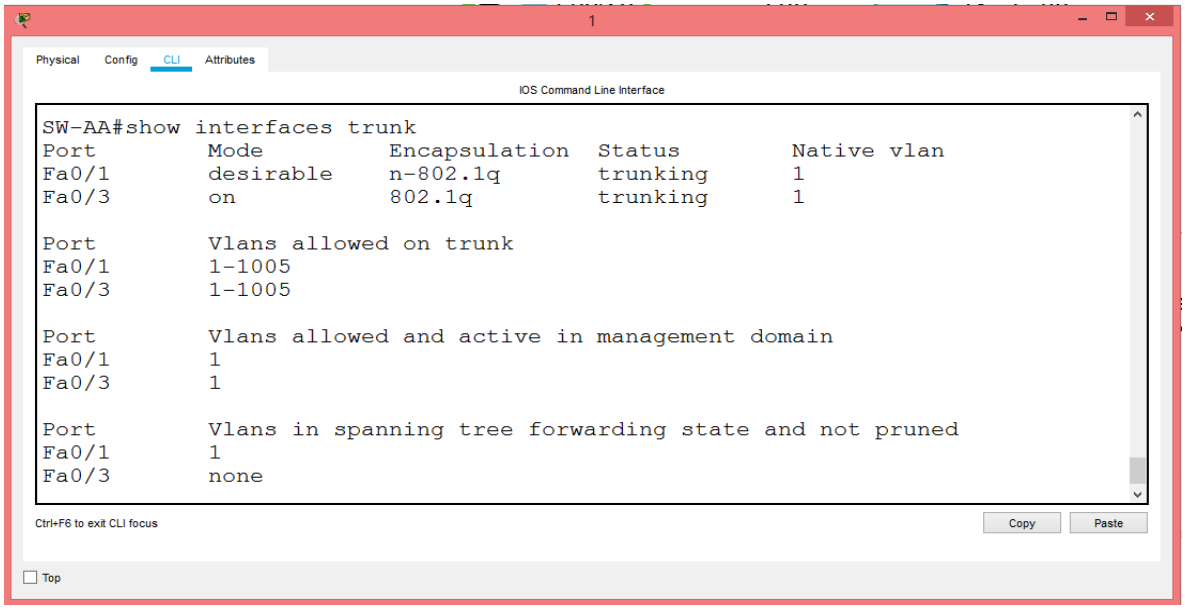
c. Configuración de enlace “trunk” estático entre SW-AA y SW-CC mediante comando **switchport mode trunk** en la interfaz F0/3 de SW-AA.

SW-AA(config)# **interface FastEthernet0/3**
SW-AA(config-if)# **switchport mode trunk**

SW-CC(config)# **interface FastEthernet0/3**
SW-CC(config-if)# **switchport mode trunk**

d. Verificación del enlace "trunk" con el comando **show interfaces trunk** en SW-AA.

Imagen 30. Salida del comando show interfaces trunk para SW-AA



e. Configuración de un enlace "trunk" permanente entre SW-BB y SW-CC.

SW-BB(config)# **interface FastEthernet0/3**
SW-BB(config-if)# **switchport mode trunk**

SW-CC(config)# **interface FastEthernet0/1**
SW-CC(config-if)# **switchport mode trunk**

Imagen 31. Salida del comando show interfaces trunk para SW-BB

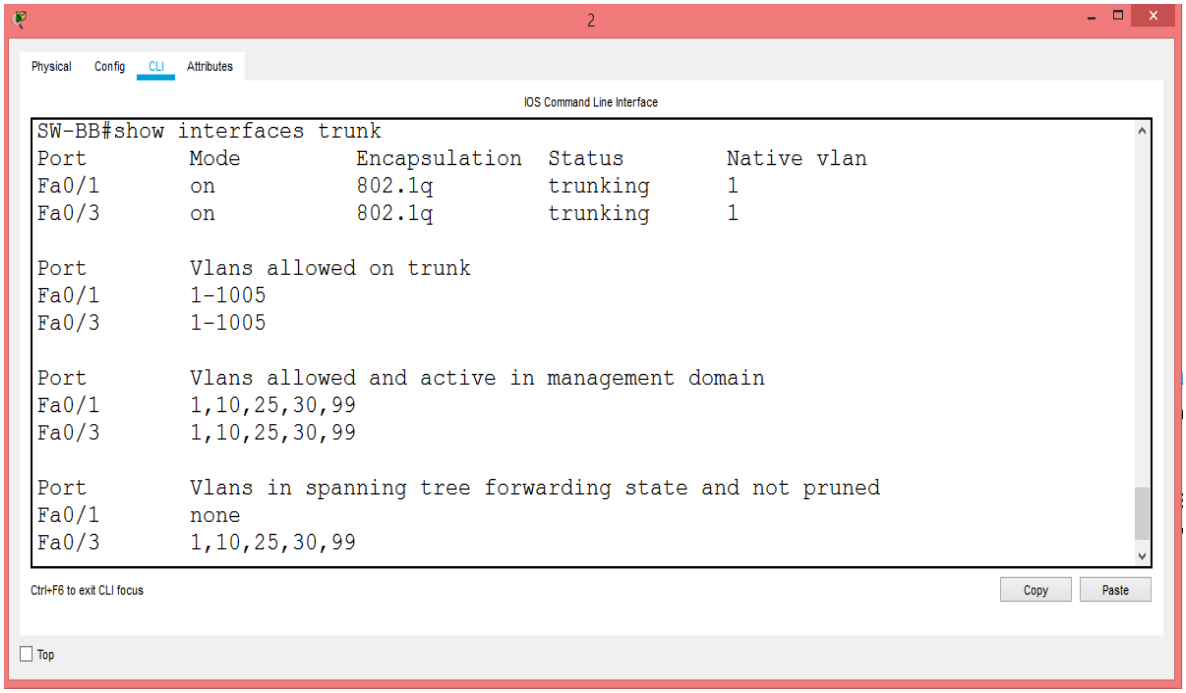
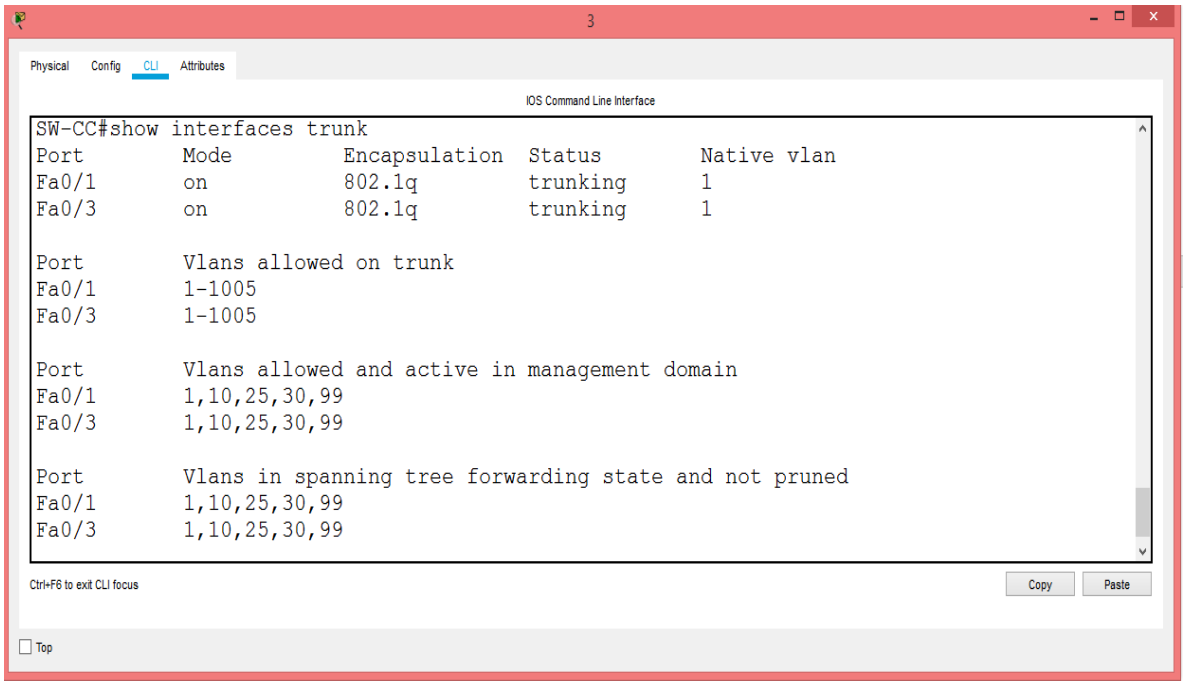


