SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

IVAN ALEXANDER CARO ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E NGENIERIAS ECBTI
INGENIERIA DE TELECOMUNICACIONES
CALI
2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

IVAN ALEXANDER CARO ROMERO

Diplomado de opción de grado presentado para optar el título de ingeniero de Telecomunicaciones

TUTOR:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E NGENIERIAS ECBTI
INGENIERIA DE TELECOMUNICACIONES

CALI
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Enrutamiento: el proceso que admite que los paquetes IP enviados por un host origen lleguen al destino de forma adecuada

Etherchannel: Es una tecnología propia CISCO basada en el estándar 802.3 full-duplex Fast Ethernet donde las conexiones EtherChannel permiten interconectar switches, routers, servidores o host.

LAN: (Local Area Network) es una red que conecta uno o más dispositivos dentro de un espacio relativamente pequeño o limitado.

Networking: Referente a las redes de cómputo que enlazan dos o más dispositivos informáticos con la intención de compartir datos.

Protocolo de comunicaciones: Son reglas que permiten que dos o más dispositivos de una red de se comuniquen para transmitirse información por medio de cualquier tipo de variación de una magnitud física.

Subnneting: hace referencia a la subdivisión de una red en varias subredes.

VLAN: (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

RESUMEN

Basado en el modelo de " Proyecto Aplicado" desarrollado sobre un ambiente de simulación Packet Tracer, herramienta propiedad del fabricante de dispositivos de comunicaciones CISCO y puesta a disposición de los estudiantes de los cursos CCNA entre otros, se desarrollan los dos escenarios propuestos que son representativos de los requerimientos propios de una infraestructura de red y configuración LAN y WAN, iniciando con la selección de equipos y la configuración por comandos de los mismos, habilitando los protocolos y las opciones de enrutamientos estudiados en el diplomando de profundización de CISCO, así como también la resolución de los problemas que surjan de la implementación y posterior puesta en marcha.

Los temas del diplomado CNNA que se abordaran en el desarrollo del escenario son: la configuración inicial de equipos en identificación y seguridad en el acceso local y remoto implementando claves y restricciones. La configuración para su óptimo funcionamiento de la infraestructura de la red por medio de la implementación de Vlans como medio para segmentar y limitar el acceso a la red con el fin de mejorar la utilización de los recursos y brindar mayor seguridad y control al tráfico circulante.

Palabras clave: CISCO, LAN,WAN, enrutamiento, subred, telecomunicaciones

ABSTRACT

Based on the “Applied Project” model developed on a Packet Tracer simulation environment, a tool owned by the manufacturer of communications devices CISCO and made available to students of CCNA courses among others, the two proposed scenarios are developed that are representative of the requirements of a network infrastructure and LAN and WAN configuration, starting with the selection of equipment and their configuration by commands, enabling the protocols and routing options studied in the CISCO in-depth diploma, as well as the resolution of the problems that arise from the implementation and subsequent start-up. The topics of the CNNA diploma that will be addressed in the development of the scenario are: the initial configuration of equipment in identification and security in local and remote access, implementing keys and restrictions. The configuration for its optimal operation of the network infrastructure through the implementation of Vlans as a means to segment and limit access to the network in order to improve the use of resources and provide greater security and control of circulating traffic.

Keywords: CISCO, LAN, Networking, WAN,routing subnneting, telecommunications

INTRODUCCION

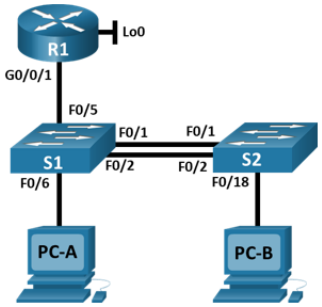
En el mercado de fabricantes de equipos de telecomunicación, cada año vemos posicionando más y más marcas, sin embargo, es de reconocer que CISCO es una de las que tiene mayor trayectoria y que por su experiencia se convierte en referente para la implementación y de redes para los nuevos profesionales que ingresan a laborar en el campo de las Telecomunicaciones. Cisco a su vez en pro de mantener y difundir ese conocimiento ofrece la oportunidad de acceder a él mediante su academia de estudio virtual y su herramienta de simulación packet tracer para las prácticas. Aprovechando esas herramientas de estudio desarrollamos el Diplomado en profundización de cisco como opción de grado

Con la presentación de este trabajo se pretende probar el conocimiento adquirido en Networking, mediante la implementación simulada de dos escenarios. En el primero estaremos abordando temas sobre comunicaciones Ethernet, direccionamiento IP, Subnneting, Vlan y Etherchannel como procesos necesarios en la implementación de la red básica propuesta.

DESARROLLO

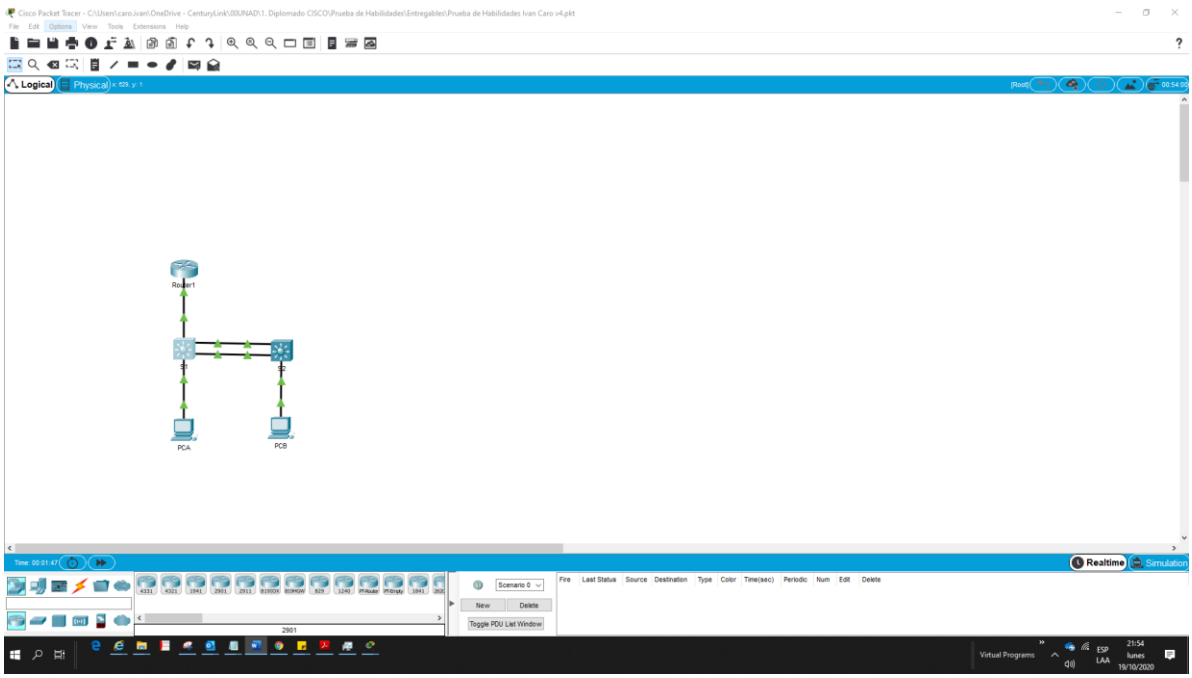
ESCENARIO 1

Figura 1 Topología de red escenario 1



Fuente: UNAD

Figura 2. Simulación en packet tracer.



Fuente: Autor.

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

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

Se inicia con el borrado de las configuraciones de inicio y de configuración de las VLAN del router y del switch y posteriormente se vuelven a cargar los dispositivos.

Tabla 1 Borrado inicial en los equipos

Tarea	Comando 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 VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat
Volver a cargar ambos switches	Switch#RELOAD

Ya con los dispositivos limpios de cualquier anterior configuración se procede con la configuración de la plantilla SDM para que permita IPv6. Cumplido esto se realiza el reinicio de los dispositivos.

Tabla 2 Configuración plantilla SDM

Tarea	Especificación
Configure la plantilla SDM para que admita IPv6	Switch#conf terminal Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing Switch#reload

Ahora se parte con la configuración del primer router al cual se le realizan las configuraciones básicas descritas en la tabla 3 y que tienen como objeto la identificación del equipo con un nombre, habilitar el acceso local y remoto con restricciones de seguridad que lo protejan de intentos no autorizados.

Tabla 3 Configurar R1.

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Escenario 1 Ivan Caro R1"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	R1(config-subif)#description Subinterface VLAN 2 BIKES R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#no shutdown R1(config-if)#
Configure el Loopback0 interface	R1(config)#interface loopback 0 R1(config-if)#description Loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa

Se pasa a realizar la misma configuración básica que se hizo en el router (R1) ahora sobre los Switch, adicionando la definición del Gateway predeterminado que van a tener.

Tabla 4 Configure S1 y S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup Switch0(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 Switch0(config)#hostname S2
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass S2(config)#enable secret ciscoenpass

Tarea	Especificación
Contraseña de acceso a la consola	S1(config-line)#password ciscoconpass S2(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd " Escenario 1 Ivan Caro S1 " S2(config)#banner motd " Escenario 1 Ivan Caro S2 "
Generar una clave de cifrado RSA	S1(config)#CRYpto key generate rsa S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config-if)#ip address 10.19.8.98 255.255.255.248 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S1(config-if)#ipv6 address FE80::98 link-local S2(config-if)#ipv6 address FE80::99 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 S1(config)#ipv6 route ::/0 2001:db8:acad:c::1 S2(config)#ip default-gateway 10.19.8.97 S2(config)#ipv6 route ::/0 2001:db8:acad:c::1

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking,

EtherChannel)

Se pasa a la parte 2 con la configuración de las Vlan sobre los dos switch, que para el escenario 1 se determinaron que van a ser 5:

Vlan 2 Bikes, Vlan 3 Trikes, Vlan 4 Management, Vlan 5 Parking y Vlan 6 Native.

Adicional para permitir la conectividad se realizará la creación de troncos sobre la Vlan 6 y la creación de un grupo de puertos Etherchannel sobre las interfaces F01/ y F 0/2.

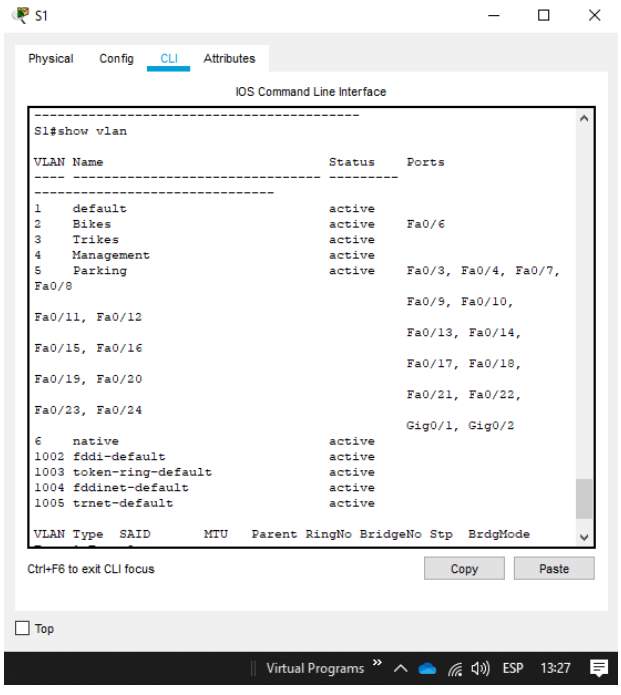
Por último, como medidas de seguridad se implementa un puerto de acceso de host, la configuración de seguridad en los puertos y la protección y apagado de los puertos no utilizados.

Tabla 5 Configurar en S1

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config)#vlan 4 S1(config-vlan)#name Management S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#channel-group 1 mode active S1(config-if)#channel-protocol lacp

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1(config)#interface range FastEthernet 0/3-4 , fastEthernet 0/7 - 24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Interfaces “INACTIVAS"

Figura 3 VLAN S1

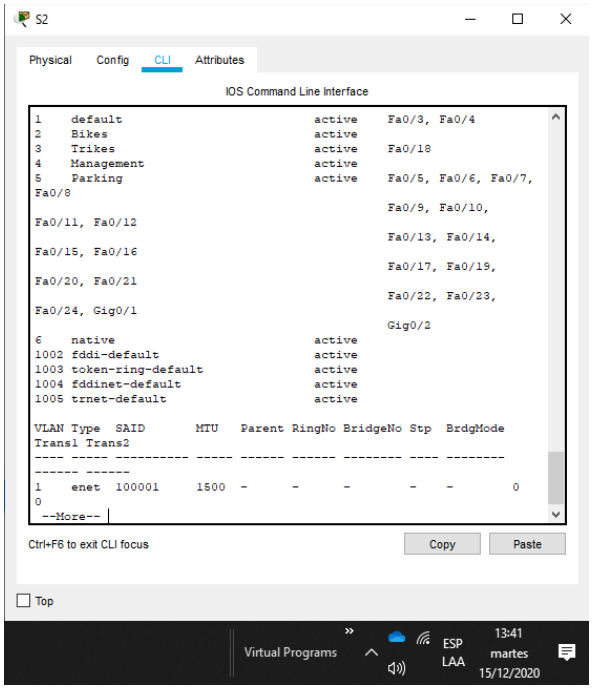


Fuente: Autor.

