SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGIA CISCO

JEISSON EMMANUEL ALARCÓN CÁRDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA- ECBTI

INGENIERIA SISTEMAS

2021

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGIA CISCO

JEISSON EMMANUEL ALARCÓN CÁRDENAS

Diplomado de opción de grado para optar el título de INGENIERO DE SISTEMAS

DIRECTOR

RAUL BAREÑO GUITIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA- ECBTI

INGENIERIA SISTEMAS

2021

NOTA DE ACEPTACIÓN

Firma de presidente de Jurado

Firma del jurado

Firma del jurado

Sogamoso, 29 de noviembre de 2021

AGRADECIMIENTOS

Primero que todo quiero agradecer a Dios y a la vida por tener la oportunidad de empezar un camino lleno de conocimientos y experiencias en la cuales ayudaran en mi futuro profesional.

De corazón agradezco a mi familia y amigos por darme apoyo en momentos difíciles teniendo paciencia y las palabras adecuadas en circunstancias llenas de dificultad para lograr seguir con mi meta propuesta y dar cumplimiento a cabalidad de cada requisito para ser un profesional

Por último, agradecerle al Ingeniero Raúl Gutiérrez quien con todo su conocimiento logrado durante la vida me dio la mejor guía, apoyo, enseñanza para dar solución a este trabajo de diplomado como opción de grado y a la universidad UNAD por brindarme esta gran oportunidad ofreciendo las guías y recursos para alimentar mis conocimientos.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Interfaz de red: Es el software de la red el cual nos ayuda en la comunicación del dispositivo de red con la capa de direccionamiento y así ingresar la información debida del direccionamiento tanto en routers, switch o equipos de cómputo.

Direccionamiento IP: Los equipos y redes que funcionan mediante el protocolo TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet)**.** Este protocolo necesita para su funcionamiento que los equipos que funcionan con él tengan dos parámetros configurados en su interfaz de red, estos son la dirección IP y la máscara de subred.

Gateway: puerta de enlace o pasarela, es un dispositivo dentro de una red de comunicaciones, que permite a través de sí mismo, acceder a otra red. En otras palabras, sirve de enlace entre dos redes con protocolos y arquitecturas diferentes.

Encriptación: Es una manera de codificar la información y así lograr protegerla de terceros.

VTY: Se trata de un conjunto de puertos virtuales utilizados para la conexión vía telnet, ssh o http al dispositivo para realizar administración o configuración remota.

RESUMEN

El presente proyecto tiene el fin de dar solución a dos Escenarios, donde se debe implementar redes funcionales, la cual se debe redistribuir por subredes para eso es esencial la máscara para así determinar las IP funcionales con su respectivo broadcast de red. Ya teniendo la distribución de direccionamiento se debe realizar el enrutamiento para que se genere una conectividad adecuada en cada componente de la topología.

Cada equipo debe responder, es decir debe existir una conmutación entre los equipos donde extremo a extremo de la red realizan la interacción de paquetes para eso debe existir un emisor y el receptor. Cada procedimiento y protocolos realizados fueron dados a conocer mediante la plataforma cisco esto con el fin de ser certificado como Profesional de redes cisco (CCNA).

Palabras claves: CISCO, CCNA, conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The present project has the purpose of solving two Scenarios, where functional networks must be implemented, which must be redistributed by subnets, for that the mask is essential to determine the functional IPs with their respective network broadcast. Already having the addressing distribution, the routing must be performed so that adequate connectivity is generated in each component of the topology.

Each team must respond, that is, there must be a switch between the teams where end-to-end of the network perform packet interaction, for that there must be a sender and a receiver. Each procedure and protocols performed were made known through the Cisco platform in order to be certified as a Cisco Network Associate (CCNA).

Keywords: CISCO, CCNA, switching, Routing, Networks, Electronics.

INTRODUCCION

En este documento encontraremos la propuesta final para dar cumplimiento y desarrollo al diplomado cisco CCNA, donde se comprendió el direccionamiento, tipo de clasificación de las redes, distribución de subredes y los beneficios. Como configurar adecuadamente Routers, switches, computadores, conexión adecuada mediane los cables UTP y sus respectivos conectores Rj45 entre otros factores esenciales en la red.

En el escenario 1 es una topología compuesta por 1 Router, 1 switch y 2 equipos de cómputo, los cuales se determina las subredes teniendo en cuenta la red 192.168.7.0 donde en la red 1 debe permitir el ingreso a 100 equipos y en la red 2 50 host. Ya después se determina la dirección IP de cada componente de la topología ipv4 finalmente realizando la configuración del Router en cada interfaz y su respectiva comprobación de conectividad. Es importante que la IP, mascara y Gateway si lo requiere estén adecuados sino no va a responder.

Ya en el Escenario 2 la cual es una topología compuesta por 3 Router conectador por interfaz Serial, 2 computadores, 3 Switch, 1 servidor y además se crean interfaz lógicas llamadas Loopback, se realiza varias distribuciones de direccionamiento tanto IPv4 e IPv6. Se realiza sus respectivos apuntamientos donde se complementa con Rutas predeterminadas para que realice el salto adecuado y reconozca el equipo siguiente.

Después se configura la seguridad de la red donde se crea bases de datos de VLAN realizando las respectivas configuraciones de troncalización y de acceso, Además se asignan a los interfaces indicados las VLAN en este caso trabajamos con la VLAN 21,23 Y 99, donde se crean subinterfaces para que se haga una distribución por un mismo puerto o interfaz físico en este caso el G0/1. Se comprueba conectividad todo responde adecuadamente.

Luego para implementar más conectividad en la red se implementa Routing Dinámico OSPF e implementando apuntamiento NAT para un servidor.

DESARROLLO

1. ESCENARIO 1

Topología

Figura 1. Topología propuesta

Fuente: Propia

Parte 1: Construya la red

Figura 2. Topología en packet tracert

Fuente: Propia

Parte 2: Desarrolle el esquema de direccionamiento IP

Tabla 1. Tabla de subredes

Numero de subred	Cantidad host requeridos	IP de subred	Primera IP	Ultima IP	Broadcast
0	100	192.168.7.0/ 25	192.168.7.1	192.168.7.126	192.168.7.127
1	50	192.168.7.128/ 26	192.168.7.129	192.168.7.190	192.168.7.191

Fuente: Propia

Se tiene la IP 192.168.7.0/ 24 un direccionamiento de clase c en la cual los 3 primeros octetos son usados para la red y el octeto restante para los hosts, se

determina como subred para 100 host la 255.255.255.128 y para la subred de 50 host la 255.255.255.192. ya determinado se procede a determinar la ip de subred con su respectivas ip funcionales y el broadcast como se muestra en la Tabla 1.

Tabla 2. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0/0	192.168.7.129	255.255.255.192	NO APLICA
	G0/0/1	192.168.7.1	255.255.255.128	NO APLICA
S1	VLAN 1	192.168.7.2	255.255.255.128	192.168.7.1
PC-A	NIC	192.168.7.126	255.255.255.128	192.168.7.1
PC-B	NIC	192.168.7.190	255.255.255.192	192.168.7.129

Fuente: Propia

Parte 3: Configure aspectos básicos

Paso 1: Configurar los aspectos básicos

Se procede a ingresar al R1 por medio de la consola del PC-B

Se realiza la configuración básica del R1 donde desactivamos búsqueda DNS, cambiamos nombre, asignamos claves para ingreso y las encriptamos adicional se procede asignar los direccionamientos a cada puerto.

Tabla 3. Configuración R1

Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo configuración
Router(config)#no ip domain-lookup	Desactivar búsqueda DNS
Router(config)#hostname R1	Asignar nombre del Router
R1(config)#ip domain-name ccna-lab.com	Asignar nombre dominio
R1(config)#enable secret ciscoenpass	Contraseña cifrada de modo privilegiado
R1(config)#line con 0	Ingreso a configuración Consola
R1(config-line)#password ciscoconpass	Asignación de contraseña
R1(config-line)#login	Cargar acceso
R1(config-line)#exit	Salir de configuración consola
R1(config)#security passwords min-length 10	Establece longitud mínima para las contraseñas
R1(config)#username admin password admin1pass	Se asigna a la base de datos el usuario y contraseña

R1(config)#line vty 0 4	Ingreso a la configuración de las líneas VTY de la 0 a la 4
R1(config-line)#password ciscocisco	Asignación de contraseña
R1(config-line)# login local	Asignación de acceso local
R1(config-line)#transport input ssh	Permitir ingreso solo por ssh
R1(config-line)#exit	Salida de configuración VTY
R1(config)#service password-encryption	Encripta todas las contraseñas actuales y futuras
R1(config)#banner motd # El acceso no autorizado puede contraer sanciones judiciales #	Mensaje de aviso al ingreso
R1(config)#interface g0/0/0	Ingreso al interfaz Gigabitethernet 0/0/0
R1(config-if)#ip address 192.168.7.129 255.255.255.192	Asignación de IP y mascara
R1(config-if)#description Interfaz LAN2	Asignación de descripción del puerto
R1(config-if)#no shutdown	Activación del interfaz
R1(config)#interface g0/0/1	Ingreso interfaz GigabitEthernet 0/0/1
R1(config-if)#ip address 192.168.7.1 255.255.255.128	Asignación de IP y mascara al interfaz g0/0/1
R1(config-if)#description Interfaz LAN1	Descripción de puerto o interfaz
R1(config-if)#NO SHUTDOWN R1(config)#ip domain name ccna-lab.com	Activar interfaz Se realiza llamado del dominio
R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.	Generar clave de cifrado RSA
How many bits in the modulus [512]: 1024	Asignación de modulo
R1#copy running-config startup-config Destination filename [startup-config]?	Guardar configuración en la NVRAM.