Imagen 32. Salida del comando show interfaces trunk para SW-CC

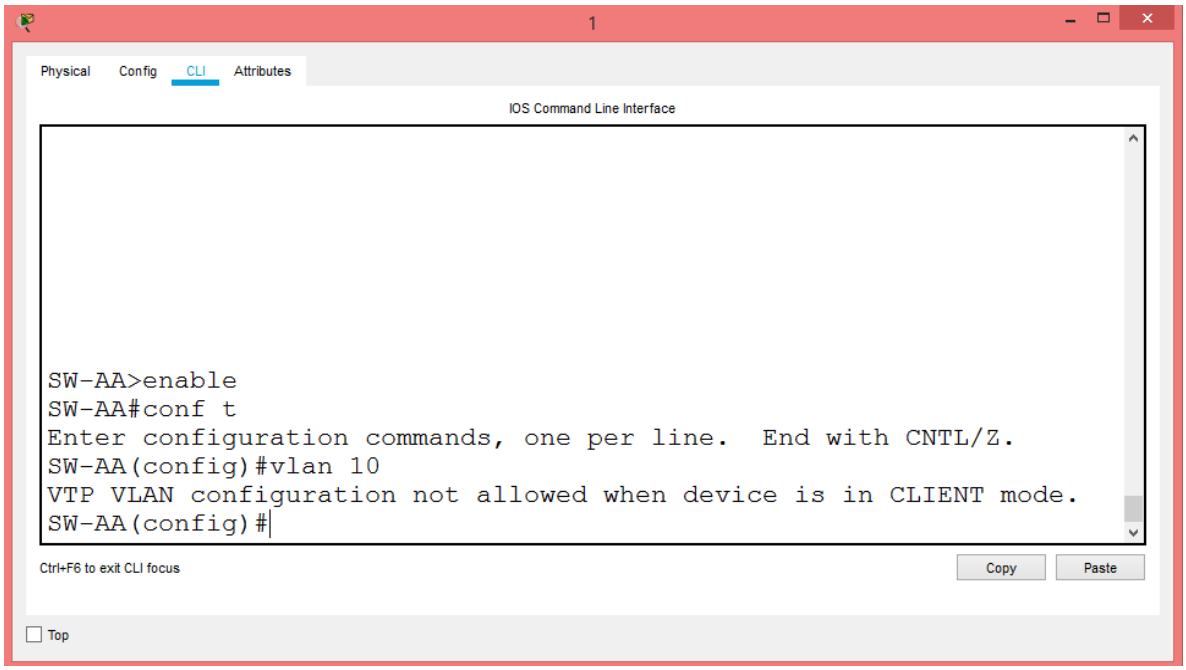


2.3 ASIGNACIÓN DE VLANS y PUERTOS

a. Asignación de VLAN 10 a SW-AA.

En modo cliente no permite creación de VLAN (Ver 2.1, c.).