Tabla 6 Configurar en S2

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config)#vlan 4 S2(config-vlan)#name Management S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config-if)#channel-group 1 mode active S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2(config)#interface range fa0/5-17 , fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Interfaces sin uso S2(config-if-range)#sh

Figura 4 VLAN S2



Fuente: Autor.

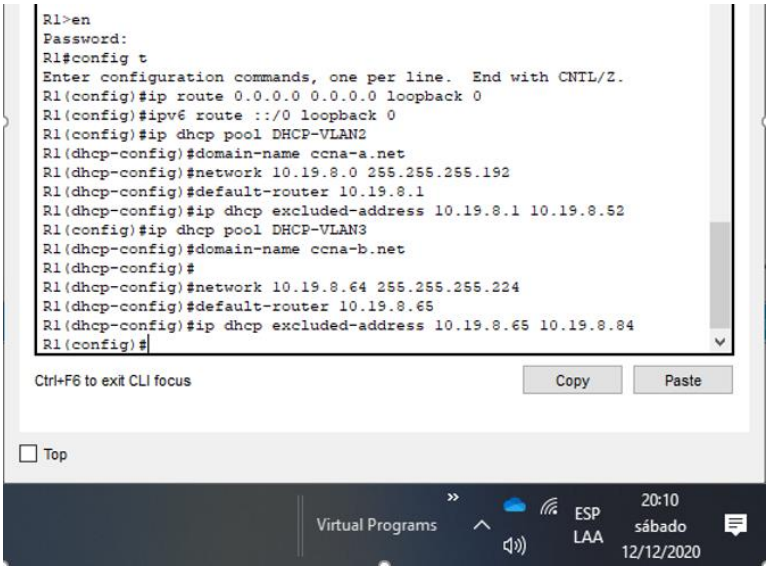
Sobre el router R1 corresponde la configuración de enrutamiento, Se establece como ruta por defecto la Loopback, la configuración del DHCP para IPv4 determinando grupos de IPs para las Vlan 2 y 3 según instrucciones.

Tabla 7. Configure R1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp pool DHCP-VLAN2 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52

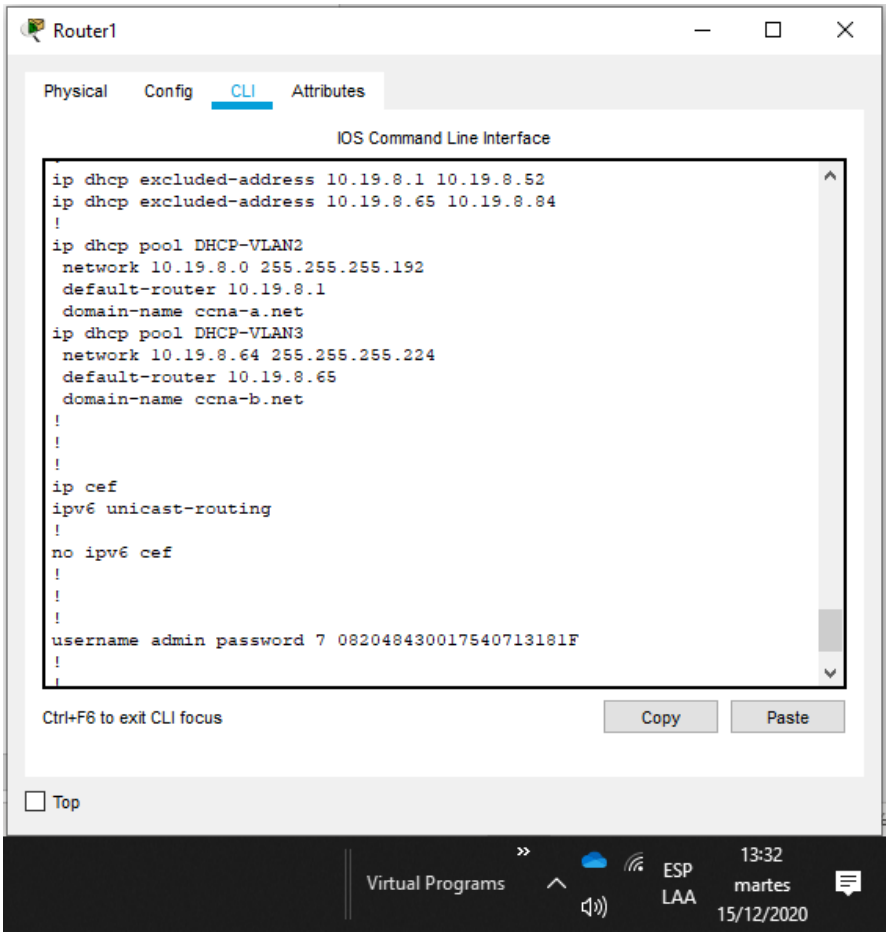
Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool DHCP-VLAN3 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

Figura 5 Configurar DHCP en R1



Fuente: Autor.

Figura 6 DHCP en R1 #Show running

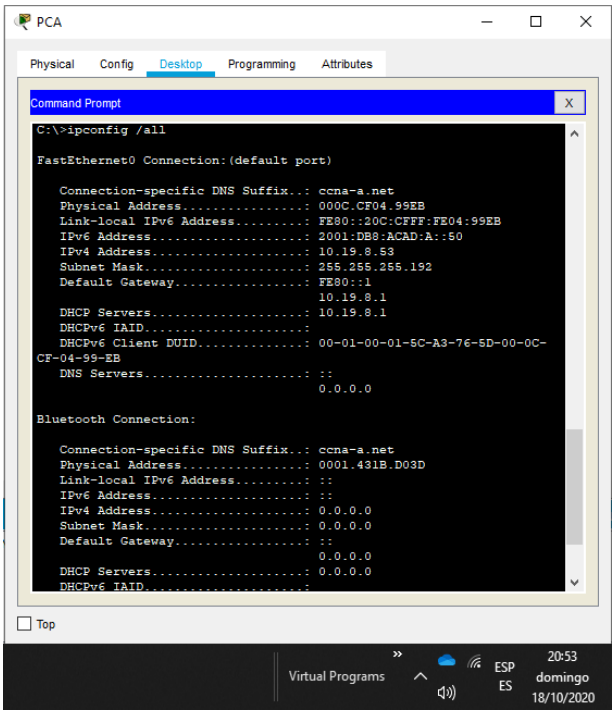


Fuente: Autor.

Paso 2 Configurar los servidores

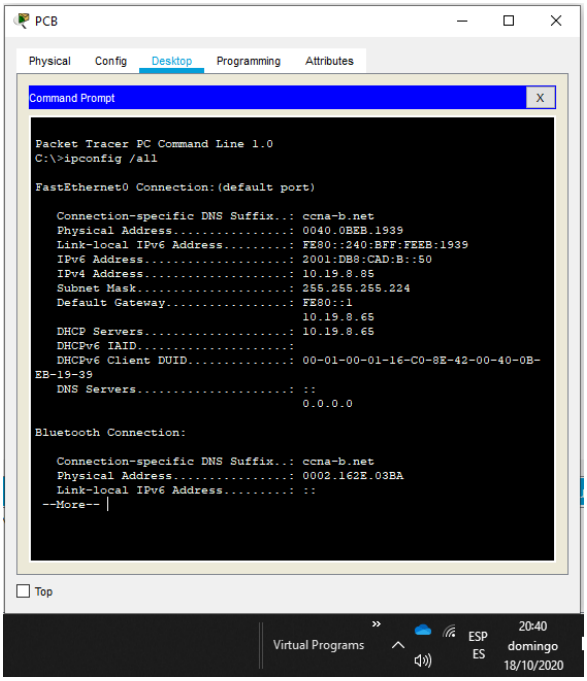
Ultimo paso de la parte 2 es la configuración en los servidores para que tomen el direccionamiento IPv4 por DHCP, el direccionamiento IPv6 para todos los parámetros se asigna estáticamente. Finalmente se comprueba y registra la configuración de cada host con el comando ipconfig /all cuyo resultado se muestra en las siguientes figuras.

Figura 7 Configuración PCA



Fuente: Autor.

Figura 8 Configuración PCB



* Fuente: Autor.

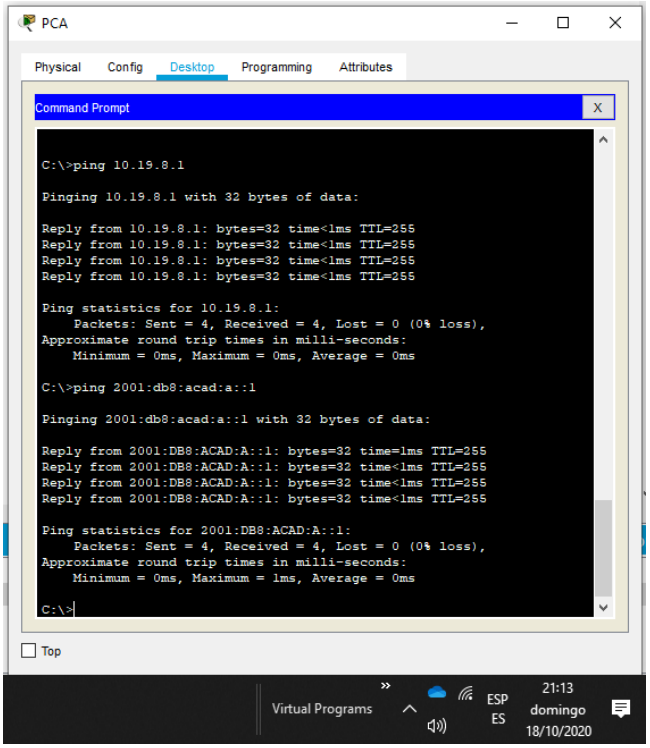
Parte 3 Probar y verificar la conectividad de extremo a extremo

En la etapa de pruebas de conectividad se utiliza se relaciona un origen y un destino al que se le debe probar el alcance de la conectividad. En la tabla 8 se registran los resultados obtenidos de la utilización del comando ping como medio para validar el alcance entre dispositivos.

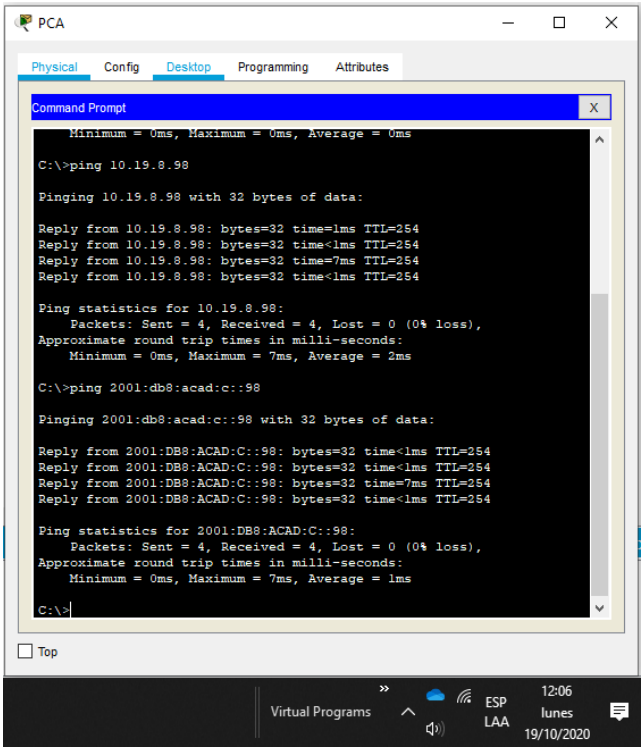
Tabla 8. Probar y verificar la conectividad de extremo a extremo

<table>
<tr><th>Desde</th><th>A</th><th>de Internet</th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td rowspan="4">PCA</td><td rowspan="2">R1, G0/0/1.2</td><td>Dirección</td><td>10.19.8.1</td><td rowspan="4">El ping alcanza su destino en R1

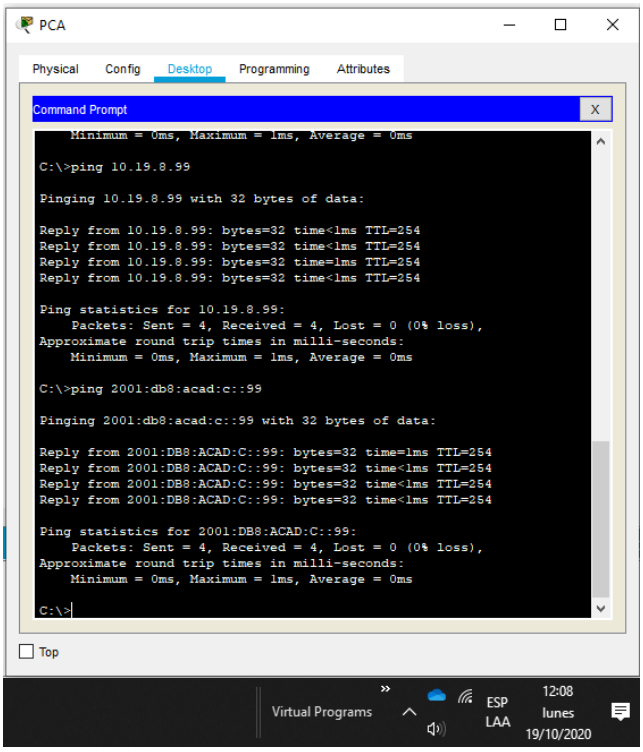
Figura 9 Conectividad desde PCA hacia R1 G0/0/1.2

