PRUEBA DE HABILIDADES PRACTICAS CCNA

OMAR GERMÁN RINCÓN GALLO

UNIVERISDAD ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA-ECBTI
INGENIERÍA DE TELECOMUNICACIONES
SOCHA 2021

PRUEBA DE HABILIDADES PRACTICAS CCNA

OMAR GERMÁN RINCÓN GALLO

Diplomado de opción de grado presentado para optar el
Título de INGENIERO DE TELECOMUNICACIONES

TUTOR:
Ing. Héctor Manuel Herrera Herrera.

UNIVERISDAD ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA-ECBTI
INGENIERÍA DE TELECOMUNICACIONES
SOCHA 2021

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SOCHA, 19 de Julio de 202

AGRADECIMIENTOS

Gracias a Dios por consentir estar en esta instancia de mi vida, su misericordia y su bondad me han permitido conocer cada día más y aprender momento a momento miles y miles de conocimientos que con su voluntad podremos desarrollar profesionalmente, a mi Madre que en cada una de sus oraciones me encomienda para que el entendimiento y la protección de Dios llene mi vida; a mis adorables hijas que quiero que vean en este triunfo una oportunidad y un ejemplo para seguir luchando por sus sueños y la esperanza de salir adelante, a esas personas especiales en mi vida que día a día, noche a noche me alientan y que sin su apoyo esto no sería posible, a esa comprensión, ese amor y esa fuerza que me das en cada momento, en cada charla de motivación y en cada mensaje, esos sueños por los que luchamos y que solo con la bendición de Dios pueden ser una realidad, a esos compañeros que en su interés de salir adelante nos brindan ese apoyo y ese empujoncito para continuar, con todo mi esfuerzo y con el corazón más que con el pensamiento, Gracias.

CONTENIDO

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

INTRODUCCION

En el mundo moderno encontramos múltiples facilidades de comunicación, hoy es posible encontrar servicios de conectividad por doquier, esto no solo nos lleva a un medio competitivo, sino que también encontramos múltiples amenazas sobre nuestros servicios; lo que hace más vulnerables las estabilidades y sistemas de seguridad; en especial de las grandes empresas que podrían llegar a tener una perdida incalculable en sus finanzas; es por ello que mediante sistemas seguros y complejos, bien definidos y estructuramos buscamos implementar diseños que estén lo más cerca posible de estos requerimientos y que ofrezcan la posibilidad de ser parte fundamental del funcionamiento del mundo moderno.

En esta prueba buscamos implementar conocimientos y practica de ellos en el trabajo sobre los escenarios propuesto; lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

1. Escenario 1

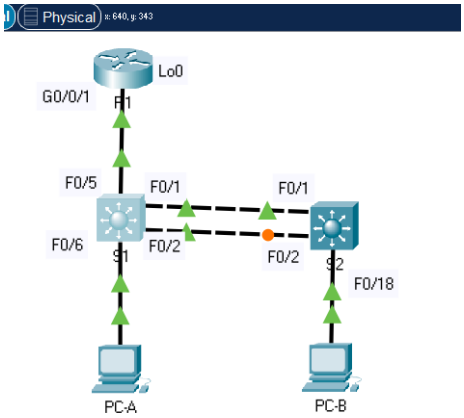


Fig.1 Topología, fuente cisco packet tracer

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 1. Tabla de VLAN

Dispositivo/interface	Dirección ip/prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1/26	No corresponde
	2001:db5:acad:a::1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65/27	No corresponde
	2001:db5:acad:b::1 /64	
1 G0/0/1.4	10.21.5.97/29	
	2001:db5:acad:c::1 /64	
1 G0/0/1.6	No corresponde	
R1 loopback0	209.165.201.1 /27	
	2001:db8:acad:209::1 /64	
S1 VLAN4	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c::99 /64	
	fe80::98	
S2 VLAN4	10.21.5.99/29	10.21.5.97
	2001:db5:acad:c::99 /64	
	Fe80::99	
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

Tabla 2. Asignación de direcciones

1.1. Configure R1.

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

Iniciamos el Router y realizamos las configuraciones iniciales (fig.2)

Router>en
Router#config ter
Router(config)#hostname R1
R1>en
Password:
R1#config ter
R1(config)#enable secret ciscoenpass

R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "AUTHORIZED ACCESS ONLY"
R1(config)#do wr

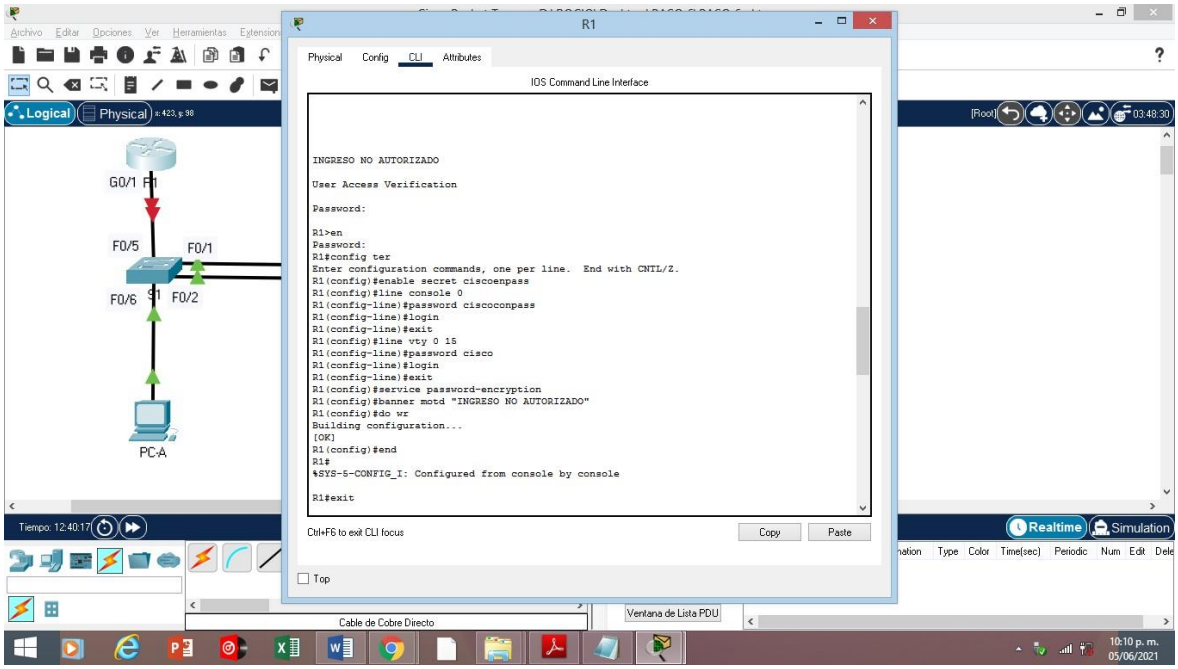


Fig.2 configuración inicial, fuente propia

1.2. Configurar switch.

Ahora realizamos las configuraciones iniciales de los switch 1 y 2 (fig.3) con los parámetros siguientes:

Switch>en
S1#config ter
Switch(config)#hostname S1 – S2
S1(config)#no ip domain-lookup
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login

S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "INGRESO NO AUTORIZADO"
S1(config)#do wr

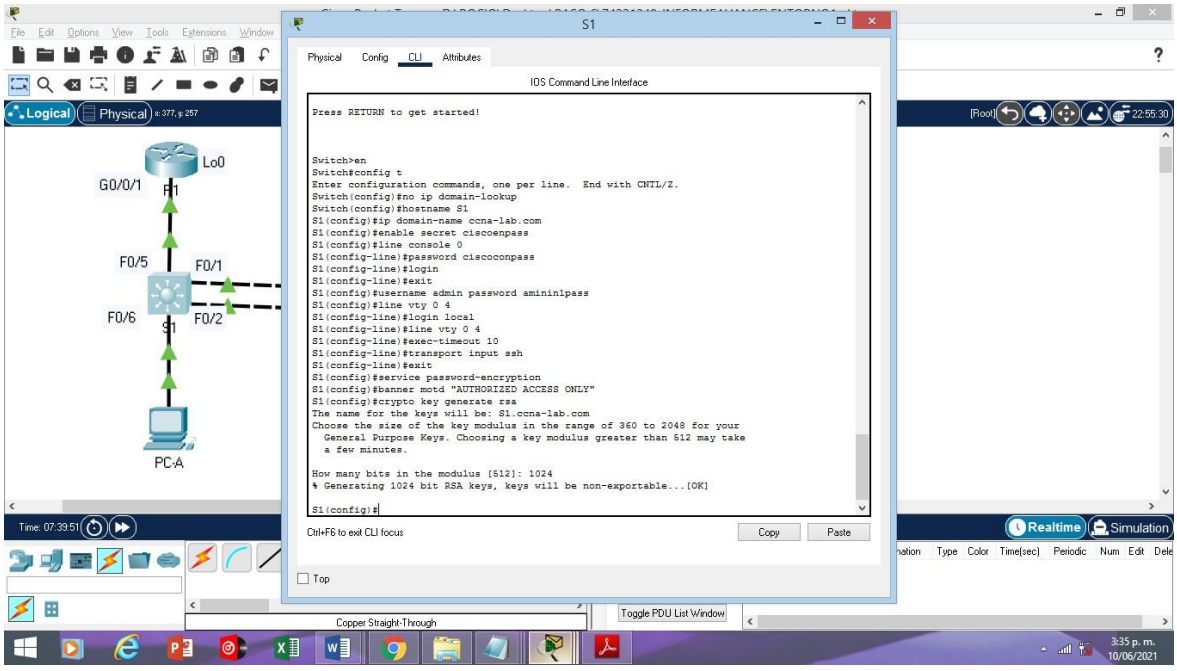


Fig.3 configuración de los Switch, fuente propia

1.3. Dominio y usuario

Configuramos el nombre del dominio, nombre de usuario, password y líneas VTY solo aceptando SSH (fig.4).

R1(config)#ip domain ccna-lab.com
R1(config)#crypto key generate rsa
R1(config)#username admin privilege 15 secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit

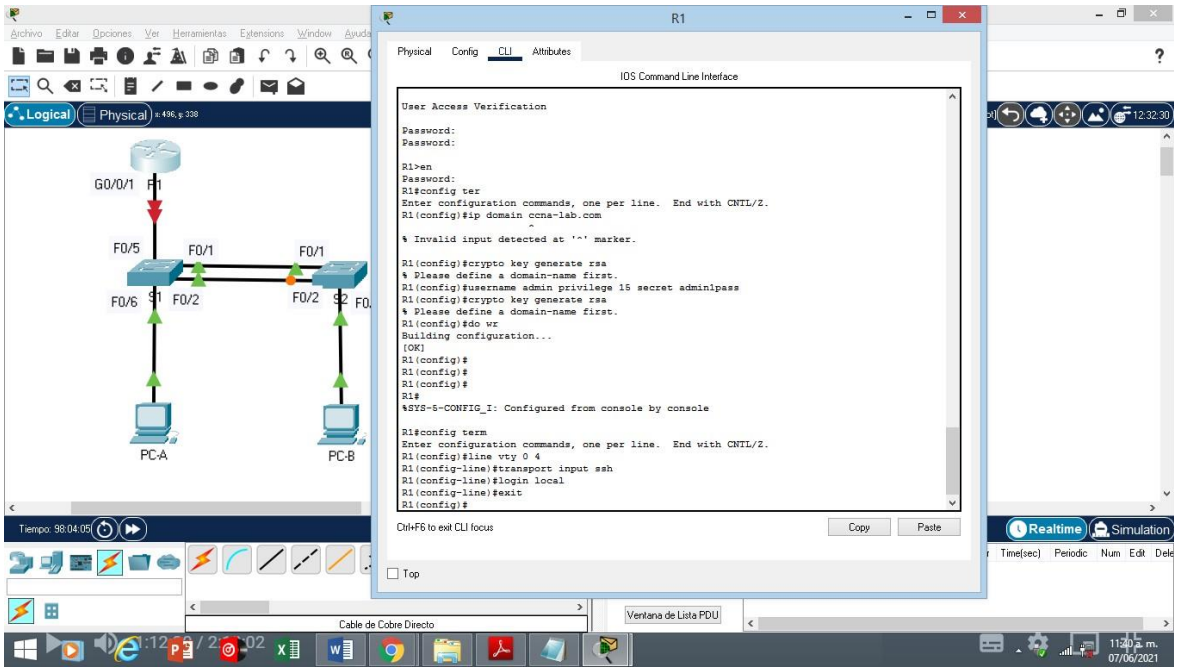


Fig.4 dominio, fuente propia

1.4. Direccionamientos ipv4 e ipv6

Configuramos las terminales G0/1, direccionamiento ipv4 e ipv6 con sus respectivas mascaras de subred, activamos la interface (fig.5), luego procedemos con la configuración loopback0.

R1(config)#interface G0/1
R1 (config-if) #ip add 10.21.5.0
R1(config-if)#ipv6 add 2001:db5:acad:1::1/64
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#description link LAN1
R1(config-if)#no shutdown
R1(config)#interface loopback0
R1(config-if)#ip add 209.165.201.1 255.255.255.0
R1(config-if)#ipv6 add 2001:db8:acad:209::1/64
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#description link Lo0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Loopback0, changed state to up

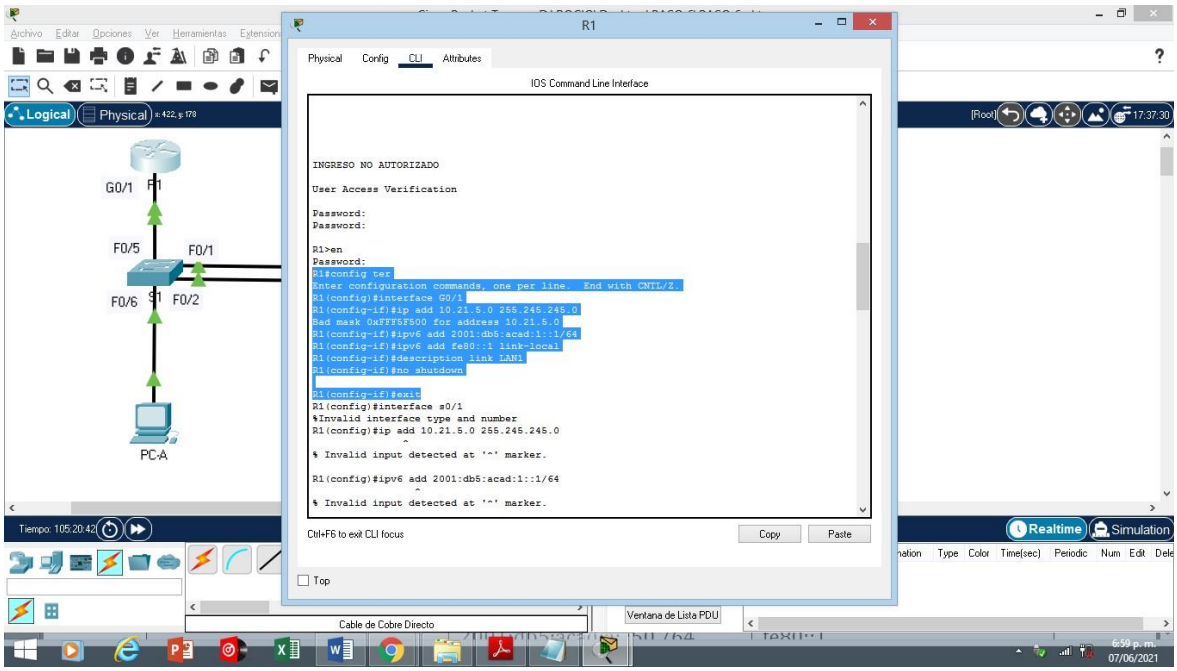


Fig.5 configuración R1 G0/1, fuente propia

1.5. Creación de VLANs

Procedemos con la creación de VLAN (fig.6) desde S1 y S2

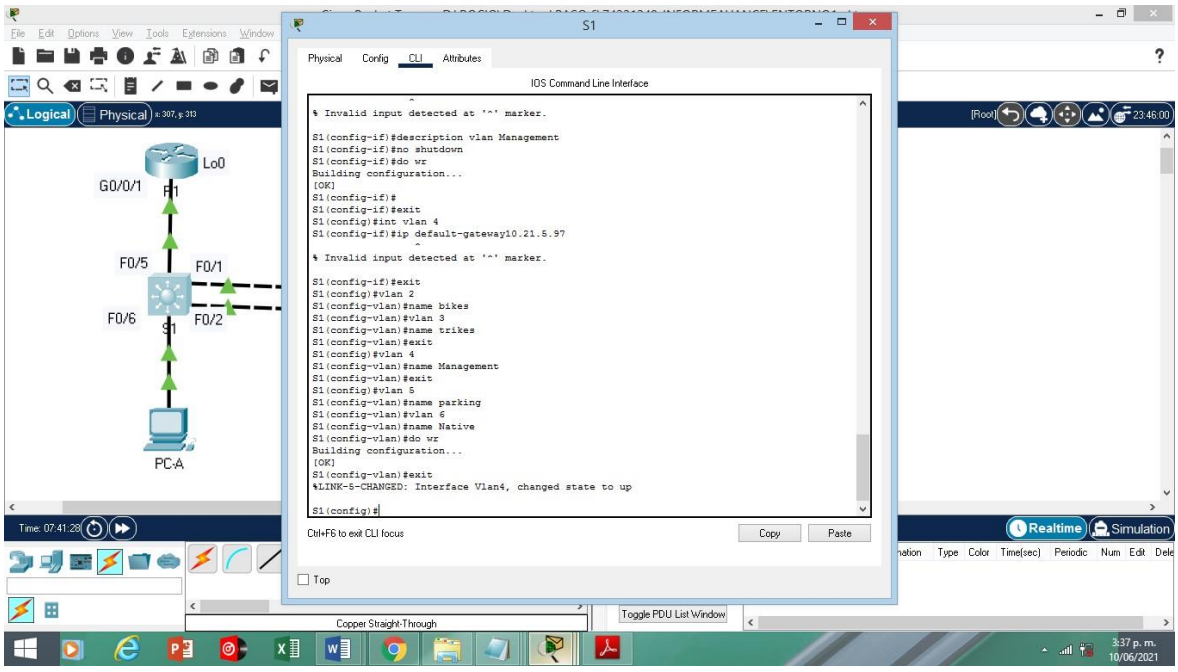


Fig.6 creación de VLAN, fuente propia

S1,S2(config)#vlan 2
S1(config-vlan)#name Bikes

S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#do wr

1.6. Creación de subinterface

Configuramos las sub interfaces de acuerdo a la tabla 2 (fig.7)

R1#config term
R1(config)#interface g0/1.2
R1(config-if)#encapsulate dotlq 2
R1(config-if)#ip add 10.21.5.1 255.255.255.192
R1(config-if)#ipv6 add 2001:db5:acad:a::1/64
R1(config-if)#exit
R1(config)#interface g0/1.3
R1(config-if)#encapsulat dotlq 3
R1(config-if)#ip add 10.21.5.65 255.255.255.224
R1(config-if)#ipv6 add 2001:db5:acad:b::1/64
R1(config-if)#exit

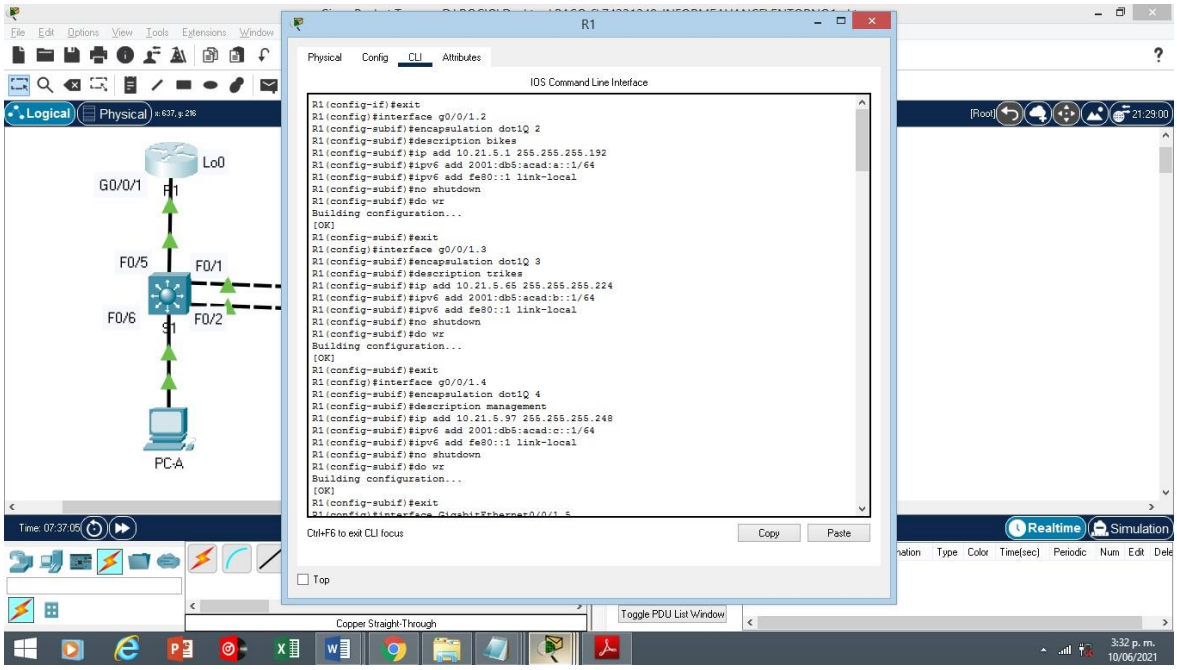


Fig.7 configuración sub interfaces, fuente propia

R1(config)#interface g0/1.4
R1(config-if)#encapsulat dotlq 4
R1(config-if)#ip add 10.21.5.97 255.255.255.248
R1(config-if)#ipv6 add 2001:db5:acad:c::1/64
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#no shutdown
R1(config-if)#exit

1.7. Configuración loopback

Con los mismos parámetros establecidos en la tabla 2 configuramos la interface loopback0 (fig.8)

R1(config)#interface L0
R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 add 2001:db8:acad:209::1/64
R1(config-if)#exit
R1(config)#do wr
Building configuration...[OK]

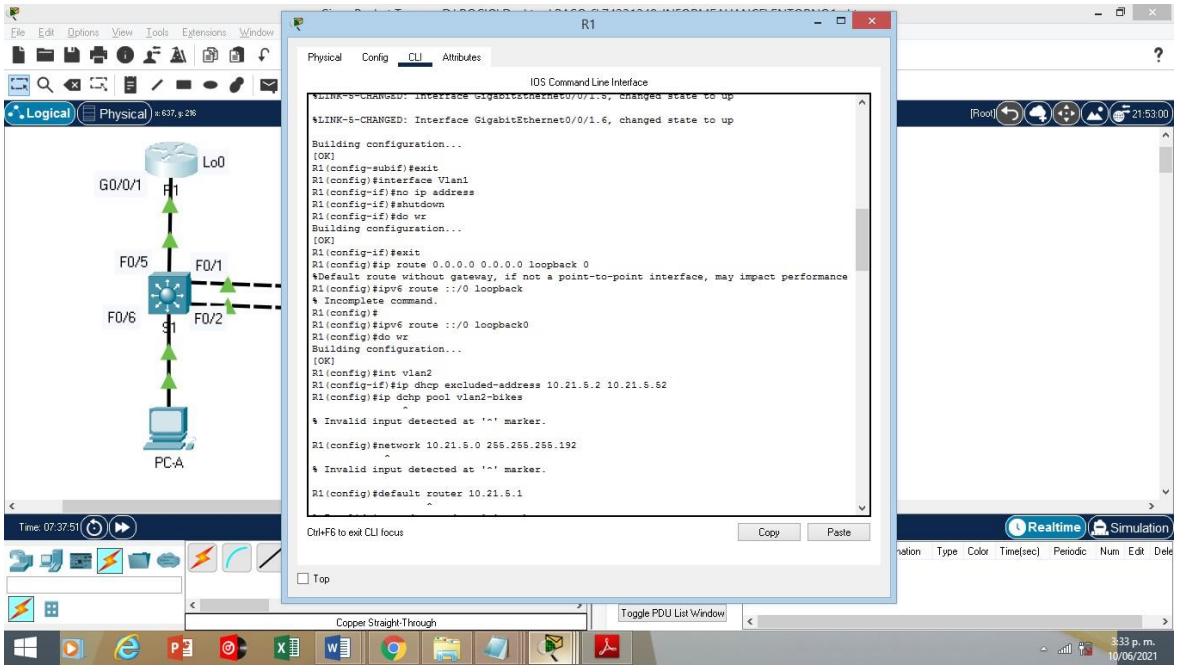


Fig.8 configuración loopback0, fuente propia

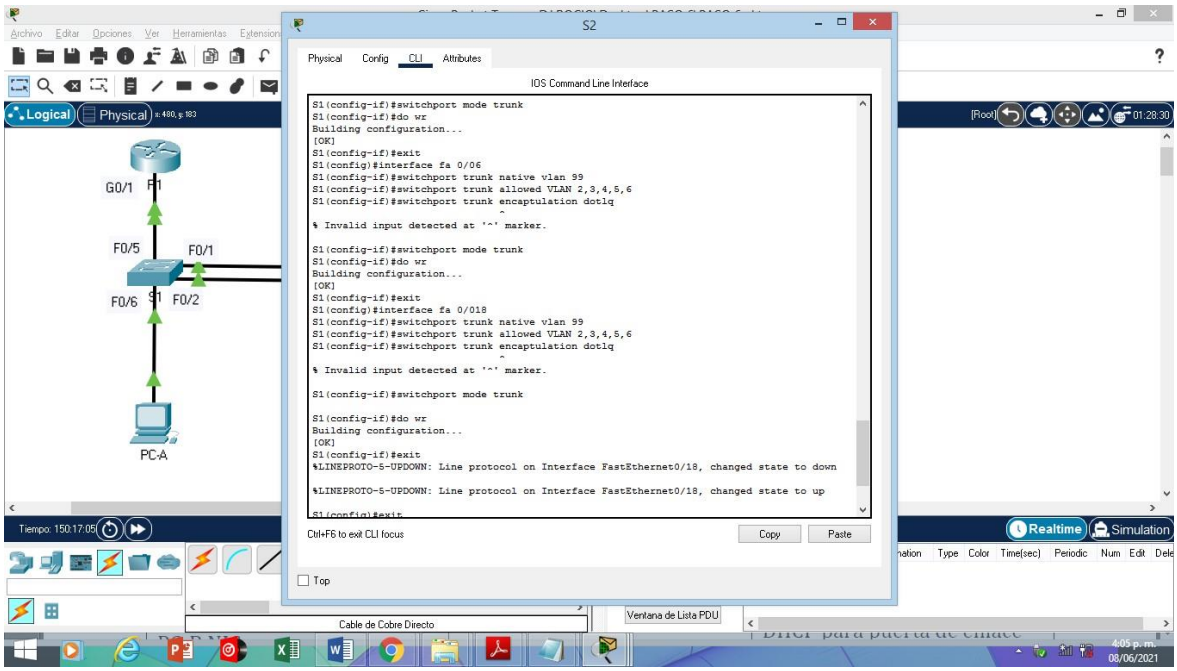


Fig.9 configuración de troncales, fuente propia

1.9. Configuración de troncales

Procedemos a configurar las troncales (fig.9) con la siguiente estructura:
interface fa 0/01
switchport trunk native vlan 99
switchport trunk allowed VLAN 2,3,4,5,6
switchport trunk encaptulation dotlq
switchport mode trunk
Con igual estructura para cada una de las interfaces.

1.9. Configuración de host

PC-A	
Descripción	
Dirección física	FaceEthernet 0/6
Dirección ip	169.254.51.70
Mascara de subred	255.255.0.0
Dirección ipv6	2001:DB5:ACAD:A::50/64
Gateway predeterminado ipv6	Fe80::1

Tabla 3. Configuración PC-A

PC-B	
Descripción	

Dirección física	FaceEthernet 0/18
Dirección ip	169.254.93.34
Mascara de subred	255.255.0.0
Dirección ipv6	2001:DB5:ACAD:A::50/64
Gateway predeterminado ipv6	Fe80::1

Tabla 4. Configuración PC-B

1.10. Conectividad de extremo a extremo.

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	*R1, G0/0/1.2*	Dirección	10.21.5.1	S=4, L=4, R=0
		IPv6	2001:db5:acad:209: :1	S=4, L=4, R=0
	R1, G0/0/1.3	Dirección	10.21.5.65	S=4, L=4, R=0
		IPv6	2001:db5:acad:b: :1	S=4, L=4, R=0
	R1, G0/0/1.4	Dirección	10.21.5.97	S=4, L=4, R=0
		IPv6	2001:db5:acad:c: :1	S=4, L=4, R=0
	S1, VLAN 4	Dirección	10.21.5.98	S=4, L=4, R=0
		IPv6	2001:db5:acad:c: :98	S=4, L=4, R=0
	S2, VLAN 4	Dirección	10.21.5.99.	S=4, L=4, R=0
		IPv6	2001:db5:acad:c: :99	S=4, L=4, R=0
PC-B	R1 Bucle 0	Dirección	209.165.201.1	S=4, L=4, R=0
		IPv6	2001:db5:acad:209: :1	S=4, L=4, R=0
	R1, G0/0/1.2	Dirección	10.21.5.1	S=4, L=4, R=0
		IPv6	2001:db5:acad:a: :1	S=4, L=4, R=0
	R1, G0/0/1.3	Dirección	10.21.5.65	S=4, L=4, R=0
		IPv6	2001:db5:acad:b: :1	S=4, L=4, R=0
	R1, G0/0/1.4	Dirección	10.21.5.97	S=4, L=4, R=0
		IPv6	2001:db5:acad:c: :1	S=4, L=4, R=0
	S1, VLAN 4	Dirección	10.21.5.98	S=4, L=4, R=0
		IPv6	2001:db5:acad:c: :98	S=4, L=4, R=0
	S2, VLAN 4	Dirección	10.21.5.99.	S=4, L=4, R=0
		IPv6	2001:db5:acad:c: :99	S=4, L=4, R=0

Tabla 5. Comprobación de conectividad por comando ping

Una vez terminamos la configuración de la red comprobamos la conectividad, Iniciamos desde los PC, ingresamos a “comand prompt” (fig.10) y enviamos el ping a cada una de las direcciones contempladas en la tabla 5.

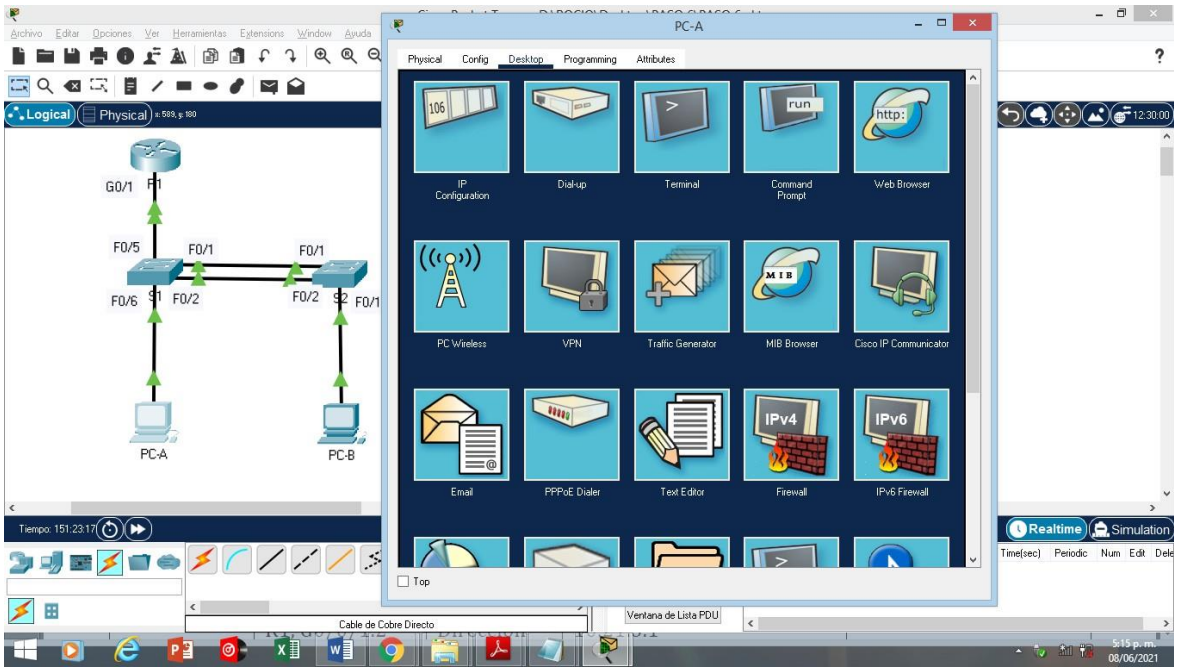


Fig.10 comand prompt, fuente propia

2. Escenario 2

En el presente escenario configuramos una pequeña red que nos permita conectividad ipv4 e ipv6, seguridad de switches y routin entre Vlans, protocolos OSPF, traducción de direcciones de red dinámicas, y estáticas, protocolos de tiempo y registros mediante comandos CLI.

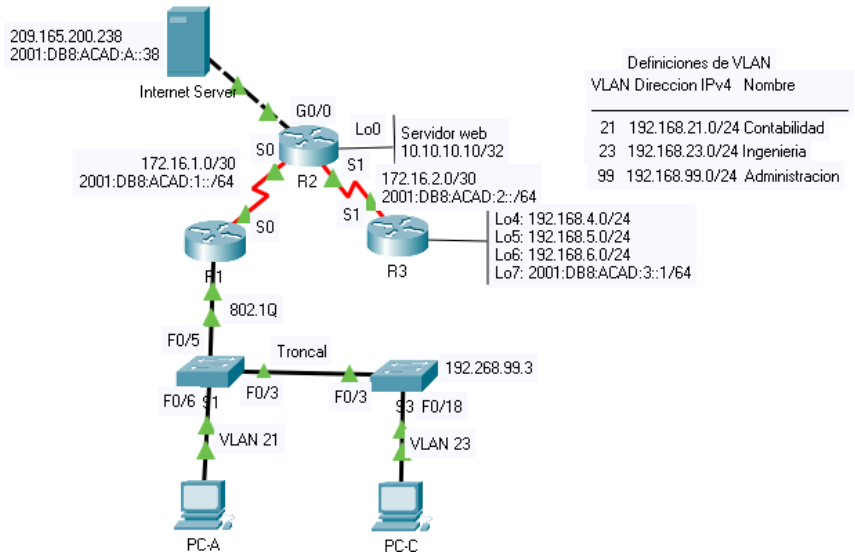


Fig.11 Topología de red, fuente propia

2.1 inicializar dispositivos

2.1.1 Inicializar y volver a cargar los Routers y Switches

Eliminamos las configuraciones iniciales, así como reiniciamos cualquier configuración que pueda ser encontrada en la RAM con el fin de evitar errores en nuestra configuración (fig.12).

TAREA	CONFIGURACION CLI
Eliminar el archivo startup-config de todos los routers	*>enable* *#erase startup-config* *#reload* *(si se encuentra el archivo vlan.dat, se elimina con #delete vlan.dat)* *>enable* *#config t* *#hostname S1*
Volver a cargar todos los routers	
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	
Volver a cargar ambos switches	
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	

Tabla 6. Configuración de switch

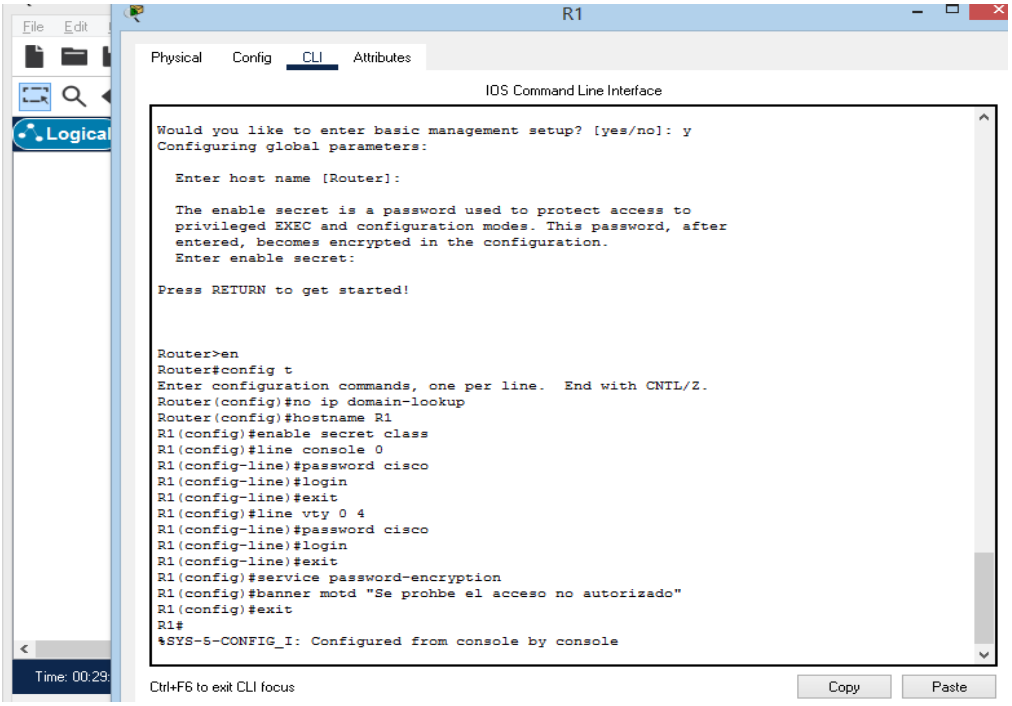


Fig.12 Configuración de Router1, fuente propia

2.2 Configurar los parámetros básicos de los dispositivos.

2.2.1 Configurar la computadora de internet.

De forma manual configuraremos los parámetros de conexión del servidor de internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::2
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 7. Configuración de Servidor

2.2.2 Configurar R1

Configuramos los parámetros iniciales en las terminales interface del router así como las rutas predeterminadas (fig.13).

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	config terminal interface serial 0/0/0 description Subred 1 ip address 172.16.1.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::1/64

	clock rate 128000 no shutdown
Rutas predeterminadas	config terminal ip route 0.0.0.0 0.0.0.0 172.16.1.2 ipv6 route ::/0 2001:DB8:ACAD:1::2

Tabla 8. Configuración R1

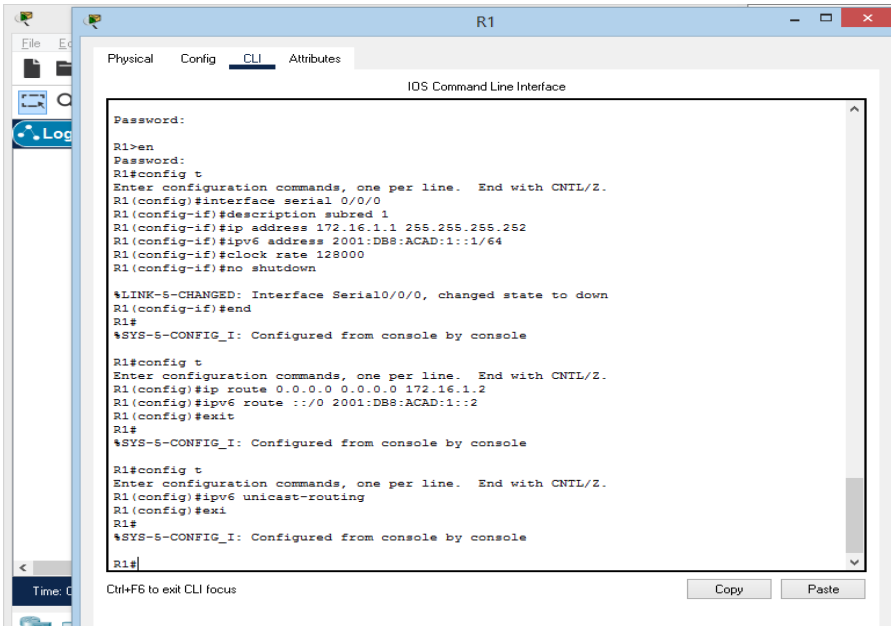


Fig.13 configuración R1, fuente propia

2.2.3 Configurar R2

Configuramos los parámetros iniciales en las terminales interface del router así como las rutas predeterminadas.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption

Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	config t interface serial 0/0/0 description Conexion a R1 ip address 172.16.1.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::2/64 no shutdown
Interfaz S0/0/1	config t interface serial 0/0/1 description Conexion a R3 ip address 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::2/64 clock rate 128000 no shutdown
Interfaz G0/0 (simulación de Internet)	config t interface gigabitEthernet 0/0 description Conexion Servidor ip address 209.165.200.233 255.255.255.248 ipv6 address 2001:DB8:ACAD:A::1/64 No shutdown
Interfaz loopback 0 (servidor web simulado)	config terminal interface loopback 0 description Conexion Servidor Web simulado ip address 10.10.10.10 255.255.255.255
Rutas predeterminadas	config terminal ip route 0.0.0.0 0.0.0.0 172.16.1.1 ipv6 route ::/0 2001:DB8:ACAD:1::1 ip route 0.0.0.0 0.0.0.0 172.16.2.1 ipv6 route ::/0 2001:DB8:ACAD:2::1 ip route 0.0.0.0 0.0.0.0 209.165.200.238 ipv6 route ::/0 2001:BD8:ACAD:A::38 ipv6 unicast-routing

Tabla 9. Configuración R2

2.2.4 Configurar R3

Configuramos los parámetros iniciales en las terminales interface del router así como las rutas predeterminadas.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	config terminal interface serial 0/0/1 description Conexion a R2 ip address 172.16.2.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::1/64 no shutdown
Interfaz loopback 4	config t interface loopback 4 description virtual 4 ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	config t interface loopback 5 description virtual 5 ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	config terminal interface loopback 6 description virtual 6 ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	config terminal interface loopback 7 description 7 ip address 2001:db8:acad:3::1/64

Tabla 10. Configuración R3

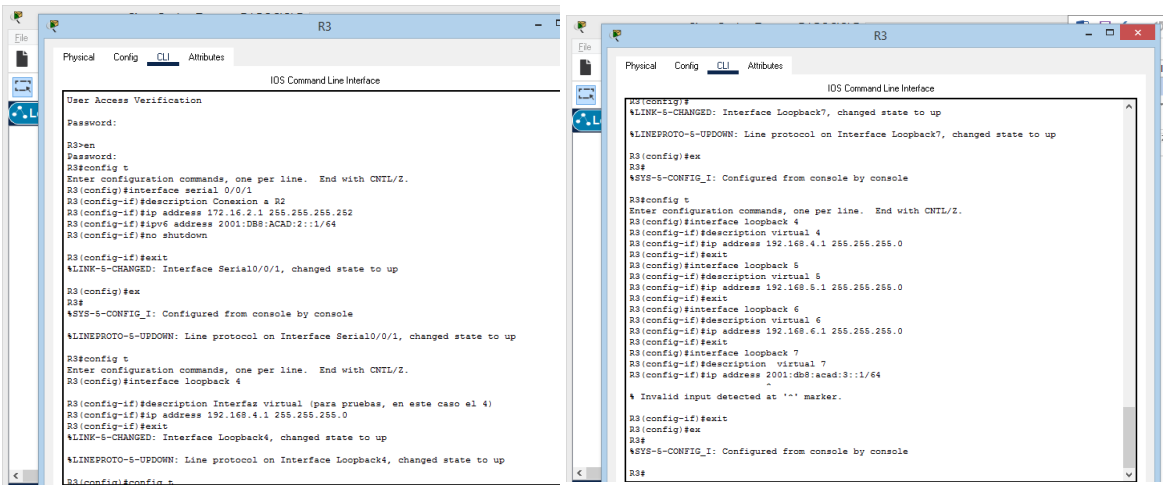


Fig.14 configuracion R3, fuente propia

2.2.5 Configurar S1

Configuramos parámetros básicos de seguridad del Switch.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 11. Configuración S1

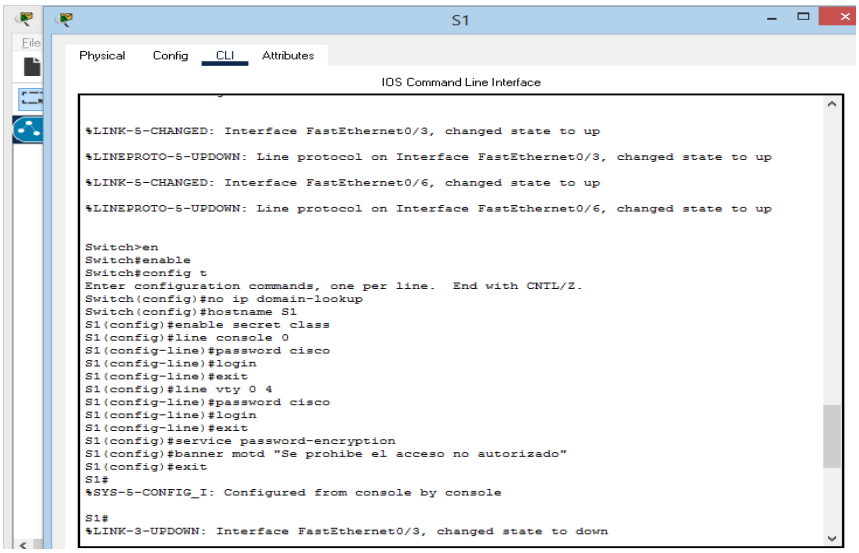


Fig.15 Configuración S1, fuente propia

2.2.6 Configurar S3

Configuramos parámetros básicos de seguridad del Switch (fig.16).

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla 12. Configuración S3

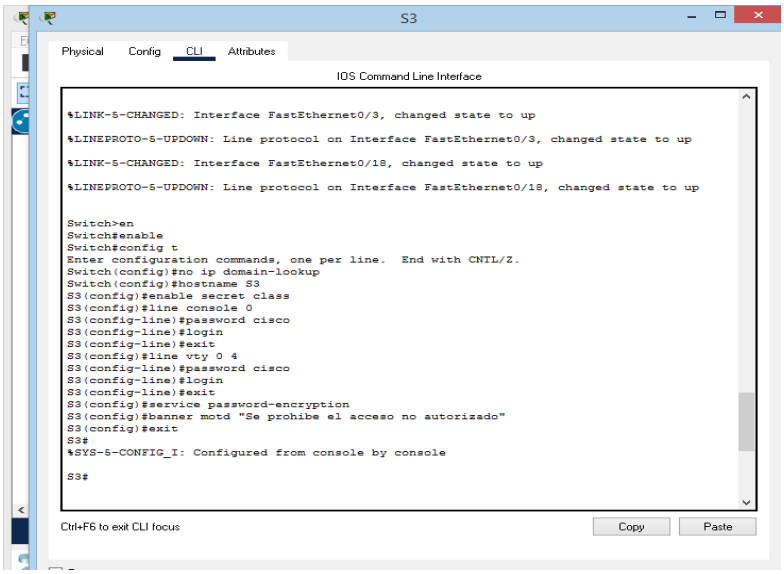


Fig.16 Configuración S3, fuente propia

2.2.7 verificar la conectividad de red

Mediante el comando *ping* verificamos conectividad de acuerdo a la siguiente tabla:

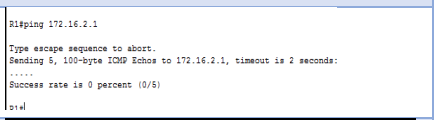
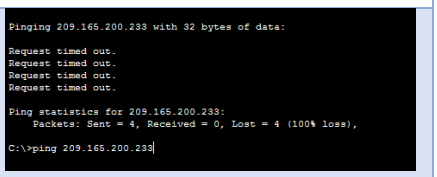
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	
R2	R3, S0/0/1	172.16.2.1	
PC de internet	Gateway predeterminado	209.165.200.233	

Tabla 13. Resultados de ping

2.3 Configurar la seguridad del switch, las VLAN y el routing entre VLAN.

2.3.1 Configuración en S1.

Creamos la base de datos de las Vlan y generamos el routing en ellas (fig.17).

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	*config terminal*

	vlan 21 *name Contabilidad* *vlan 23* *name Ingeniería* *vlan 99* *name Administración*
Asignar la dirección IP de administración.	*config terminal* *interface Vlan 99* *ip address 192.168.99.2 255.255.255.0*
Asignar el Gateway predeterminado	*config terminal* *ip default-Gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	*config terminal* *interface fastEthernet 0/3* *switchport mode trunk* *switchport trunk native vlan 1*
Forzar el enlace troncal en la interfaz F0/5	*config terminal* *interface fastEthernet 0/5* *switchport mode trunk* *switchport trunk native vlan 1*
Configurar el resto de los puertos como puertos de acceso	*config terminal* *interface range fastEthernet 0/1-2, f0/4, f0/6-24, g0/1-2* *switchport mode access*
Asignar F0/6 a la VLAN 21	*config terminal* *interface fastEthernet 0/6* *switchport access vlan 21*
Apagar todos los puertos sin usar	*config terminal* *interface range fastEthernet 0/1-2, f0/4, f0/7-24, g0/1-2* *shutdown*

Tabla 14. Configuración de VLAN S1

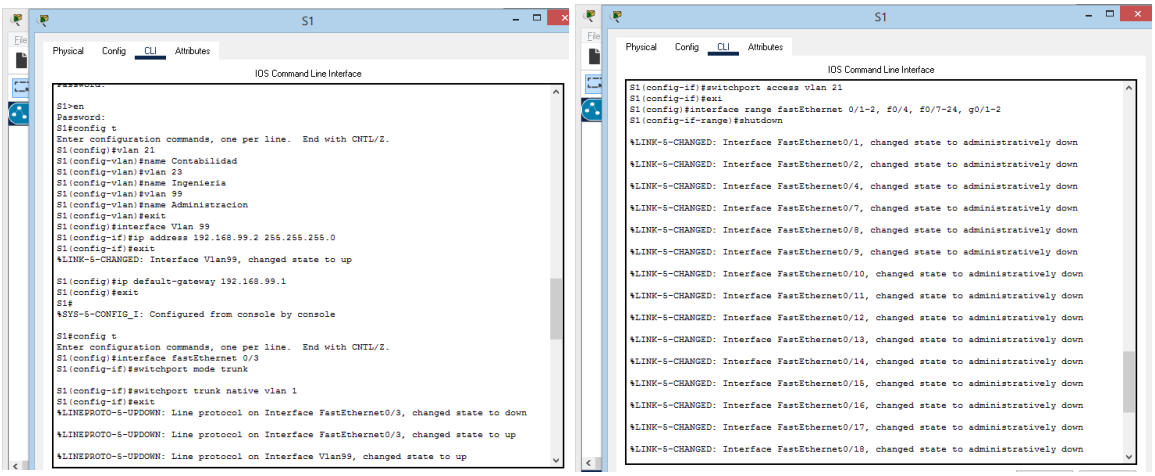


Fig.17 VLANS en S1, fuente propia

2.3.2 Configuración en S3.

Iniciamos la configuración de seguridad del Switch, luego creamos las Vlan y generamos el routing en ellas.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	*config terminal* *vlan 21* *name Contabilidad* *vlan 23* *name Ingenieria* *vlan 99* *name Administración*
Asignar la dirección IP de administración.	*config terminal* *interface Vlan 99* *ip address 192.168.99.3 255.255.255.0*
Asignar el Gateway predeterminado	*config t* *ip default-gateway 192.168.99.1*
Forzar el enlace troncal en la interfaz F0/3	*config terminal* *interface fastEthernet 0/3* *switchport mode trunk* *switchport trunk native vlan 1*
Configurar el resto de los puertos como puertos de acceso	*config terminal* *interface range fastEthernet 0/1-2, f0/4-24, g0/1-2* *switchport mode access*

Asignar F0/18 a la VLAN 23	*config terminal* *interface fastEthernet 0/18* *switchport access vlan 23*
Apagar todos los puertos sin usar	*config terminal* *interface range fastEthernet 0/1-2, f0/4-17, f0/19-24, g0/1-2* *shutdown*

Tabla 15. Configuración de seguridad S3

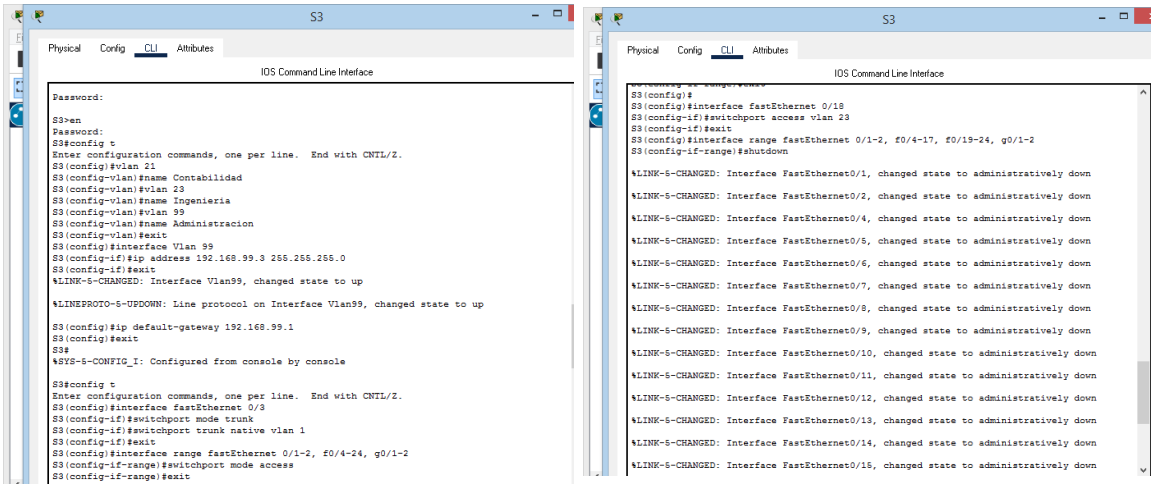


Fig.18 VLANS en S3, fuente propia

2.3.3 Configuración en R1.

Realizamos la configuración de las subinterfaces, dentro del protocolo 802.1 Q, dentro de la interface G0/1(fig.19).

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	*config terminal* *interface gigabitEthernet 0/1.21* *encapsulation dot1Q 21* *ip address 192.168.21.1 255.255.255.0* *description LAN de contabilidad VLAN 21* *no shutdown*
Configurar la subinterfaz 802.1Q .23 en G0/1	*config terminal* *interface gigabitEthernet 0/1.23* *encapsulation dot1Q 23* *ip address 192.168.23.1 255.255.255.0* *description LAN de Ingenierai VLAN 23* *no shutdown*

Configurar la subinterfaz 802.1Q .99 en G0/1	*config terminal* *interface gigabitEthernet 0/1.99* *encapsulation dot1Q 99* *ip address 192.168.99.1 255.255.255.0* *description LAN de Administración VLAN 99* *no shutdown*
Activar la interfaz G0/1	*config t* *interface gigabitEthernet 0/1* *no shutdown*

Tabla 16. Configuración de seguridad R1

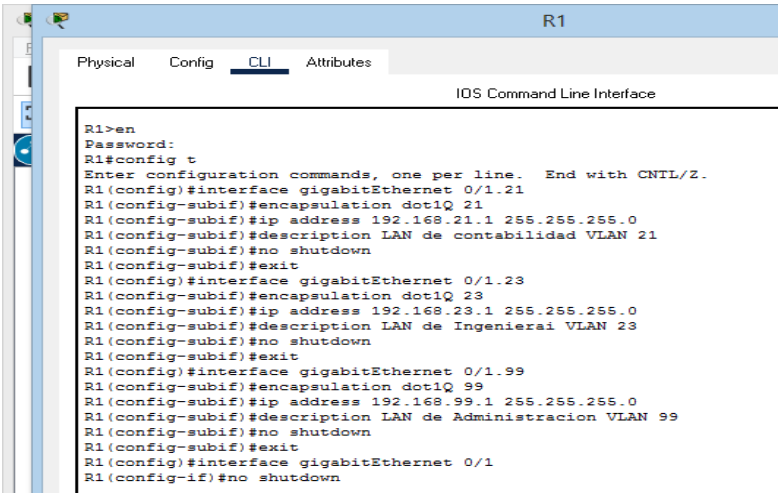


Fig.19 Subinterfaces en R1, fuente propia

2.3.4 Verificar la conectividad de red

Mediante el comando *ping* (fig.20) verificamos conectividad de acuerdo a la siguiente tabla:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Tabla 17. Resultados de ping

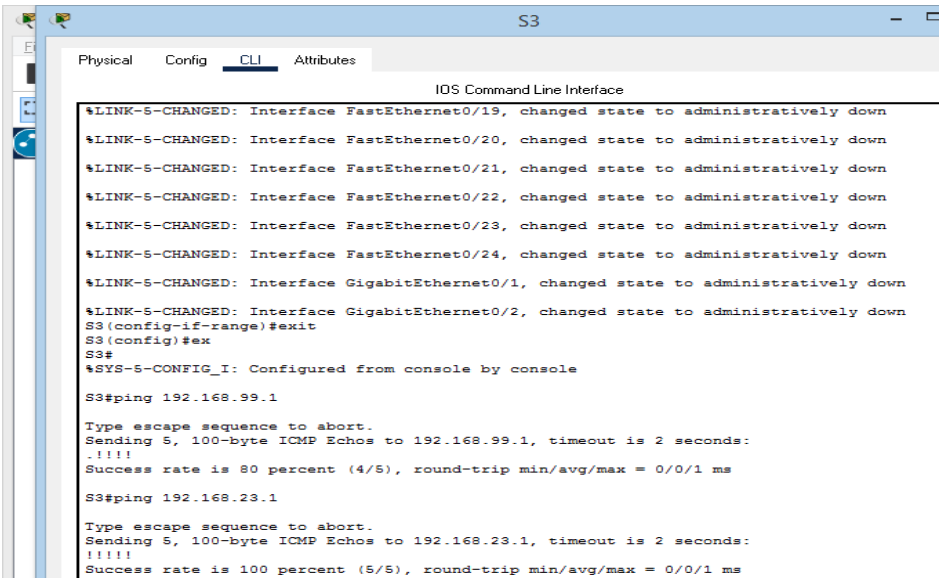


Fig.20 ping desde Switchs, fuente propia

2.4 Configurar el protocolo de routing dinámico OSPF

2.4.1 Configurar OSPF en el R1

OSPF es un protocolo de enrutamiento abierto del tipo link state, es utilizado para encontrar la mejor ruta entre dos puntos, de acuerdo a la tabla iniciamos la configuración en R1 (fig.21).

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	*config t* *router ospf 1* *network 172.16.1.0 0.0.0.3 area 0*
Anunciar las redes conectadas directamente	*network 192.168.21.0 0.0.0.255 area 0* *network 192.168.23.0 0.0.0.255 area 0* *network 192.168.99.0 0.0.0.255 area 0*
Establecer todas las interfaces LAN como pasivas	*passive-interface gigabitEthernet 0/1.21* *passive-interface gigabitEthernet 0/1.23* *passive-interface gigabitEthernet 0/1.99*
Desactive la sumarización automática	*no auto-summary*

Tabla 18. Configuración de OSPF R1

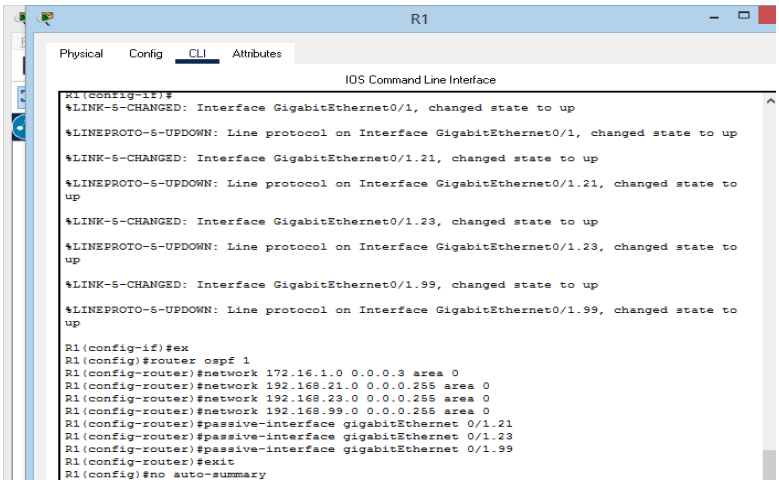


Fig.21 configuración OSPF en R1, fuente propia

2.4.2 Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	*config terminal* *router ospf 1* *network 10.10.10.10 0.0.0.0 area 0*
Anunciar las redes conectadas directamente	*network 172.16.1.0 0.0.0.255 area 0* *network 172.16.2.0 0.0.0.255 area 0*
Establecer la interfaz LAN (loopback)como pasivas	*passive-interface loopback 0*
Desactive la sumarización automática	*no auto-summary*

Tabla 19. Configuración de OSPF R1

2.4.3 Configurar OSPFv3 en el R2

Continuamos las configuraciones del protocolo OSPFv3 para IPv6 en los routers y terminamos con el R2 (fig.22).

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	*router ipv6 ospf 1*
Anunciar las redes IPv4 conectadas directamente	*config terminal* *interface gigabitEthernet 0/0* *ipv6 ospf 1 area 0*

	interface serial 0/0/0 *ipv6 ospf 1 area 0* *interface serial 0/0/1* *ipv6 ospf 1 area 0*
Establecer todas las interfaces LAN IPv4 (loopback) como pasivas	*passive-interface loopback 4* *passive-interface loopback 5* *passive-interface loopback 6* *passive-interface loopback 7*
Desactive la sumarización automática	*no auto-summary*

Tabla 20. Configuración de OSPFv3 R2

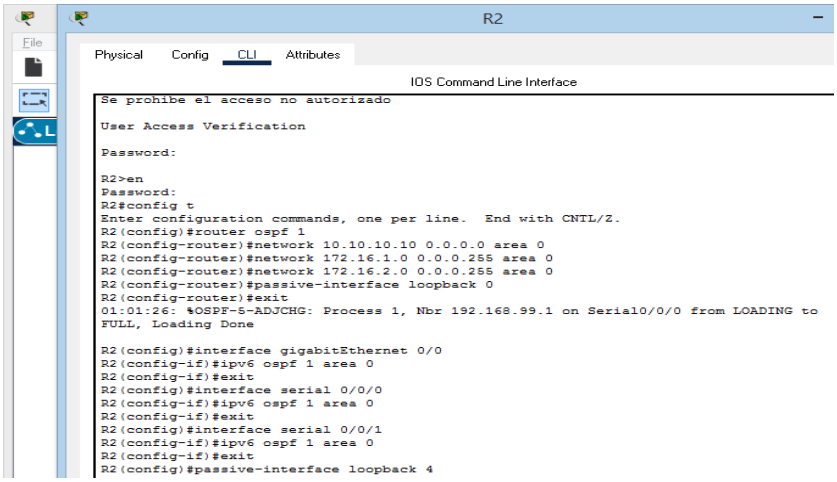


Fig.22 configuración OSPFv3 en R2, fuente propia

2.4.4 Verificación de la información de OSPF

¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?

Show running-configuration

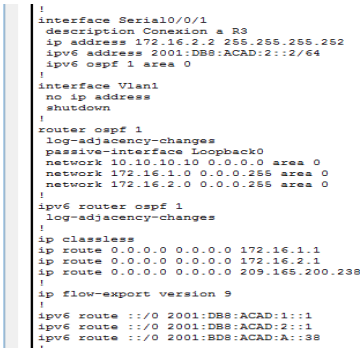


Fig.23 show running-config, fuente propia

¿Qué comando muestra solo las rutas OSPF?
show ip route ospf

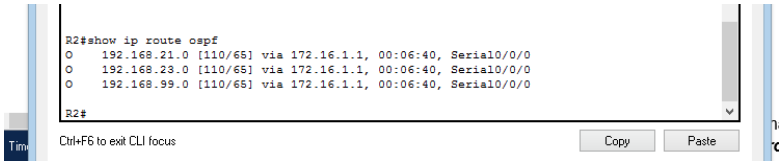


Fig.25 show ip route ospf, fuente propia

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?
Show ip ospf interface<*interface*>

2.5 Implementar DHCP y NAT para IPv4

2.5.1 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	*config terminal* *ip dhcp excluded-address 192.168.21.1 192.168.21.20*
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	*config terminal* *ip dhcp excluded-address 192.168.23.1 192.168.23.20*
Crear un pool de DHCP para la VLAN 21.	*config terminal* *ip dhcp pool ACCT* *network 192.168.21.0 255.255.255.0* *default-router 192.168.21.1* *dns-server 10.10.10.10* *domain-name ccna-sa.com*
Crear un pool de DHCP para la VLAN 23	*config terminal* *ip dhcp pool ENGNR* *network 192.168.23.0 255.255.255.0* *default-router 192.168.23.1* *dns-server 10.10.10.10* *domain-name ccna-sa.com* *(fig.26)*

Tabla 21. Configuración de R1 como servidor

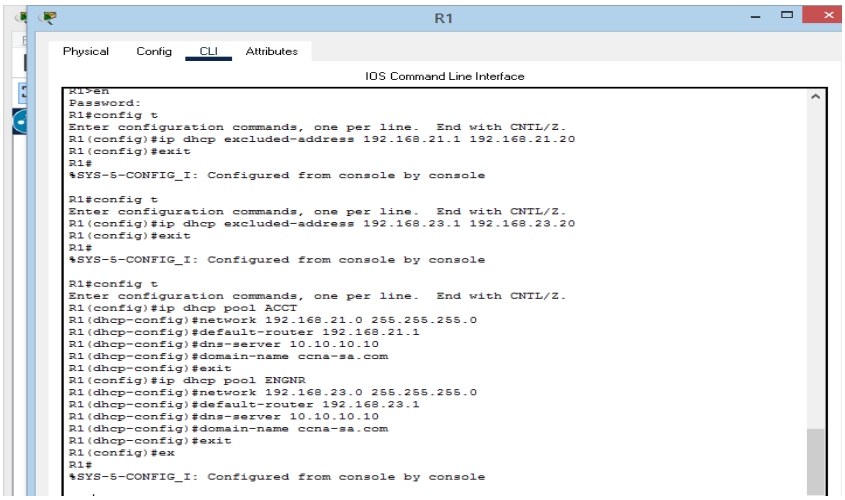


Fig.26 R1 como servidor, fuente propia

2.5.2 Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	*config terminal* *username webuser privilege 15 password cisco12345*
Habilitar el servicio del servidor HTTP	*Packet Tracert no recibe ip http server*
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	*Packet Tracert no recibe ip http server*
Crear una NAT estática al servidor web.	*Dirección global interna: 209.165.200.229*
Asignar la interfaz interna y externa para la NAT estática	*config terminal* *ip nat inside source static 10.10.10.10 209.165.200.229*
Configurar la NAT dinámica dentro de una ACL privada	*config terminal* *interface gigabitEthernet 0/0* *ip nat outside* *interface loopback 0* *ip nat inside* *config t* *access-list 1 permit 192.168.21.0 0.0.0.255* *access-list 1 permit 192.168.23.0 0.0.0.255*

	access-list 1 permit 192.168.4.0 0.0.0.255 *access-list 1 permit 192.168.5.0 0.0.0.255* *access-list 1 permit 192.168.6.0 0.0.0.255*
Defina el pool de direcciones IP públicas utilizables.	*config terminal* *ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248* *exit*
Definir la traducción de NAT dinámica	*config terminal* *ip nat inside source list 1 pool INTERNET (fig.27)*

Tabla 22. Configuración de la NAT

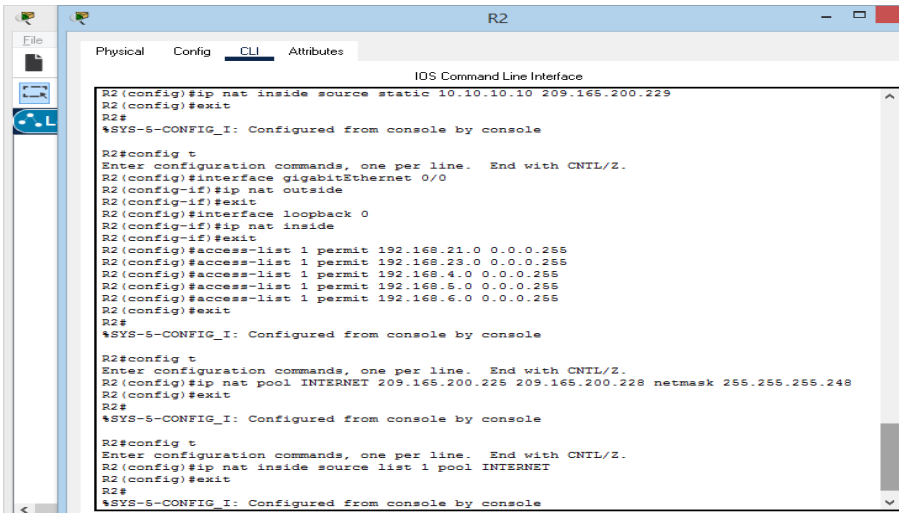
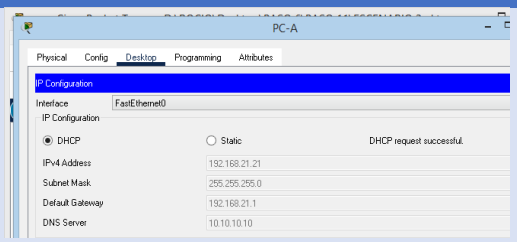
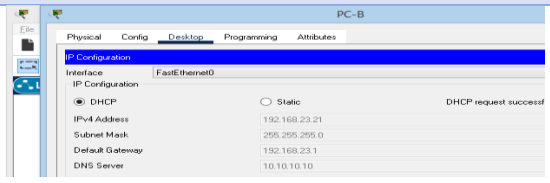


Fig.27 configuración NAT, fuente propia

2.5.3 Verificar el protocolo DHCP y la NAT estática

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

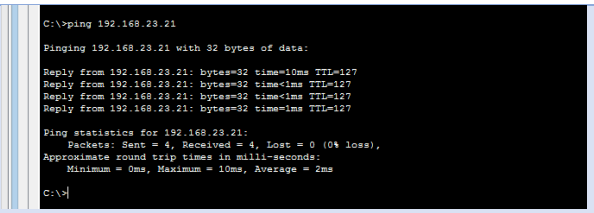
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

Tabla 23. Protocolo DHCP y NAT estática

En la tabla 23 observamos que en su mayoría el protocolo de asignación de direcciones DHCP está funcionando correctamente (fig.28).

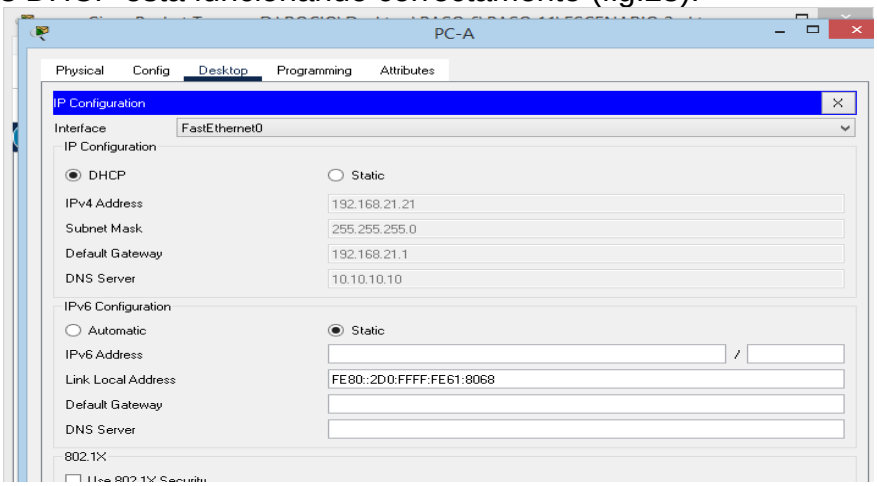


Fig.28 pin PC-A a PC-C, fuente propia

2.6 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	*clock set 09:00:00 05 March 2016*
Configure R2 como un maestro NTP.	*config terminal* *ntp master 5*
Configurar R1 como un cliente NTP.	*config terminal* *ntp server 172.16.1.2*

Configure R1 para actualizaciones de calendario periódicas con hora NTP.	*config terminal* *ntp update-calendar*

Verifique la configuración de NTP en R1.	*show clock detail*
	`R1#show clock detail`
	`11:44:51.891 UTC Sat Mar 5 2016`
	`Time source is NTP`
	`R1#`

Tabla 24. Configuración NTP

2.7 Configurar y verificar las listas de control de acceso (ACL)

2.7.1 Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	*config terminal* *ip access-list standard ADMIN-MGT* *permit host 172.16.1.1*
Aplicar la ACL con nombre a las líneas VTY	*config terminal* *line vty 0 4* *access-class ADMIN-MGT in*
Permitir acceso por Telnet a las líneas de VTY	*config terminal* *line vty 0 4* *transport input telnet*

Verificar que la ACL funcione como se espera	*show access-list*
	`R2>en`
	`Password:`
	`R2#show access-list`
	`Standard IP access list 1`
	`10 permit 192.168.21.0 0.0.0.255`
	`20 permit 192.168.23.0 0.0.0.255`
	`30 permit 192.168.4.0 0.0.0.255`
	`40 permit 192.168.5.0 0.0.0.255`
	`50 permit 192.168.6.0 0.0.0.255`
	`Standard IP access list ADMIN-MGT`
	`10 permit host 172.16.1.1`

Tabla 25. Restricción de accesos

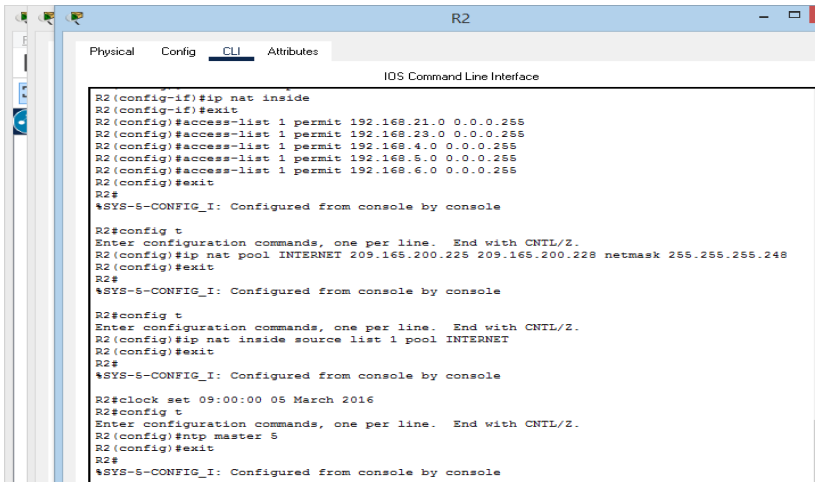


Fig.29 restricción de accesos, fuente propia

2.7.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente:

Descripción del comando	Entrada del estudiante (comando)

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	*show access-list*
	`R2>en`
	`Password:`
	`R2#show access-list`
	`Standard IP access list 1`
	`10 permit 192.168.21.0 0.0.0.255`
	`20 permit 192.168.23.0 0.0.0.255`
	`30 permit 192.168.4.0 0.0.0.255`
	`40 permit 192.168.5.0 0.0.0.255`
	`50 permit 192.168.6.0 0.0.0.255`
	`Standard IP access list ADMIN-MGT`
	`10 permit host 172.16.1.1`

Restablecer los contadores de una lista de acceso	*clear ip access-list counters*
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	*Show ip access-list*

¿Con qué comando se muestran las traducciones NAT?	*Show ip nat translations*
	`R2#show ip nat translations`
	`Pro Inside global Inside local Outside local Outside global`
	`--- 209.165.200.229 10.10.10.10 --- ---`
	`R2#`

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*clear ip nat translations*

Tabla 26. Comandos CLI

CONCLUSIONES

Es fundamental el presentar una estructura definida, el llevar el paso a paso en el momento de configurar la red nos permitirá llevar a cabo lo planeado.

La utilización de herramientas que nos permitan la configuración correcta y ágil de las redes dentro de una estructura definida nos permitirá observar, contemplar, analizar y ejecutar los planteamientos requeridos.

El conocer la estructura de las direcciones ipv4 e ipv6 nos permite implementarlas y aplicarlas de una forma más fácil y eficaz.

La herramienta paket-tracer nos permitió conocer y trabajar sobre un ambiente simulado, las diferentes configuraciones, conexiones y protocolos de configuración en equipos intermedios, trabajando en ellos sobre un sistema seguro y confiable.

El escenario 2 nos permite ahondar conocimientos sobre direccionamiento ospf, además de la configuración de VLAN en subredes, se configura el Router como servidor DHCP y sus conexiones desde y hacia los Switch de modo troncal, a su vez, cada Switch se conecta a su LAN con modo de acceso.

BIBLIOGRAFÍA

CISCO NETWORKYN ACADEMY, Prueba de habilidades prácticas CCNA, © 2021.

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference.

Luis T. Wayar, Protocolo de red ipv6, edición 1

MarioTechAcademy. (11 de Noviembre de 2013). CS071 21.02 OSPF - Configuracion OSPF en Packet Tracer. Obtenido de https://youtu.be/lw-IekHi9eY

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

Por: Rincón Gallo Omar G.

Resumen-En este documento configuramos una pequeña red LAN, mediante la utilización del Software Packet Tracer de la CISCO NETWORKING ACADEMY en su versión 8.0, en el utilizamos Routers, Switchts y host finales en los que configuramos la seguridad, de los dispositivos, protocolo de routing dinámico OSPF, direcciones red dinámicas y estáticas y listas de control de acceso, entre otras; hemos trabajado cada uno de los pasos para llegar al fin, operación y conectividad de la red montada en el simulador.

I INTRODUCCION

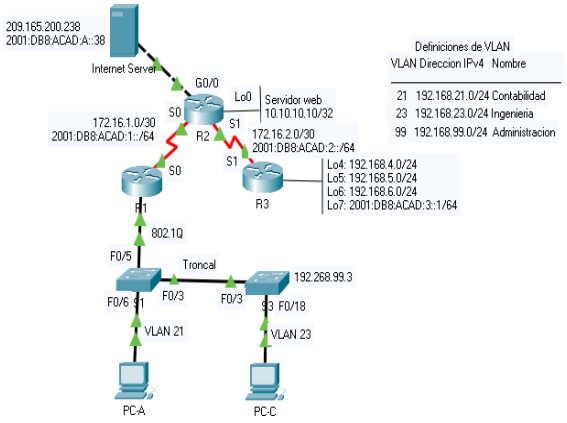
En el afán de encontrar soluciones de conectividad y para suplir muchos de los requerimientos de un mercado que día a día es más exigente; y que cada competencia nos trae retos y nuevos e innovadores propuestas, no solo encontramos la diversidad en el servicio, sino que también encontramos múltiples amenazas sobre ellos; lo que hace más vulnerables las estabilidades y sistemas de seguridad; en especial de las grandes empresas que podrían llegar a tener una perdida incalculable en sus finanzas; es por ello que mediante sistemas seguros y complejos, bien definidos y estructurados buscamos implementar diseños que estén lo más cerca posible de estos requerimientos y que ofrezcan la posibilidad de ser parte fundamental del funcionamiento del mundo moderno.

En esta prueba buscamos implementar conocimientos y practica de ellos en el trabajo sobre el escenario propuesto; lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Cada uno de los requerimientos han sido evaluados, investigados y probados en el simulador *Packet Tracer* de la CISCO NETWORKING ACADEMY, herramienta que nos ha permitido mediante la implementación de diferentes escenarios y de manera virtual, el diseño de topologías, montaje y conexión de ellas, y llegar mediante la prueba y error a configurar y plantear la solución al problema propuesto.

Se aplicaron los conocimientos adquiridos a lo largo del curso, sobre todo con los protocolos de enrutamiento OSPF, aplicamos su configuración básica en dispositivos de red, desactivamos actualizaciones de enrutamiento en las interfaces adecuadas, así como verificamos sistemáticamente la conectividad entre los dispositivos de la topología.

II SOLUCION DEL CASO



Topología de la Red.

Encontramos una pequeña Red LAN con un servidor de internet, tres (3) Routers CISCO 1941, dos (2) Switchs C2960 y dos (2) computadoras genéricas como Host finales; en la topología podemos observar el direccionamiento de cada uno de los dispositivos y la configuración de la red, la identificación de cada una de las interfaces físicas y virtuales (VLAN).

a. inicializar dispositivos

Eliminamos las configuraciones iniciales, así como reiniciamos cualquier configuración que pueda ser encontrada en la RAM con el fin de evitar errores en la ejecución de la solución y nueva configuración de la red, para ello iniciamos ingresando a los dispositivos en la ventana CLI de configuración, ingresamos al modo exec privilegiado mediante el comando *enable*, una vez nos encontramos en este, ingresamos el comando *erase startup-config*, con el fin de eliminar la configuración, volvemos a cargar la configuración de fábrica con el comando *reload*, revisamos si se encuentra el archivo *vlan.dat* mediante el comando *show vlan*, de encontrarse los eliminamos mediante el comando *delete vlan.dat.*

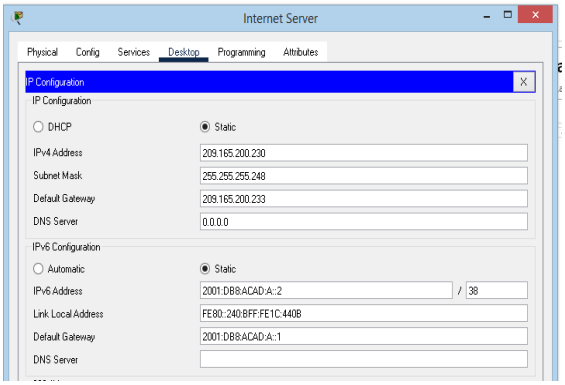
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]

```
Router>en
Router#show vlan.dat
                ^
% Invalid input detected at '^' marker.

Router#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------
```

Show vlan

***b.* Configurar la computadora de internet.**

Ingresamos a la configuración del servidor de internet en la ventana de servicios habilitamos HTTP y HTTPS, ingresamos a desktop y configuramos las direcciones de forma manual.



Internet server

***c.* Configurar Routers**

Dentro de las configuraciones iniciales de los routers, desactivamos la búsqueda de DNS; en los dispositivos si escribimos el nombre de un comando y se comete un error en el nombre, el enrutador Cisco supondrá que el nombre debe ser resuelto mediante una búsqueda de DNS, durante este proceso se bloqueará el teclado y generará demoras al ingresar comandos de configuración, es por ello que desactivamos por completo las búsquedas de DNS (*No ip domain-lookup*). Asignamos un nombre as los routers (R1, R2, R3), asignamos las contraseñas correspondientes (*cisco, class*) y encriptamos para evitar sean visualizadas (*service password-encryption*); iguales configuraciones que realizamos en los **Switchs** (S1 y S3), luego en los Routers configuramos las terminales y las rutas predeterminadas.

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0/0
R2(config-if)#description Conexion a R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown

R2(config-if)#exit
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config)#ex
R2#
%SYS-5-CONFIG_I: Configured from console by console

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0/1
R2(config-if)#description Conexion a R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no shutdown
```

Interfaces y rutas predeterminadas

***d.* verificar la conectividad de red.**

Mediante la aplicación del comando ping verificamos la conexión existente entre los dispositivos configurados hasta el momento y es así como vamos revisando metódicamente el avance de la solución al escenario propuesto, esta es una herramienta utilizable en el momento de comprobar la efectividad de nuestra simulación, al realizarla durante todo el proceso podemos identificar y controlar los posibles errores en cada una de las etapas de este.

```
R1#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Comando ping

***e.* Configurar VLAN en los Switchs**

Iniciamos creando la base de datos de las VLAN, asignamos la dirección IP a la VLAN 99 como administrativa.

```
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#interface Vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config)#ip default-gateway 192.168.99.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Base de datos VLAN

Configuramos un Gateway predeterminado con el que conectara el Switch, forzamos los enlaces con las troncales *switchport mode trunk;* los enlaces troncales son para facilitar la inter-comunicación entre las distintas VLANs [1], configuramos los demás puertos y desactivamos los demás puertos que no han sido asignados a ningún dispositivo.

f. Configuración de subinterfaces en R1

Configuramos las subinterfaces en R1, correspondientes a las VLAN (21, 23, 99), en ellas encapsulamos de acuerdo a 802.1Q, asignamos una dirección IP con su respectiva mascara de subred y asignamos una descripción; luego activamos la subinterface mediante el comando *no shutdown*.

```
R1(config)#interface gigabitEthernet 0/1.21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#description LAN de contabilidad VLAN 21
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#description LAN de Ingenierai VLAN 23
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#description LAN de Administracion VLAN 99
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown
```

Subinterfaces.

g. Verificar conectividad

Nuevamente realizamos una revisión de la conectividad utilizando el comando ping, así verificamos la eficacia de la solución y revisamos si hasta el momento tenemos algún posible error en conexión entre los dispositivos.

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Pin desde Switchs

h. Configurar OSPF en el R1

OSPF es un protocolo de enrutamiento abierto del tipo link state, es utilizado para encontrar la mejor ruta entre dos puntos, de acuerdo a la tabla iniciamos la configuración en R1 [2]. Configuramos OSPF área 0, anunciamos las redes conectadas directamente, establecemos todas las LAN (21, 23, 99) como pasivas y desactivamos la autosumarizacion.

IOS Command Line Interface

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to
up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to
up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to
up

R1(config-if)#ex
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface gigabitEthernet 0/1.21
R1(config-router)#passive-interface gigabitEthernet 0/1.23
R1(config-router)#passive-interface gigabitEthernet 0/1.99
R1(config-router)#exit
R1(config)#no auto-summary
```

OSPF en R1

i. Configurar OSPF y OSPFv3 en el R2

Al igual que en el R1 Configuramos OSPF área 0; tenemos en cuenta que para OSPFv3 la configuración es *router ipv6 ospf 1*, anunciamos las redes conectadas directamente, establecemos la loopback como pasiva e igualmente desactivamos la sumarizacion.

IOS Command Line Interface

```
Se prohibe el acceso no autorizado

User Access Verification

Password:

R2>en
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#network 172.16.1.0 0.0.0.255 area 0
R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
R2(config-router)#passive-interface loopback 0
R2(config-router)#exit
01:01:26: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to
FULL, Loading Done

R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#interface serial 0/0/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#passive-interface loopback 4
```

OSPFv3 en R2

j. Verificación de la información de OSPF

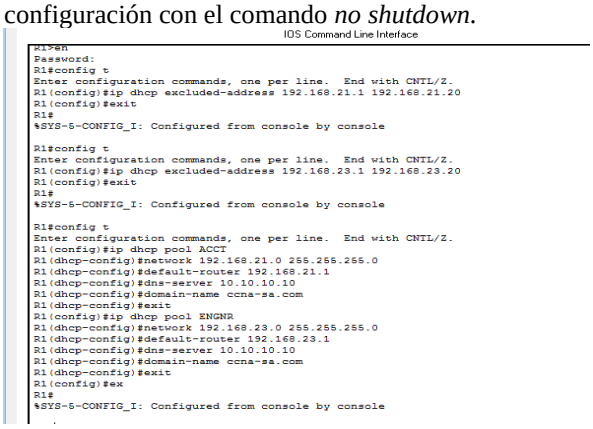
Mediante el comando *Show running-configuration podemos observar la ID del proceso OSPF así como la ID del router, las redes de routing, así como las interfaces pasivas.*

```
!
interface Serial0/0/1
 description Conexion a R3
 ip address 172.16.2.2 255.255.255.252
 ipv6 address 2001:DB8:ACAD:2::2/64
 ipv6 ospf 1 area 0
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback0
 network 10.10.10.10 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
!
ipv6 router ospf 1
 log-adjacency-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip route 0.0.0.0 0.0.0.0 172.16.2.1
ip route 0.0.0.0 0.0.0.0 209.165.200.238
!
ip flow-export version 9
!
ipv6 route ::/0 2001:DB8:ACAD:1::1
ipv6 route ::/0 2001:DB8:ACAD:2::1
ipv6 route ::/0 2001:BD8:ACAD:A::38
!
```

Show running-configuration

k. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Establecemos el rango de IP´s excluidas del conjunto (pool) de direcciones que podrá asignar el servicio indicando la ip inicial y final del rango, ambas incluidas *ip dhcp excluded-address 192.168.21.1 192.168.21.20*, reservamos un grupo de direcciones IP en la VLAN para configuraciones estáticas, así como creamos un pool para las VLAN 21y23; una vez terminamos la configuración el servicio DHCP en el router, observamos que no hay conexión entre el router y el Switch, esto se debe a que por defecto la interface viene desactivada, es por ello que terminamos la configuración con el comando *no shutdown*.



R1 como servidor DHCP

l. Configurar la NAT estática y dinámica en el R2

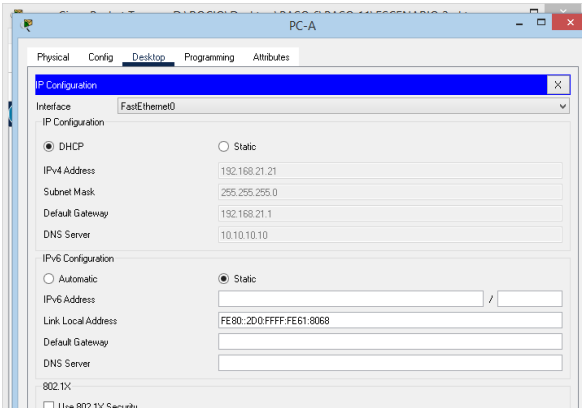
Las NAT son mecanismos utilizados por los routers para intercambiar paquetes con redes que difieren en sus direcciones IP [3], es la transformación para comunicación de una red privada en una red pública. Iniciamos con la creación de una base de datos local, a el le asignamos un nombre, una contraseña y un nivel de privilegio de usuario; nos pide habilitar el servidor HTTP; en el simulador la versión del IOS no nos permite habilitar con el comando *ip http server*, es por ello que lo habilitamos de manera manual en la configuración inicial del servidor (*numeral b.*); creamos la NAT estática para el sistema, asignamos la dirección IP con su respectiva mascara de red, asignamos la terminal y configuramos la NAT dinámica asignando la lista de acceso y definimos el pool de direcciones IP públicas.

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface loopback 0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración de NAT

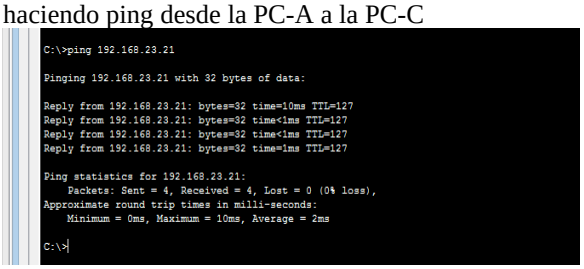
m. Verificar el protocolo DHCP y la NAT estática

Una vez hemos configurado los dispositivos vamos al PC-A ingresamos en el desktop y en ip configuration, ordenamos configurar IP DHCP, de esta manera comprobamos que ha sido activada y configurada de manera correcta en el R1, repetimos la operación en el PC-C.



DHCP en PC-A y C

Luego verificamos la conectividad éntrelos dos PC haciendo ping desde la PC-A a la PC-C



Ping de PC-A a PC-C

n. Configurar NTP

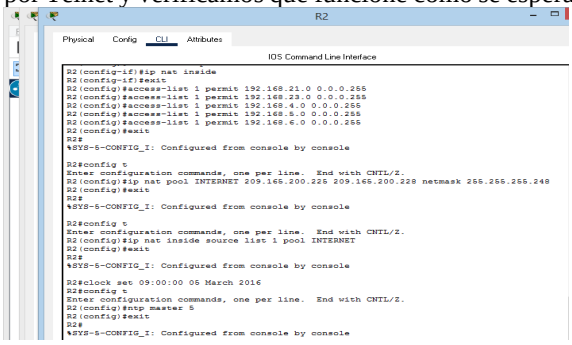
Network Time Protocol nos permite sincronizar los dispositivos de la red, de ello dependen varios servicios que requieren la sincronización en la red. En R2 ajustamos la hora y lo configuramos como maestro NTP, luego en R1 lo configuramos como cliente y le ordenamos realizar actualizaciones de calendario; verificamos la configuración con *show clock detail.*

```
R1#show clock detail
11:44:51.891 UTC Sat Mar 5 2016
Time source is NTP
R1#
```

Show clock detail.

o. Restringir el acceso a las líneas VTY en el R2

Configuramos una lista de acceso con nombre (ADMIN-MGT), la que establece que solo R1 establece conexión Telnet con R2, aplicamos access class a las líneas VTY, permitimos el acceso a estas por Telnet y verificamos que funcione como se espera.



Restricción de accesos

p. comando de CLI

El comando show en este caso nos ayudará a trabajar con dispositivos CISCO, con la utilización de diferentes parámetros, este nos muestra información sobre ellos, como listas de acceso (*show access-list)*, traducciones de NAT (Show ip nat translations); al igual que con el comando *clear* podemos eliminarlas.

```
R2>en
Password:
R2#show access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.0.255
    40 permit 192.168.5.0 0.0.0.255
    50 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
```

Show access-list

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.229   10.10.10.10        ---                ---

R2#
```

Show ip nat translations

III CONCLUSIÓN

En la investigación y desarrollo de la solución propuesta hemos logrado ahondar conocimientos sobre direccionamiento ospf, además de la configuración de VLAN en subredes, se configura el Router como servidor DHCP y sus conexiones desde y hacia los Switch de modo troncal, a su vez, cada Switch se conecta a su LAN con modo de acceso.

La herramienta paket-tracer nos permitió conocer y trabajar sobre un ambiente simulado, las diferentes configuraciones, conexiones y protocolos de configuración en equipos intermedios, trabajando en ellos sobre un sistema seguro y confiable.

Es fundamental el presentar una estructura definida, el llevar el paso a paso en el momento de configurar la red nos permitirá llevar a cabo lo planeado.

Uno de los pasos esenciales dentro del diseño y programación de la red y la configuración de cada uno de los elementos que encontramos en ellas, es muy importante llevar un proceso sistemático y ordenado, el llevar la bitácora bien definida nos permite no solo llevar un control en cada uno de los procesos, sino que nos brinda información continua para poder llegar a buen término nuestro objetivo en la configuración de ellas.

NOTA: Las siguiente son recomendaciones muy útiles en la solución de problemas durante la ejecución de una simulación:
Asegúrese de que todas las interfaces que se encuentran en funcionamiento se encuentran activas (up).
Verifique la correcta conexión del cableado.
Verifique que la IP y su debida mascara de subred, sean las correctas en cada interface.
Evite utilizar y elimine comandos innecesarios, o aquellos que fueron reemplazados.

APENDICE

Algunos comandos CLI en CISCO [4]

Comando	*Función*
enable	Modo privilegiado

Config terminal	Modo de configuración global.
no ip domain-loopbak	Desactiva la traducción de nombres a dirección del dispositivo.
Service password-encryption	Cifrado débil para las contraseñas
show versión	Información acerca del dispositivo.
Show vlan	Buscar configuraciones anteriores de vlans no deseadas.
show protocols	Observamos los protocolos capa 3 configurados.
show clock	Hora del dispositivo
show ip interface brief	Resumen de todas las interfaces.
show startup-config	Configuración grabada en la NVRAM
Show run	Configuración que se encuentra corriendo en la RAM
show ip route	Tabla de enrutamiento
Show ntp	Hora y fecha actual, cambio del servidor y los NTP
show access-list	Listas de acceso
Show ip nat translations	Muestra las ACL en la interface o dirección IP en las que se aplica
Show ip dhcp binding	Mostrar asignaciones DHCP
show ip dhcp pool	Mostrar ámbitos o pool DHCP
show vlan-membership	lista de vlans y las interfaces asignadas a cada vlan

RECONOCIMIENTO

Gracias a Dios por permitirme estar en esta instancia de mi vida, su misericordia y su bondad me han permitido conocer cada día más y aprender momento a momento miles y miles de conocimientos que con su voluntad podremos desarrollar profesionalmente, a mi Madre que en cada una de sus oraciones me encomienda para que el entendimiento y la protección de Dios llene mi vida; a mis adorables hijas que quiero que vean en este triunfo una oportunidad y un ejemplo para seguir luchando por sus sueños y la esperanza de salir adelante, a esas personas especiales en mi vida que día a día, noche a noche me alientan y que sin su apoyo esto no sería posible, a esa comprensión, ese amor y esa fuerza que me das en cada momento, en cada charla de motivación y en cada mensaje, esos sueños por los que luchamos y que solo con la bendición de Dios pueden ser una realidad, a esos compañeros que en su interés de salir adelante nos brindan ese apoyo y ese empujoncito para continuar, con todo mi esfuerzo y con el corazón más que con el pensamiento Gracias.

REFERENCES

[1] https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/
[2]https://www.ibm.com/docs/es/i/7.2?topic=routing-open-shortest-path-first
[3]wordpress.com/2011/11/26/configurar-nat-estático/
[4]https://www.solvetic.com/tutoriales/article/170-comandos-cisco-show/

BIOGRAFIA

Omar Germán Rincón Gallo, nacido el 22 de Octubre de 1974 en la ciudad de Socha, Boyacá, Colombia. De familia muy humilde y orígenes campesinos, estudio su primaria y bachillerato en una escuela normal publica; a los 16 años se recibe como Bachiller Pedagógico, en el año 2001 se recibe como Técnico Profesional en Minería Bajo Tierra; base de la economía de su región y es desde allí que junto a su gran amigo de estudios, Edwin Rolando Duran (QEPD), decide iniciar sus estudios en ingeniería electrónica en la UNAD; años más tarde su compañero fallece y es cuando toma la decisión de trasladar sus estudios a ingeniería de Telecomunicaciones; después de afrontar molestias de salud y superar algunos golpes de la vida decide terminar sus estudios y recibirse como ingeniero. Tras la pandemia a nivel mundial encuentra el tiempo y el momento para terminar sus estudios y sus tiempos libres los utiliza en la formación de jóvenes en las áreas de matemáticas, colaborándoles en sus dificultades de aprendizaje desde casa debido al distanciamiento social.