Imagen 33. Comando no autorizado en SW-AA

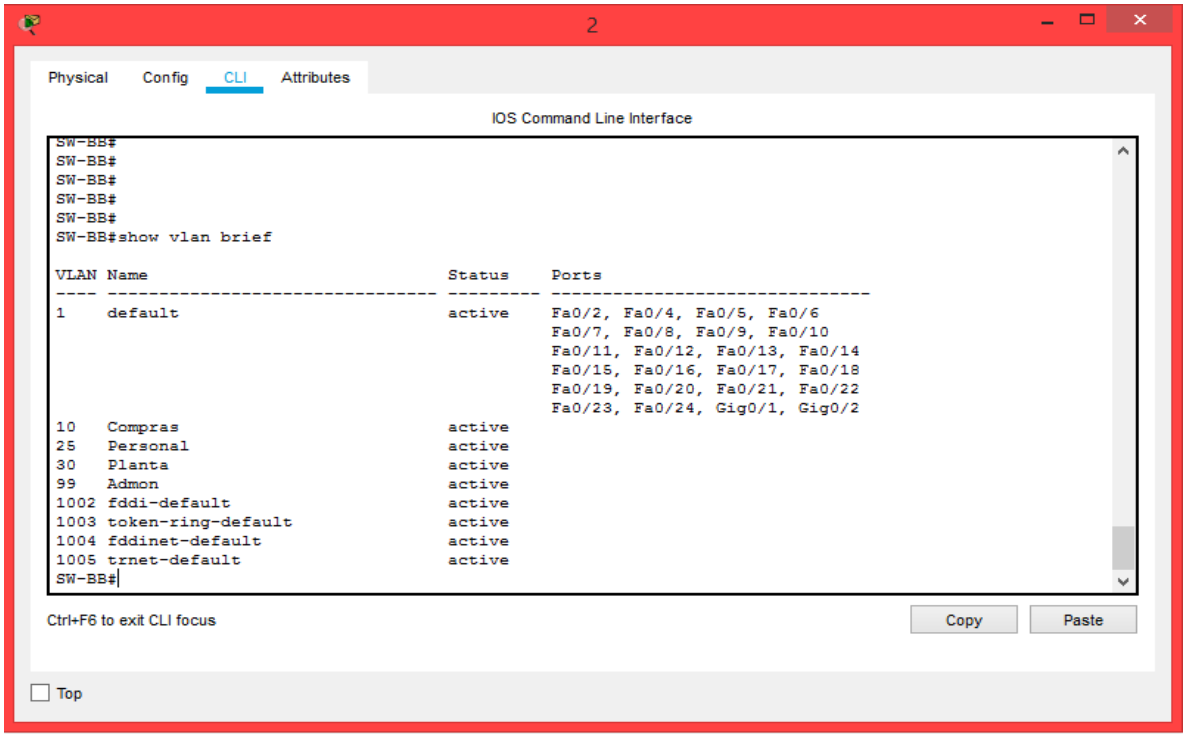


b. Asignación a SW-BB de VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

SW-BB (config)# **vlan 10**
SW-BB (config-vlan)# **name Compras**
SW-BB (config-vlan)# **exit**
SW-BB (config)# **vlan 25**
SW-BB (config-vlan)# **name Personal**
SW-BB (config-vlan)# **exit**
SW-BB (config)# **vlan 30**
SW-BB (config-vlan)# **name Planta**
SW-BB (config-vlan)# **exit**
SW-BB (config)# **vlan 99**
SW-BB (config-vlan)# **name Admon**
SW-BB (config-vlan)# **exit**

c. Verificación de las VLANs agregadas correctamente.

Imagen 34. Salida del comando show vlan brief para SW-BB



d. Asociación de los puertos a las VLAN y configuración de las direcciones IP de acuerdo con la siguiente tabla:

Tabla 2. Información para la asociación de puertos VLAN

SWITCH	INTERFAZ	VLAN	DIRECCIÓN IP	MÁSCARA
SW-AA	F0/10	VLAN 10	190.108.10.1	255.255.255.0
SW-AA	F0/15	VLAN 25	190.108.20.2	255.255.255.0
SW-AA	F0/20	VLAN 30	190.108.30.3	255.255.255.0
SW-BB	F0/10	VLAN 10	190.108.10.4	255.255.255.0
SW-BB	F0/15	VLAN 25	190.108.20.5	255.255.255.0
SW-BB	F0/20	VLAN 30	190.108.30.6	255.255.255.0
SW-CC	F0/10	VLAN 10	190.108.10.7	255.255.255.0
SW-CC	F0/15	VLAN 25	190.108.20.8	255.255.255.0
SW-CC	F0/20	VLAN 30	190.108.30.9	255.255.255.0

e. Configuración del puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asignación a la VLAN 10

SW-AA (configf)# **interface fa0/10**
SW-AA (config-if)# **description PC1**
SW-AA (config-if)# **switchport mode access**
SW-AA (config-if)# **switchport access vlan 10**
SW-AA (config-if)# **no shut**
SW-AA (config-if)# **end**

SW-BB (configf)# **interface fa0/10**
SW-BB (config-if)# **description PC4**
SW-BB (config-if)# **switchport mode access**
SW-BB (config-if)# **switchport access vlan 10**
SW-BB (config-if)# **no shut**
SW-BB (config-if)# **end**

SW-CC (configf)# **interface fa0/10**
SW-CC (config-if)# **description PC7**
SW-CC (config-if)# **switchport mode access**
SW-CC (config-if)# **switchport access vlan 10**
SW-CC (config-if)# **no shut**
SW-CC (config-if)# **end**

f. Configuración de puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC, asignación de las VLANs y las direcciones IP de los PCs de acuerdo con la Tabla 2.

SW-AA (config)# **interface fa0/15**
SW-AA (config-if)# **description PC2**
SW-AA (config-if)# **switchport mode access**
SW-AA (config-if)# **switchport access vlan 25**
SW-AA (config-if)# **no shut**
SW-AA (config-if)# **end**

SW-AA (config)# **interface fa0/20**
SW-AA (config-if)# **description PC3**
SW-AA (config-if)# **switchport mode access**
SW-AA (config-if)# **switchport access vlan 30**
SW-AA (config-if)# **no shut**
SW-AA (config-if)# **end**

SW-BB (config)# **interface fa0/15**
SW-BB (config-if)# **description PC5**
SW-BB (config-if)# **switchport mode access**

SW-BB (config-if)# **switchport access vlan 25**
SW-BB (config-if)# **no shut**
SW-BB (config-if)# **end**

SW-BB (config)# **interface fa0/20**
SW-BB (config-if)# **description PC6**
SW-BB (config-if)# **switchport mode access**
SW-BB (config-if)# **switchport access vlan 30**
SW-BB (config-if)# **no shut**
SW-BB (config-if)# **end**

SW-CC (config)# **interface fa0/15**
SW-CC (config-if)# **description PC8**
SW-CC (config-if)# **switchport mode access**
SW-CC (config-if)# **switchport access vlan 25**
SW-CC (config-if)# **no shut**
SW-CC (config-if)# **end**

SW-CC (config)# **interface fa0/20**
SW-CC (config-if)# **description PC9**
SW-CC (config-if)# **switchport mode access**
SW-CC (config-if)# **switchport access vlan 30**
SW-CC (config-if)# **no shut**
SW-CC (config-if)# **end**

2.4 CONFIGURACIÓN DE DIRECCIONES IP EN LOS SWITCHES

a. Asignación de direcciones IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y activación de la interfaz.

Tabla 3. Información para la asignación de direcciones IP para VLAN

EQUIPO	VLAN	DIRECCIÓN IP	MÁSCARA
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

SW-AA (config)# **interface vlan 99**
SW-AA (config-if)# **ip address 190.108.99.1 255.255.255.0**
SW-AA (config-if)# **no shut**

SW-BB (config)# **interface vlan 99**

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

SW-CC (config)# **interface vlan 99**
SW-CC (config-if)# **ip address 190.108.99.3 255.255.255.0**
SW-CC (config-if)# **no shut**

2.5 VERIFICACIÓN DE LA CONECTIVIDAD EXTREMO A EXTREMO

a. Ejecución de Ping desde cada PC a los demás y explicación de resultados.

Para evitar falsos enlaces, se deshabilitan los puertos no utilizados. El comando es **shutdown** se utiliza con cada interfaz.