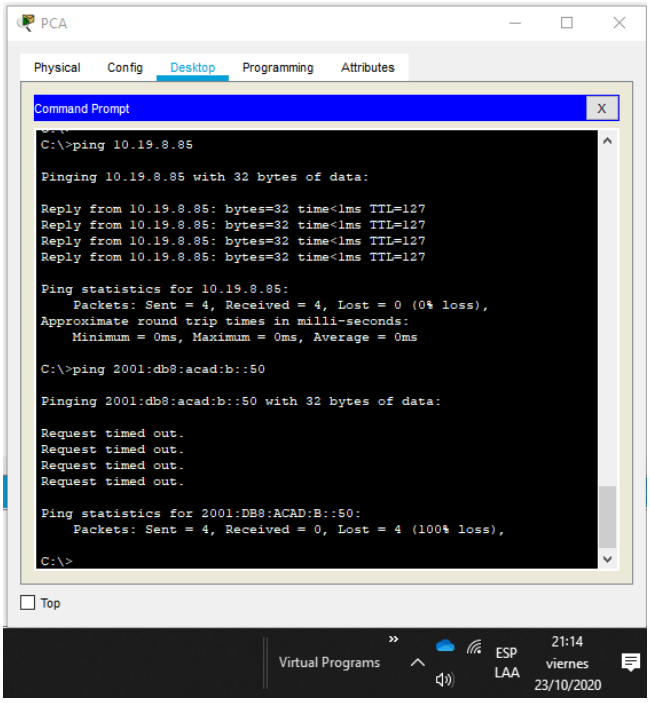
Fuente: Autor</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:a::1</td></tr>
<tr><td></td><td>IPv6</td><td>2001:db8:acad:b::1</td></tr>
<tr><td></td><td>IPv6</td><td>2001:db8:acad:c::1</td></tr>
</table>

Desde	A	de Internet	Dirección IP	Resultados de ping
PCA	S1, VLAN 4	Dirección	10.19.8.98	El ping alcanza su destino en S1 Figura 10 Conectividad desde PCA hacia S1 VLAN4  *Fuente: Autor.

Desde	A	de Internet	Dirección IP	Resultados de ping
PCA	S2, VLAN 4	Dirección	10.19.8.99.	El ping alcanza su destino en S2
		IPv6	2001:db8:acad:c::99	Figura 11 Conectividad desde PCA hacia S2 VLAN4

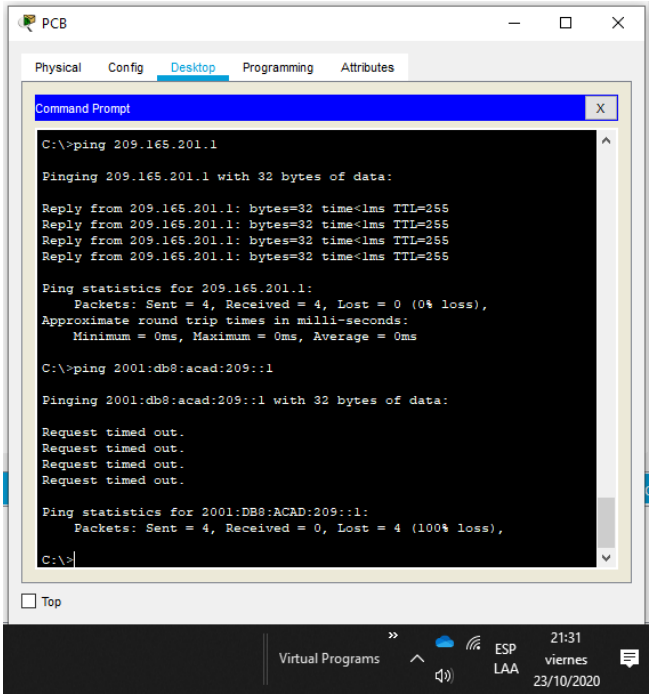


Fuente: Autor

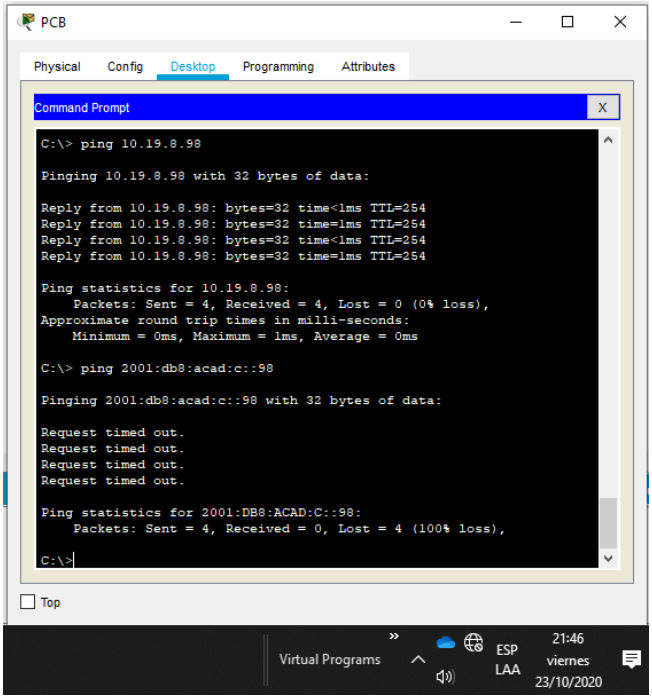
Desde	A	de Internet	Dirección IP	Resultados de ping
PCA	PC-B	Dirección	10.19.8.85	EL ping alcanza su destino en PCB solo para IPv4 Figura 12 Conectividad desde PCA hacia PCB  Fuente Autor.
		IPv6	2001:db8:acad:b::50	

<table>
<tr><th>Desde</th><th>A</th><th>de Internet</th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td rowspan="3">PC B</td><td rowspan="2">R1 Bucle 0</td><td>Dirección</td><td>209.165.201.1</td><td rowspan="3">El ping alcanza su destino en R1 solo para IPv4.

Figura 13 Conectividad desde PCB hacia R1 Bucle 0

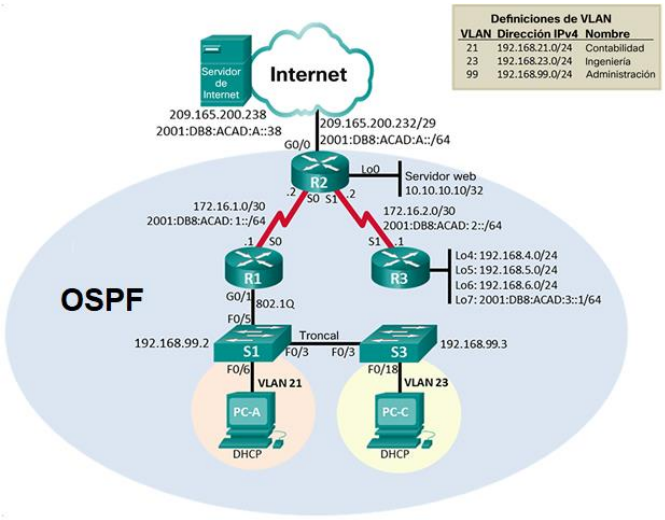
 

Fuente: Autor.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:209::1</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Desde	A	de Internet	Dirección IP	Resultados de ping
PCB	S1, VLAN 4	Dirección	10.19.8.98	El ping alcanza su destino en S1 solo para IPv4. Figura 14 Conectividad desde PCB hacia S1 VLAN4  Fuente: Autor.
		IPv6	2001:db8:acad:c::98	

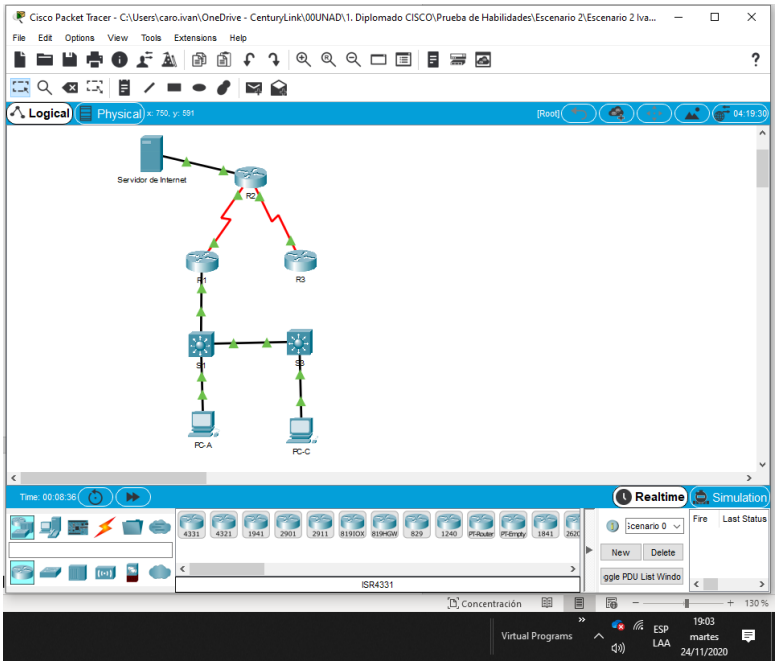
ESCENARIO 2

Figura 15 Topología de red escenario 2



Fuente: UNAD

Figura 16 Simulación en packet tracer escenario 2



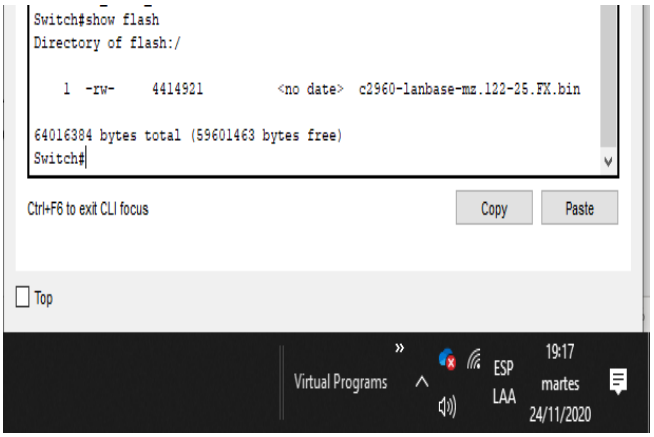
Fuente: Autor

Parte 1: Inicializar dispositivos

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

Se inicia con el borrado de las configuraciones de inicio y de la configuración de las VLAN del router y de los switch y posteriormente se vuelven a cargar los dispositivos.

Tabla 9 Inicializar equipos

Tarea	Comando 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 VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat
Volver a cargar ambos switches	Switch#RELOAD
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Figura 17 Verifica borrado del archivo de Vlans  Fuente: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

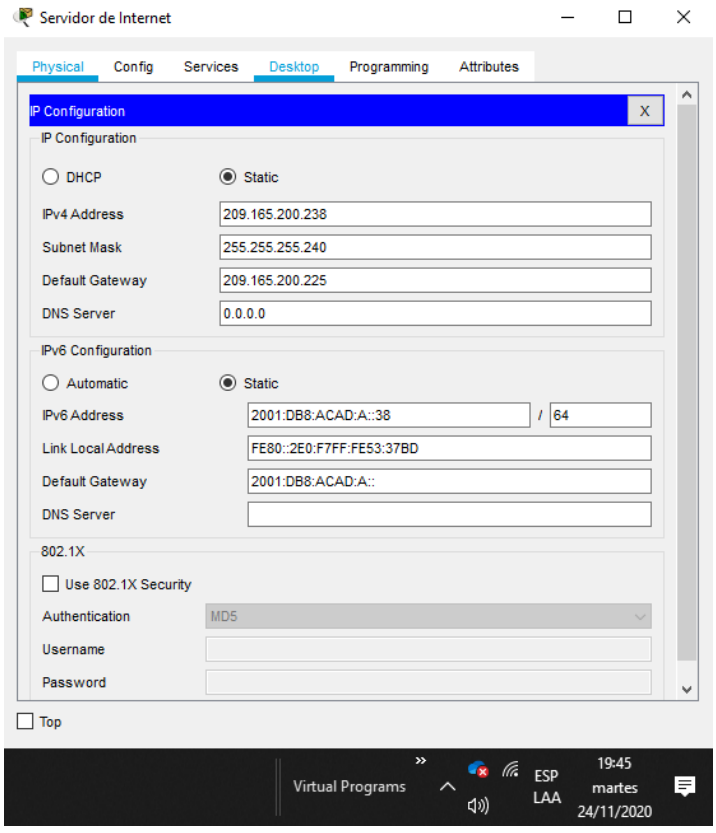
Paso 1: Configurar la computadora de Internet

De acuerdo con la información obtenida de la topología entregada. se realiza de forma estática la asignación de direccionamiento y de parámetros relacionados sobre el servidor de internet

Tabla 10 Configuración servidor de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	/28 255.255.255.240
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Figura 18 Configuración la computadora de Internet



Fuente: Autor

Paso 2:Configurar R1

Se continua con la configuración del router R1 al cual se le realizan las configuraciones básicas descritas que tienen como objeto la identificación del equipo con un nombre, habilitar el acceso local y remoto con restricciones de seguridad que lo protejan de intentos no autorizados. Adicional se realiza la descripción a la interfaz S 0/0/0 y el registro de las rutas predeterminadas.