Fuente: Propia

Figura 3. Sh ip route- R1

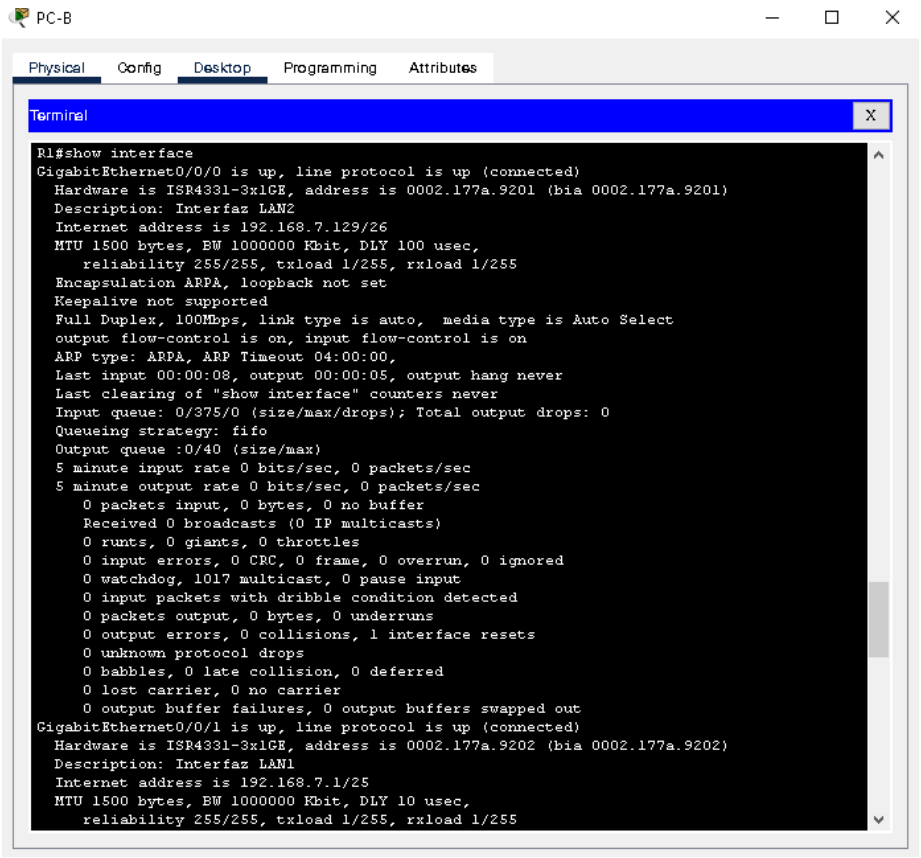
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP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

Gateway of last resort is not set

     192.168.7.0/24 is variably subnetted, 4 subnets, 3 masks
C       192.168.7.0/25 is directly connected, GigabitEthernet0/0/1
L       192.168.7.1/32 is directly connected, GigabitEthernet0/0/1
C       192.168.7.128/26 is directly connected, GigabitEthernet0/0/0
L       192.168.7.129/32 is directly connected, GigabitEthernet0/0/0
```

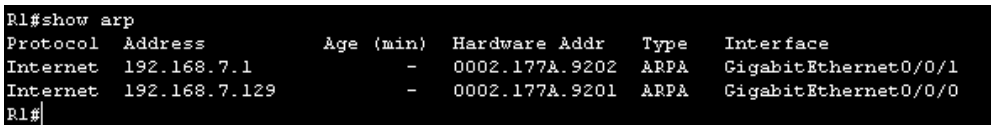
Fuente: Propia

Figura 4. Show interface- R1



Fuente: Propia

Figura 5. Show arp- R1



Fuente: Propia

Se procede a ingresar al S1 por medio de consola por el PC-A

Se procede a realizar la configuración básica del S1 donde cambiamos el nombre, se desactiva búsqueda DNS, se aplica contraseñas de ingreso y se encriptan además se asigna la IP de Vlan1.

Tabla 4. Configuración S1

Switch>enable	Ingreso al modo privilegiado
Switch#configure terminal	Ingreso al modo configuración
Switch(config)#no ip domain-lookup	Desactivar búsqueda DNS
Switch(config)#hostname S1	Asignar nombre
S1(config)#ip domain-name ccna-lab.com	Nombre del dominio
S1(config)#enable secret ciscoenpass	Contraseña de modo privilegiado
S1(config)#line con 0	Ingreso a línea de consola
S1(config-line)#password ciscoconpass	Asignación de contraseña
S1(config-line)#login	Permitir acceso
S1(config-line)#exit	Salida de línea de consola
S1(config)#username admin password admin1pass	Creación de usuario y contraseña
S1(config)#line vty 0 15	Ingreso a las líneas VTY
S1(config-line)#password ciscocisco	Asignación de contraseña
S1(config-line)#login local	Asignación de acceso local
S1(config-line)#transport input ssh	Permitir ingreso solo por ssh
S1(config-line)#exit	Salida de VTY
S1(config)#service password-encryption	Encriptar todas las contraseñas actuales y futuras
S1(config)#banner motd # El acceso no autorizado puede contraer perjuicios judiciales #	Mensaje de ingreso
S1(config)#ip domain name ccna-lab.com	Llamado del dominio
S1(config)#crypto key generate rsa	Activación de cifrado RSA
How many bits in the modulus [512]: 1024	Asignación modulo
S1(config)#interface vlan1	Ingreso a la interfaz virtual

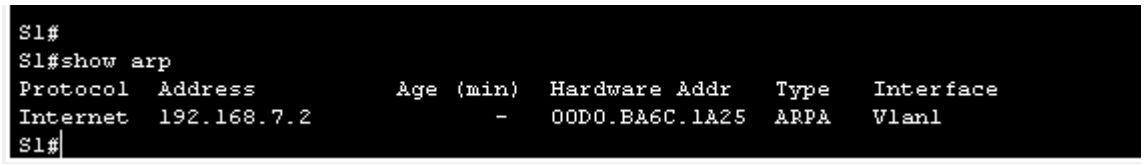
S1(config-if)#ip address 192.168.7.2 255.255.255.128	Asignación de IP y mascara
S1(config-if)#ip default-gateway 192.168.7.1	Asignación de Gateway
S1(config-if)#no shutdown	Activación de interfaz
S1#copy running-config startup-config Destination filename [startup-config]? Building configuration...	Guardar la configuración actual en la NVRAM.

Fuente: Propia

Figura 6. Sh interface vlan 1en S1

Fuente: Propia

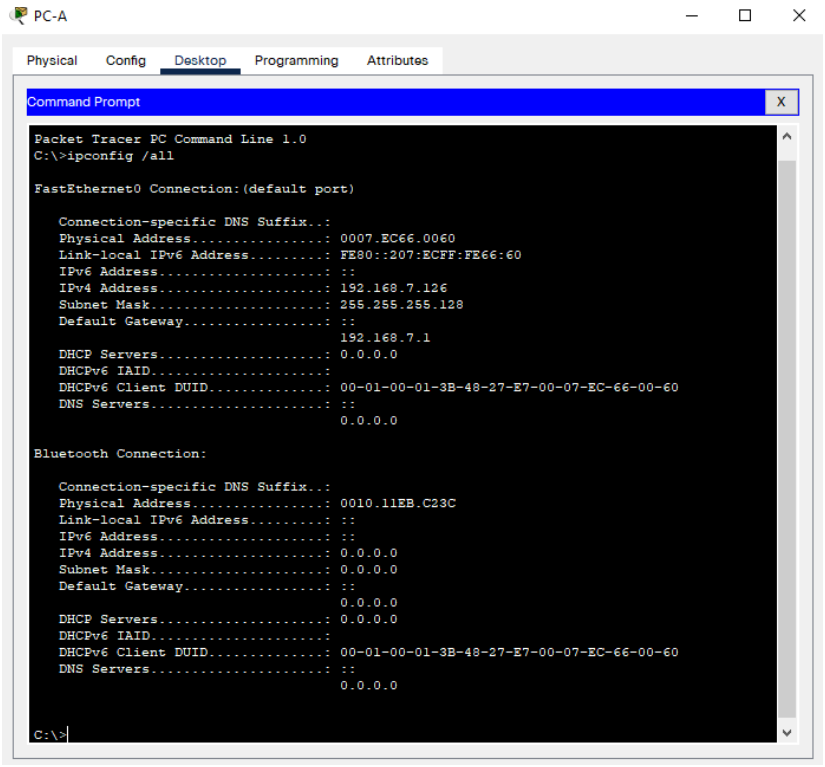
Figura 7. Show arp en S1



Fuente: Propia

Paso 2: Configurar los equipos

Figura 8. Configuración PC-A



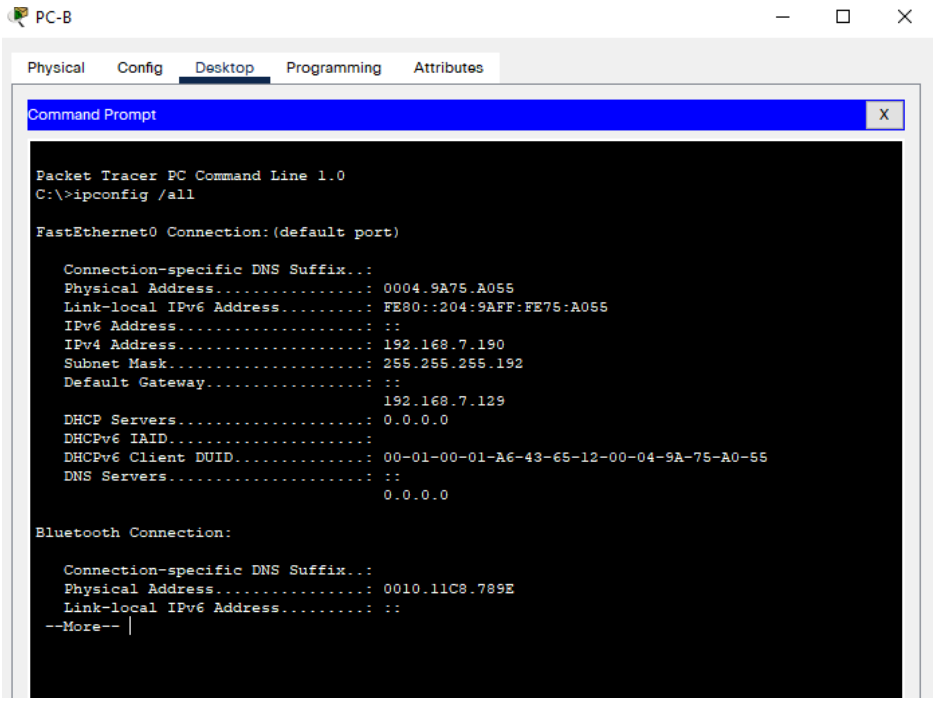
Fuente: Propia

Tabla 5. Configuración PC-A

CONFIGURACION RED PC-A	
Descripción	PC-A
Dirección Física	00:07:EC:66:00:60
Dirección IP	192.168.7.126
Mascara de subred	255.255.255.128
Gateway Predeterminado	192.168.7.1

Fuente: Propia

Figura 9. Configuración PC-B



Fuente: Propia

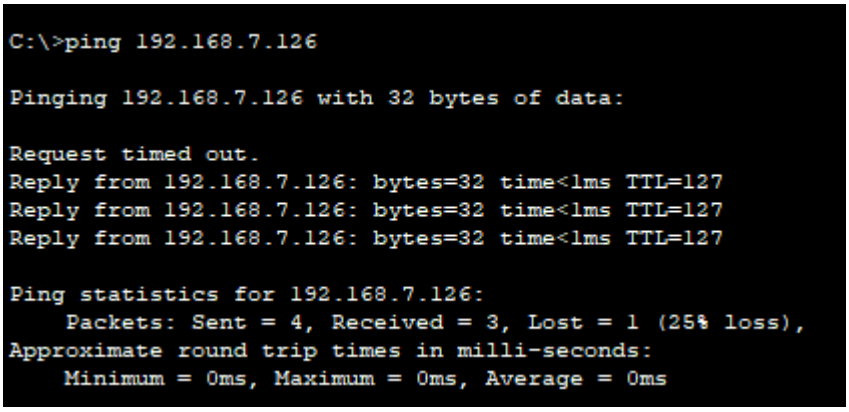
Tabla 6. Configuración PC-B

CONFIGURACION RED PC-B	
Descripción	PC-B
Dirección Física	00:04:9A:75:A0:55
Dirección IP	192.168.7.190
Mascara de subred	255.255.255.192
Gateway Predeterminado	192.168.7.129

Fuente: Propia

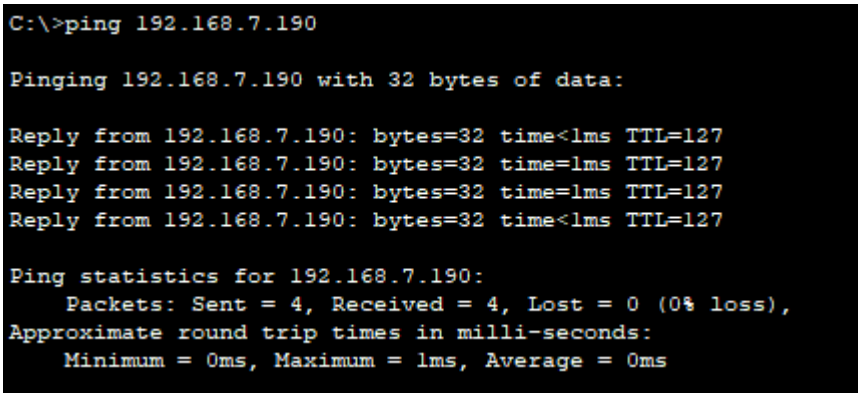
Pruebas conectividad

Figura 10. Conectividad PC-B a PC-A



Fuente: Propia

Figura 11. Conectividad PC-A a PC-B



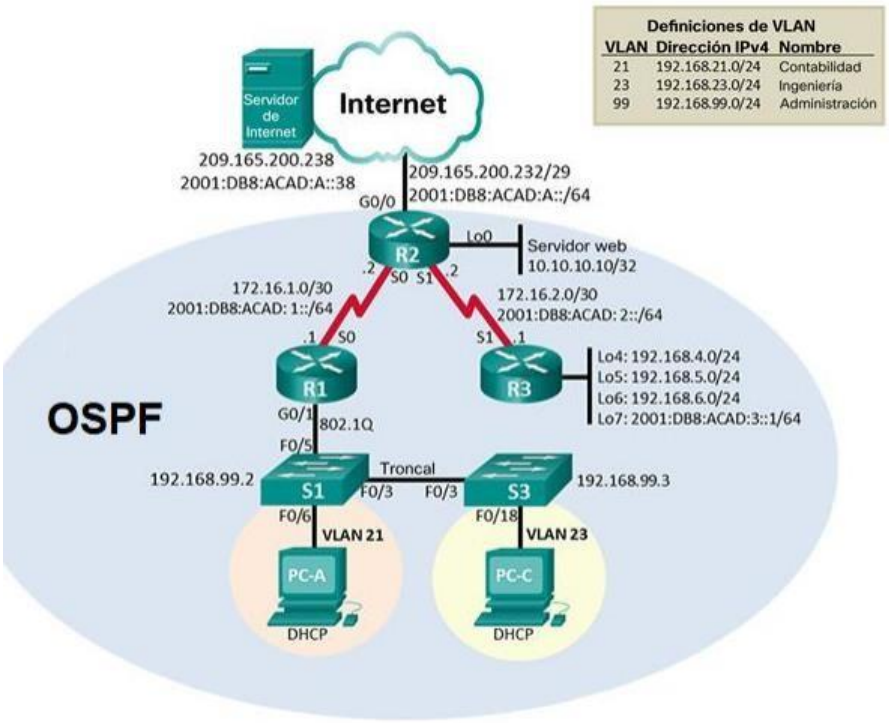
Fuente: Propia

2. ESCENARIO 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, Routing entre VLAN, el protocolo de Routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

TOPOLOGIA

Figura 12. Topología Propuesta Escenario 2



Fuente: Propia

Parte 1: Inicializar Dispositivos

Paso 1: Inicializar y volver a cargar los routers y los Switches

Elimine las configuraciones de inicio y vuelve a cargar los dispositivos.

Tabla 7. Inicializar y volver a cargar

Tarea	Comandos de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de la VLAN anterior	Switch#erase startup-config
Volver a cargar ambos Switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches	Switch>enable Switch#show flash

Fuente: Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

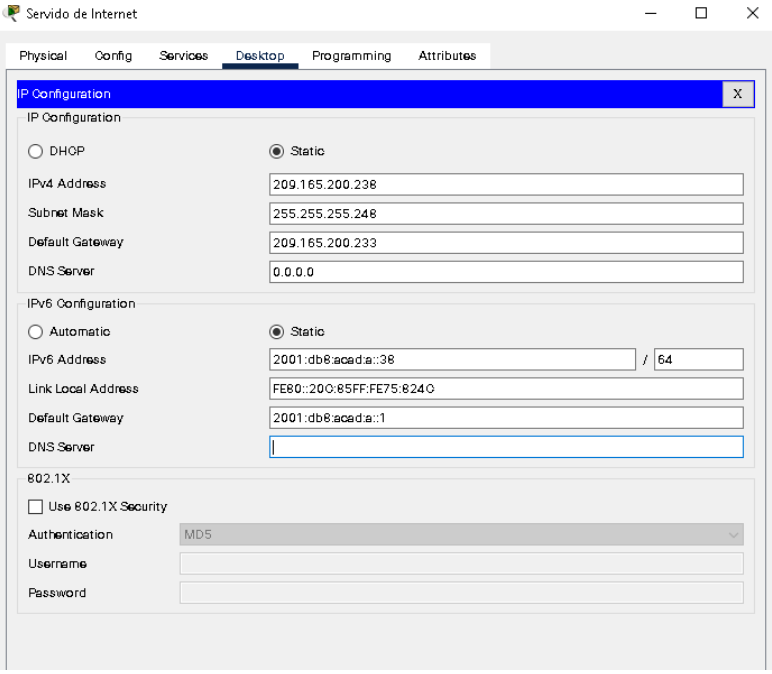
Las tareas de configuración del servidor de internet incluyen lo siguiente:

Tabla 8. Configuración de Servidor

Elemento o tarea de configuración	Especificación
Direccion Ipv4	209.165.200.238
Mascara de subred para Ipv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Direccion IPv6/ subred	2001:DB8:ACAD:A::38/ 64
Gateway Predeterminado IPv6	2001:DB8:ACAD:A::1/ 64

Fuente: Propia

Figura 13. Configuración Servidor Internet



Fuente: Propia

Paso 2: Configurar R1

Se procede a realizar la configuración básica del R1 donde se configura el nombre, contraseñas de acceso aplicando texto cifrado para mayor seguridad, mensaje motd y finalmente la configuración solicitada en la interfaz S0/0/0.

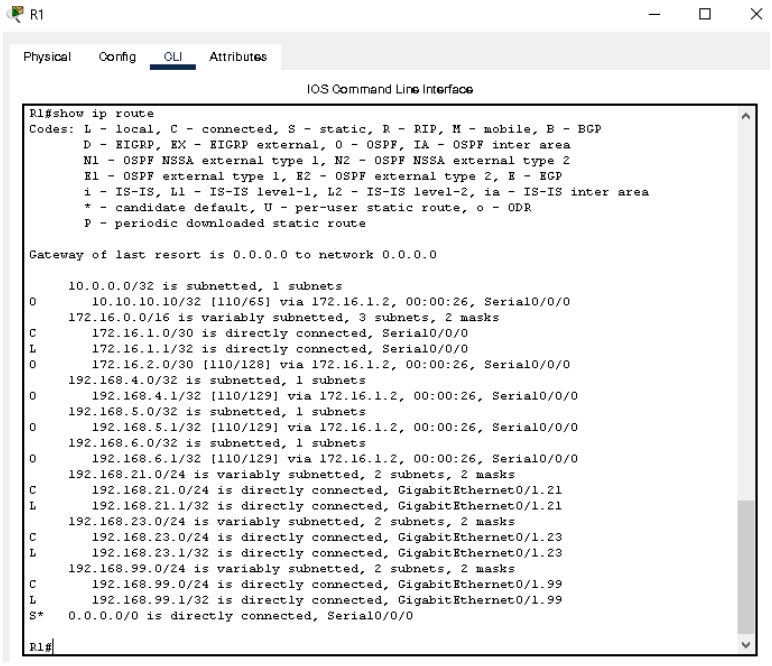
Tabla 9. Configuración R1- Escenario 2

Router>enable	Ingreso al modo privilegiado
Router#configure terminal	Ingreso al modo configuración
Router(config)#no ip domain-lookup	Desactivar búsqueda DNS
Router(config)#hostname R1	Asignar nombre Router
R1(config)#enable secret class	Contraseña cifrada de modo privilegiado
R1(config)#line con 0	Ingreso a configuración de consola
R1(config-line)#password cisco	Contraseña de consola
R1(config-line)#login	Cargar acceso
R1(config-line)#exit	Salida de configuración consola
R1(config)#line vty 0 4	Ingreso a telnet
R1(config-line)#password cisco	Asignación de contraseña
R1(config-line)#login	Cargar acceso

R1(config)#service password-encryption	Encriptar todas las contraseñas actuales y futuras
R1(config)#banner motd #Se prohibe el acceso no autorizado. #	Mensaje de aviso al ingreso
R1(config)#ipv6 unicast-routing	Activación de IP versión 6
R1(config)#interface s0/0/0	Ingreso a la interfaz serial 0/0/0
R1(config-if)#description Interfaz al R2	descripción del puerto o interfaz
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Asignación de IP y mascara versión 4
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64	Asignación de IP con su respectiva mascara versión 6
R1(config-if)#clock rate 128000	Establecer frecuencia de reloj
R1(config-if)#no shutdown	Activar el interfaz
R1(config-if)#exit	Salida de configuración interfaz
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0	Asignación de ruta predeterminada IPv4
R1(config)#ipv6 route ::/0 s0/0/0	asignación de ruta predeterminada IPv6
R1#copy running-config startup-config	Guardar configuración en la NVRAM

Fuente: Propia

Figura 14. Sh ip route en R1- Escenario 2



Fuente: Propia

Parte 3: Configurar R2

Se procede a configurar el router 2, donde se predetermina desactivar búsqueda DNS, cambiar nombre, asignar contraseñas y encriptarlas, configurar interfaz de los seriales, el gigabitethernet y el loopback.

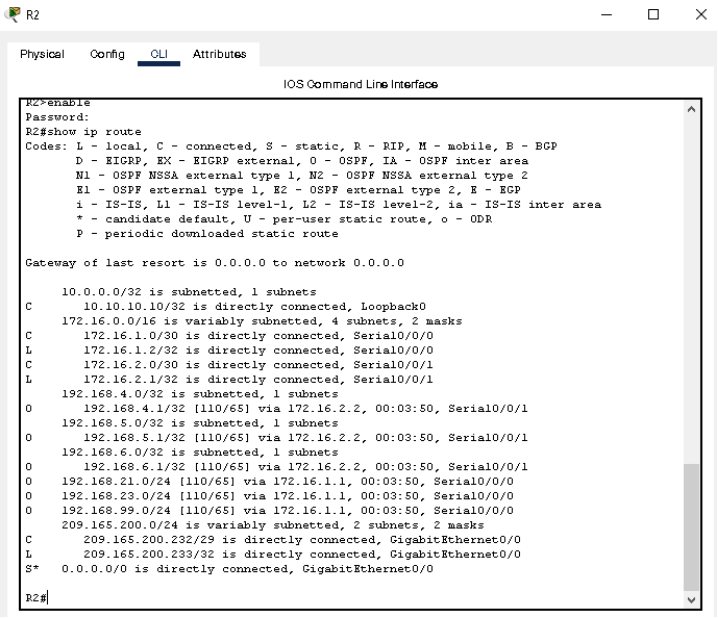
Tabla 10. Configuración R2- Escenario 2

Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso al modo global o configuración
Router(config)#no ip domain-lookup	Desactivar búsqueda DNS.
Router(config)#hostname R2	Realizar cambio de nombre.
R2(config)#enable secret class	Contraseña cifrada de modo privilegiado
R2(config)#line con 0	Ingreso a configuración de consola
R2(config-line)#password cisco	Asignación de contraseña consola
R2(config-line)#login	Cargar acceso
R2(config-line)#line vty 0 4	Ingreso a configuración telnet
R2(config-line)#password cisco	Asignación de contraseña telnet
R2(config-line)#login	Carga de acceso
R2(config-line)#exit	Salida de configuración telnet
R2(config)#service password-encryption	Encriptar contraseñas actuales y futuras
R2(config)#ip http server	Activación de servidor http
R2(config)#banner motd #Se prohibe el acceso no autorizado #	Mensaje de aviso de ingreso
R2(config)#ipv6 unicast-routing	Activación de direccionamiento IPv6
R2(config)#interface s0/0/0	Ingreso al interfaz serial 0/0/0
R2(config-if)#description Interfaz a R1	Descripción del puerto o interfaz
R2(config-if)#ip address 172.16.1.2 255.255.255.252	Asignación de IP y mascara de subred versión 4
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64	asignación de IP con mascara de subred 64 en versión 6
R2(config-if)#no shutdown	Activar el interfaz
R2(config-if)#interface s0/0/1	Ingreso a interfaz serial 0/0/1
R2(config-if)#description interfaz a R3	Descripción de interfaz
R2(config-if)#ip address 172.16.2.1 255.255.255.252	Asignación de IP versión 4
R2(config-if)#ipv6 address 2001:db8:acad:2::1/64	asignación de IP versión 6
R2(config-if)#clock rate 128000	Velocidad del reloj
R2(config-if)#no shutdown	Activar interfaz
R2(config)#interface g0/0	Ingreso a interfaz gigabitethernet 0/0

R2(config-if)#description interfaz a Internet	descripción del interfaz
R2(config-if)#ip address 209.165.200.233 255.255.255.248	Asignación de IP versión 4
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64	Asignación de IP versión 6
R2(config-if)#no shutdown	Activar interfaz
R2(config)#interface loopback 0	Se activa interfaz lógica interna del router
R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up	Confirma la carga del interfaz
R2(config-if)#description Interfaz de servidor web	Descripción del interfaz
R2(config-if)#ip address 10.10.10.10 255.255.255.255	asignación de IP con su respectiva mascara de subred versión 4
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0	asignación de salto o ruta predeterminada IPv4
R2(config)#ipv6 route ::/0 g0/0	Asignación de salto o ruta predeterminada IPv6
R2#copy running-config startup-config	Guardar configuración R2

Fuente: Propia

Figura 15. Sh ip route en R2- Escenario 2



Fuente: Propia

Paso 4: Configurar R3

Se configura el R3 teniendo en cuenta la configuración básica y la configuración de red para dar la conectividad adecuada a cada uno de los interfaces, en este caso se configura adicional varios interfaces loopback que son interfaces de lógica interna en el router. Además de rutas predeterminadas que generan saltos para continuar con la conectividad entre dispositivos intermedios.

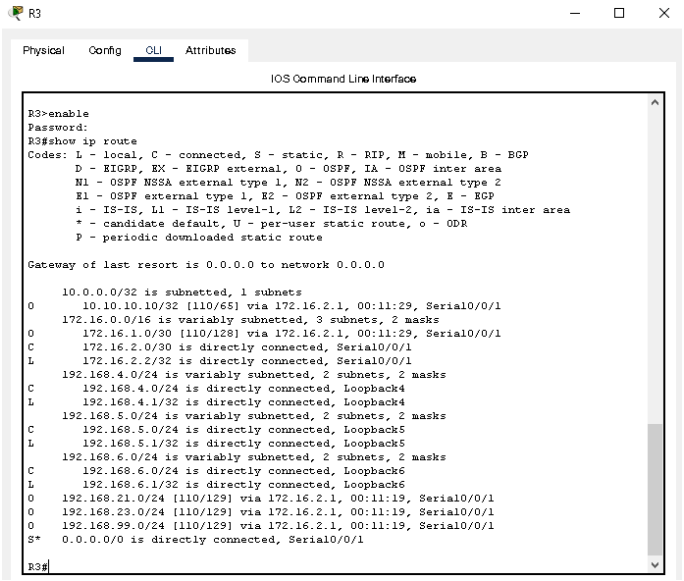
Tabla 11. Configuración R3

Router>ENABLE	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo configuración
Router(config)#no ip domain-lookup	Desactivar búsqueda DNS
Router(config)#hostname R3	Cambiar nombre del equipo
R3(config)#enable secret class	Contraseña cifrada en modo privilegiado
R3(config)#line con 0	Ingreso a configuración de consola
R3(config-line)#password cisco	Asignación de contraseña ingreso consola
R3(config-line)#login	Cargar acceso
R3(config-line)#line vty 0 4	Ingreso a configuración telnet
R3(config-line)#password cisco	Contraseña ingreso telnet
R3(config-line)#login	Cargar acceso
R3(config-line)#exit	Salida de configuración telnet
R3(config)#service password-encryption	Cifrar todas las contraseñas actuales y futuras
R3(config)#banner motd #Se prohibe el acceso no autorizado #	Mensaje de inicio o de aviso
R3(config)#ipv6 unicast-routing	Activación de versión 6 en direccionamiento.
R3(config)#interface s0/0/1	Ingreso al interfaz serial 0/0/1
R3(config-if)#description Interfaz a R2	Descripción del interfaz
R3(config-if)#ip address 172.16.2.2 255.255.255.252	Asignación de IP y mascara de subred del interfaz
R3(config-if)#ipv6 address 2001:db8:acad:2::2/64	Asignación de IP con su respectiva mascara en versión 6
R3(config-if)#no shutdown	Activar interfaz
R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up	Mensaje de alerta de interfaz arriba o cargado
R3(config-if)#interface loopback 4	Ingreso y activación de interfaz lógica en el puerto 4
R3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up	Mensaje de interfaz arriba o cargado

R3(config-if)#ip address 192.168.4.1 255.255.255.0	Asignación de IPv4 en la interfaz lógica 4
R3(config)#interface loopback 5	Ingreso y activación de interfaz lógica 5
R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up	Mensaje de apertura
R3(config-if)#ip address 192.168.5.1 255.255.255.0	Asignación de IP con su respectiva mascara 24 IPv4
R3(config-if)#interface loopback 6	Ingreso y activación del interfaz lógico 6
R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up	Mensaje de apertura y carga
R3(config-if)#ip address 192.168.6.1 255.255.255.0	Asignación de IP con su respectiva mascara 24
R3(config-if)#interface loopback 7	Ingreso y activación de interfaz lógica 7
R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up	Aviso de apertura
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64	Asignación de IP y su respectiva mascara versión 6
R3(config-if)#exit	Salida de configuración de interfaz
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1	Asignación de ruta predeterminada IPv4
R3(config)#ipv6 route ::/0 s0/0/1	Asignación de ruta predeterminada IPv6
R3(config)#exit	Salida de modo configuración
R3#copy running-config startup-config	Guardar configuración en la NVRAM.

Fuente: Propia

Figura 16. Show ip route en R3- Escenario 2



Fuente: Propia

Paso 5: Configurar S1

Tabla 12. Configuración S1

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo configuración
Switch(config)#no ip domain-lookup	Desactivar búsqueda DNS
Switch(config)#hostname S1	Cambiar nombre del equipo
S1(config)#enable secret class	Contraseña cifrada de modo privilegiado
S1(config)#line con 0	Ingreso a configuración de consola
S1(config-line)#password cisco	Asignación de contraseña
S1(config-line)#login	Cargar acceso
S1(config-line)#line vty 0 15	Ingreso a configuración de telnet
S1(config-line)#password cisco	Contraseña
S1(config-line)#login	Cargar acceso
S1(config)#service password-encryption	Encriptar todas las contraseña actuales y futuras.
S1(config)#banner motd #Se prohibe el acceso no autorizado#	Mensaje de aviso de ingreso
S1#copy running-config startup-config	Guardar configuración

Fuente: Propia

Paso 6: Configurar S3

Tabla 13. Configuración S3

Switch>enable	Ingreso al modo Privilegiado
Switch#configure terminal	Ingreso al modo configuración
Switch(config)#no ip domain-lookup	Desactivar búsqueda DNS
Switch(config)#hostname S3	Cambiar nombre al equipo
S3(config)#enable secret class	Asignar contraseña al modo privilegiado
S3(config)#line con 0	Ingreso a la configuración de consola
S3(config-line)#password cisco	Asignación de contraseña por conexión de consola
S3(config-line)#login	Cargar acceso
S3(config-line)#line vty 0 15	Ingreso a configuración telnet
S3(config-line)#password cisco	Asignación de contraseña
S3(config-line)#login	Cargar acceso
S3(config)#service password-encryption	Encriptar todas las contraseñas actuales y futuras.
S3(config)#banner motd # Se prohibe el acceso no autorizado #	Mensaje de ingreso
S3#copy running-config startup-config	Guardar configuración

Fuente: Propia

Paso 7: Verificar la conectividad de la red

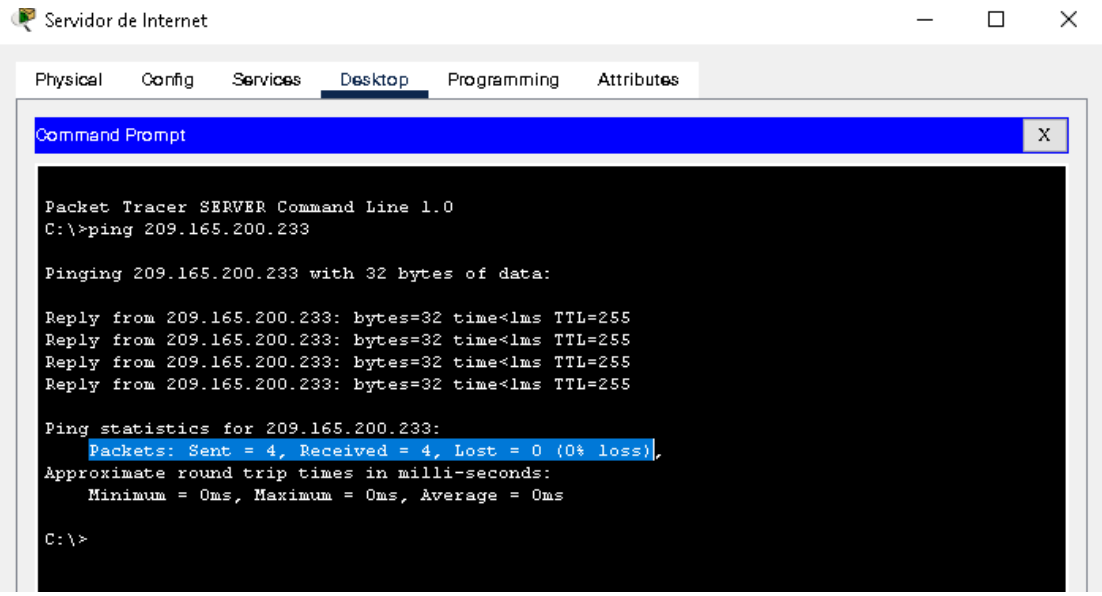
Mediante el interfaz de los routers se usa el comando ping para comprobar la conectividad entre dispositivos intermedios y el servidor.

Tabla 14. Verificación de conectividad Escenario 2

Desde	A	Dirección IP	Resultados ping
R1	R2, S0/0/0	172.16.1.2	!!!!!
R2	R3, S0/0/1	172.16.2.2	!!!!!
PC de Internet	Gateway predeterminado	209.165.200.233	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Fuente: Propia

Figura 17. Conectividad de PC Internet a Gateway



Fuente: Propia

Parte 3: Configurar la seguridad del switch, las VLAN y el Routing entre VLAN

Paso 1: Configurar S1

Se crean las bases de datos de las VLAN donde se determina las Vlan a usar y el nombre que tendrán, igualmente se asignara IP y Gateway a la Vlan de administración que son las que contienen los Switch.

Tabla 15. Crear bases de datos VLAN S1

S1>enable	Ingreso al modo privilegiado
S1#configure terminal	Ingreso al modo configuración
S1(config)#vlan 21	Crear VLAN 21
S1(config-vlan)#name Contabilidad	Asignar nombre a la VLAN
S1(config-vlan)#vlan 23	Crear VLAN 23
S1(config-vlan)#name Ingenieria	Asignar nombre a la VLAN
S1(config-vlan)#vlan 99	Crear VLAN 99
S1(config-vlan)#name Administración	Asignar nombre a la VLAN
S1(config-vlan)#exit	Salida de configuración de VLAN
S1(config)#interface vlan 99	Ingreso a la interfaz de la VLAN 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0	Asignación de y IP con su respectiva mascara de subred
S1(config-if)#no shutdown	Completar carga de interfaz

S1(config)#ip default-gateway 192.168.99.1	Asignación de puerta de enlace predeterminada del S1

Fuente: Propia

Figura 18. Show interface Vlan 99 en S1- Escenario 2

```
Sl#sh interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 00d0.d39d.7001 (bia 00d0.d39d.7001)
  Internet address is 192.168.99.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out

Sl#
```

Fuente: Propia

Se procede a forzar el enlace troncal en las interfaces que están conectados, se asigna la vlan 21 al puerto fastethernet 0/6 del S1, finalmente se apaga los puertos sin usar.

Tabla 16. Configuración de las interfaces S1

S1(config)#interface f0/3	Ingreso a la interfaz fastethernet 0/3
S1(config-if)#switch mode trunk	Establecer en modo troncal
S1(config-if)#switchport trunk native vlan 1	Asignación de la troncal a clan 1 como nativa
S1(config)#interface f0/5	Ingreso a la interfaz fastethernet 0/5
S1(config-if)#switch mode trunk	Establecer en modo troncal
S1(config-if)#switchport trunk native vlan 1	Asignación de Vlan nativa en la troncal con la Vla1
S1(config)#interface range f0/1 - f0/2	Ingreso a rango de interfaz
S1(config-if-range)#switchport mode Access	Asignación de modo puertos de acceso
S1(config)#interface range f0/4	Ingreso al rango de interfaz f0/4
S1(config-if-range)#switchport mode Access	Asignación modo de acceso
S1(config)#interface range f0/6 - f0/24	Ingreso a rango de interfaz establecidos

S1(config-if-range)#switchport mode Access	Asignación de modo acceso
S1(config)#interface f0/6	Ingreso a la configuración de la interfaz f0/6
S1(config-if)#sw access vlan 21	Se le asigna al puerto de la vlan 21
S1(config)#interface range f0/1 - f0/2	Ingreso a la configuración del rango establecido
S1(config-if-range)#shutdown	Pasar a estado down
S1(config)#interface range f0/4	Ingreso a la configuración de f 0/4
S1(config-if-range)#shutdown	Deshabilitar puerto
S1(config)#interface range f0/7 - f0/24	Ingreso a la configuración del rango de interfaz
S1(config-if-range)#shutdown	Deshabitar los puertos o interfaces es decir pasarlos a estado down.

Fuente: Propia

Paso 2: Configurar S3

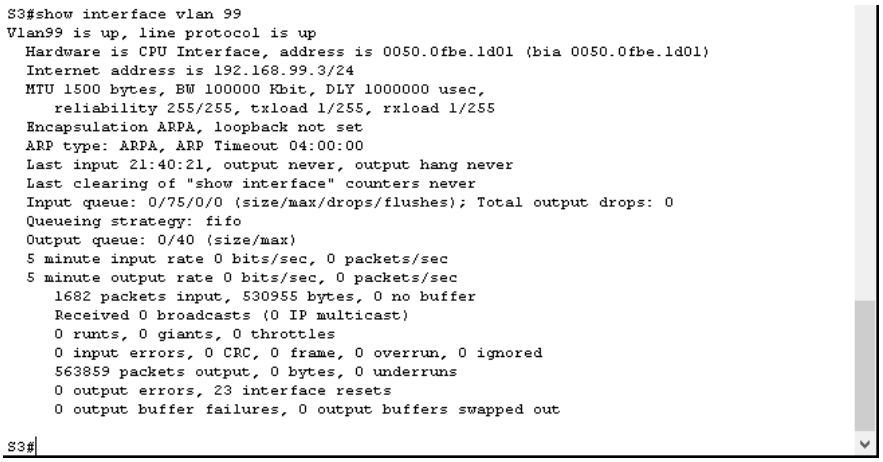
Se crean las bases de datos de las VLAN donde se determina las vlan a usar y el nombre que tendrán, igualmente se asignara IP y Gateway a la Vlan de administración que son las que contienen los Switch.

Tabla 17. Crear bases de datos VLAN S1

S3#configure terminal	Ingreso al modo configuración
S3(config)#vlan 21	Se crea vlan 21
S3(config-vlan)#name Contabilidad	Se asigna nombre a la vlan
S3(config-vlan)#vlan 23	Se crea vlan 23
S3(config-vlan)#name Ingenieria	Se asigna nombre a la vlan
S3(config-vlan)#vlan 99	Se crea y se ingresa a la configuración vlan
S3(config-vlan)#name administración	Se asigna nombre
S3(config-vlan)#interface vlan 99	Se ingresa a la configuración de la vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0	Se asigna la IP indicada con su respectiva mascara de subred
S3(config-if)#no shutdown	Se carga puerto o interfaz
S3(config-if)#exit	Salida de configuración de interfaz
S3(config)#ip default-gateway 192.168.99.1	Se asigna puerta de enlace predeterminada

Fuente: Propia

Figura 19. Show interface vlan 99 en S3- Escenario 2



Fuente: Propia

Se procede a forzar el enlace troncal en las interfaces que están conectados, se asigna la vlan 23 al puerto fastethernet 0/18 del S3, finalmente se apaga los puertos sin usar.

Tabla 18. Configuración de las interfaces S3

S3(config)#interface f0/3	Ingreso a la configuración del interfaz f0/3
S3(config-if)#switchport mode trunk	Se establece puerto como modo troncal
S3(config-if)#switchport trunk native vlan 1	Se determina la vlan 1 con nativa para la troncal
S3(config-if)#exit	Salida de configuración de f0/3
S3(config)#interface range f0/1 - f0/2	Ingreso al rango de interfaz indicadas
S3(config-if-range)#switchport mode Access	Se establece puertos como modo acceso
S3(config-if-range)#interface range f0/4 - f0/24	Ingreso al rango de interfaz
S3(config-if-range)#switchport mode Access	Se establece puertos en modo acceso
S3(config)#interface f0/18	Ingreso al interfaz fastethernet 0/18
S3(config-if)#sw mode Access	Se confirma modo acceso
S3(config-if)#switchport access vlan 23	Se determina o relaciona puerto con vlan 23
S3(config-if)#exit	Salida de configuración de interfaz
S3(config)#interface range f0/1 - f0/2	Ingreso al rango de interfaces
S3(config-if-range)#shutdown	Se desactiva puerto
S3(config-if-range)#interface range f0/4 - f0/17	Ingreso al rango de interfaces

S3(config-if-range)#shutdown	Se cambia a estado down
S3(config-if-range)#interface range f0/19 - f0/24	Ingreso a rango de interfaces
S3(config-if-range)#shutdown	Se procede apagar los puertos o poner en estado down.

Fuente: Propia

Paso 3: Configurar R1

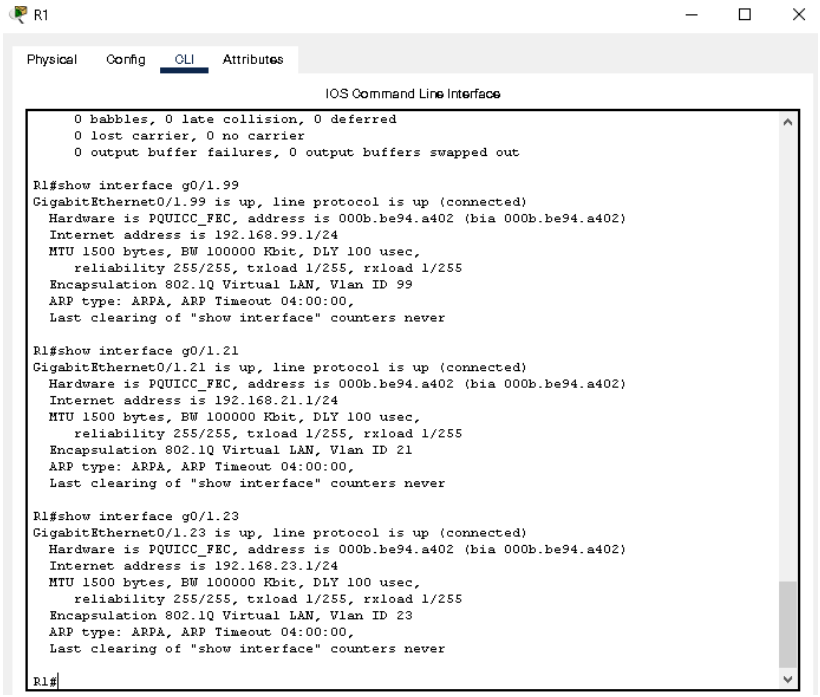
Se Configura las subinterfaces los cuales relacionan las vlan creadas en los pasos anteriores.

Tabla 19. Configuración de las subinterfaces.

R1(config)#interface g0/1.21	Se crea la subinterfaz .21
R1(config-subif)#description LAN de Contabilidad	Se establece la descripción de la subinterfaz creada
R1(config-subif)#encapsulation dot1Q 21	Se encapsula asignando la vlan 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0	Asignación de la IP con su respectiva subred
R1(config-subif)#interface g0/1.23	Se crea subinterfaz 23
R1(config-subif)#description LAN de Ingenieria	Se establece descripción del interfaz
R1(config-subif)#encapsulation dot1Q 23	Se encapsula determinando la vlan 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0	Se asigna la IP de la subinterfaz
R1(config)#interface g0/1.99	Se crea la subinterfaz 99
R1(config-subif)#description LAN de Administración	Se establece la descripción del interfaz
R1(config-subif)#encapsulation dot1Q 99	Se establece encapsulamiento o relación a la vlan 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0	Se asigna ipv4 con su respectiva mascara de subred
R1(config)#interface g0/1	Se ingresa a la configuración de la interfaz
R1(config-if)#no shutdown	Se activa el interfaz

Fuente: Propia

Figura 20. Configuración de subinterfaces



Fuente: Propia

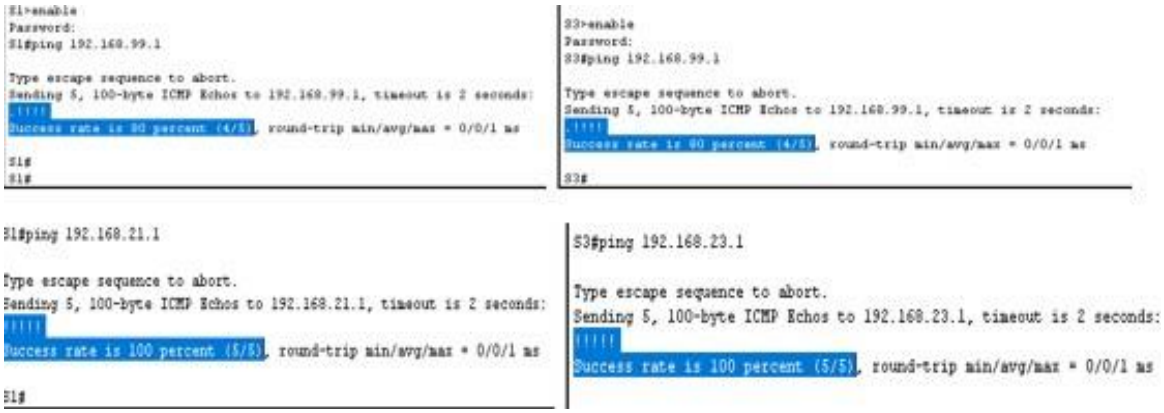
Paso 4: Verificar la conectividad de la red

Tabla 20. Respuesta de ping VLAN

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	.!!!! Success rate is 80 percent (4/5)
S3	R1, dirección VLAN 99	192.168.99.1	.!!!! Success rate is 80 percent (4/5)
S1	R1, dirección VLAN 21	192.168.21.1	!!!!! Success rate is 100 percent (5/5)
S3	R1, dirección VLAN 23	192.168.23.1	!!!!! Success rate is 100 percent (5/5)

Fuente: Propia

Figura 21. Respuestas ping VLAN



Fuente: Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

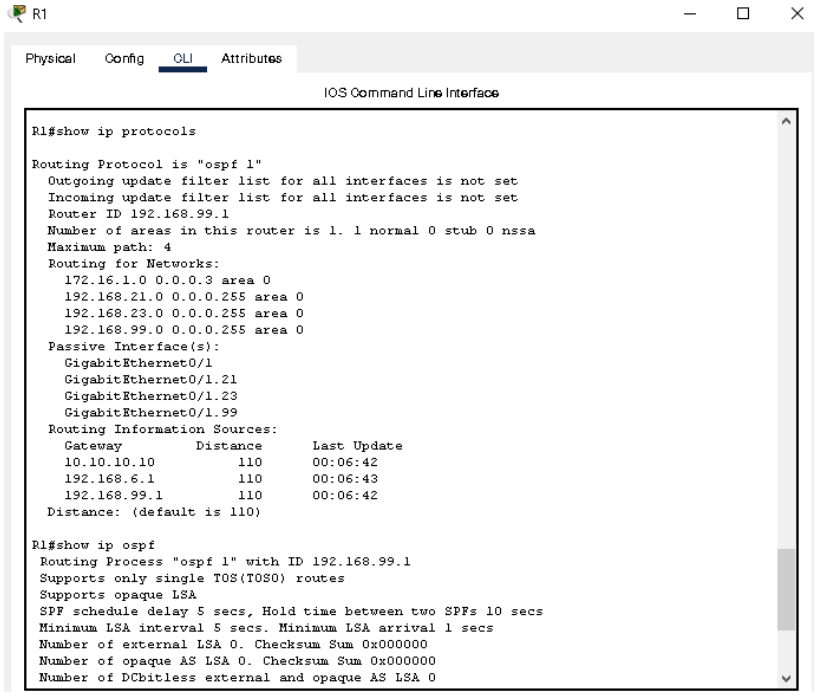
Paso 1: Configurar OSPF en el R1

Tabla 21. Configuración OSPF R1

R1(config)#router ospf 1	Ingresar a la configuración ospf
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0	Anunciar la red conectada en el serial 0/0/0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0	Anunciar la red conectada en g0/1.21
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0	Anunciar la red conectada en g0/1.23
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0	Anunciar la red conectada en g0/1.99
R1(config-router)#passive-interface gigabitEthernet 0/1	Interfaz LAN pasiva
R1(config-router)#passive-interface gigabitEthernet 0/1.21	Subinterfaz LAN pasiva
R1(config-router)#passive-interface gigabitEthernet 0/1.23	Subinterfaz LAN pasiva
R1(config-router)#passive-interface gigabitEthernet 0/1.99	Subinterfaz LAN pasiva

Fuente: Propia

Figura 22. Validación OSPF R1



Fuente: Propia

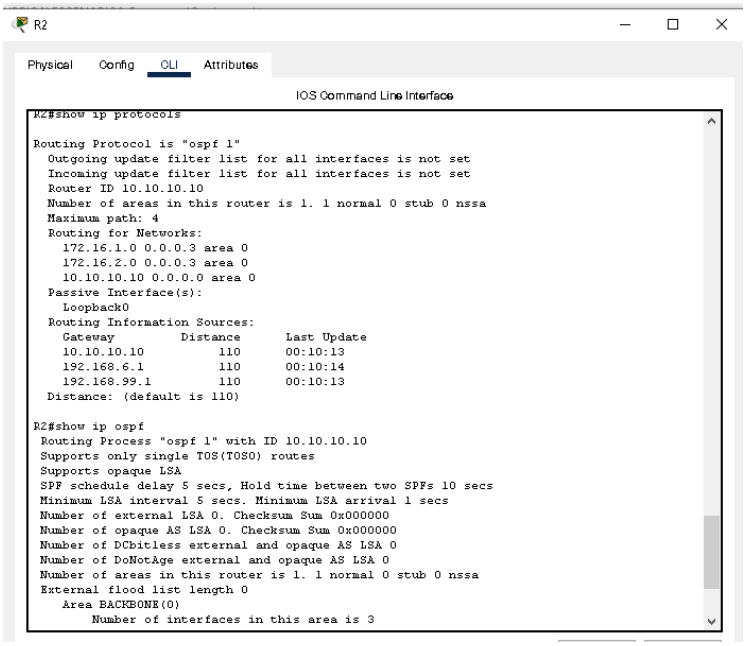
Paso 2: Configurar OSPF en el R2

Tabla 22. Configuración OSPF R2

R2(config)#router ospf 1	Ingresar a la configuración ospf
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0	Anunciar la red conectada en serial 0/0/0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0	Anunciar la red conectada en serial 0/0/1
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0	Anunciar la red conectada en LoopBack 0
R2(config-router)#passive-interface loopback 0	Interfaz LAN Pasiva

Fuente: Propia

Figura 23. Validación OSPF R2



Fuente: Propia

Paso 3: Configurar OSPFv3 en el R2

Tabla 23. Configuración OSPFv3 R2

R2(config)#ipv6 router ospf 2	Configurar ospf 2
R2(config-rtr)#router-id 1.1.1.1	Asignación del id del router

Fuente: Propia

Paso 3.1: Configuración OSPF en el R3

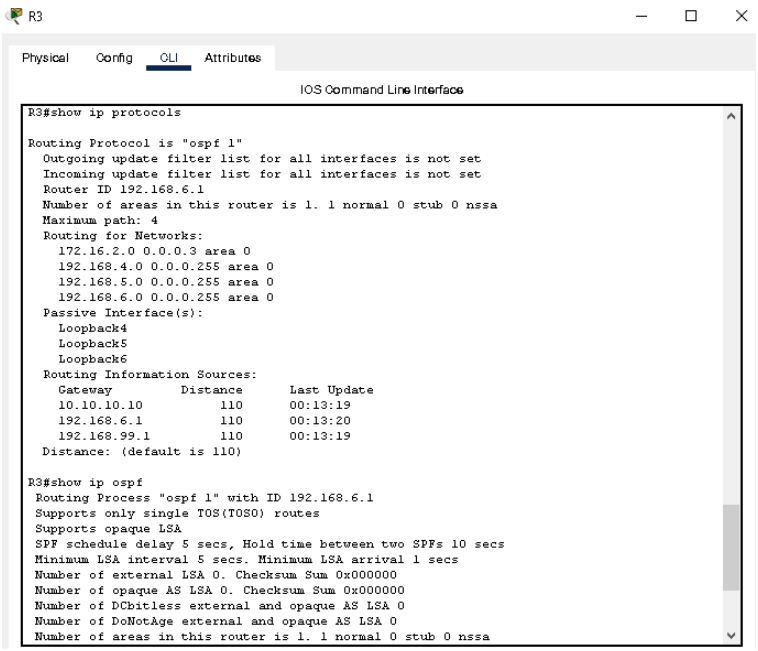
Tabla 24. Configuración OSPF R3

R3(config)#router ospf 1	Establecer la configuración ospf
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0	Anunciar la red conectada en el serial 0/0/1
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0	Anunciar la red conectada en el Loopback 4
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0	Anunciar la red conectada en el Loopback 5
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0	Anunciar la red conectada en el Loopback 6
R3(config-router)#passive-interface loopback 4	Asignar como interfaz pasiva
R3(config-router)#passive-interface loopback 5	Asignar como interfaz pasiva

R3(config-router)#passive-interface loopback 6	Asignar como interfaz pasiva

Fuente: Propia

Figura 24. Validación OSPF R3



Fuente: Propia

Paso 4: Verificar la información de OSPF

¿Con que comando se muestra la ID del proceso OSPF, la ID del router, las redes routing y las interfaces pasivas configuradas en un router? **Rta: Show ip ospf**

Figura 25. Id del proceso OSPF

```
R2#show ip ospf
 Routing Process "ospf 1" with ID 10.10.10.10
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x01455d
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Fuente: Propia

¿Qué comando muestra solo las rutas OSPF? **Rta: Show ip route ospf**

Figura 26. Rutas OSPF

```
R2#show ip route ospf
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/65] via 172.16.2.2, 00:54:16, Serial0/0/1
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/65] via 172.16.2.2, 00:54:16, Serial0/0/1
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/65] via 172.16.2.2, 00:54:16, Serial0/0/1
O    192.168.21.0 [110/65] via 172.16.1.1, 00:54:16, Serial0/0/0
O    192.168.23.0 [110/65] via 172.16.1.1, 00:54:16, Serial0/0/0
O    192.168.99.0 [110/65] via 172.16.1.1, 00:54:16, Serial0/0/0
```

Fuente: Propia

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

Rta: Show ip protocols

Figura 27. Sección OSPF

```
R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    10.10.10.10 0.0.0.0 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10           110      00:25:52
    192.168.6.1           110      00:25:53
    192.168.99.1          110      00:25:52
  Distance: (default is 110)
```

Fuente: Propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor DHCP para las VLAN 21 y 23

En el R1 se reservan en la VLAN 21 Y 23 las primeras 20 direcciones IP para direccionamiento estático y con las IP´s restantes se crea un pool DHCP.

Tabla 25. Configuración de Pool DHCP.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20	Se reserva o se excluye las ips del rango establecido en este caso las primero 20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20	Se reserva las primeras 20 ips para direccionamiento estático.
R1(config)#ip dhcp pool ACCT	Se crea el pool con el nombre ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0	Se indica el direccionamiento del pool
R1(dhcp-config)#dns-server 10.10.10.10	Se indica el direccionamiento del servidor DNS
R1(dhcp-config)#domain-name ccna-sa.com	Se indica el nombre del dominio
R1(dhcp-config)#default-router 192.168.21.1	Se establece la puerta de enlace predeterminada
R1(config)#ip dhcp pool ENGNR	Se crea el pool dhcp con el nombre ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0	Se indica el direccionamiento del pool
R1(dhcp-config)#dns-server 10.10.10.10	Se establece la dirección del servidor DNS
R1(dhcp-config)#domain-name ccna-sa.com	Se indica el dominio
R1(dhcp-config)#default-router 192.168.23.1	Se establece la puerta de enlace predeterminada.

Fuente: Propia

Paso 2: Configurar la NAT estática y dinámica en el R2

Tabla 26. Configuración NAT R2

R2(config)#username webuser privilege 15 password cisco12345	Se crea una base de datos local
R2(config)#ip http server ^ % Invalid input detected at '^' marker	Se habilita el servicio http del servidor, pero sale error porque packet tracer no lo soporta
R2(config)#ip http authentication local ^ % Invalid input detected at '^' marker.	Configura el servidor http para autentificación con la base de datos creada anteriormente. No lo soporta packet tracert
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229	Se crea un direccionamiento NAT o también llamado apuntamiento DMZ.

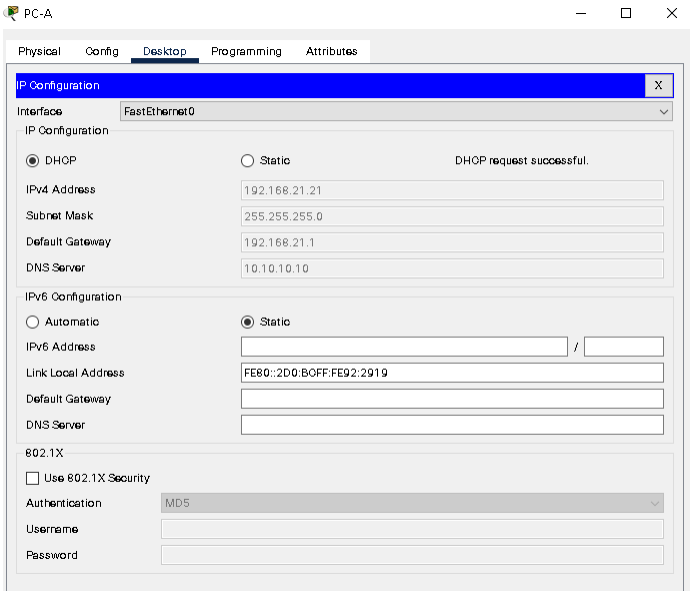
R2(config)#interface g0/0	Ingreso a configuración de interfaz
R2(config-if)#ip nat outside	Indica que trabaja externamente de la red
R2(config-if)#interface s0/0/0	Ingreso a configuración interfaz
R2(config-if)#ip nat inside	Indica que trabaja de internamente
R2(config-if)#interface s0/0/1	Ingreso Interfaz
R2(config-if)#ip nat inside	Indica que trabaja internamente.
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255	Indica que la NAT dinamita permite la ACL privada de contabilidad
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255	Indica que la NAT dinamita permite la ACL privada de Ingeniería
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255	Permite la traducción del loopback.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248	Se crea y define el pool llamado INTERNET se aplica el rango con su respectiva mascara
R2(config)#ip nat inside source list 1 pool INTERNET	Se define la traducción NAT DINAMICA.

Fuente: Propia

Paso 3: Verificar el producto DHCP y la NATestática.

Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

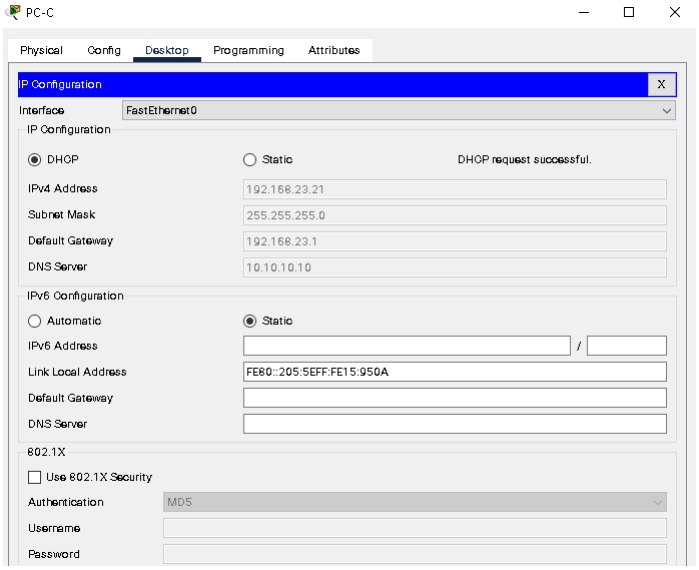
Figura 28. PC- A asignación de IP del servidor



Fuente: Propia

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

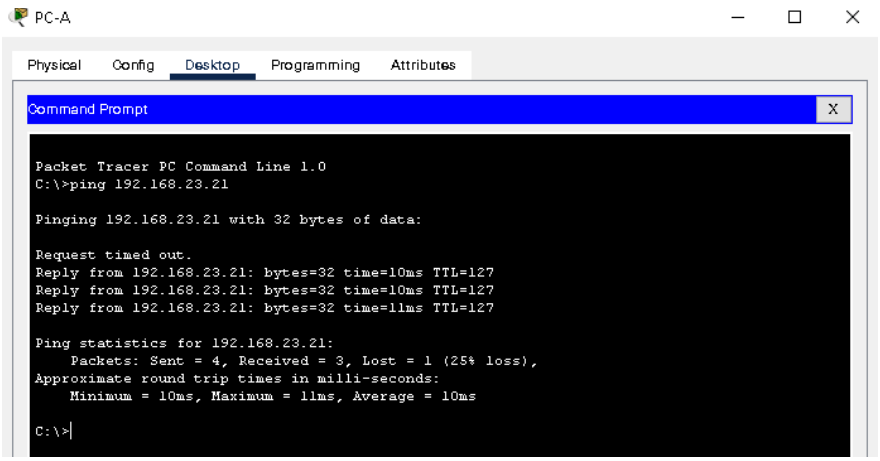
Figura 29. PC-C asignación de IP del servidor.



Fuente: Propia

Verificar que la PC-A pueda hacer ping a la PC-C

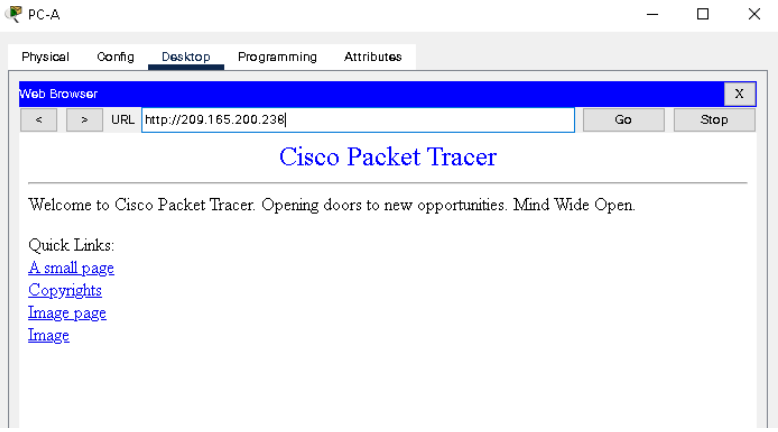
Figura 30. Ping del PC-A al PC-C



Fuente: Propia

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figura 31. Acceso al servidor Web



Fuente: Propia

Parte 6: Configurar NTP

Tabla 27.Configuración NTP

R2#clock set 09:00:00 05 march 2016	Se ajusta la fecha y hora
R2#configure terminal	Se ingresa al modo configuracionR2
R2(config)#ntp master 5	Se establece como un maestro NTP
R1#configure terminal	Ingreso al modo configuración R1
R1(config)#ntp server 172.16.1.2	Se establece como un cliente NTP
R1(config)#ntp update-calendar	Se activa actualizaciones de calendario
R1#sw ntp associations	Validar configuración, pero comando no lo soporta packet tracert

Fuente: Propia

Parte 7: Configurar y verificar las listas de control de acceso ACL

Paso 1: Restringir el acceso a las líneas VTY en el R2.

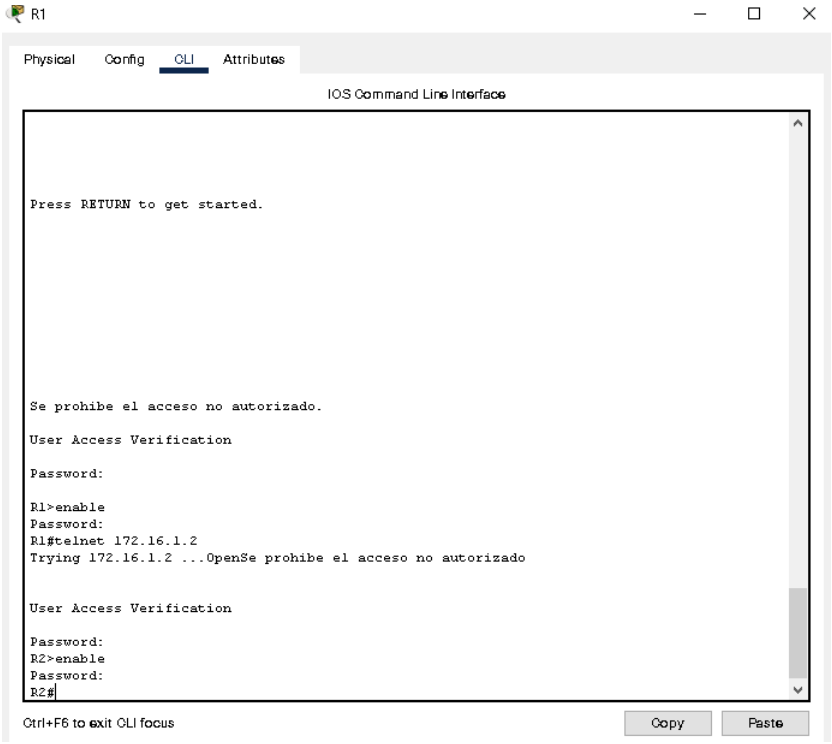
Tabla 28. Configuraciones líneas VTY R2

R2#configure terminal	Ingreso al modo de configuración
R2(config)#ip access-list standard ADMIN-MGT	Lista de nombre con acceso
R2(config-std-nacl)#permit host 172.16.1.1	Se indica la ip de la cual se permite el ingreso
R2(config-std-nacl)#deny any	Se indica que se debe negar cualquier otra dirección.

R2(config-std-nacl)#exit	Salida de configuración de lista
R2(config)#line vty 0 4	Ingreso a configuración líneas VTY
R2(config-line)#ip access-class ADMIN-MGT IN	Se indica que las líneas trabajen con la lista creada
R2(config-line)#transport input telnet	
R2(config-line)#exit	Salida de configuración líneas vty

Fuente: Propia

Figura 32. Comprobación de ingreso por telnet



Fuente: Propia

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Mostrar las condiciones recibidas por una lista de acceso desde la última vez que se restableció. **Rta: R2#sh access-lists**

Figura 33. Lista de acceso

```
R2#sh access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255 (10 match(es))
    20 permit 192.168.23.0 0.0.0.255 (16 match(es))
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
    20 deny any
```

Fuente: Propia

Restablecer los contadores de una lista de acceso. **Rta: R2#clear ip access-list counters**

¿Qué comando se usa para mostrar que ACL se aplica a una interfaz y la dirección en que se aplica? **Rta: R2#sh ip nat translations**

Figura 34. Mostrar ACL

```
R2#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.226:1 192.168.21.21:1    209.165.200.238:1  209.165.200.238:1
icmp 209.165.200.226:2 192.168.21.21:2    209.165.200.238:2  209.165.200.238:2
icmp 209.165.200.226:3 192.168.21.21:3    209.165.200.238:3  209.165.200.238:3
icmp 209.165.200.226:4 192.168.21.21:4    209.165.200.238:4  209.165.200.238:4
icmp 209.165.200.227:5 192.168.23.21:5    209.165.200.238:5  209.165.200.238:5
icmp 209.165.200.227:6 192.168.23.21:6    209.165.200.238:6  209.165.200.238:6
icmp 209.165.200.227:7 192.168.23.21:7    209.165.200.238:7  209.165.200.238:7
icmp 209.165.200.227:8 192.168.23.21:8    209.165.200.238:8  209.165.200.238:8
---  209.165.200.229   10.10.10.10        ---                ---
---  209.165.200.238   10.10.10.10        ---                ---
tcp 209.165.200.226:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
```

Fuente: Propia

¿Qué comando se utiliza para eliminar las traducciones nat dinámicas?

Rta: R2#clear ip nat translation *

CONCLUSIONES

Después de comprender y conocer cada una de las temáticas del diplomado con colaboración con La plataforma cisco que ofrece gran variedad de información para comprender y saber implementar una red adecuadamente tanto en su estructura como en su respectiva configuración de los equipos cisco como Router, Switch, Hub, Firewall entre otros. Los cuales está compuesta por niveles en los cuales en el diplomado se adquirió conocimiento de CP CCNA 1 – CP CCNA 2.

En la configuración básica está establecido asignación de nombre, avisos motd, asignación de contraseñas con su encriptación lo cual colabora en la seguridad de ingreso sea por medio consola que es conexión directa por el pc o mediante telnet para realizar las respectivas configuraciones en los equipos. Por otra parte, la manipulación de las subredes para interpretar la cantidad de subredes que se pueden implantar y la cantidad de host o equipos finales que soporta cada subred. Ya después mejorando la seguridad la red mediante bases de datos, subdivisión de interfaces, protocolos DHCP para la distribución dinámica de direccionamiento, OSPF, apuntamientos o direccionamientos NAT y PAT.

En el primer escenario se implementó lo esencial que son las configuraciones básicas, manipulación e implementación de las subredes, comprensión de cómo se interpreta la marcara de subred y como se puede determinar una continuidad de direccionamiento para cada área.

Ya en el segundo escenario se fortaleció los conocimientos adquiridos sobre distribución DHCP que mediante un servidor o el propio Router se crean unos parámetros de que segmentación, que rango son IP fija, y que rango se pueden distribuir dinámicamente. Además de cómo se destina apuntamientos o direccionamientos NAT y PAT, lo cual nos colabora en relaciona o unir una IP local o interna con una IP externa que nos entrega el proveedor de servicio.

BIBLIOGRAFIA

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-5). IEEE.

BAREÑO, Gutiérrez, R., Cárdenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Páez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, *16*(1), 75-84.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, *12*(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, *14*(1), 127-138.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-6). IEEE.