Imagen 35. Salida del comando ping para PC1 hacia PC4 y PC7 (VLAN10)

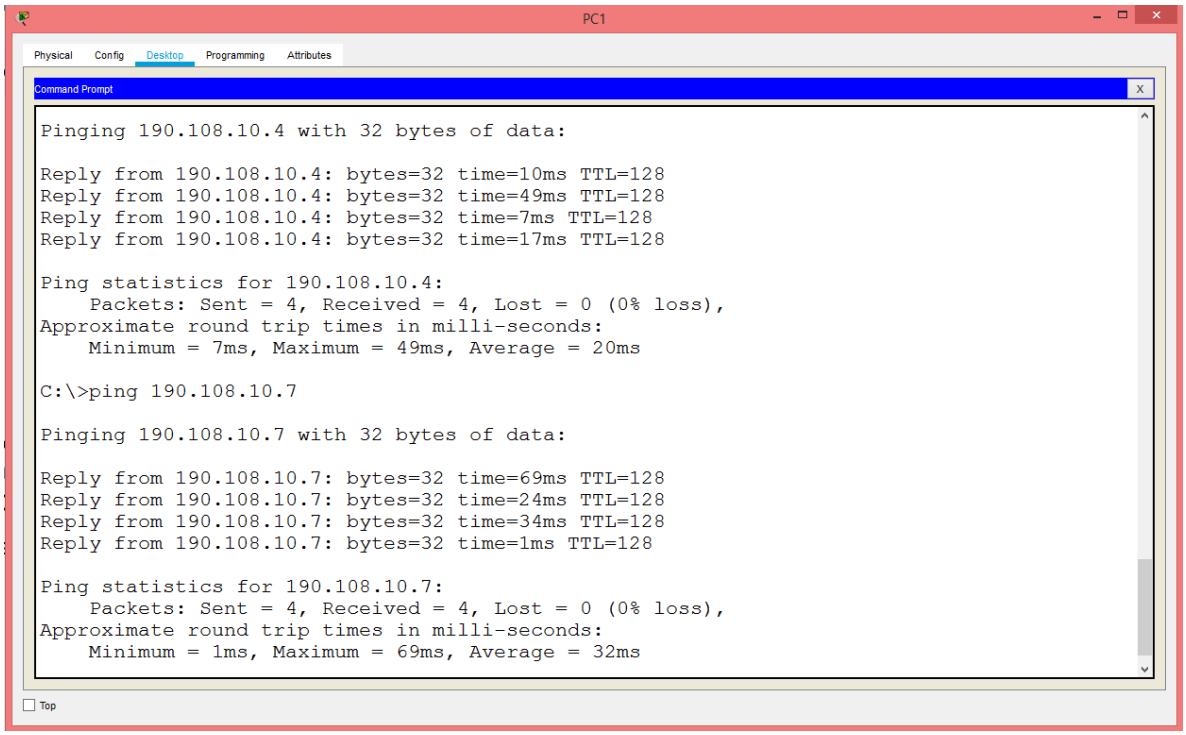


Tabla 4. Resultados de la verificación de conectividad PC-PC

ORIGEN	DESTINO	RESULTADO	EXPLICACIÓN
PC1	PC2	0%	Los casos con 0% son originados por la existencia de dispositivos en diferentes VLAN, ya que los switches impiden la migración de tramas. Los casos con 100% son el resultado de los enlaces troncales configurados, teniendo en cuenta que esta condición facilita la operación de una misma VLAN a través de diferentes switches. PC1, PC4 y PC7 pertenecen a VLAN 10, PC2, PC5 y PC8 a VLAN 25 y PC3, PC6 y PC9 a VLAN 30.
PC1	PC3	0%	
PC1	PC4	100%	
PC1	PC5	0%	
PC1	PC6	0%	
PC1	PC7	100%	
PC1	PC8	0%	
PC1	PC9	0%	
PC2	PC3	0%	
PC2	PC4	0%	
PC2	PC5	100%	
PC2	PC6	0%	
PC2	PC7	100%	
PC2	PC8	0%	
PC2	PC9	0%	
PC3	PC4	0%	
PC3	PC5	0%	
PC3	PC6	100%	
PC3	PC7	0%	
PC3	PC8	0%	
PC3	PC9	100%	
PC4	PC5	0%	
PC4	PC6	0%	
PC4	PC7	100%	
PC4	PC8	0%	
PC4	PC9	0%	
PC5	PC6	0%	
PC5	PC7	0%	
PC5	PC8	100%	
PC5	PC9	0%	
PC6	PC7	0%	
PC6	PC8	0%	
PC6	PC9	100%	
PC7	PC8	0%	
PC7	PC9	0%	
PC8	PC9	0%	
PC8	PC9	0%	

Imagen 36. Salida del comando ping para PC2 hacia PC5 y PC8 (VLAN 25)

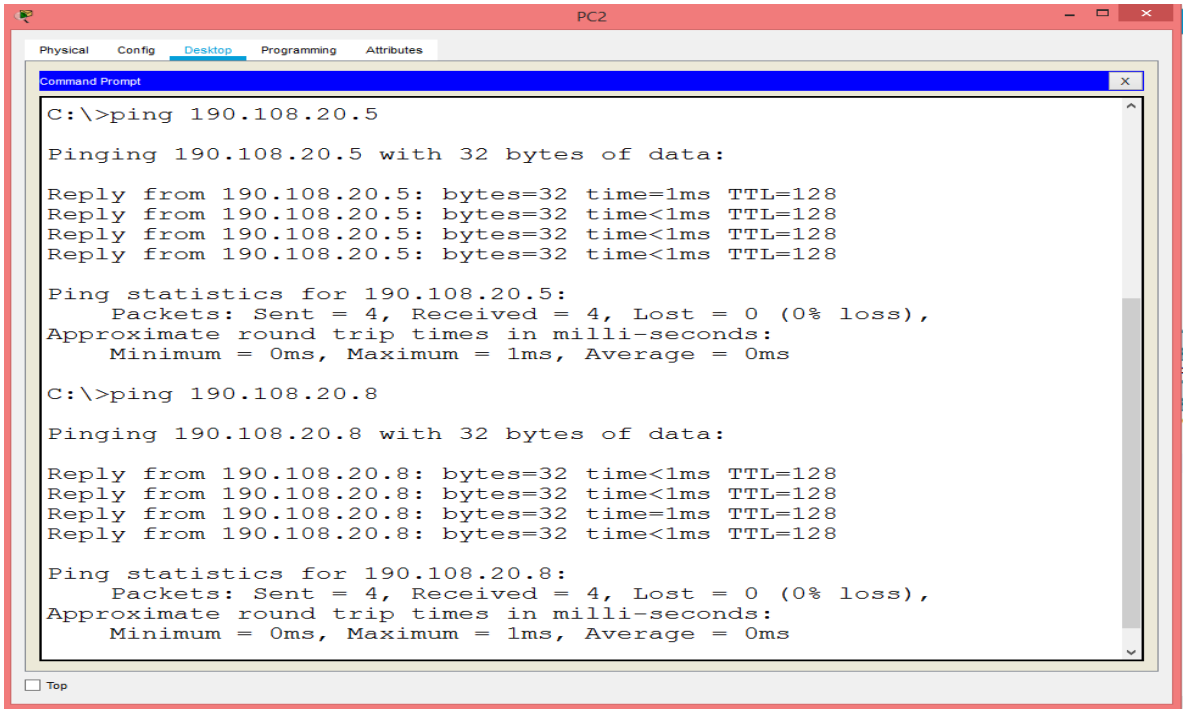


Imagen 37. Salida del comando ping para PC3 hacia PC6 y PC9 (VLAN 30)