Tabla 11 Configurar R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description "INTERFAZ A R2" R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 R1(config)#ipv6 route ::/0 serial 0/0/0

Nota: En este punto aún no se configura la interfaz G0/1

Paso 3:Configurar R2

Se realizan las mismas configuraciones que se adelantaron en el paso anterior para R1 ahora para R2.

Tabla 12 Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	No soportado por Packet Tracer
Mensaje MOTD	R2(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	R2(config-if)#description "INTERFAZ 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

Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#des R2(config-if)#description INTERFAZ A R3" R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 201:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description "SALIDA INTERNET" R2(config-if)#ip address 209.165.200.225 255.255.255.240 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

Paso 4:Configurar R3

Se realizan las mismas configuraciones ahora para R3.

Tabla 13 Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class

Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#pas R3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description "INTERFAZ R2" R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown R3(config-if)#
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64

Paso 5:Configurar S1

Se realizan las configuraciones tal cual como se hicieron para los routers ahora para el Switch S1

Tabla 14 Configurar S1

	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco
Contraseña de acceso Telnet	S1(config)#line vty 04 S1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Se prohibe el acceso no autorizado"

Paso 6: Configurar el S3

Se realizan las configuraciones básicas para el Switch S3.

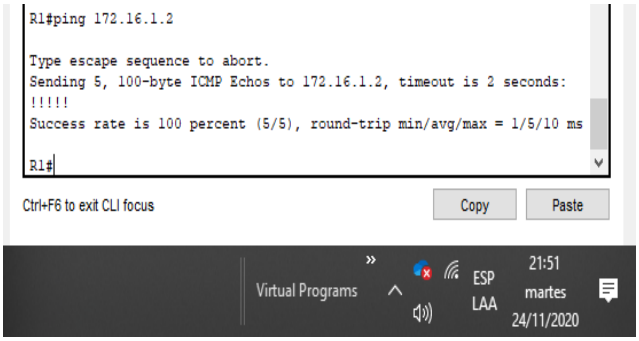
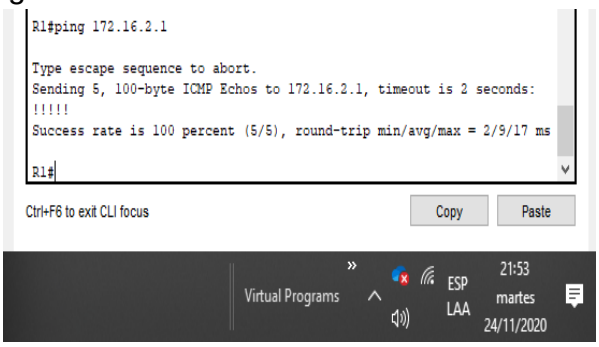
Tabla 15 Configurar S3

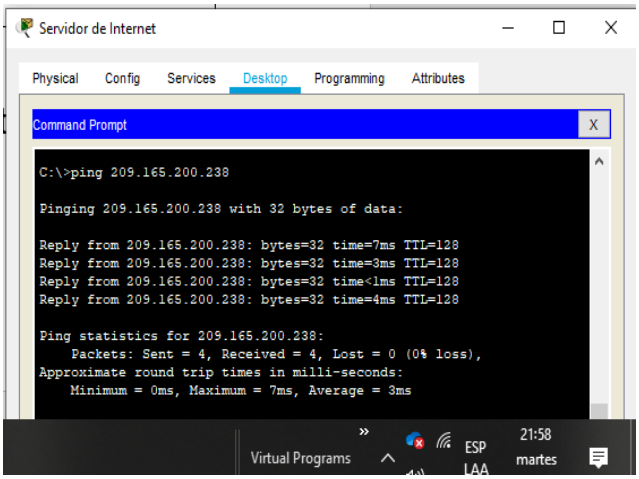
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd "Se prohibe el acceso no autorizado"

Paso 7:Verificar la conectividad de la red

Como último paso de la parte 2 se realiza las respectivas pruebas de conectividad.

Tabla 16 Verificar conectividad de red

Desde	A	IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Figura 19. Conectividad ping de R1 hacia R2.  Fuente: Autor.
R2	R3, S0/0/1	172.16.2.1	Figura 20. Conectividad de R1 hacia R3  Fuente: Autor.

PC de Internet	Gateway predeterminado		Figura 21. Conectividad del PC de internet al Gateway predeterminado  Fuente: Autor

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

Paso 1: Configurar S1

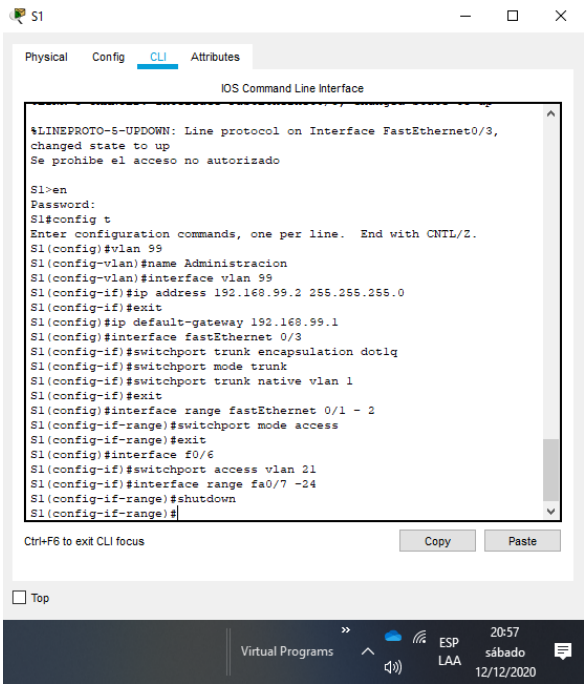
En esta parte se aborta la configuración de seguridad, la creación de las Vlans requeridas y el enrutamiento de las mismas, iniciando por la configuración en S1

Tabla 17 Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config-if)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1

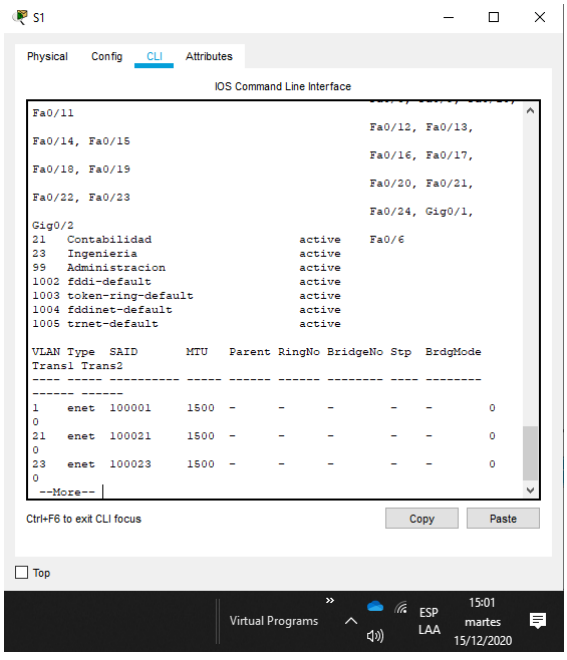
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fastEthernet 0/1 - 2 S1(config-if-range)#ccccccccc S1(config)#interface fastEthernet 0/4 S1(config-if-range)#switchport mode access S1(config)#interface range fastEthernet 0/6 - 24 S1(config-if-range)#switchport mode access S1(config)#interface range gigabitEthernet 0/1 - 2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range fa0/7 -24 S1(config-if-range)#shutdown S1(config)#interface range fastEthernet 0/1 - 2 S1(config-if-range)#shutdown S1(config)#interface fastEthernet 0/4 S1(config-if)#shutdown S1(config)#interface range gigabitEthernet 0/1 - 2 S1(config-if-range)#shutdown

Figura 22 VLAN y el routing entre VLAN en S1



Fuente: Autor.

Figura 23 VLAN en S1 #show vlan



Fuente: Autor

Paso 2: Configurar el S3

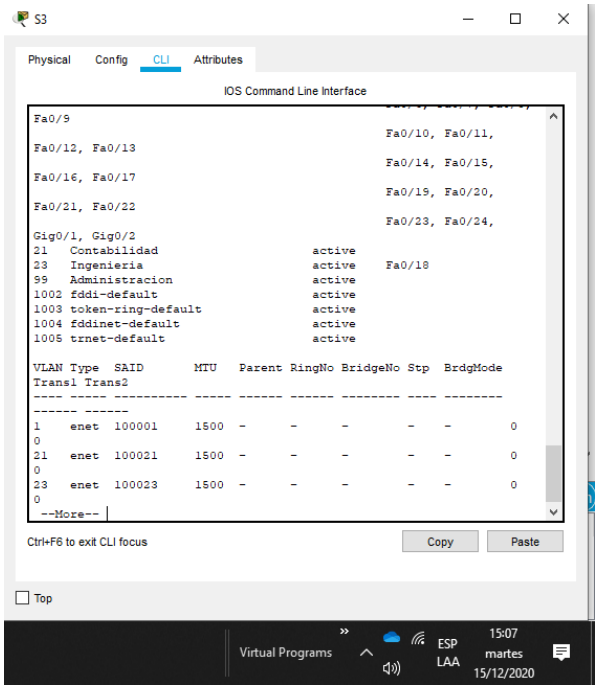
Se prosigue con la misma configuración ahora para S3

Tabla 18 Configurar S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#inter fa0/3 S3(config-if)#switchport trunk encapsulation dot1q S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1 - 2 S3(config-if-range)#switchport mode access S3(config)#interface range fa0/4 - 17 S3(config-if-range)#sw mo access S3(config)#interface range fa0/19 - 24 S3(config-if-range)#switchport mode access S3(config)#interface range gigabitEthernet 0/1-2 S3(config-if-range)#switchport mode access

Asignar F0/18 a la VLAN 23	S3(config)#inter fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1 - 2 S3(config-if-range)#shutdown S3(config-if-range)#interface range fa0/4 - 17 S3(config-if-range)# shutdown S3(config-if-range)#interface range fa0/19 - 24 S3(config-if-range)#shutdown S3(config-if-range)#interface range gigabitEthernet 0/1-2 S3(config-if-range)#shutdown

Figura 24 Vlan en S3



Fuente: Autor.

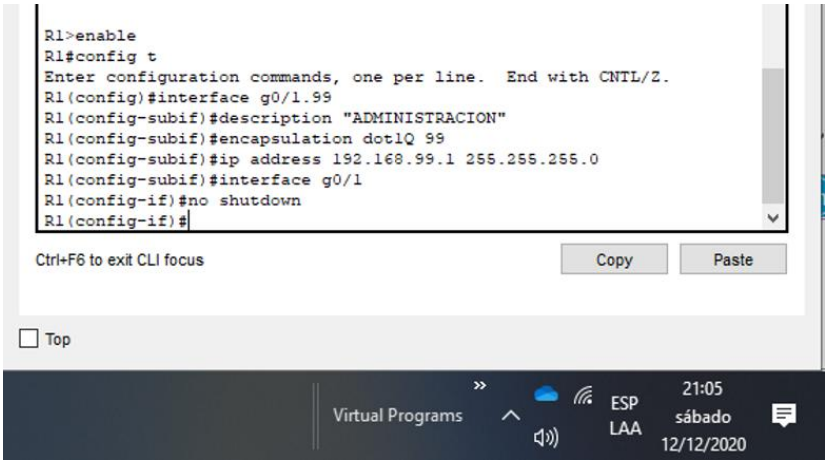
Paso 3:Configurar R1

Se procede con la configuración en el R1 de las subinterfaces que van a corresponder a cada Vlan sobre la interface física G0/1. Se le configura la descripción solicitada y su asignación IP.