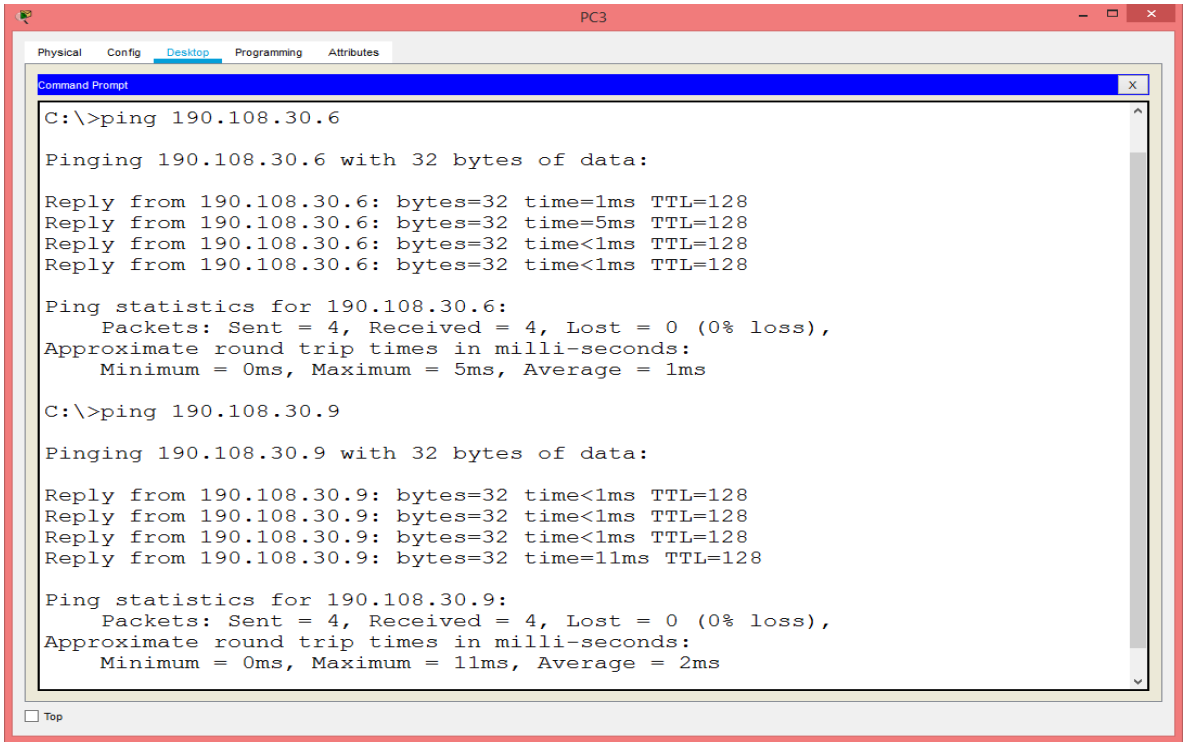
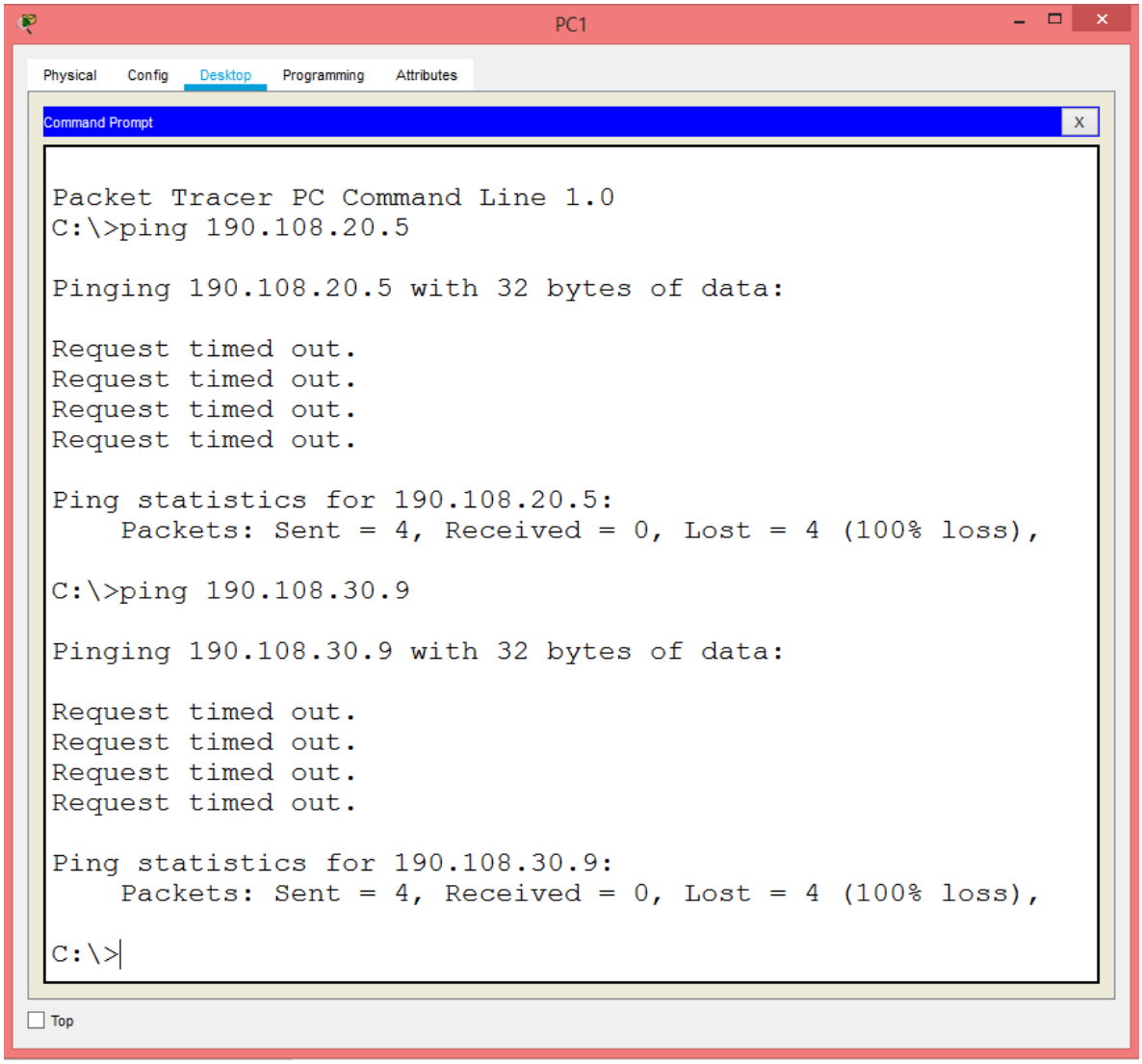


Imagen 38. Salida del comando ping para PC1 (VLAN 10) hacia PC5 (VLAN 25) y PC9 (VLAN 30)



b. Ejecución de Ping desde cada Switch a los demás y explicación de resultados.

Tabla 5. Resultados de la verificación de conectividad SW-SW

ORIGEN	DESTINO	RESULTADO	EXPLICACIÓN
SW-AA	SW-BB	100%	Son dispositivos configurados con la Misma VLAN (VLAN 99), cada switch tiene asociada una IP particular a la VLAN con la cual se identifica el origen / destino dentro de la estructura de las tramas que transitan en la red y además hay enlaces troncales configurados para comunicación entre los dispositivos.
SW-AA	SW-CC	100%	
SW-BB	SW-CC	100%	
SW-BB	SW-CC	100%	

Imagen 39. Salida del comando ping para SW-AA hacia SW-BB y SW-CC

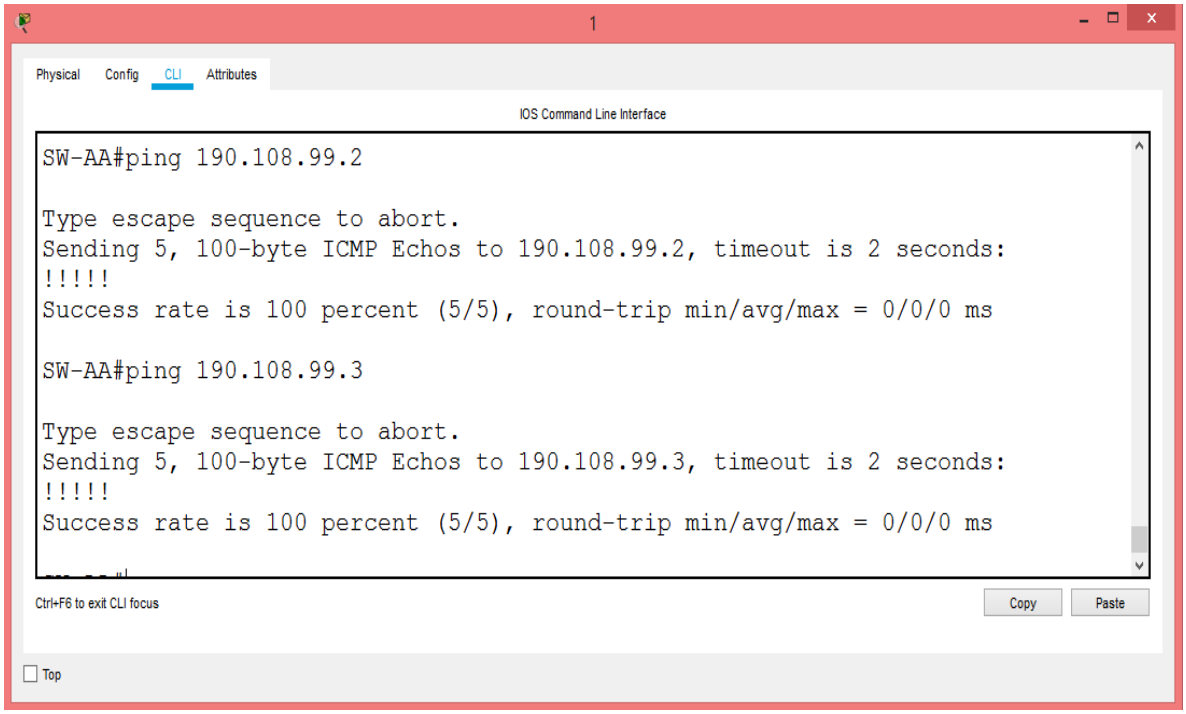


Imagen 40. Salida del comando ping para SW-BB hacia SW-AA y SW-CC

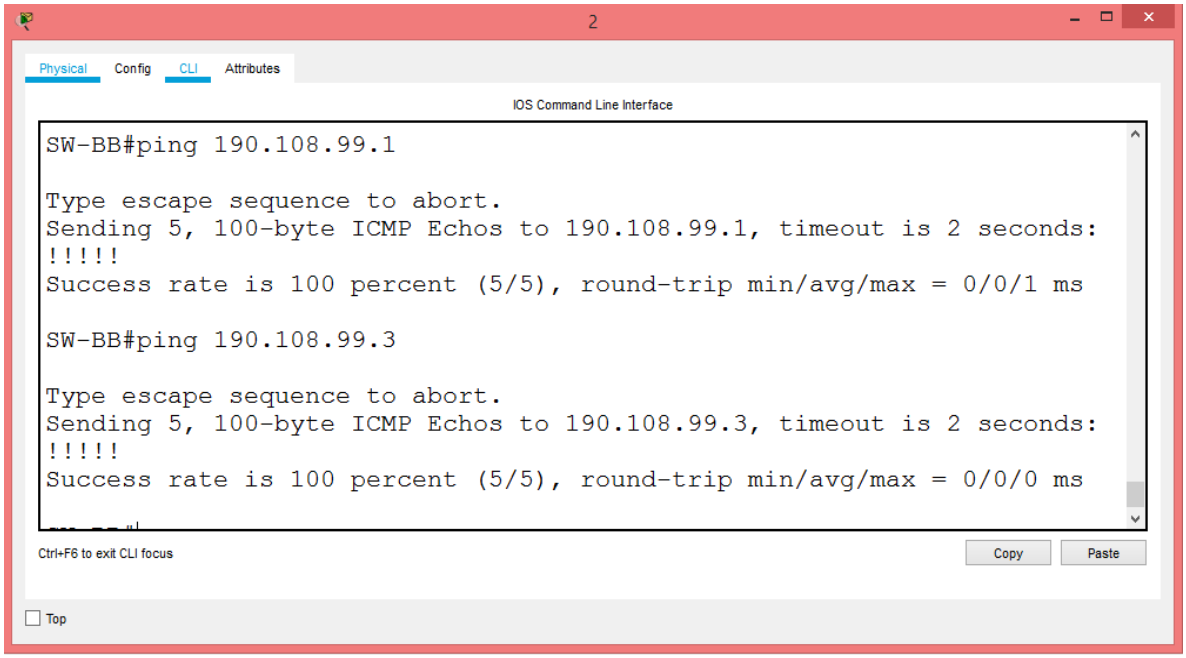
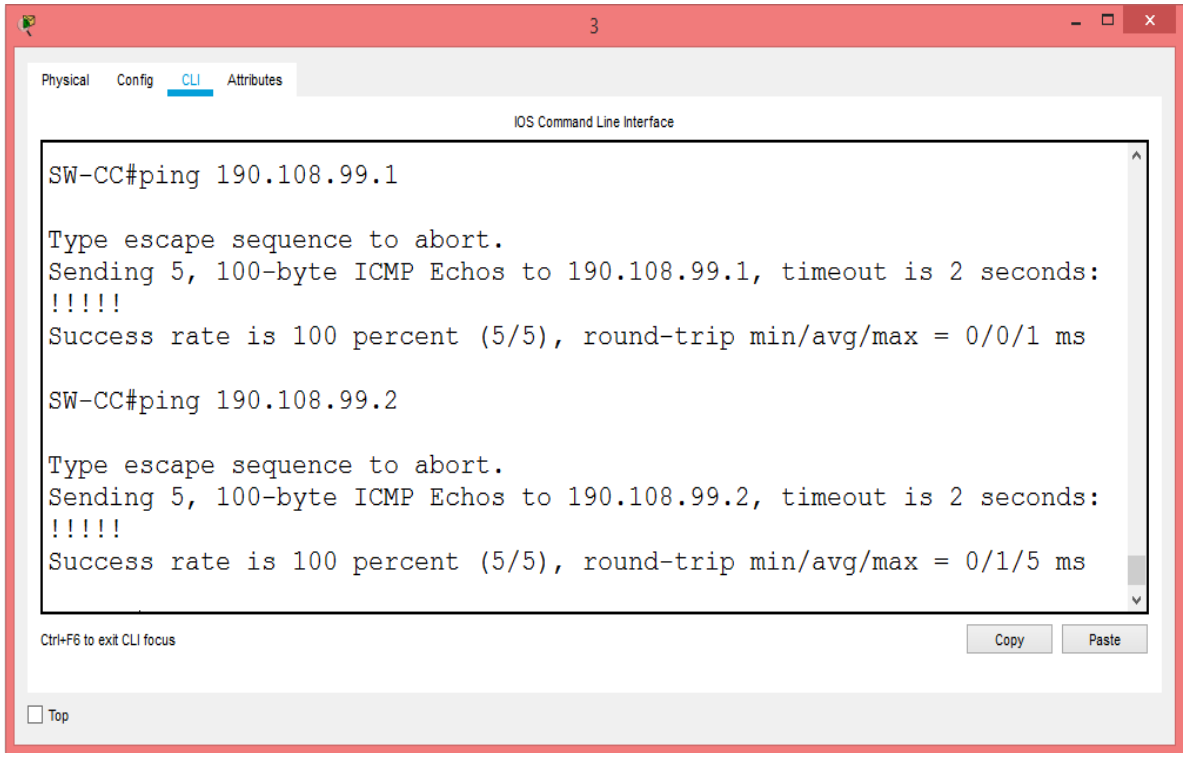