Tabla 19 Configurar R1

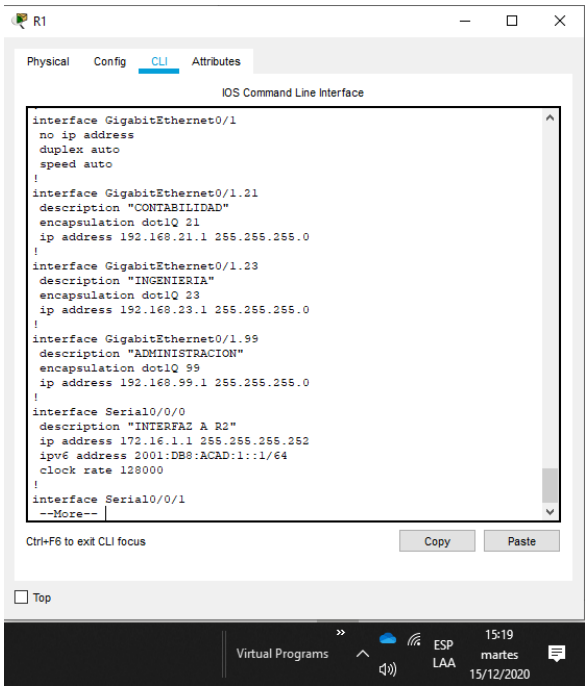
Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description "CONTABILIDAD" R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface g0/1.23 R1(config-subif)#description "INGENIERIA" R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface g0/1.99 R1(config-subif)#description "ADMINISTRACION" R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shutdown

Figura 25 Subinterfaces de las Vlan en R1



Fuente: Autor

Figura 26 Subinterfaces en R1

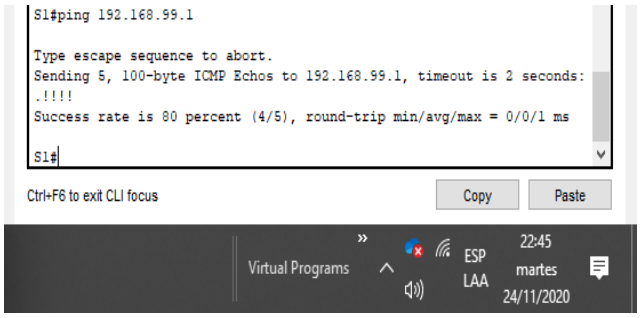
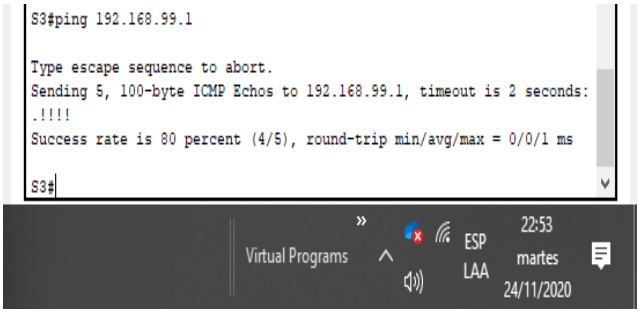


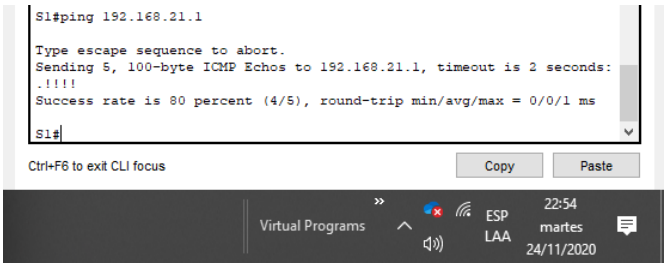
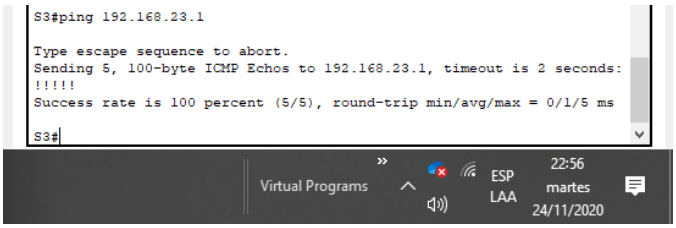
Fuente: Autor

Paso 4:Verificar la conectividad de la red

En el paso de verificación de conectividad por medio del comando ping se realiza la validación desde los orígenes hasta los destinos indicados a continuación.

Tabla 20 Verificar la conectividad de la red

Desde	A	IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Figura 27 Conectividad de S1 hacia R1  Fuente: Autor.
S3	R1, dirección VLAN 99	192.168.99.1	Figura 28 Conectividad de S3 hacia VLAN99  Fuente: Autor

S1	R1, dirección VLAN 21	192.168.21.1	Figura 29 Resultado ping de S1 hacia VLAN21  *Fuente: Autor
S3	R1, dirección VLAN 23	192.168.23.1	Figura 30 Resultado ping de S3 hacia VLAN23  *Fuente: Autor.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1:Configurar OSPF en el R1

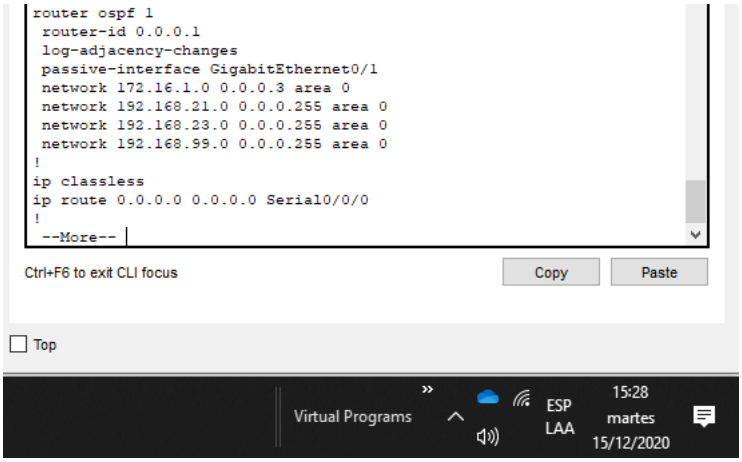
Se entra a configurar el protocolo de enrutamiento que para este escenario el seleccionado es OSPF. El primer dispositivo por configurar es R1

Tabla 21 Configurar OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 0.0.0.1

Anunciar las redes conectadas directamente	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
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	No aplica para OSPF

Figura 31 OSPF en R1



Fuente: Autor

Paso 2:Configurar OSPF en el R2

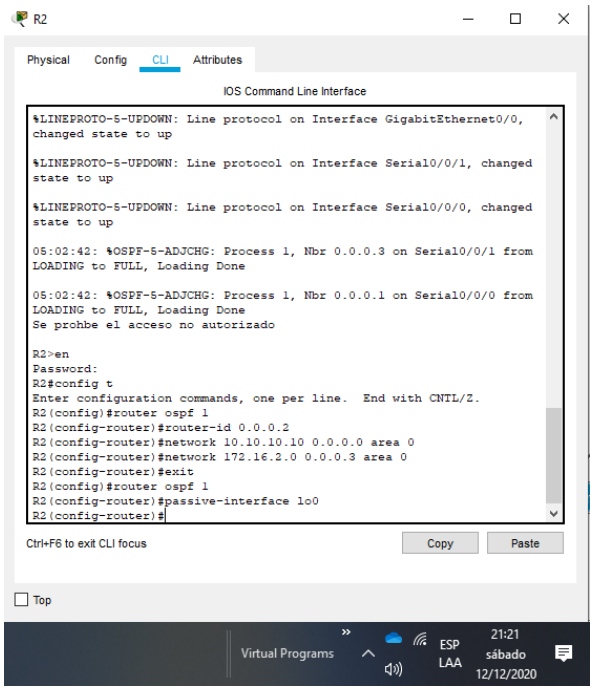
Se continua con la configuración correspondiente en R2 para habilitar el protocolo OSPF

Tabla 22 Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 0.0.0.2

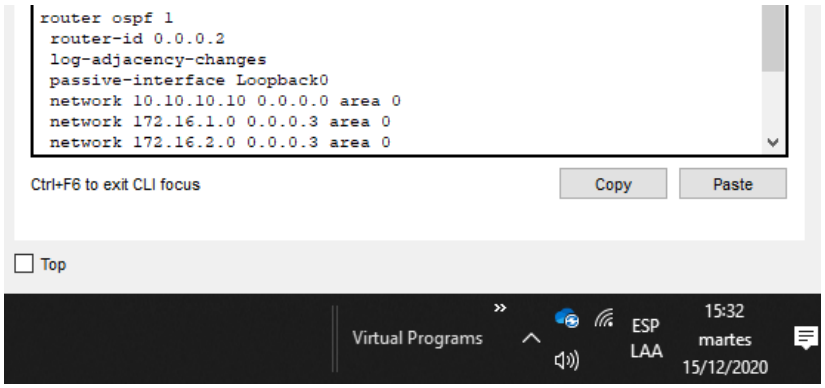
Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0.	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (Loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	No aplica para OSPF

Figura 32 Habilitar Protocolo OSPF



Fuente: Autor

Figura 33 OSPF en R2



Fuente: Autor

Paso 3: Configurar OSPF en el R3

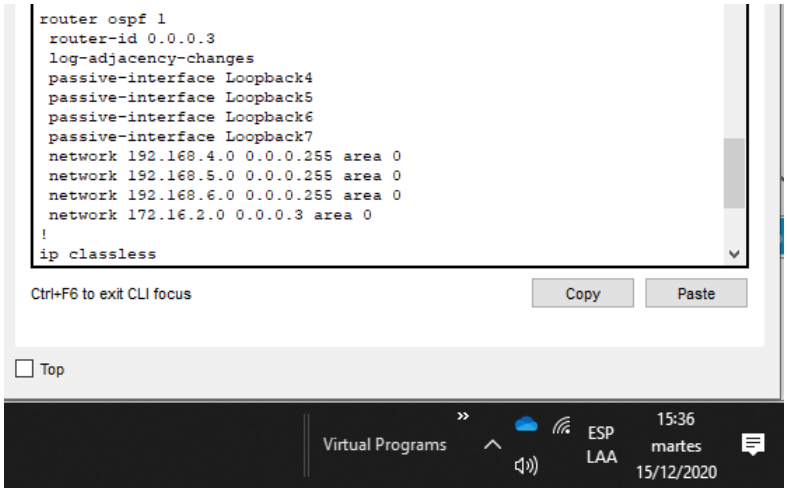
Se continua con la configuración en R3 para habilitar el protocolo OSPF

Tabla 23 Configurar OSPF en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 0.0.0.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 R3(config-router)#network 172.16.2.0. 0.0.0.3 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#passive-interface lo7
Desactive la sumarización automática.	No aplica para OSPF

Figura 34 OSPF en R3



Fuente: Autor.

Paso 4: Verificar la información de OSPF

Se da respuesta a las preguntas propuestas.

¿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?

R/ R1# Show ip ospf interface

¿Qué comando muestra solo las rutas OSPF?

R/ R1# Show ip route ospf

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

R/ R1# Show ip ospf neighbor

Parte 5: Implementar DHCP y NAT para IPv4.

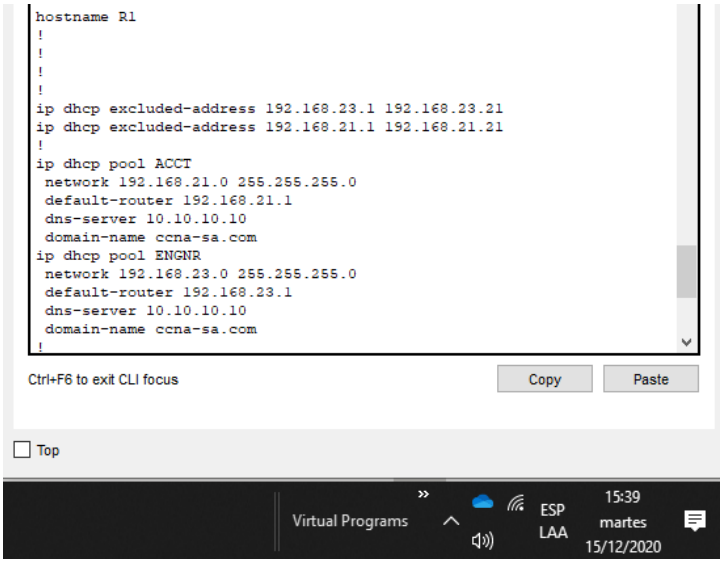
Paso 1:Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Para la parte 5 se habilita la asignación de direccionamiento por medio de DHCP en R1.

Tabla 24 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	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#network 192.168.23.0 255.255.255.0

Figura 35DHCP en R1

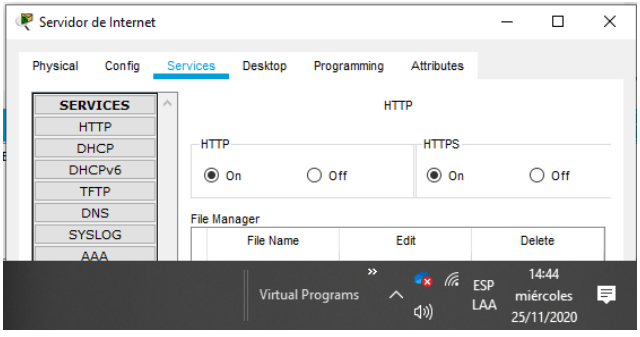


Fuente: Autor.

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

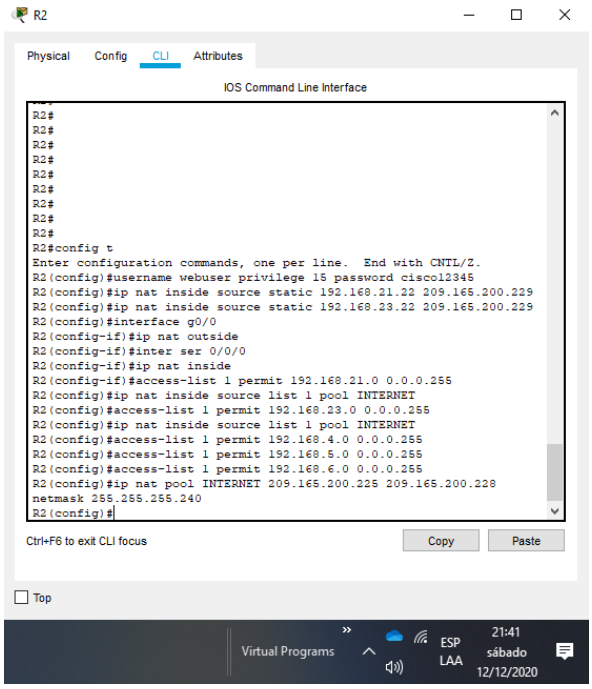
En R2 se implementa el protocolo de enmascaramiento de IPv4 conocido como NAT tanto en su opción estática como en su opción dinámica.

Tabla 25 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	R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	Figura 36 Servicio HTTP.  Fuente: Autor.

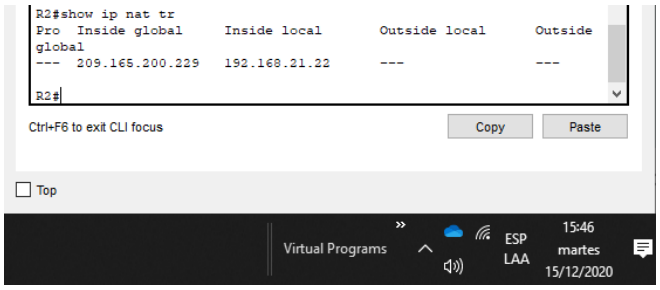
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No aplica para Packet Tracer
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 192.168.21.22 209.165.200.229 R2(config)#ip nat inside source static 192.168.23.22 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config)#inter ser 0/0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#ip nat inside source list 1 pool INTERNET 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
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.240
Definir la traducción de NAT dinámica	

Figura 37 Configuración de NAT en R2.



Fuente: Autor

Figura 38 NAT en R2.

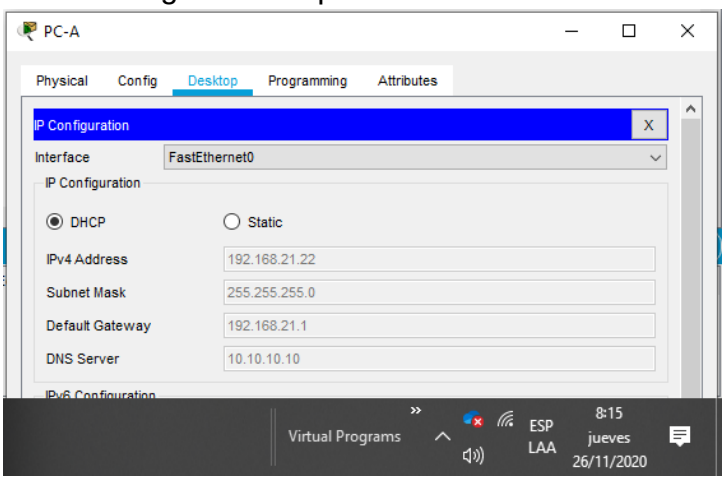
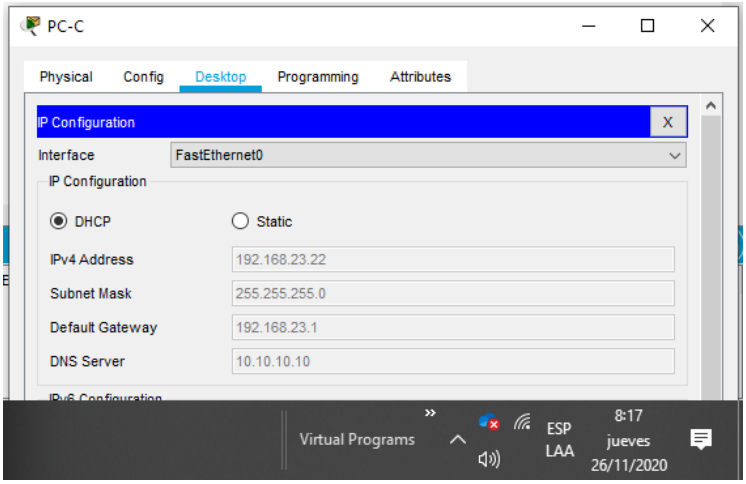


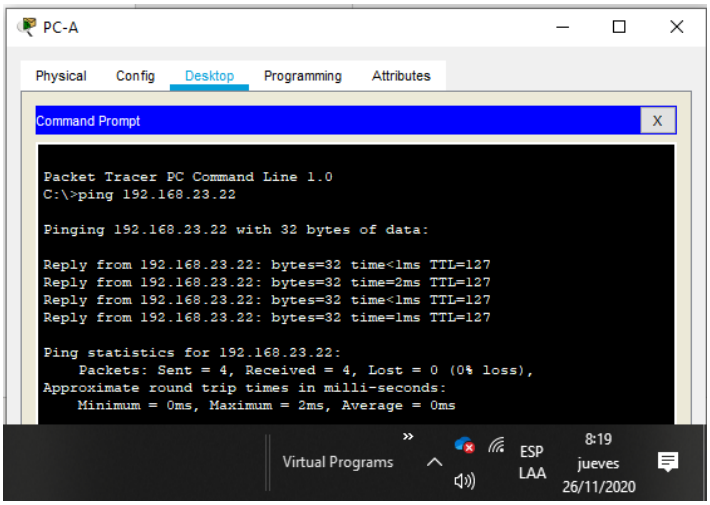
Fuente: Autor.

Paso 3:Verificar el protocolo DHCP y la NAT estática

En el paso de verificación desde los PC se valida que esté tomando el direccionamiento por DHCP y la conectividad entre los mismos

Tabla 26 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 39 IP por DHCP en PC-A  Fuente: Autor.
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 40 IP por DHCP en PC-C  Fuente: Autor.

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Figura 41 Conectividad desde PC-A hacia PC-C  Fuente: Autor.
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**	No se puede realizar ya que HTTP no fue posible activarlo en R2 en el ambiente de simulación Packet Tracer

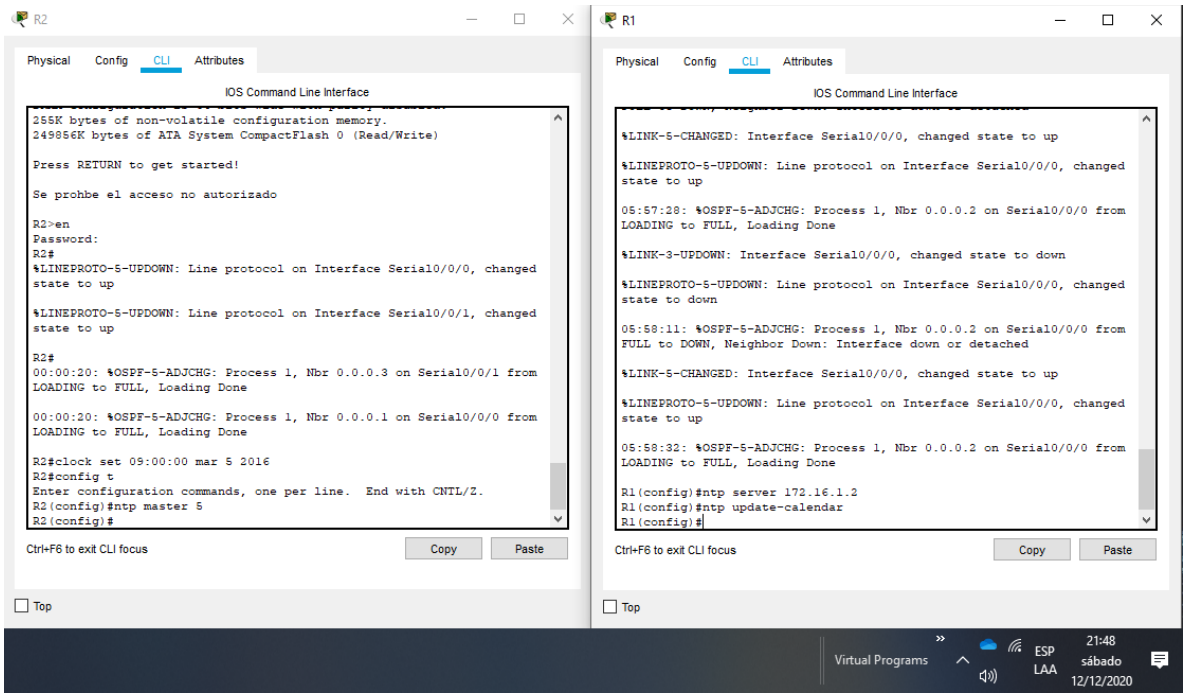
Parte 6: Configurar NTP

En R2 se implementa el protocolo de sincronización de relojes conocido como NTP

Tabla 27 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 mar 5 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar}
Verifique la configuración de NTP en R1.	R1#show ntp associations

Figura 42 Configuración de NTP



Fuente: Autor.

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

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

Desde R2 y por medio de una lista de acceso (ACL) se restringe la conexión a R2 para solo sea permitida para R1

Tabla 28 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	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in

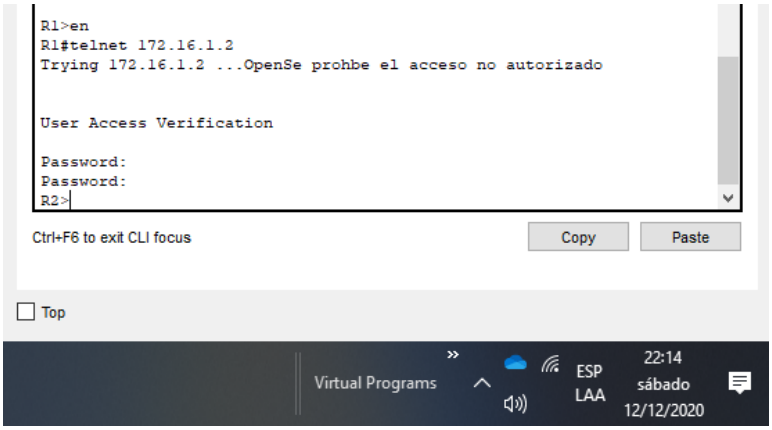
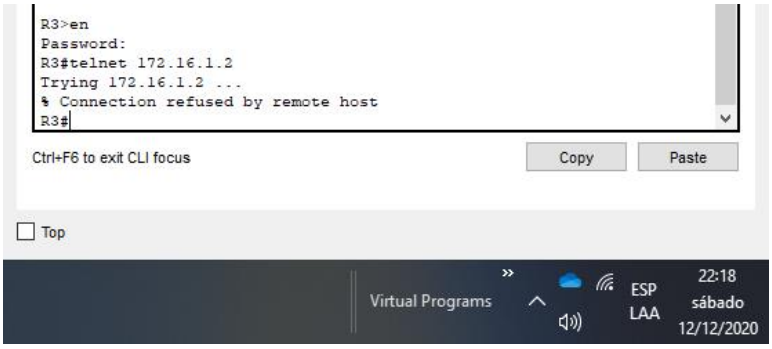
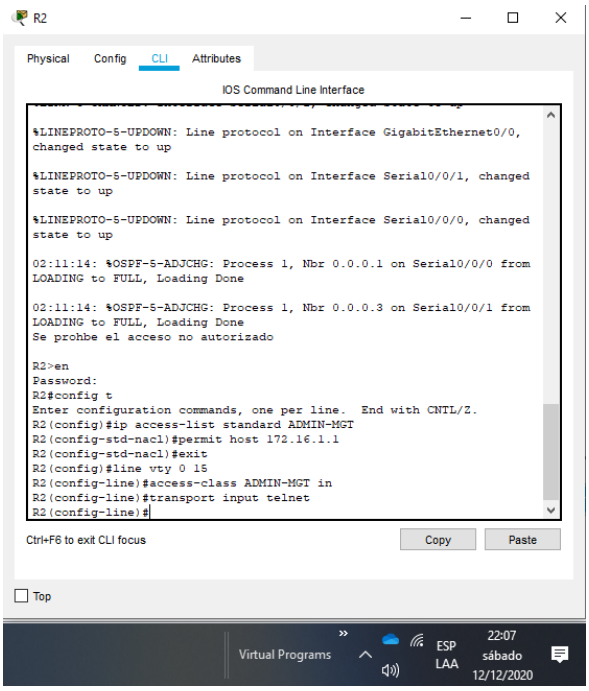
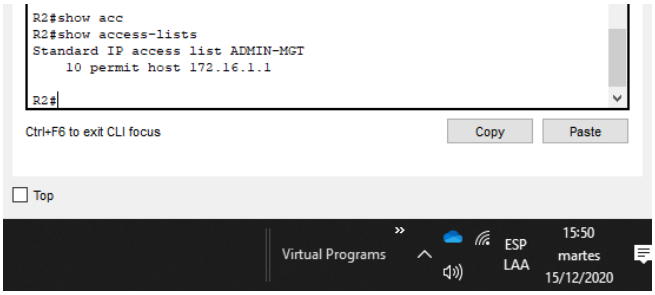
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	Desde R1 se tiene acceso vía Telnet Figura 43 Telnet a R2 desde R1  Fuente: Autor. Desde R3 no se tiene acceso vía Telnet Figura 44 Telnet a R2 desde R3  Fuente: Autor.

Figura 45 Configurar ACL en R2



Fuente: Autor

Figura 46 ACL en R2



Fuente: Autor.

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

A continuación se presentan los comandos requeridos para obtener el resultado que describen en la primera columna de la tabla.

Tabla 29 Comando de CLI adecuados para los resultados requeridos

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters ADMIN-MGT
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

CONCLUSIONES

Se adquiere destreza en el reconocimiento de una topología física y lógica para la posterior practica de la selección y uso de los dispositivos de red, su interconexión y configuración con la respectiva comprobación del correcto funcionamiento.

Se asimilaron los conceptos propuestos VLAN, Trunking, EtherChannel, su objetivo y funcionamiento. Por medio de la herramienta de simulación packet tracer se puso en práctica la forma como se configuran en los dispositivos de una red.

Se comprende y reconocen los comandos necesarios para la implementación de listas de acceso ACL así como su función de medio de control de accesos y filtro de tráfico de la red.

Se comprende y reconocen los comandos necesarios para la implementación del protocolo de enrutamiento OSPF así como su capacidad de identificar y utilizar el camino más corto para el envío de paquete basado en el número de saltos

Se comprende y reconocen los comandos necesarios para la implementación del protocolo DHCP herramienta que facilita la administración de la asignación del direccionamiento automatizándolo lo que previene conflictos por doble asignación de IPs.

NAT para enmascarar la red interna y poder salir a través de una única dirección pública a internet, obteniendo con esto grandes ahorros en direcciones IPv4

BIBLIOGRAFIA

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

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA].

Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking.

Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO (2014) Principios básicos de routing y switching. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE503/es/index.html

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

ANEXOS 1

El siguiente es el link de acceso al drive donde se almacena para consulta lo Siguiente:

Archivo PKT de simulación del escenario 1.

Archivo PKT de simulación del escenario 2.

Artículo científico.

Link de Google drive

https://drive.google.com/drive/folders/1Fs-Wtbzhv3-lHC8OPqzwUlu5cFR9n-Rd?usp=sharing

ANEXO 2

SOLUCIÓN DE UN ESCENARIO PRESENTE EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

Iván Alexander Caro Romero
Universidad Nacional Abierta y a Distancia UNAD, iacaror@unadvirtual.edu.co

Resumen

Basado en el modelo de " Proyecto Aplicado" desarrollado sobre un ambiente de simulación Packet Tracer, herramienta propiedad del fabricante de equipos de comunicaciones CISCO y puesta a disposición de los estudiantes de los cursos CCNA entre otros, se desarrollo un escenario que representa los requerimientos de infraestructura y configuración para una red LAN y WAN, partiendo de la selección de equipos y aplicación sobre los mismos de los protocolos y las opciones de enrutamientos estudiados, así como también la resolución de los problemas que surjan de la implementación y posterior puesta en marcha.

Los temas del curso CNNA que se abordaran en el desarrollo del escenario son: la configuración inicial de equipos en identificación y seguridad en el acceso local y remoto implementando claves y restricciones. La configuración para su óptimo funcionamiento de la infraestructura de la red por medio de la implementación de Vlans como medio para segmentar y limitar el acceso a la red con el fin de mejorar la utilización de los recursos y brindar mayor seguridad y control al tráfico circulante.

Palabras claves: **CISCO, LAN,WAN, enrutamiento, subred, telecomunicaciones**

***Abstract*:**

Based on the model of "Applied Project" developed on an environment of simulation Packet Tracer, tool property of the communications equipment manufacturer CISCO and made available to the students of the courses CCNA among others, a scenario was developed that represents the requirements of infrastructure and configuration for a LAN and WAN, starting from the selection of equipment and application on them of the protocols and routing options studied, as well as the resolution of problems arising from the implementation and subsequent implementation

Keywords: **CISCO, LAN, Networking, WAN, routing subnneting. telecommunications**

I. INTRODUCCION

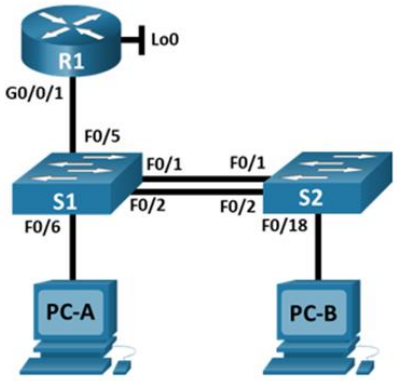
Siendo para el hombre la comunicación una necesidad propia para relacionarse con el medio y que según Berlo [1] su objetivo fundamental es convertir al hombre en un agente efectivo que le permita alterar la relación original que existe entre su organismo y su medio circundante; era de esperarse que este campo revolucionara de forma exponencial con el paso del tiempo hasta llegar a las actuales tecnologías de telecomunicación. pero en el momento en que se logró la fusión de comunicación entre sistemas se convirtió en parte vital e indispensable de la humanidad aplicable a cualquier campo de acción, industria, salud, educación, cultura bajo la globalización que concede la INTERNET. Bajo esta necesidad comunicación en línea la industria de equipos tecnológicos ha crecido a la par y dentro de este grupo se ha destacado en el mercado de fabricantes de componentes de telecomunicación la compañía CISCO. Contreras [2] comparte el siguiente aparte del informe publicado por dicha compañía que vaticina que en el año 2022 se generará más tráfico de Internet que en los 32 años anteriores. El 51% de ese tráfico estará sobre redes WIFI, el 29% sobre redes fijas, el 20% sobre 5G o 4G. "Eso significa que la demanda de tecnología inalámbrica va a ser enorme. Más allá de las tecnologías tradicionales de colaboración, empresas o Gobierno. Con esta visión del futuro Cisco con su experiencia se quiere convertir en referente para la implementación y de redes para los nuevos profesionales que ingresan a laborar en el campo de las Telecomunicaciones. Ellos en pro de mantener y difundir ese conocimiento y el reconocimiento de su tecnología, ponen a disposición su academia de estudio virtual con los cursos certificados CNNA, CCNP y otros más que junto a su herramienta de simulación packet tracer permiten convertirse en un especialista de este campo.

Aprovechando el conocimiento brindado por el curso CNNA y la herramienta de estudio Packet Tracer se desarrolla el escenario que es tema de este articulo donde se expondrá las etapas desarrolladas, los resultados obtenidos y las conclusiones a las que se llegaron.

II. METODOLOGIA

Se propone el escenario planteado en la figura 1con la información de direccionamiento IP de la Tabla 1 y el listado de Vlans de la Tabla 2 requerimientos específicos se realizará la implementación simulada sobre la herramienta de CISCO Packet tracer con el objeto de satisfacerlo y garantizar el correcto funcionamiento

Figura 1 Topología de red escenario 1



Fuente: UNAD

Se presenta en la tabla 1 el direccionamiento asignado para el escenario propuesto.

Tabla 1 direccionamiento IP

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Las Vlan que se requieren son las siguientes

Tabla 2 Lista de Vlans

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

Se inicia con la configuración inicial de los equipos que comprende el borrado de la configuración de las Vlan, la configuración de la plantilla SDM para la admisión de IPv6. Los comandos ejecutados se exponen las Tablas 3 y 4

Posterior a la selección de los equipos, se inicia con la configuración básica sobre R1 descritas en la tabla 3 la identificación del equipo con un nombre, habilitar el acceso local y remoto con restricciones de seguridad que lo protejan de intentos no autorizados.

Tabla 3 Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Escenario 1 Ivan Caro R1"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config-subif)#description Subinterface VLAN 2 BIKES R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#no shutdown R1(config-if)#
Configure el Loopback0 interface	R1(config)#interface loopback 0 R1(config-if)#description Loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local

Continuando con la configuración inicial de la red propuesta, lo siguiente es realizar la configuración correspondiente a los switchs S1 y S2 con las mismas configuraciones básicas del router pero adicionando el establecimiento del Gateway predeterminado.

Tabla 4 Configurar los Switch S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup Switch0(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 Switch0(config)#hostname S2
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config-line)#password ciscoconpass S2(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd " Escenario 1 Ivan Caro S1 " S2(config)#banner motd " Escenario 1 Ivan Caro S2 "
Generar una clave de cifrado RSA	S1(config)#CRYpto key generate rsa S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config-if)#ip address 10.19.8.98 255.255.255.248 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S1(config-if)#ipv6 address FE80::98 link-local S2(config-if)#ipv6 address FE80::99 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 S1(config)#ipv6 route ::/0 2001:db8:acad:c::1 S2(config)#ip default-gateway 10.19.8.97 S2(config)#ipv6 route ::/0 2001:db8:acad:c::1

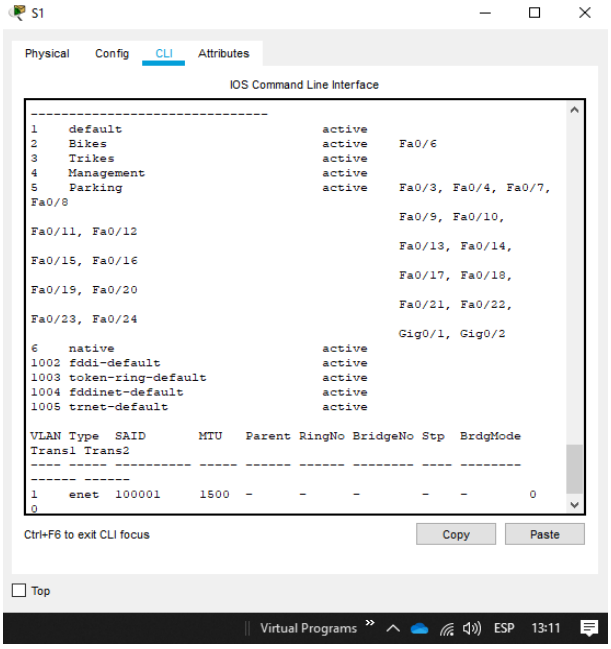
En la segunda parte se procede con la estructuración de la red con la implementación de las Vlans en S1 . La creación del tronco sobre la Vlan 6 y la creación de un grupo de puertos EtherChannel agrupando las interfaces F01/ y F 0/2. se configura el puerto de acceso para la Vlan 2 por la interface F0/6. Los comandos para implementar lo requerido se describe en las Tablas 5.

Tabla 5 Configuración de Vlan en S1

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config)#vlan 4 S1(config-vlan)#name Management S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#channel-group 1 mode active S1(config-if)#channel-protocol lacp
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1(config)#interface range FastEthernet 0/3-4 , fastEthernet 0/7 - 24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Interfaces “INACTIVAS"

En la figura 2, mediante el uso del comando show vlan se evidencia la configuración de las Vlan sobre S1

Figura 2 Vlan en S1



Fuente: Autor

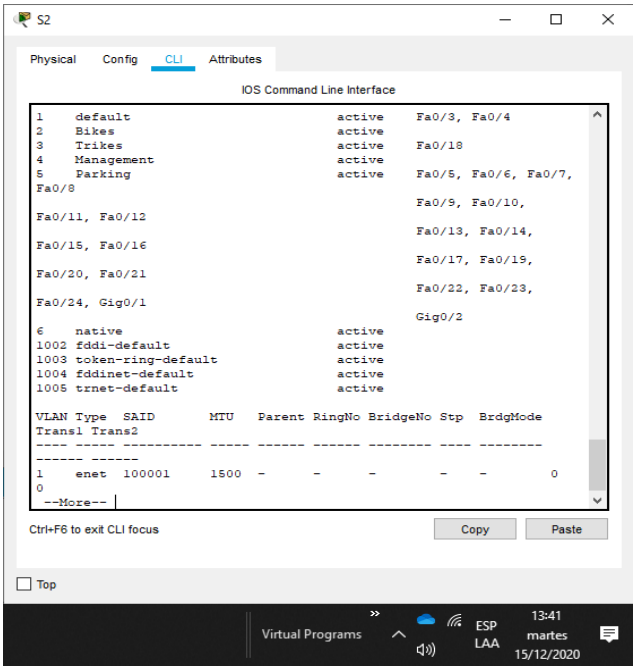
Se continua con la misma configuración para lo correspondiente a S2. Para este equipo se configura el puerto de acceso para la Vlan 3 por la interface F0/18. Los comandos para implementar lo requerido se describe en las Tablas 6.

Tabla 6 Configuración de Vlan en S2

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config)#vlan 4 S2(config-vlan)#name Management S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config-if)#channel-group 1 mode active S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2(config)#interface range fa0/5-17 , fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Interfaces sin uso S2(config-if-range)#sh

En la figura 3 mediante el comando show Vlan se evidencia la configuración de las Vlan sobre S2

Figura 3 Vlan en S2



Fuente: Autor

Sobre el router R1 corresponde la configuración de enrutamiento, Se establece como ruta por defecto la Loopback la configuración del DHCP para IPv4 determinando un pool de IPs para la Vlan 2 y 3 según instrucciones.

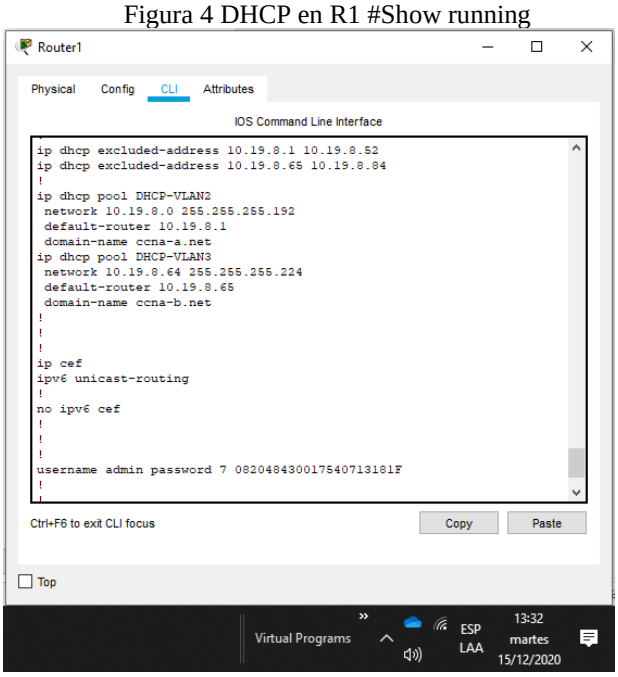
Tabla 7 Configuración del Router R1.

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0

Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp pool DHCP-VLAN2 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool DHCP-VLAN3 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

En la figura 4 mediante el comando show running-config se evidencia la configuración de las Vlan en R1.

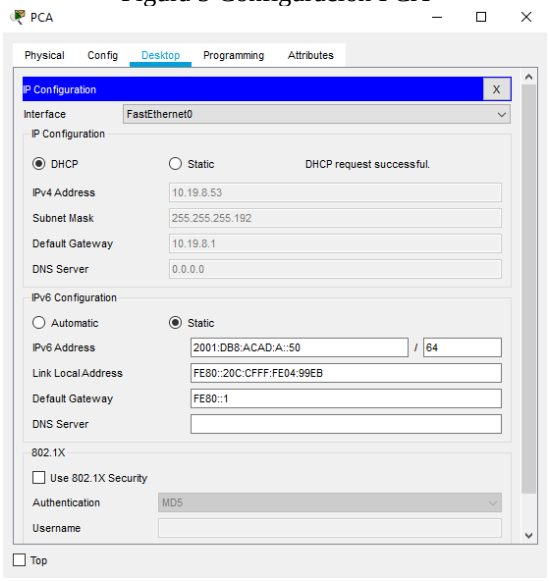
Figura 4 DHCP en R1 #Show running



Fuente: Autor.

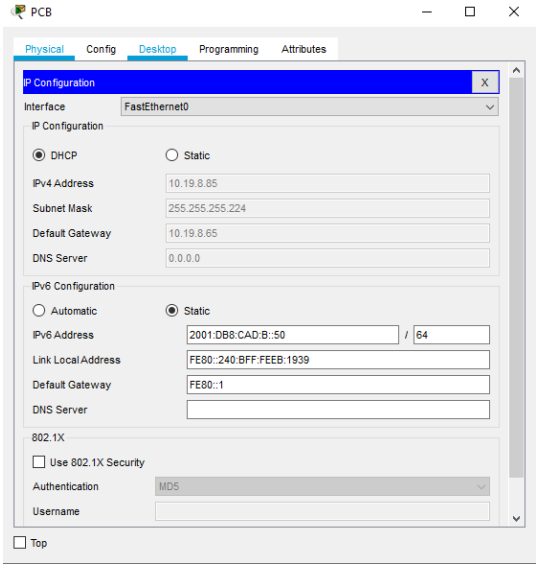
El siguiente y último paso fue la configuración de los equipos host PCA y PCB de modo que para tomar direccionamiento utilizaran DHCP, utilizando la primera ip disponible del pool dispuesto para cada Vlan en IPv4. Se asigna de forma estática el direccionamiento IPv6. En las figuras 5 y 6 se observa los parametros que se configuraron en cada uno y como toman la IP.

Figura 5 Configuración PCA



Fuente: Autor.

Figura 6 Configuración PCB



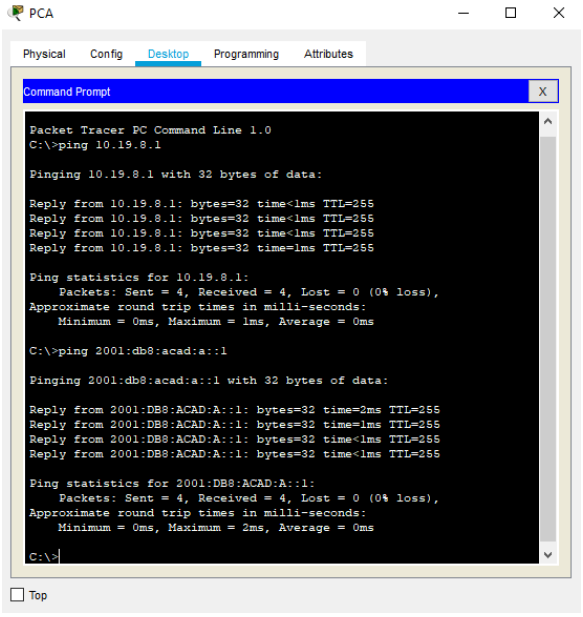
Fuente: Autor.

III. RESULTADOS

Finalizado los pasos necesarios para cumplir con los requerimientos del ejercicio propuesto se procedió a realizar las validaciones de conectividad de extremo a extremo. El comando ping ejecutado en cada dispositivo de la red fue el medio utilizado para hacer la comprobación.

Se realizó validación de conectividad desde el PCA a R1 interfaz G0/0/1.2 Demostrando que alcanzaba el destino. El resultado positivo se visualiza en la figura 7 tanto para IPv4 como para IPv6.

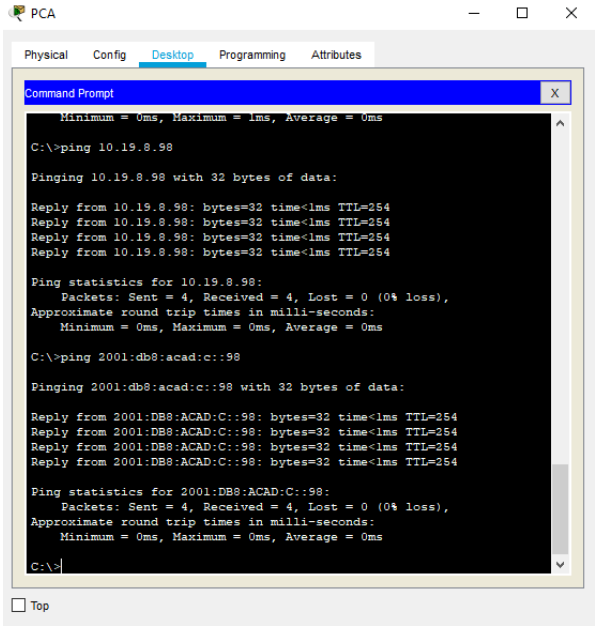
Figura 7 Ping de PCA a R1 interfaz G0/0/1.2.



Fuente: Autor

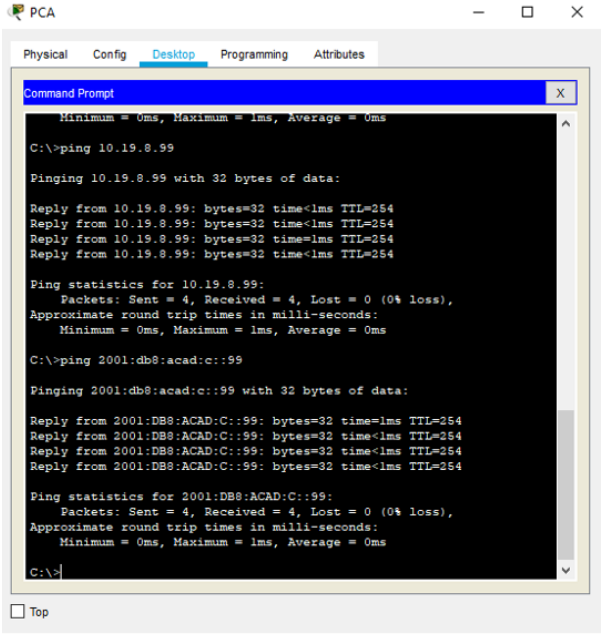
Se realizó validación de conectividad desde el PCA a S1 Vlan4 Demostrando que alcanzaba el destino. El resultado positivo se visualiza en la figura 8 tanto para IPv4 como para IPv6.

Figura 8 Ping de PCA a S1 Vlan4



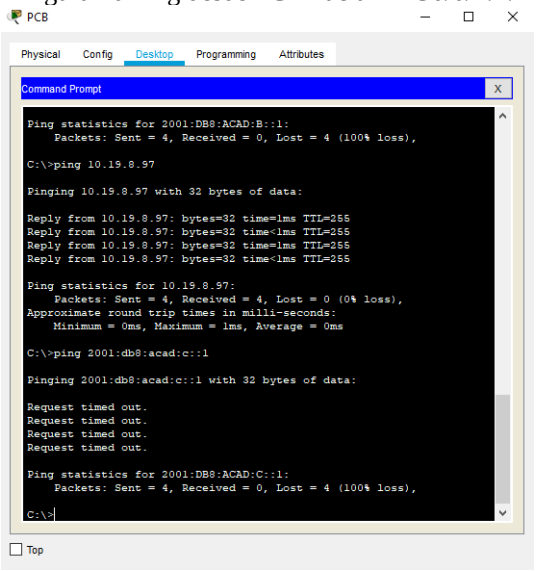
Se realizó validación de conectividad desde el PCA a S2 Vlan4 Demostrando que alcanzaba el destino. El resultado positivo se visualiza en la figura 9 tanto para IPv4 como para IPv6.

Figura 9 Ping de PCA a S2 Vlan4



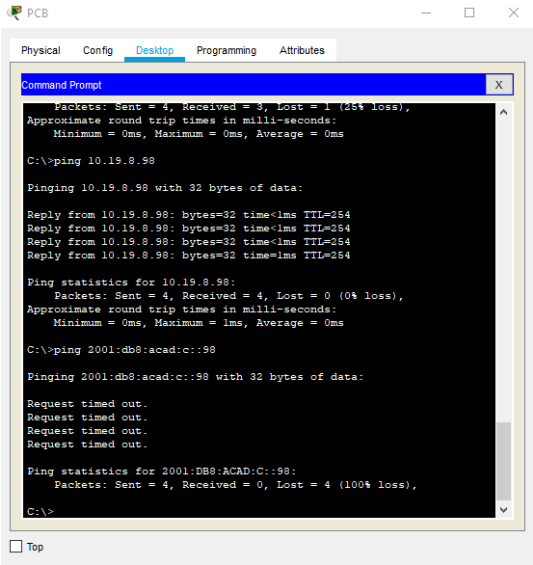
Se realizó validación de conectividad desde el PCB a R1 G0/0/1.4. El resultado positivo se visualiza en la figura 10 para IPv4 mas no para IPv6

Figura 10 Ping desde PCB hacia R1 G0/0/1.4.



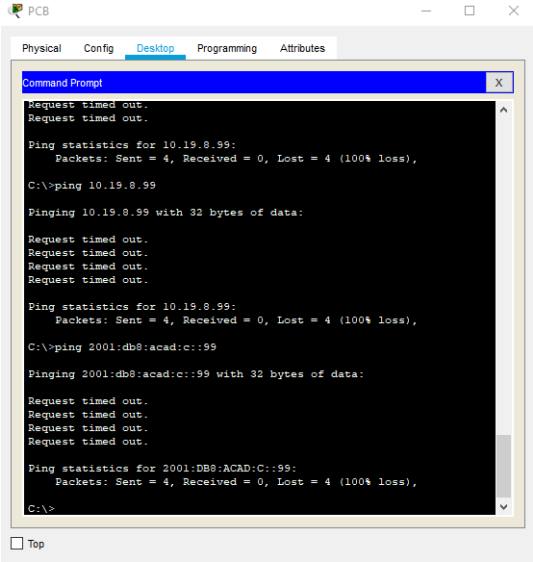
Se realizó validación de conectividad desde el PCB a S1 Vlan4. El resultado positivo se visualiza en la figura 11 para IPv4 mas no para IPv6

Figura 11 Ping desde PCB hacia S1 Vlan4



Se realizó validación de conectividad desde el PCB a S2 Vlan4. El resultado negativo se visualiza en la figura 12 tanto para IPv4 como para IPv6

Figura 12 Ping desde PCB hacia S2 Vlan4



En este punto finalizan las pruebas de conectividad y alcance entre dispositivos.

IV. CONCLUSIONES

El desarrollo del escenario permitió adquirir destreza en el reconocimiento de una topología física y lógica en la selección y uso de los dispositivos de red, su interconexión y configuración con la respectiva comprobación del correcto funcionamiento para satisfacer las necesidades de comunicación de un proyecto

Se asimilaron los conceptos propuestos en temas propios del networking como son VLAN, Trunking, EtherChannel, comprendiendo a fondo su objetivo y funcionamiento dentro de una rede de comunicaciones.

Por medio de la herramienta de simulación packet tracer se recreó el escenario, se puso en práctica la teoría estudiada en cuanto al proceso como se configuran n los dispositivos de una red como son los routers y switchs

V. REFERENCIAS

D. Berlo, El Proceso de la Comunicación. Buenos Aires. 1969.

C. Contreras.(2020) Cisco: La digitalización será el motor de las empresas en 2020. [en línea]. Disponible en: https://www.estrategiaynegocios.net/tecnologia/1352724-330/digitalizacion-sera-motor-de-las-empresas-en-2020

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

J. Vesga (2014) Diseño y configuración de redes con Packet Tracer [OVA] [en línea]. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. [en línea]. Disponible en: https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

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. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

VI .BIOGRAFIA

Iván Alexander Caro Romero. Nació en Bogota – Colombia el 7 de Noviembre de 1975. Se graduó de la Universidad Unicatólica como tecnólogo en telecomunicaciones, adelanta estudios en ingeniería en telecomunicaciones en la Universidad Nacional Abierta y a Distancia UNAD. Su experiencia profesional incluye el Banco de Occidente, Orión Contact center S. A. S. Lumen Colombia. En estas empresas ha ocupado cargos en el área de tecnología específicamente en el ramo de las telecomunicaciones para servicios telefónicos en las dos primeras y en la tercera en la prestación de servicios de telecomunicaciones y datacenter.