Imagen 41. Salida del comando ping para SW-CC hacia SW-AA y SW-BB



c. Ejecución de Ping desde cada Switch a cada PC y explicación de resultados.

Imagen 42. Salida del comando ping para SW-AA (VLAN 99) hacia PC1 (VLAN 10), PC5 (VLAN 25) y PC9 (VLAN 30)

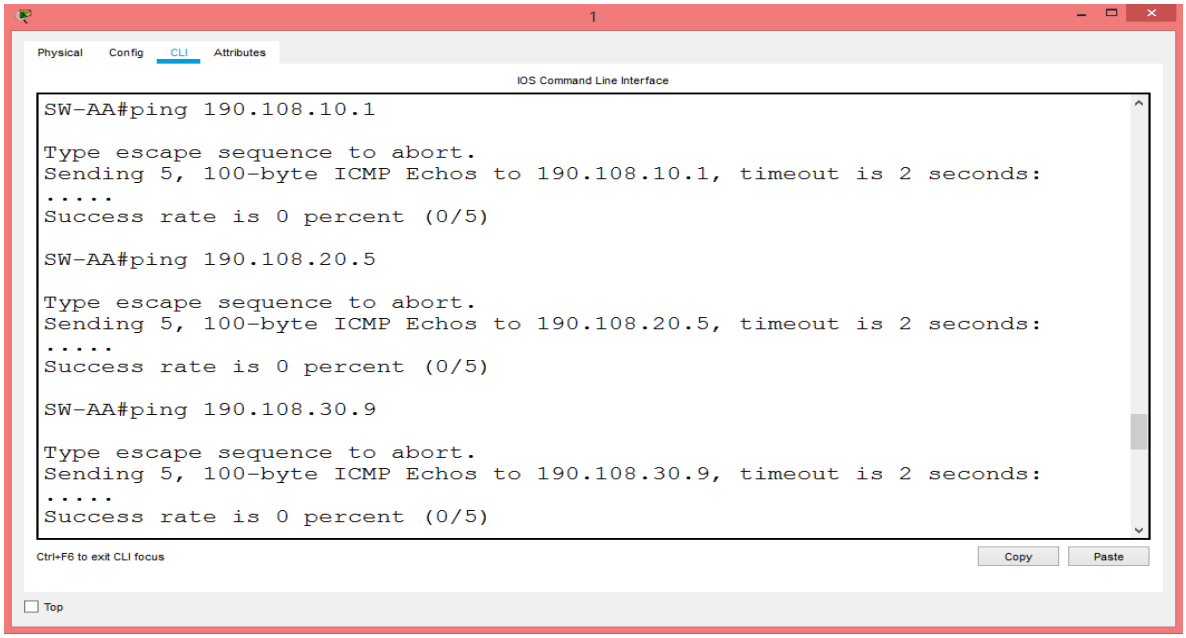


Imagen 43. Salida del comando ping para SW-BB (VLAN 99) hacia PC7 (VLAN 10), PC2 (VLAN 25) y PC6 (VLAN 30)

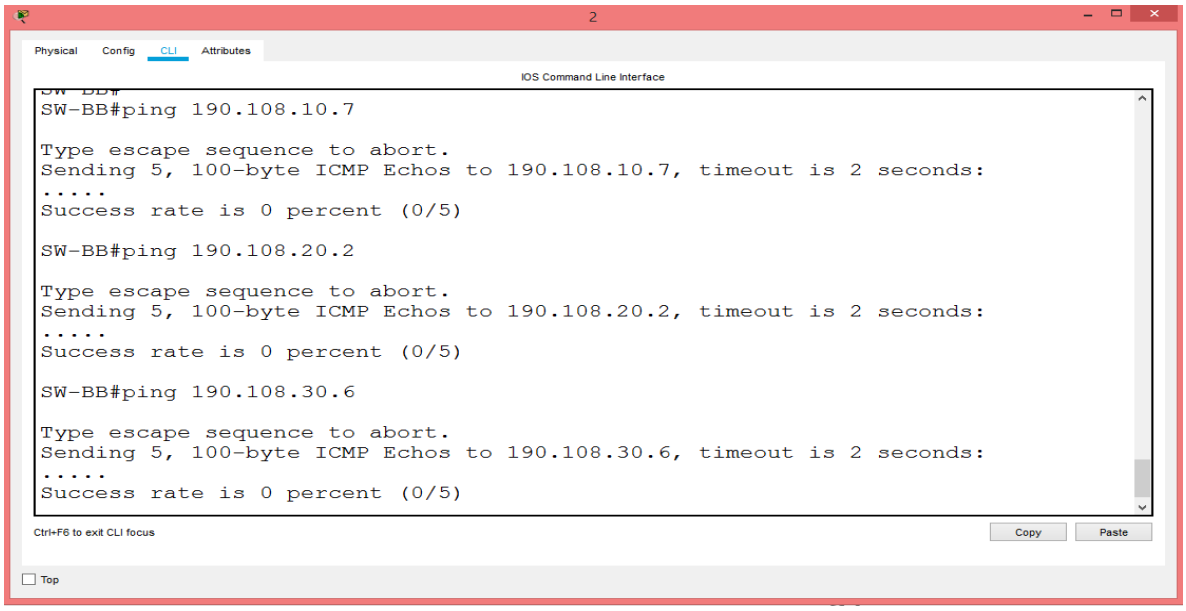


Imagen 44. Salida del comando ping para SW-CC (VLAN 99) hacia PC4 (VLAN 10), PC8 (VLAN 25) y PC3 (VLAN 30)

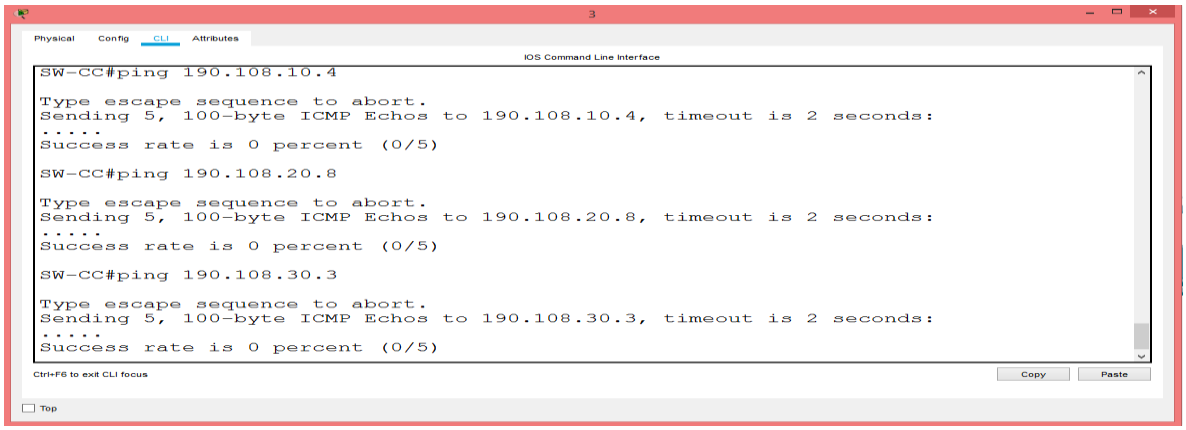


Tabla 6. Resultados de la verificación de conectividad SW-PC

ORIGEN	DESTINO	RESULTADO	EXPLICACIÓN
SW-AA	PC1	0%	
SW-AA	PC2	0%	
SW-AA	PC3	0%	
SW-AA	PC4	0%	
SW-AA	PC5	0%	
SW-AA	PC6	0%	La conmutación se realiza entre dispositivos que cuentan con una IP y están asociados a una VLAN común. En este caso particular, los switches tienen asociada la misma VLAN, que es diferente a las de los PC, por lo que se impide la migración de tramas dando como resultado la imposibilidad de establecer comunicación.
SW-AA	PC7	0%	
SW-AA	PC8	0%	
SW-AA	PC9	0%	
SW-BB	PC1	0%	
SW-BB	PC2	0%	
SW-BB	PC3	0%	
SW-BB	PC4	0%	
SW-BB	PC5	0%	
SW-BB	PC6	0%	
SW-BB	PC7	0%	
SW-BB	PC8	0%	
SW-BB	PC9	0%	
SW-CC	PC1	0%	
SW-CC	PC2	0%	
SW-CC	PC3	0%	
SW-CC	PC4	0%	
SW-CC	PC5	0%	
SW-CC	PC6	0%	
SW-CC	PC7	0%	
SW-CC	PC8	0%	
SW-CC	PC9	0%	

3. CONCLUSIONES

El Protocolo de Puerta de Frontera (Border Gateway Protocol – BGP), fue desarrollado para facilitar el intercambio de datos de enrutamiento y la identificación de opciones de envió de datos entre dispositivos ubicados en diferentes Sistemas Autónomos, es decir aquellos que se encuentran administrados de manera común a través de un mismo dominio. Facilita el intercambio de datos de enrutamiento entre dispositivos del mismo sistema autónomo (IBGP) o entre elementos de sistemas autónomos diferente (EBGP), esta última en preferencia relacionada con la Internet. Una vez el dispositivo ha sido enlazado para el intercambio de datos, pasa a ser reconocido como “vecino”.

La configuración de BGP se basa en términos generales en tres pasos: definir el proceso BGP a través del comando **router bgp** + (AS), establecer las relaciones entre vecinos mediante el comando **neighbor** + (dirección IP) + **remote-as** + (AS), el anuncio de las redes dentro del proceso BGP mediante el comando **network** + (dirección IP) **mask** + (máscara de subred), y finalmente la generación de rutas estáticas para evitar el uso de protocolos adicionales.

El Protocolo para VLAN Troncales (VLAN Trunking Protocol – VTP), fue creado específicamente para la gestión de VLANs, es decir, permite la creación, eliminación, cambio de nombre y sincronización; para lo cual un switch debe actuar en modo servidor (o transparente pera el caso de las VLANs locales). También son un requisito indispensable el nombre del dominio y la clave.

Es una característica particular de los switches la de compartir difusiones únicamente a través de puertos configurados en la Misma VLAN, lo que genera la necesidad de utilizar un router o dispositivo de capa 3 en caso de requerir comunicación entre dispositivos ubicados en diferentes VLANs.

La combinación de modos DTP de dos puertos da como resultado un estado permanente en modo **access port** o en modo **trunk port**. El primero representa un enlace no troncal para comunicación entre anfitrión – switch lo que sirve como canal de comunicación entre dispositivos asignados a la misma VLAN, y el segundo un enlace troncal para comunicación switch – switch para compartir información de las VLANs y definir el puerto de salida / entrada de las tramas.

BIBLIOGRAFÍA

FROOM, Richard. Y FRAHIM, Erum. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide – CCNP SWITCH 300-115. Indianapolis: CISCO Press, 2015. 785 p. Disponible en internet en (https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ)

GALLO, Michael A. y WILLIAM M. Hancock. Comunicación entre computadoras y tecnologías de redes, Cengage Learning, México D.F.: Thomson Learning. 2002. pp. 587 - 615. Disponible en (https://link-gale-com.bibliotecavirtual.unad.edu.co/apps/doc/CX4059900020/GVRL?u=unad&sid=GVRL&xid=a7f103a8).

GRAZIANI, Rich., TEARE, Diane., y VACHON, Bob. Implementing Cisco IP Routing (ROUTE) - Foundation Learning Guide – CCNP ROUTE 300-101. Indianapolis: CISCO Press, 2015. 726 p. Disponible en internet en (https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx).