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

CARLOS JAVIER ARROYO GALVIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERIA ELECTRÓNICA

SAN MARCOS – SUCRE

2020

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

CARLOS JAVIER ARROYO GALVIZ

Diplomado de opción de grado presentado para obtener el título de
INGENIERO DE ELECTRONICA

DIRECTOR

Esp. DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA ELECTRÓNICA

SAN MARCOS – SUCRE

2020

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

San Marcos, Diciembre 13 de 2020

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

GLOSARIO

BANNER MOTD: Es un comando que especifica el mensaje que se muestra como Mensaje del día, el primer mensaje que se muestra en una conexión entrante. Este comando define solo el mensaje; el comando motd - banner habilita o deshabilita la visualización.

DHCP: Significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

ETHERCHANNEL: Es una tecnología de agregación de enlaces de puertos desarrollada por Cisco, que proporciona enlaces de alta velocidad tolerantes a fallas entre conmutadores, enrutadores y servidores. La tecnología EtherChannel permite que varios enlaces Ethernet físicos (Fast Ethernet o Gigabit Ethernet) se combinen en un canal lógico.

GATEWAY: Un Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

NVRAM: La NVRAM o “Non-Volatile Random Access Memory”, es una memoria de acceso aleatorio no volátil capaz de almacenar información y no perderla al retirar la alimentación eléctrica del componente.

PORT-SECURITY: Es una característica de los switches Cisco que les permite retener las direcciones MAC conectadas a cada puerto del dispositivo y permitir solamente a esas direcciones MAC comunicarse a través de esa entrada del switch. Si un dispositivo con otra dirección MAC intenta comunicarse a través de esa esa entrada, port-security deshabilitará el puerto.

TRUNKING: En telecomunicaciones, el enlace troncal es una forma de proporcionar acceso a la red a muchos clientes compartiendo un conjunto de líneas o frecuencias en lugar de proporcionarlas individualmente.

VLAN: Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

El diplomado de profundización CISCO se enfoca en realizar de manera correcta pruebas en rutandolos para un aprendizaje practico, utilizando herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento,

atreves de la administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP, diseña políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.

Atreves de los avances tecnológicos es posible aplicar como ingeniero electrónico en escenarios corporativos y residenciales configurando esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs y las bondades de administrardominios de broadcast independientes.

En este trabajo permitido diseñar un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP

ABSTRACT

The CISCO in-depth diploma focuses on correctly carrying out routing tests for practical learning, using simulation tools and remote access laboratories in order to establish LAN / WAN scenarios that allow an analysis of the behavior of various protocols and routing metrics,

Through the network administration available in the IOS to solve the problems of data networks, evaluating the performance of routers and switches, through the use of specialized commands in network management and compatible with the SMNP protocol, it designs static routing policies and / or dynamic (RIP and OSPF), under a classless IP addressing scheme, to provide scalable network and connectivity solutions, through the use of packet routing and switching principles in LAN and WAN environments.

Through technological advances, it is possible to apply as an electronic engineer in corporate and residential settings, configuring switching schemes, through the use of protocols based on STP and VLANs and the benefits of managing independent broadcast domains.

In this work allowed to design an IP addressing scheme to provide connectivity; security and access to the WAN using the DHCP protocol.

INTRODUCCIÓN

Este trabajo es de gran importancia para el desarrollo de nuestra carrera ya que se fundamenta en el enriquecimiento de nuestro conocimiento como futuros ingenieros permitiendo el desarrollo intelectual, a través de la realización del Paso 6 Entrega Avance Documento Final con realización de ejercicios que se presentaran durante este diplomado, con la ayuda del tutor y los compañeros del curso para así obtener un buen desarrollo de todas las actividades que a lo largo del curso se presentaran

Se puede afirmar mediante la realización de esta actividad como avanzar en el desarrollo de estrategias que buscan el buen desempeño de ejercicios a través de routers y los switches buscando una buena configuración y luego una buena programación, para así, tener los resultados esperados demostrando y colocando todo el conocimiento obtenido en el curso y luego llevarlo a la práctica, para así, presentar la mejor respuesta a esta fase que es importante a para el desarrollo de nuestra carrera como ingenieros y al mismo tiempo reconocer la importancia de la tecnología en un mundo cámbiate que evoluciona cada vez más en post de la comunicación digital.

DESARROLLO DE PRÁCTICAS

Escenario 1

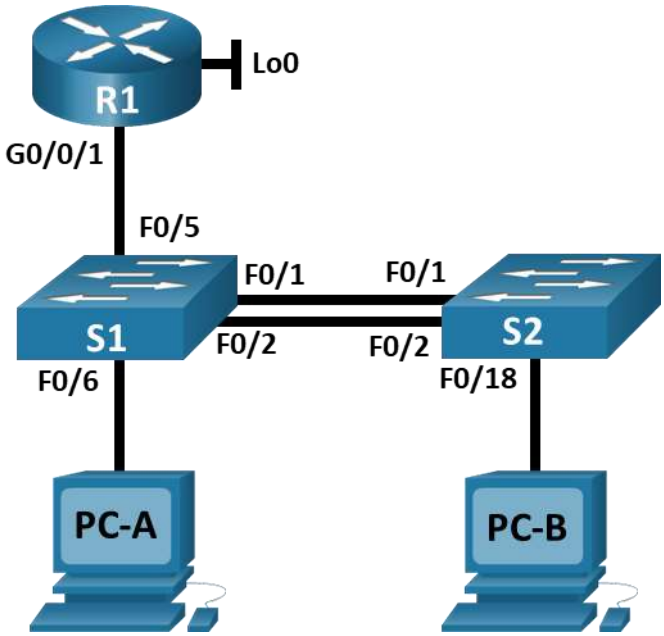


Ilustración 1

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management

VLAN	Nombre de la VLAN
5	Parking
6	Native

Tabla 1

Tabla de asignación de direcciones

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

Tabla 2

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

INSTRUCIONES

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

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

1.1. Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

En R1

```
Router>en
Router#erase startup-config
Router#reload
```

En S1

```
Switch>en
Switch#erase startup-config
Switch#reload
```

En S2

```
Switch>en
Switch#erase startup-config
Switch#reload
```

1.2. Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

En S1

```
Switch>en
Switch#conf t
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload
```

En S2

```
Switch>en
Switch#conf t
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#exit
Switch#reload
```

1.3. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Pasó 2: Configurar R1 - Las tareas de configuración para R1 incluyen las siguientes:

2.1. Desactivar la búsqueda DNS

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

2.2. Nombre del router – R1

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

2.3. Nombre de dominio - ccna-lab.com

```
R1(config)# ip domain name ccna-lab.com
```

2.4. Contraseña cifrada para el modo EXEC privilegiado - ciscoenpass

```
R1(config)#enable secret ciscoenpass
```

2.5. Contraseña de acceso a la consola - ciscoconpass

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
```

```
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

2.6. Establecer la longitud mínima para las contraseñas – 10 caracteres

```
R1(config)#security passwords min-length 10
```

2.1. Crear un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass

```
R1(config)#username admin secret admin1pass
```

2.2. 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
```

2.3. Configurar VTY solo aceptando SSH

```
R1(config-line)#transport input ssh
R1(config-line)#exit
```

2.4. Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
```

2.5. Configure un MOTD Banner

```
R1(config)#banner motd “Prohibido el acceso no autorizado”
```

2.6. Habilitar el routing IPv6

```
R1(config)#ipv6 unicast-routing
```

2.7. Configurar interfaz G0/1 y subinterfaces

```
R1(config)# int g0/1.2
R1(config-subif)#encapsulation dot1Q 2
```

```
R1(config-subif)#description Vlan-->Bikes
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit


R1(config)# int g0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Vlan-->Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit


R1(config)#int g0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Vlan-->Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit


R1(config)#int g0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Vlan-->Native
R1(config-subif)#exit


R1(config)#int g0/1
R1(config-if)#no shutdown
```

2.8. Configure el Loopback0 interface

```
R1(config)#int Loopback 0
R1(config-if)#description Loopback
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
R1(config-if)#exit
```

2.9. Generar una clave de cifrado RSA - Módulo de 1024 bits

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

2.10. Nombre del router – R1

```
R1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Paso 3: Configure S1 y S2 - Las tareas de configuración incluyen lo siguiente:

3.1. Desactivar la búsqueda DNS.

S1 y S2

```
Switch>en
Switch#conf t
Switch(config)#no ip domain lookup
```

3.2. Nombre del switch – S1 y S2

S1

```
Switch(config)#hostname S1
S1(config)#
```

S2

```
Switch(config)#hostname S2
S2(config)#
```

3.3. Nombre de dominio

```
S1(config)# ip domain name ccna-lab.com
S2(config)# ip domain name ccna-lab.com
```

3.4. Contraseña cifrada para el modo EXEC privilegiado - ciscoenpass

```
S1(config)# enable secret ciscoenpass
S2(config)# enable secret ciscoenpass
```

3.5. Contraseña de acceso a la consola - ciscoconpass

```
S1(config)# line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
```

```
S2(config)# line console 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
```

3.6. Crear un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass

```
S1(config)# username admin secret admin1pass

S2(config)# username admin secret admin1pass
```

3.7. 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
```

3.8 Configurar las líneas VTY para que acepten únicamente las conexiones SSH

```
S1(config-line)#transport input ssh
S1(config-line)#exit


S2(config-line)#transport input ssh
S2(config-line)#exit
```

3.9. Cifrar las contraseñas de texto no cifrado

```
S1(config)# service password-encryption
S2(config)# service password-encryption
```

3.10. Configurar un MOTD Banner

```
S1(config)#banner motd “Prohibido el acceso no autorizado”
S2(config)#banner motd “Prohibido el acceso no autorizado”
```

3.11. Generar una clave de cifrado RSA - Módulo de 1024 bits

```
S1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

```
S2(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
```

3.12. Configurar la interfaz de administración (SVI)

```
S1(config)#int vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#no shutdown
S1(config-if)#exit
```

```
S2(config)#int vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#no shutdown
S2(config-if)#exit
```

3.13. Configuración del gateway predeterminado

```
S1(config)# ip default-gateway 10.19.8.97
S2(config)# ip default-gateway 10.19.8.97
```

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

Paso 4: Configurar S1 - La configuración del S1 incluye las siguientes tareas:

4.1. Crear VLAN

```
S1(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)#exit
```

4.2. Crear troncos 802.1Q que utilicen la VLAN 6 nativa - Interfaces F0/1, F0/2 y F0/5

```
S1(config)#int f0/1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit

S1(config)#int f0/2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit


S1(config)#int f0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit
```

4.3. Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 - Usar el protocolo LACP para la negociación

```
S1(config)#int f0/1
S1(config-if)#channel-group 1 mode active
S1(config-if)#exit


S1(config)#int f0/2
S1(config-if)#channel-group 1 mode active
S1(config-if)#exit
```

4.4. Configurar el puerto de acceso de host para VLAN 2 - Interface F0/6

```
S1(config)#int f0/6
```

```
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
```

4.5. Configurar la seguridad del puerto en los puertos de acceso - Permitir 3 direcciones MAC

```
S1(config-if)#switchport port-security maximum 3
```

4.6. Nombre del router – R1

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

4.7. Proteja todas las interfaces no utilizadas - Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar.

```
S1(config)#int range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

```
S1(config)#int range f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

```
S1(config)#int range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Desabilitada
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

Paso 5: Configure el S2 - Entre las tareas de configuración de S2 se incluyen las siguientes:

5.1. Crear VLAN

```
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit
```

5.2. Crear troncos 802.1Q que utilicen la VLAN 6 nativa - Interfaces F0/1 y F0/2

```
S2(config)#int f0/1
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if)#exit

S2(config)#int f0/2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if)#exit
```

5.3. Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 - Usar el protocolo LACP para la negociación

```
S2(config)#int f0/1
S2(config-if)#channel-group 1 mode active
S2(config-if)#exit

S2(config)#int f0/2
S2(config-if)#channel-group 1 mode active
S2(config-if)#exit
```

5.4. Configurar el puerto de acceso de host para VLAN 3 - Interface F0/18

```
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
```

5.5. Configure port-security en los access ports - permite 3 MAC addresses

```
S2(config-if)#switchport port-security maximum 3
```

5.6 Asegure todas las interfaces no utilizadas - Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar.

```
S2(config)#int range f0/3-17
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Desabilitada
S2(config-if-range)#shutdown
S2(config-if-range)#exit

S2(config)#int range f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Desabilitada
S2(config-if-range)#shutdown
S2(config-if-range)#exit

S2(config)#int range g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Desabilitada
S2(config-if-range)#shutdown
S2(config-if-range)#exit
```

Parte 2: Configurar soporte de host

Paso 1: Configure R1 - Las tareas de configuración para R1 incluyen las siguientes:

1.1. Configure Default Routing - Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
```

1.2. Configurar IPv4 DHCP para VLAN 2 - Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

```
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool Vlan2-Bikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

1.3. Configurar DHCP IPv4 para VLAN 3 - Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

```
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool Vlan3-Trikes
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit
```

Paso 2: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

PC-A Network Configuration	
Descripción	*FastEthernet0 Connection:(default port)*
Dirección física	*0009.7CA1.36A0*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*

PC-A Network Configuration	
Gateway predeterminado IPv6	*FE80::209:7CFF:FEA1:36A0*

Configuración de red de PC-B	
Descripción	*FastEthernet0 Connection:(default port)*
Dirección física	*000C.CFB6.5835*
Dirección IP	*169.254.88.53*
Máscara de subred	*255.255.0.0*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::20C:CFFF:FEB6:5835*

Parte 3: Probar y verificar la conectividad de extremo a extremo

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Si*
		IPv6	2001:db8:acad:a: :1	*Si*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Si*
		IPv6	2001:db8:acad:b: :1	*Si*

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	*Si*
		IPv6	2001:db8:acad:c: :1	*Si*
	S1, VLAN 4	Dirección	10.19.8.98	*Si*
		IPv6	2001:db8:acad:c: :98	*Si*
	S2, VLAN 4	Dirección	10.19.8.99.	*Si*
		IPv6	2001:db8:acad:c: :99	*Si*
	PC-B	Dirección	IP address will vary.	*Si*
		IPv6	2001:db8:acad:b: :50	*Si*
	R1 Bucle 0	Dirección	209.165.201.1	*Si*
		IPv6	2001:db8:acad:209: :1	*Si*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Si*
		IPv6	2001:db8:acad:209: :1	*Si*
	R1, G0/0/1.2	Dirección	10.19.8.1	*Si*
		IPv6	2001:db8:acad:a: :1	*Si*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Si*
		IPv6	2001:db8:acad:b: :1	*Si*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Si*
		IPv6	2001:db8:acad:c: :1	*Si*
	S1, VLAN 4	Dirección	10.19.8.98	*Si*
		IPv6	2001:db8:acad:c: :98	*Si*
	S2, VLAN 4	Dirección	10.19.8.99.	*Si*
		IPv6	2001:db8:acad:c: :99	*Si*

PANTALLAZOS – SHOW RUNNING-STARTUP

R1

Ilustración 2

Ilustración 3

Ilustración 4

Ilustración 5

S1

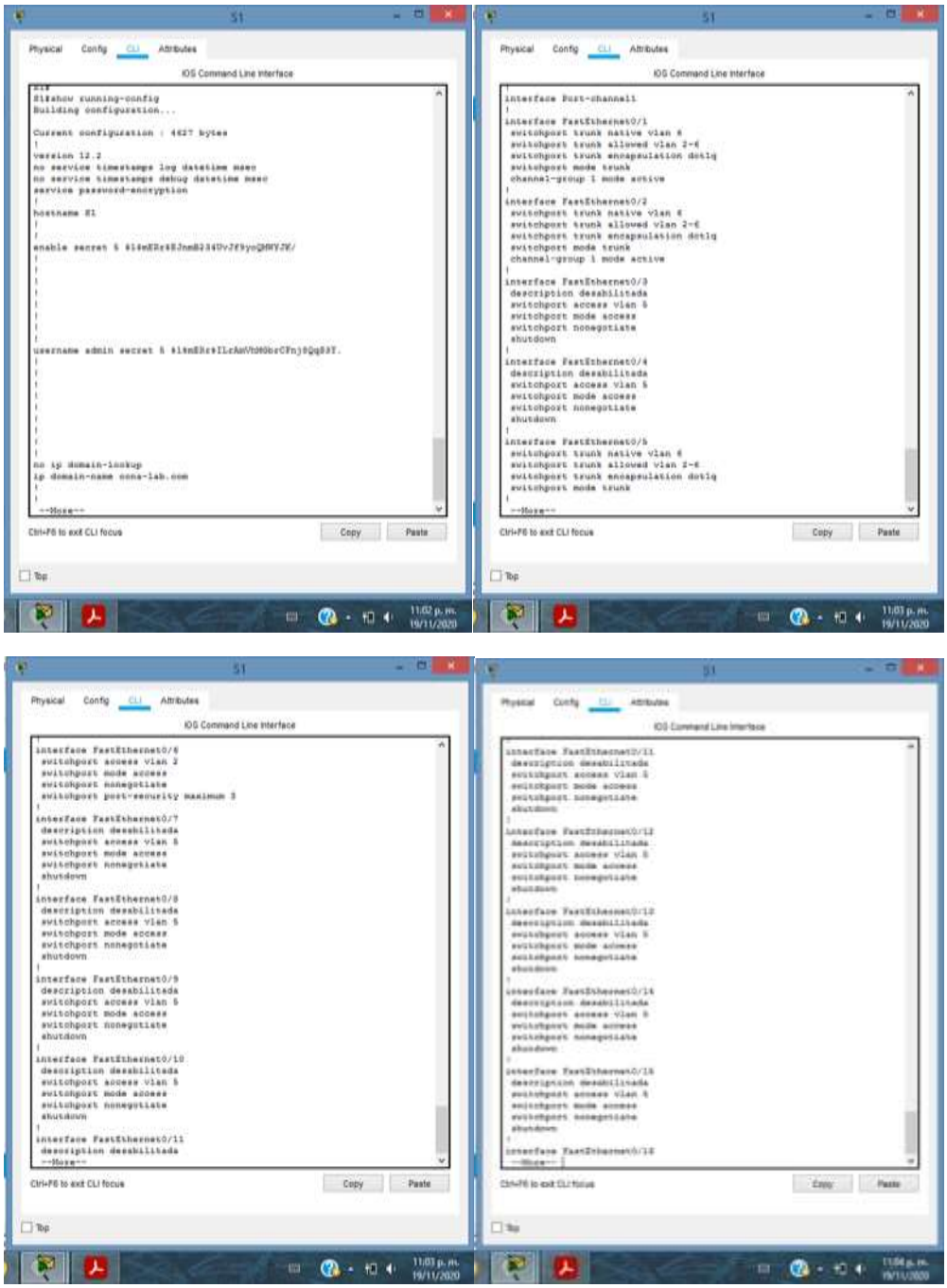


Ilustración 6

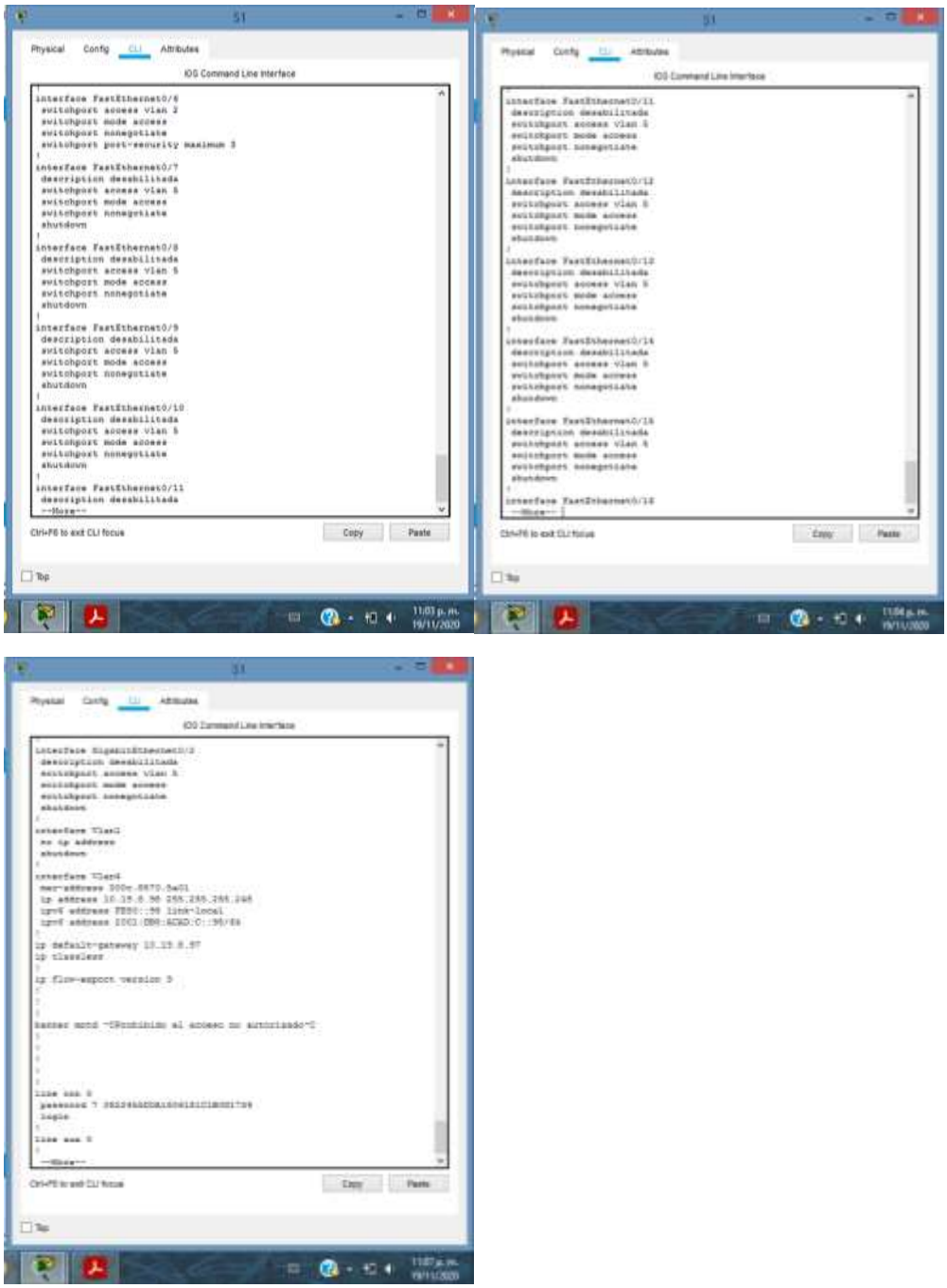


Ilustración 7

S2

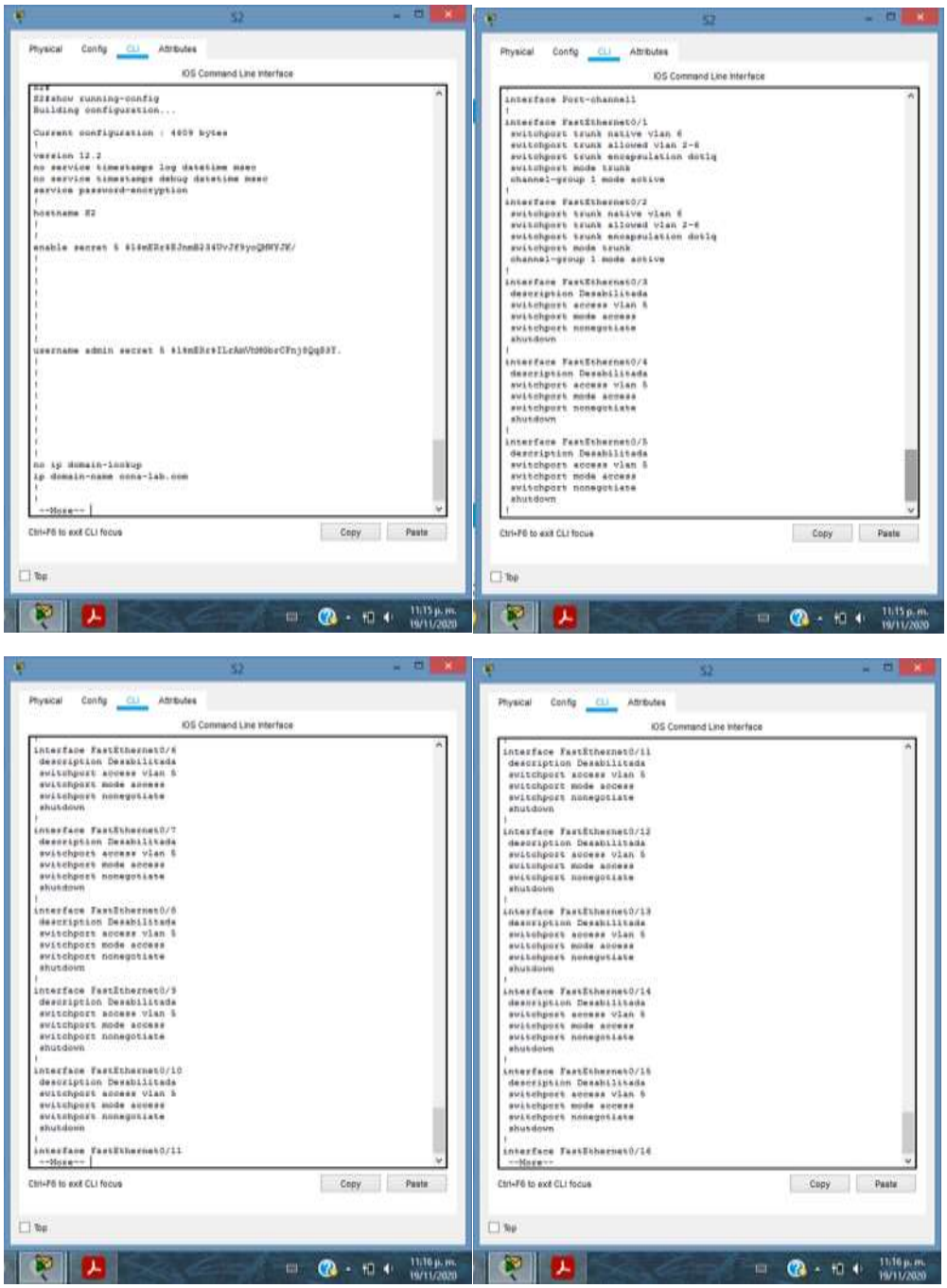
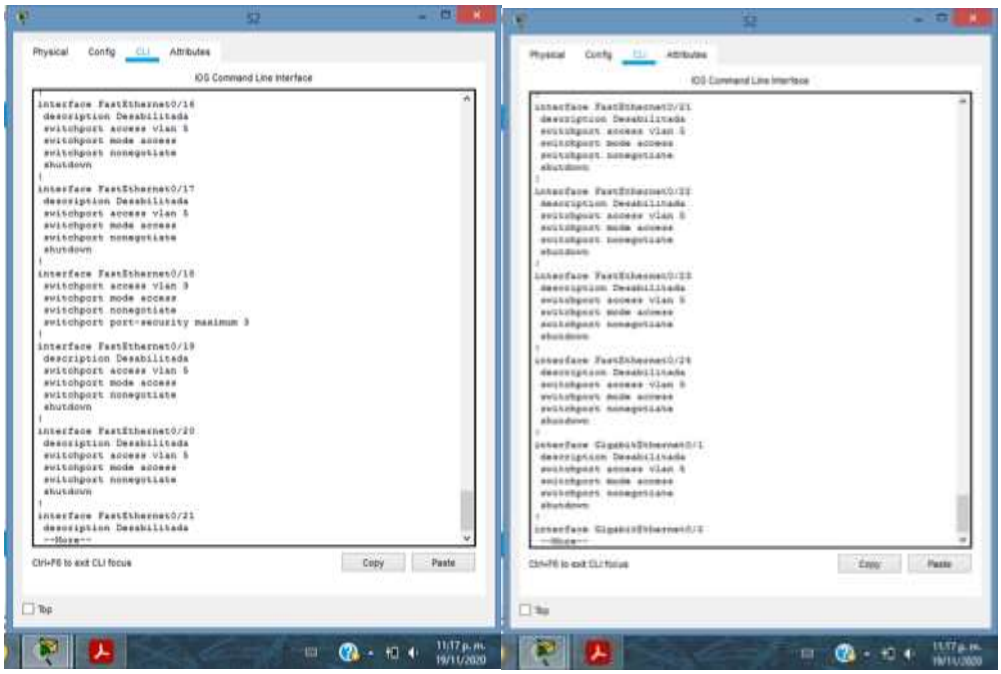


Ilustración 8



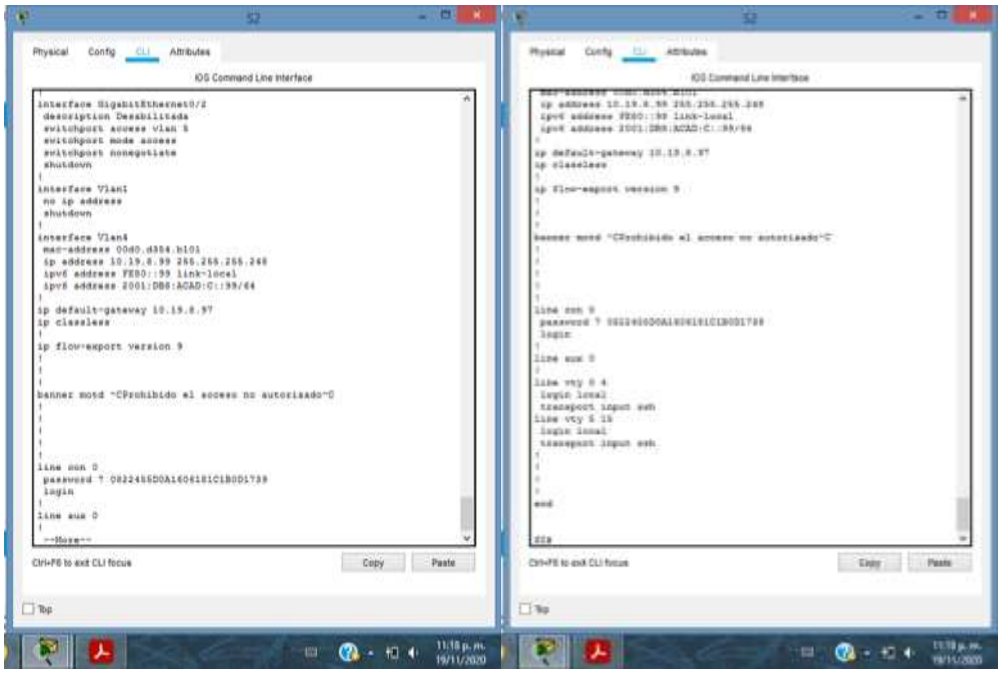
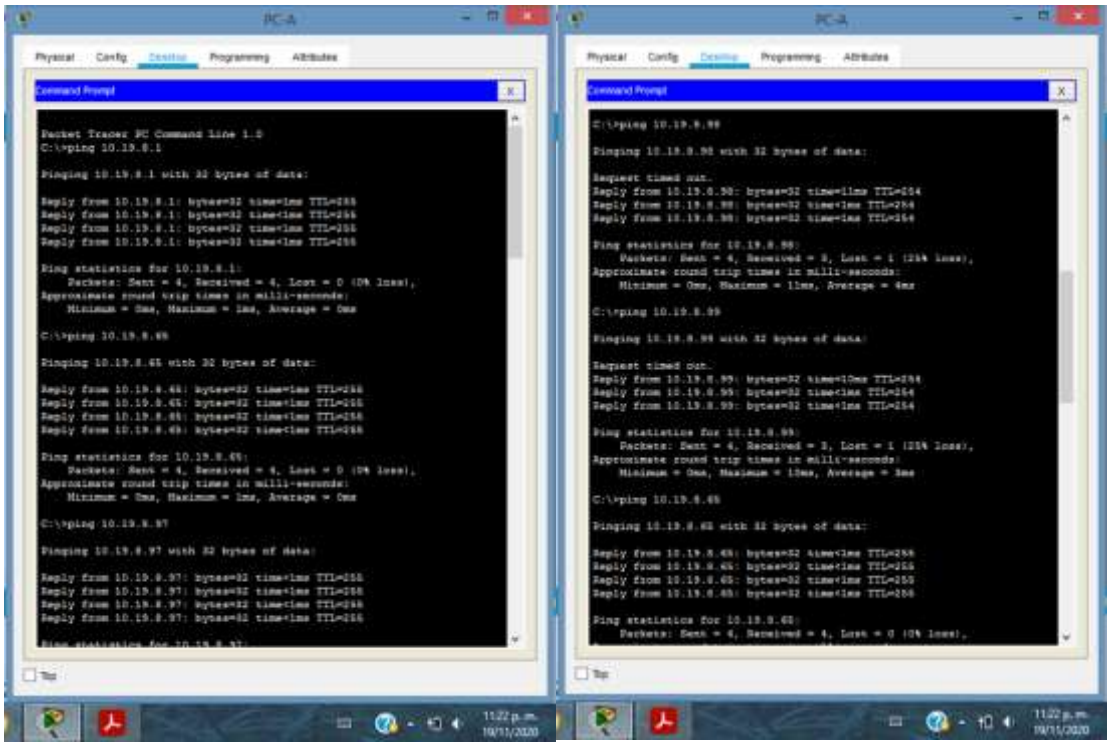


Ilustración 9

PRUEBA DE CONECTIVIDAD

PING EN EL PC-A



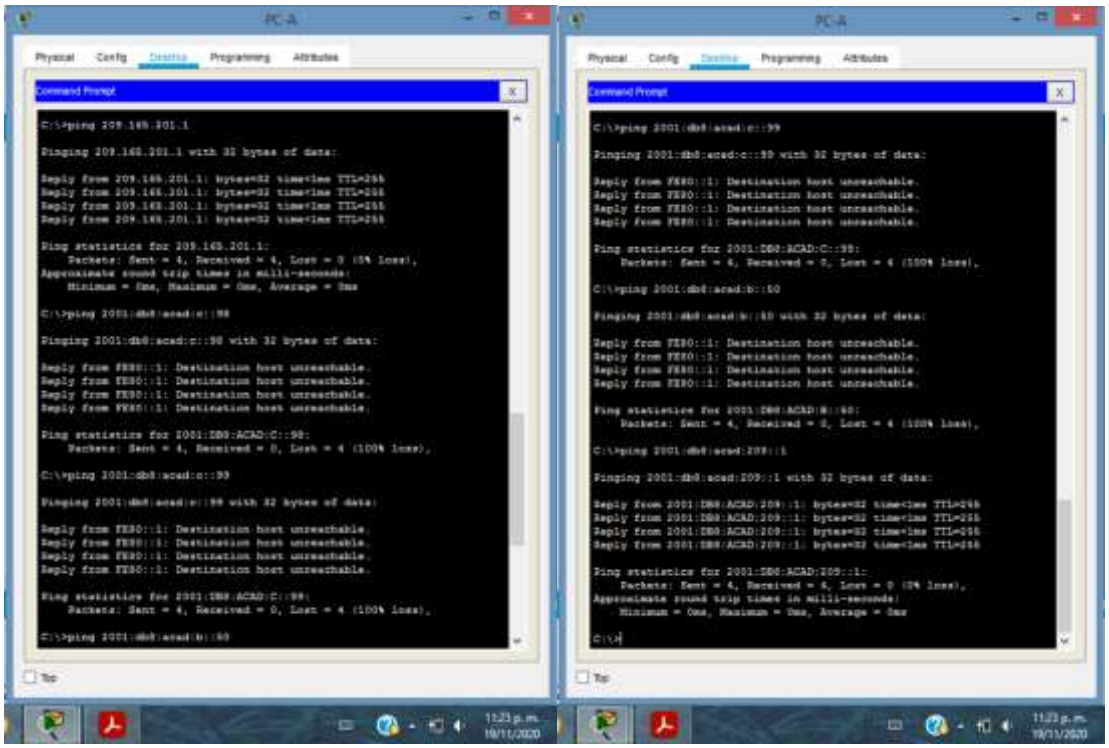
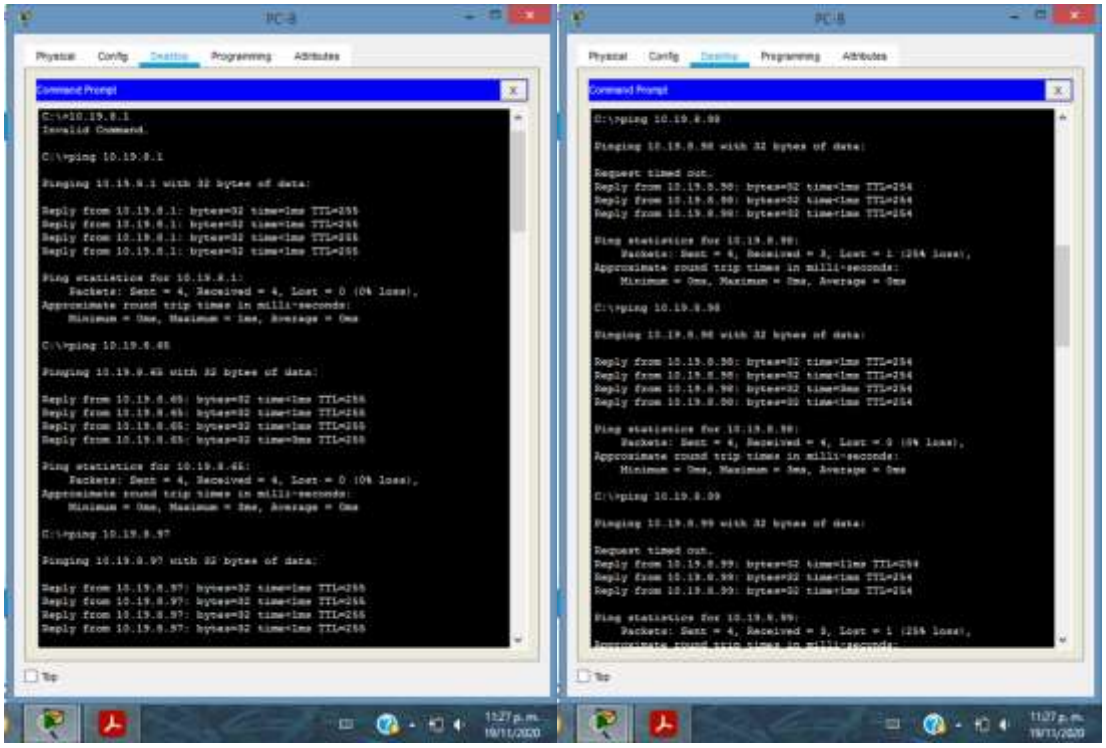


Ilustración 10

PING EN EL PC-B



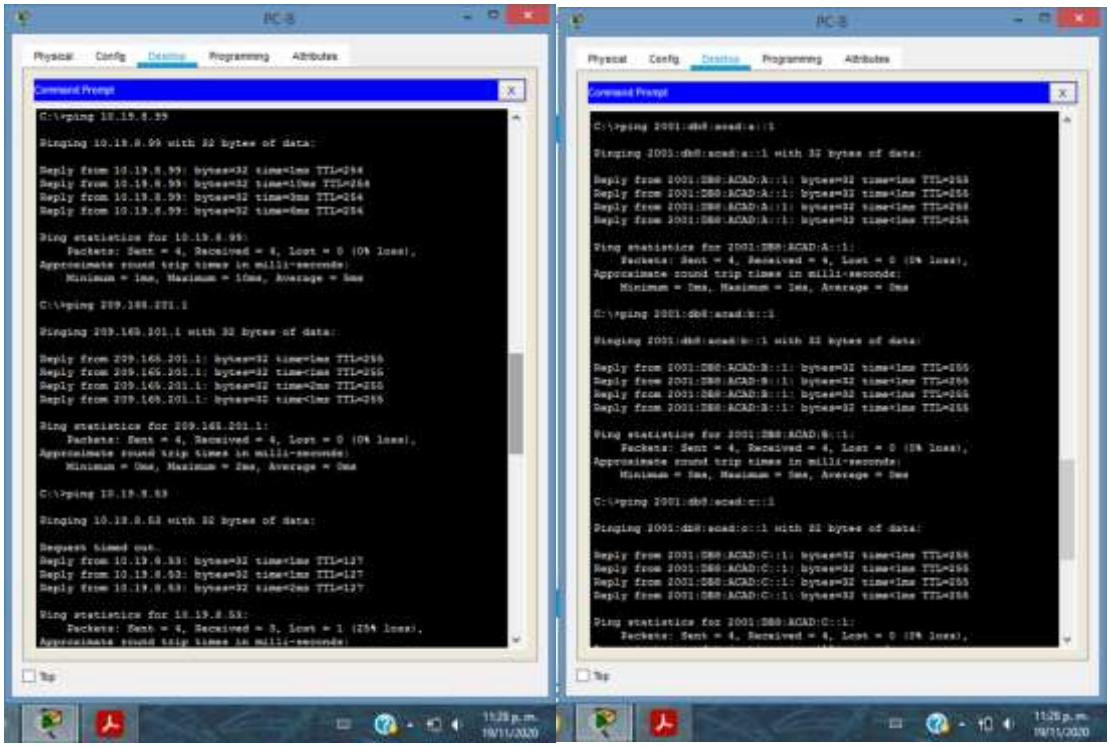


Ilustración 11

Escenario 2

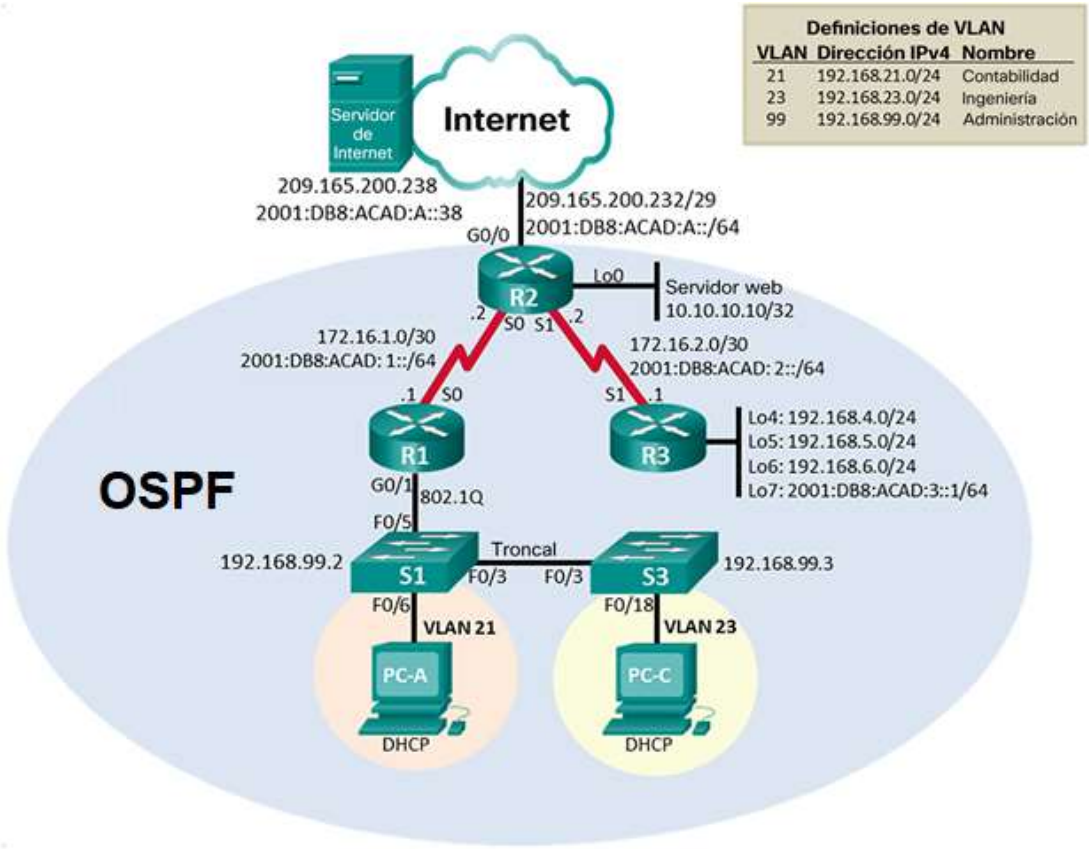


Ilustración 12

Parte 1: Inicializar dispositivos

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

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

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

1.1. Eliminar el archivo startup-config de todos los routers

```
Router>en
Router#erase startup-config
```

1.2. Volver a cargar todos los routers

```
Router#reload
```

1.3. Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

```
Switch>en
Switch#erase startup-config
Switch#delete vlan.dat
```

1.4. Volver a cargar ambos switches

```
Switch#reload
```

1.5. Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

```
Switch#dir flash:
```

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38 /64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1 - Las tareas de configuración para R1 incluyen las siguientes:

2.1. Desactivar la búsqueda DNS

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

2.2. Nombre del router

```
Router(config)#hostname R1
R1(config)#
```

2.3. Contraseña de exec privilegiado cifrada

```
R1(config)#enable secret class
```

2.4. Contraseña de acceso a la consola

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

2.5. Contraseña de acceso Telnet

```
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

2.6. Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
```

2.7. Mensaje MOTD

```
R1(config)#banner motd 'Prohibido el acceso no autorizado'
```

2.8. Configuración de la Interfaz S0/0/0

```
R1(config)# int s0/0/0
R1(config-if)#description R1 --> 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 shutdown
R1(config-if)#exit
```

2.9. Rutas predeterminadas

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)# ipv6 route ::/0 s0/0/0
```

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2 - La configuración del R2 incluye las siguientes tareas:

3.1. Desactivar la búsqueda DNS

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

3.2. Nombre del router

```
Router(config)#hostname R2
R2(config)#
```

3.3. Contraseña de exec privilegiado cifrada

```
R2(config)#enable secret class
```

3.4. Contraseña de acceso a la consola

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

3.5. Contraseña de acceso Telnet

```
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

3.6. Cifrar las contraseñas de texto no cifrado

```
R2(config)#service password-encryption
```

3.7. Mensaje MOTD

```
R2(config)#banner motd 'Prohibido el acceso no autorizado'
```

3.8. Configuración de la Interfaz S0/0/0

```
R2(config)# int s0/0/0
R2(config-if)#description R2 --> 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)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
```

3.9. Configuración de la Interfaz S0/0/1

```
R2(config)# int s0/0/1
R2(config-if)#description R2 --> R3
R2(config-if)#ip address 172.16.2.1 255.255.255.252
```

```
R2(config-if)#ipv6 address 2001:db8:acad:2::1/64
R2(config-if)# clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
```

3.10. Configuración de la Interfaz G0/0

```
R2(config)# int g0/0
R2(config-if)#description R2 --> Internet
R2(config-if)#ip address 209.165.200.232 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:A::1/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

3.11. Configuración de la Interfaz loopback 0

```
R2(config)# int loopback 0
R2(config-if)#description R2 --> Loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
```

3.12. Rutas predeterminadas

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
R2(config)# ipv6 route ::/0 g0/0
```

Paso 4: Configurar R3 - La configuración del R3 incluye las siguientes tareas:

4.1. Desactivar la búsqueda DNS

```
Router>en
Router#conf t
Router(config)#no ip domain-lookup
```

4.2. Nombre del router

```
Router(config)#hostname R3
R3(config)#
```

4.3. Contraseña de exec privilegiado cifrada

```
R3(config)#enable secret class
```

4.4. Contraseña de acceso a la consola

```
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#
```

4.5. Contraseña de acceso Telnet

```
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
```

4.6. Cifrar las contraseñas de texto no cifrado

```
R3(config)#service password-encryption
```

4.7. Mensaje MOTD

```
R3(config)#banner motd ‘Prohibido el acceso no autorizado’
```

4.8. Configuración de la Interfaz S0/0/1

```
R3(config)# int s0/0/1
R3(config-if)#description R3 --> R2
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
```

4.9. Configuración de la Interfaz loopback 4

```
R3(config)# int loopback 4
R3(config-if)#description R3 --> Loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
```

```
R3(config-if)#exit
```

4.10. Configuración de la Interfaz loopback 5

```
R3(config)# int loopback 5
R3(config-if)#description R3 --> Loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
```

4.11. Configuración de la Interfaz loopback 6

```
R3(config)# int loopback 6
R3(config-if)#description R3 --> Loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
```

4.12. Configuración de la Interfaz loopback 7

```
R3(config)# int loopback 7
R3(config-if)#description R3 --> Loopback 7
R3(config-if)# ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#exit
```

4.13. Rutas predeterminadas

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)# ipv6 route ::/0 s0/0/1
```

Paso 5: Configurar S1 - La configuración del S1 incluye las siguientes tareas:

5.1. Desactivar la búsqueda DNS

```
Switch>en
Switch#conf t
Switch(config)#no ip domain-lookup
```

5.2. Nombre del switch

```
Switch(config)#hostname S1
```

```
S1(config)#
```

5.3. Contraseña de exec privilegiado cifrada

```
S1(config)#enable secret class
```

5.4. Contraseña de acceso a la consola

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

5.5. Contraseña de acceso Telnet

```
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
```

5.6. Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
```

5.7. Mensaje MOTD

```
S1(config)#banner motd ‘Prohibido el acceso no autorizado’
S1(config)#
```

Paso 6: Configurar el S3 - La configuración del S3 incluye las siguientes tareas:

6.1. Desactivar la búsqueda DNS

```
Switch>en
Switch#conf t
Switch(config)#no ip domain-lookup
```

6.2. Nombre del switch

```
Switch(config)#hostname S3
S3(config)#
```

6.3. Contraseña de exec privilegiado cifrada

```
S3(config)#enable secret class
```

6.4. Contraseña de acceso a la consola

```
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#
```

6.5. Contraseña de acceso Telnet

```
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
```

6.6. Cifrar las contraseñas de texto no cifrado

```
S3(config)#service password-encryption
```

6.7. Mensaje MOTD

```
S3(config)#banner motd ‘Prohibido el acceso no autorizado’
```

Paso 7: Verificar la conectividad de la red - Utilice el comando ping para probar la conectividad entre los dispositivos de red.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping

R1	R2, S0/0/0	172.16.1.2	`R1#ping 172.16.1.2`
			`Type escape sequence to abort.`
			`Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:`
			`!!!!!`
			`Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms`

R2	R3, S0/0/1	172.16.2.2	`R2#ping 172.16.2.2`
			`Type escape sequence to abort.`
			`Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:`
			`!!!!!`
			`Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms`

PC de Internet	Gateway predeterminado	209.165.200.225	….

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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

Paso 1: Configurar S1 - La configuración del S1 incluye las siguientes tareas:

1.1. Crear la base de datos de VLAN - Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican

```
S1>en
S1#conf t
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)#
```

1.2. Asignar la dirección IP de administración. - Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología

```
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#
```

1.3. Asignar el gateway predeterminado - Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

```
S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#
```

1.4. Forzar el enlace troncal en la interfaz F0/3 - Utilizar la red VLAN 1 como VLAN native

```
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

1.5. Forzar el enlace troncal en la interfaz F0/5 - Utilizar la red VLAN 1 como VLAN native

```
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

1.6. Configurar el resto de los puertos como puertos de acceso - Utilizar el comando interface range

```
S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

1.7. Asignar F0/6 a la VLAN 21

```
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

1.8. Apagar todos los puertos sin usar

```
S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

Paso 2: Configurar el S3 – La configuración del S3 incluye las siguientes tareas:

2.1. Crear la base de datos de VLAN - Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.

```
S3>en
S3#conf t
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#
```

2.2. Asignar la dirección IP de administración. - Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología

```
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#
```

2.3. Asignar el gateway predeterminado - Asignar la primera dirección IP en la subred como gateway predeterminado.

```
S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#
```

2.4. Forzar el enlace troncal en la interfaz F0/3 - Utilizar la red VLAN 1 como VLAN native

```
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
```

2.5. Configurar el resto de los puertos como puertos de acceso - Utilizar el comando interface range

```
S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#switchport mode access
```

2.6. Asignar F0/18 a la VLAN 23

```
S3(config)#int f0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 23
S3(config-if)#exit
```

2.7. Apagar todos los puertos sin usar

```
S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit
```

Paso 3: Configurar R1 - Las tareas de configuración para R1 incluyen las siguientes:

3.1. Configurar la subinterfaz 802.1Q .21 en G0/1 – Descripción: LAN de Contabilidad - Asignar la VLAN 21 - Asignar la primera dirección disponible a esta interfaz.

```
R1>en
R1#conf t
R1(config)#int g0/1.21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
```

3.2. Configurar la subinterfaz 802.1Q .23 en G0/1 - Descripción: LAN de Ingeniería - Asignar la VLAN 23 - Asignar la primera dirección disponible a esta interfaz.

```
R1(config)#int g0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

3.3. Configurar la subinterfaz 802.1Q .99 en G0/1 - Descripción: LAN de Administración - Asignar la VLAN 99 - Asignar la primera dirección disponible a esta interfaz.

```
R1(config)#int g0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
```

3.4. Activar la interfaz G0/1

```
R1(config)#int g0/1
R1(config-if)#no shutdown
```

Paso 4: Verificar la conectividad de la red
Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

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# 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 = 0/0/2 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 = 0/0/1 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

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1 - Las tareas de configuración para R1 incluyen las siguientes:

1.1. Configurar OSPF área 0

```
R1>en
R1#conf t
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#
```

1.2. Anunciar las redes conectadas directamente - Asigne todas las redes conectadas directamente.

```
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)#
```

1.3. Establecer todas las interfaces LAN como pasivas

```
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#exit
```

1.4. Desactive la sumarización automática

```
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#exit
```

Paso 2: Configurar OSPF en el R2 - La configuración del R2 incluye las siguientes tareas:

2.1. Configurar OSPF área 0

```
R2>en
R2#conf t
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#
```

2.2. Anunciar las redes conectadas directamente - Nota: Omitir la red G0/0.

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#
```

2.3. Establecer la interfaz LAN (loopback) como pasiva

```
R2(config-router)#passive-interface g0/1
R2(config-router)#exit
```

2.4. Desactive la sumarización automática

```
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#exit
```

Paso 3: Configurar OSPFv3 en el R2 - La configuración del R3 incluye las siguientes tareas:

3.1. Configurar OSPF área 0

```
R3>en
R3#conf t
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#
```

3.2. Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#
```

3.3. Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

```
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#passive-interface loopback 7
R3(config-router)#exit
```

3.4. Desactive la sumarización automática

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

Paso 4: Verificar la información de OSPF - Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Pregunta	Respuesta
¿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 ip protocols**
¿Qué comando muestra solo las rutas OSPF?	**show ip route ospf**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	**show running-config**

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 - Las tareas de configuración para R1 incluyen las siguientes:

1.1. Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.

```
R1>en
R1#conf t
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#
```

1.2. Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas.

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

1.3. Crear un pool de DHCP para la VLAN 21. - Nombre: ACCT - Servidor DNS: 10.10.10.10 - Nombre de dominio: ccna-sa.com - Establecer el gateway predeterminado.

```
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)#exit
```

1.4. Crear un pool de DHCP para la VLAN 23 - Nombre: ENGNR - Servidor DNS: 10.10.10.10 - Nombre de dominio: ccna-sa.com - Establecer el gateway predeterminado.

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#exit
```

Paso 2: Configurar la NAT estática y dinámica en el R2 - La configuración del R2 incluye las siguientes tareas:

2.1. Crear una base de datos local con una cuenta de usuario - Nombre de usuario: webuser - Contraseña: cisco12345 - Nivel de privilegio: 15.

```
R1(config)#user webuser privilege 15 secret cisco12345
```

2.2. Habilitar el servicio del servidor HTTP

```
R1(config)# ip http server
```

2.3. Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

```
R1(config)# ip http authentication local
```

2.4. Crear una NAT estática al servidor web. - Dirección global interna: 209.165.200.229

```
R1(config)#ip nat inside source static 10.10.10.1 209.165.200.229
```

2.5. Asignar la interfaz interna y externa para la NAT estática

```
R1(config)#int g0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#int g0/1
R1(config-if)#ip nat inside
R1(config-if)#exit
```

2.6. Configurar la NAT dinámica dentro de una ACL privada - Lista de acceso: 1 - Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 - Permitir la traducción de un resumen de las redes LAN (loopback) en el R3

```
R1(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R1(config)#
```

2.7. Defina el pool de direcciones IP públicas utilizables. - Nombre del conjunto: INTERNET - El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228.

```
R1(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248
```

2.8. Definir la traducción de NAT dinámica

```
R1(config)#ip nat inside source list 1 pool INTERNET
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Parte 6: Configurar NTP

6.1. Ajuste la fecha y hora en R2. - 5 de marzo de 2016, 9 a. m.

```
R2(config)#exit
R1#clock set 09:00:00 5 March 2016
```

6.2. Configure R2 como un maestro NTP. - Nivel de estrato: 5

```
R2(config)#ntp master 5
```

6.3. Configurar R1 como un cliente NTP. - Servidor: R2

```
R1(config)# ntp server 172.16.1.1
```

6.4. Configure R1 para actualizaciones de calendario periódicas con hora NTP.

```
R1(config)# ntp update-calendar
```

6.5. Verifique la configuración de NTP en R1.

```
R1# show ntp associations
```

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

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

1.1. Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 - Nombre de la ACL: ADMIN-MGT

```
R1#conf t
R1(config)#ip access-list standard ADMIN-MGT
R1(config)#host 172.16.1.1
172.16.1.1(config)#
```

1.2. Aplicar la ACL con nombre a las líneas VTY

```
172.16.1.1(config)#line vty 0 4
172.16.1.1(config-line)#access-class ADMIN-MGT in
172.16.1.1(config-line)#exit
```

1.3. Verificar que la ACL funcione como se espera

```
172.16.1.1(config)#exit
172.16.1.1#telnet 172.16.2.2
172.16.1.1#telnet 172.16.2.1
172.16.1.1#
```

Paso 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-lists
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 running-config

¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

PRUEBA

R1 - Show running-config

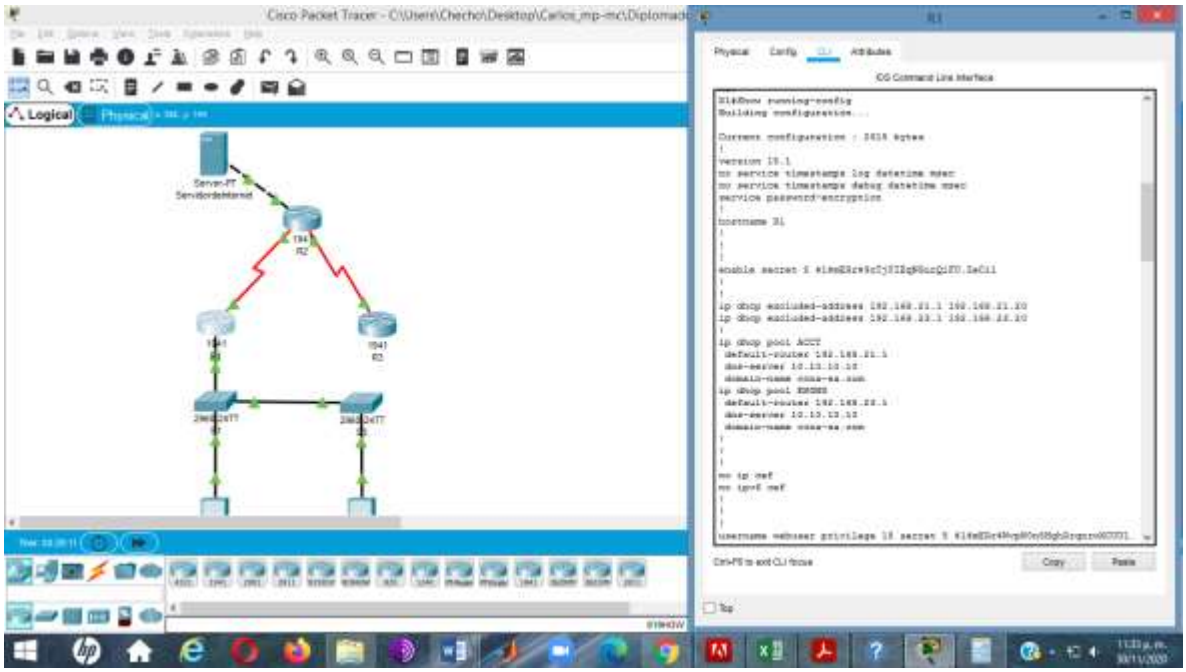
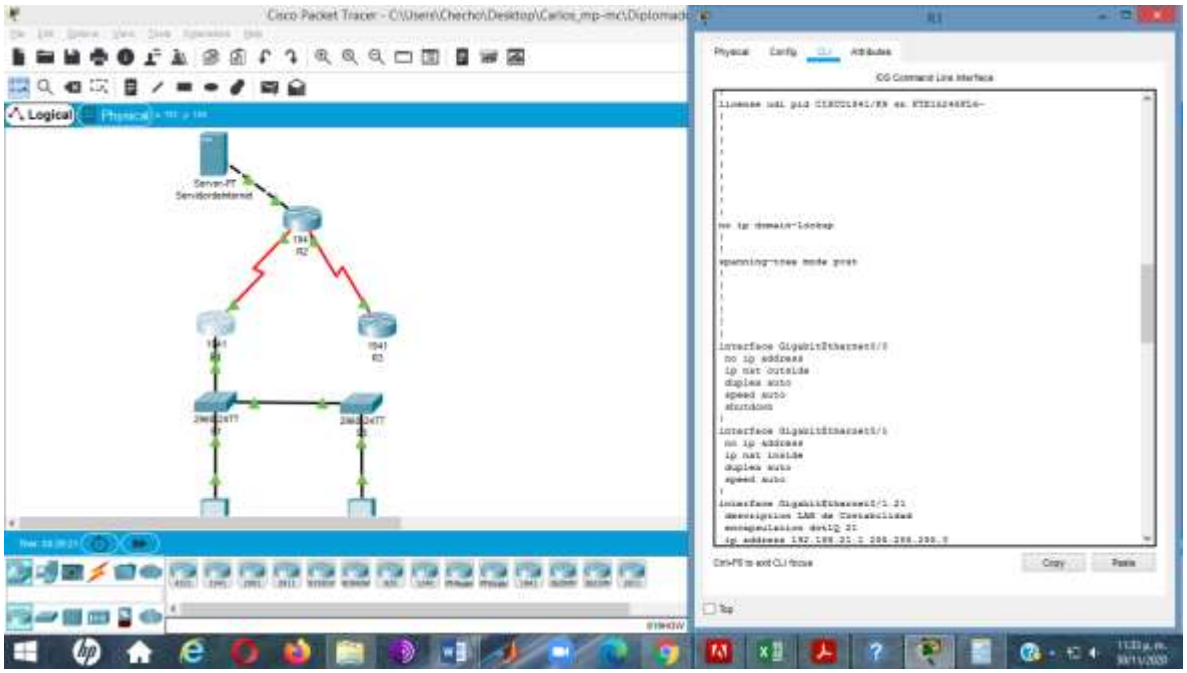


Ilustración 13



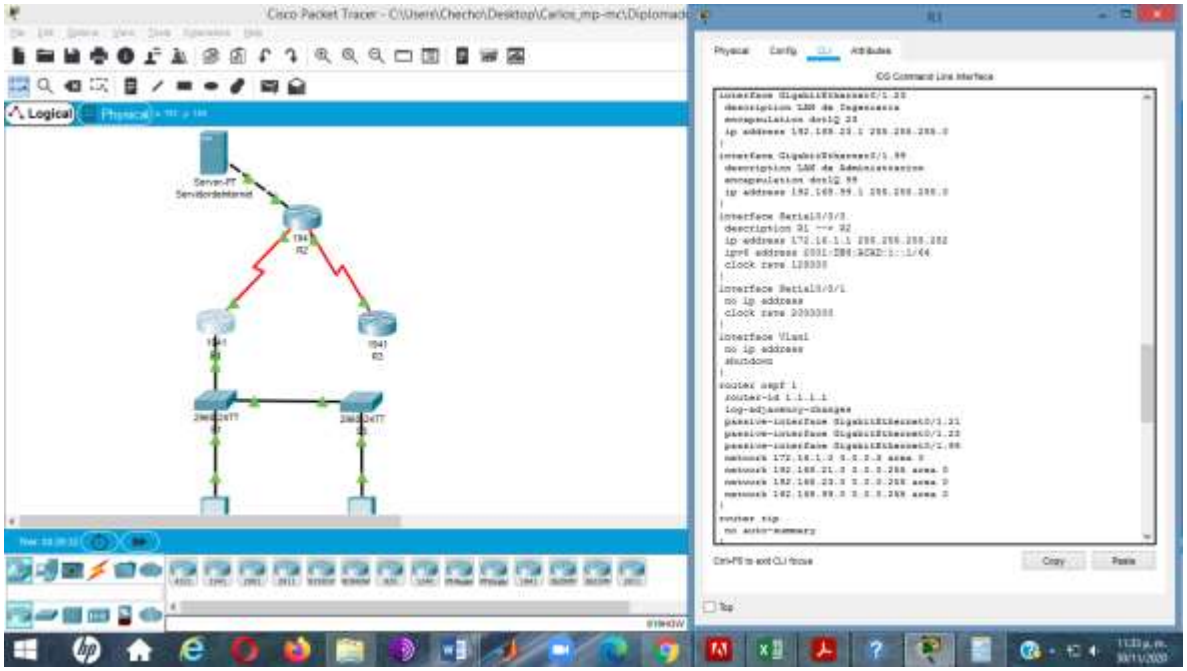
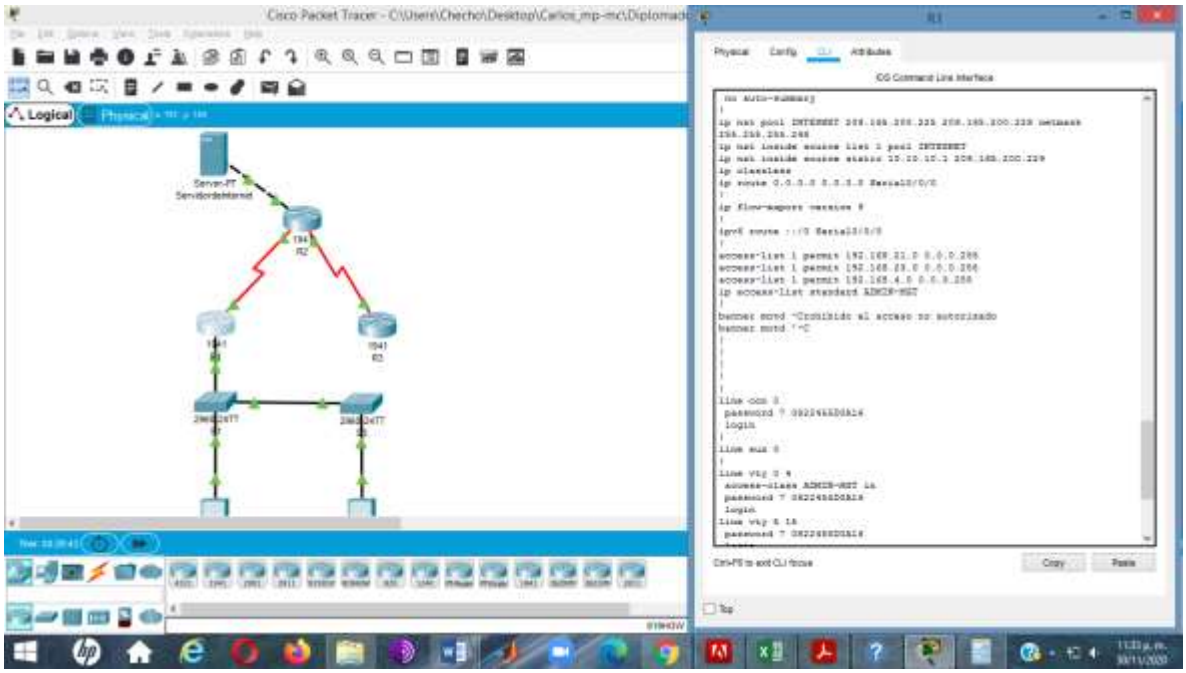


Ilustración 14



R2 - Show running-config

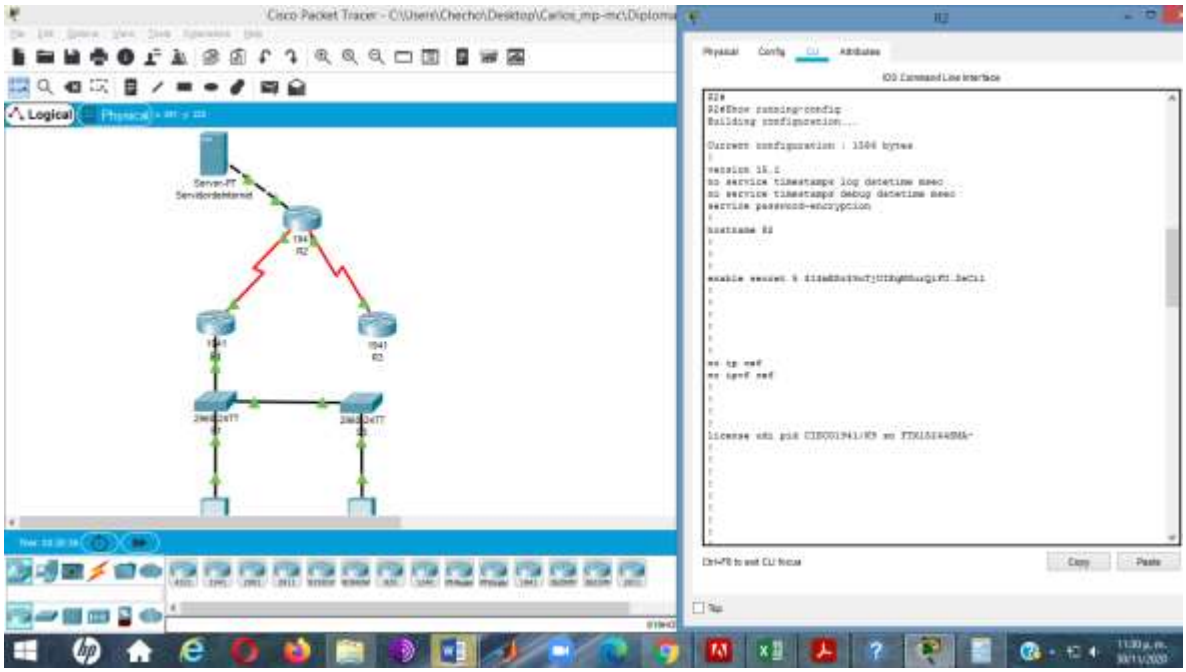
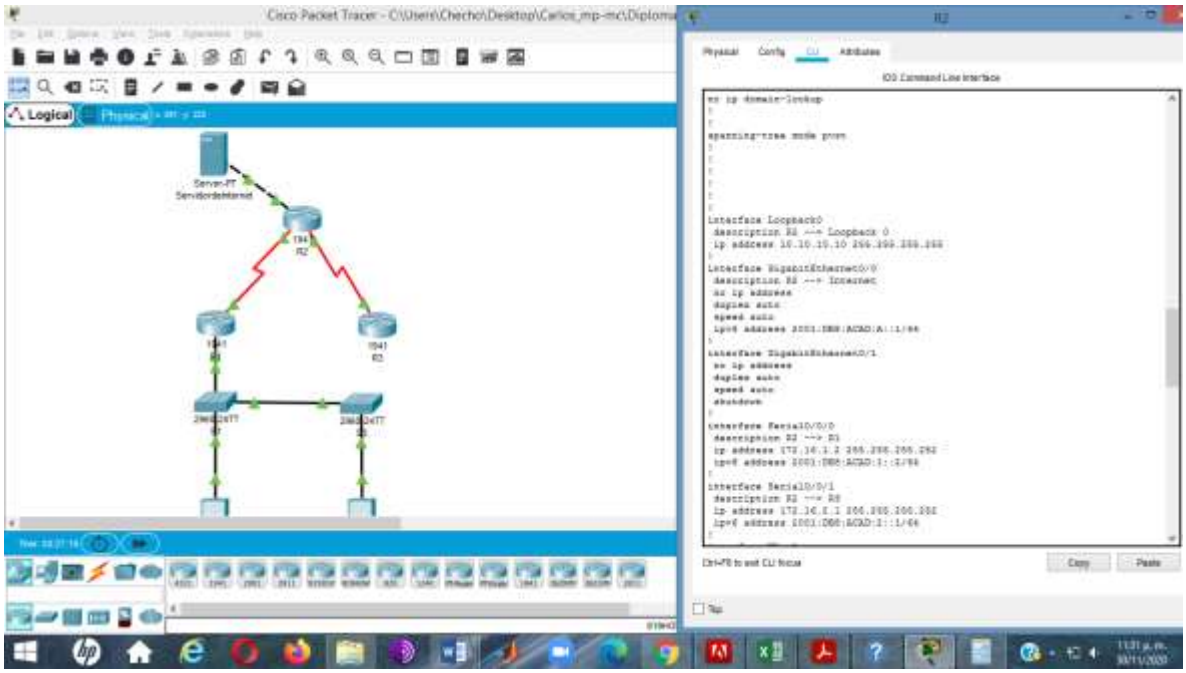


Ilustración 15



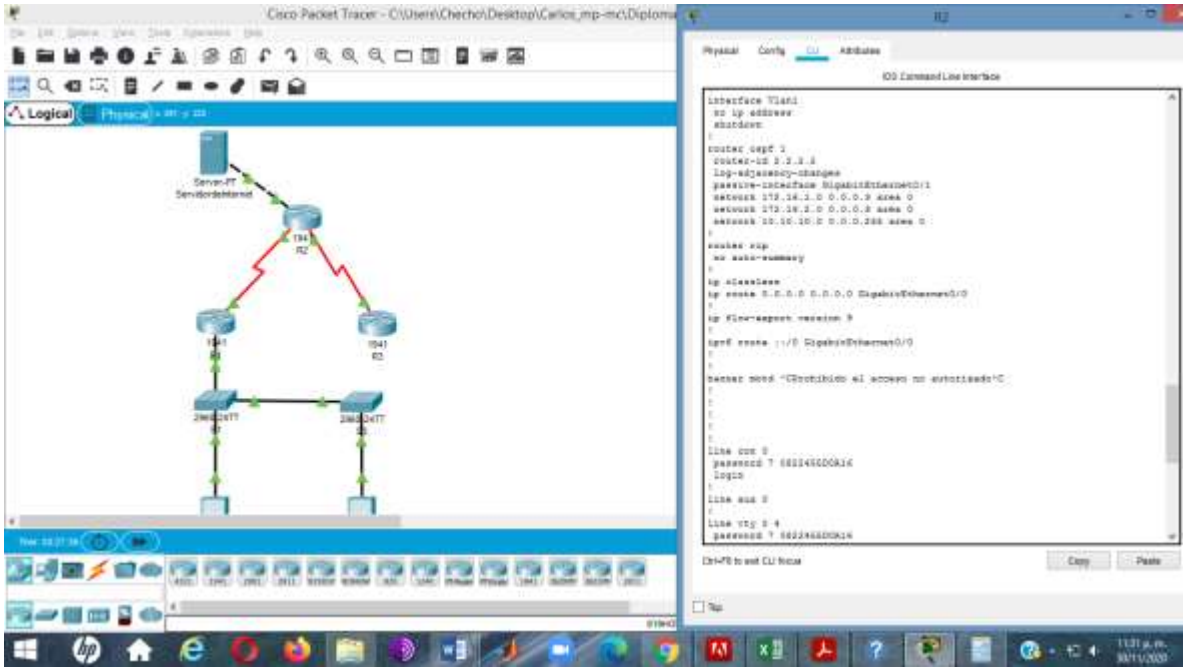
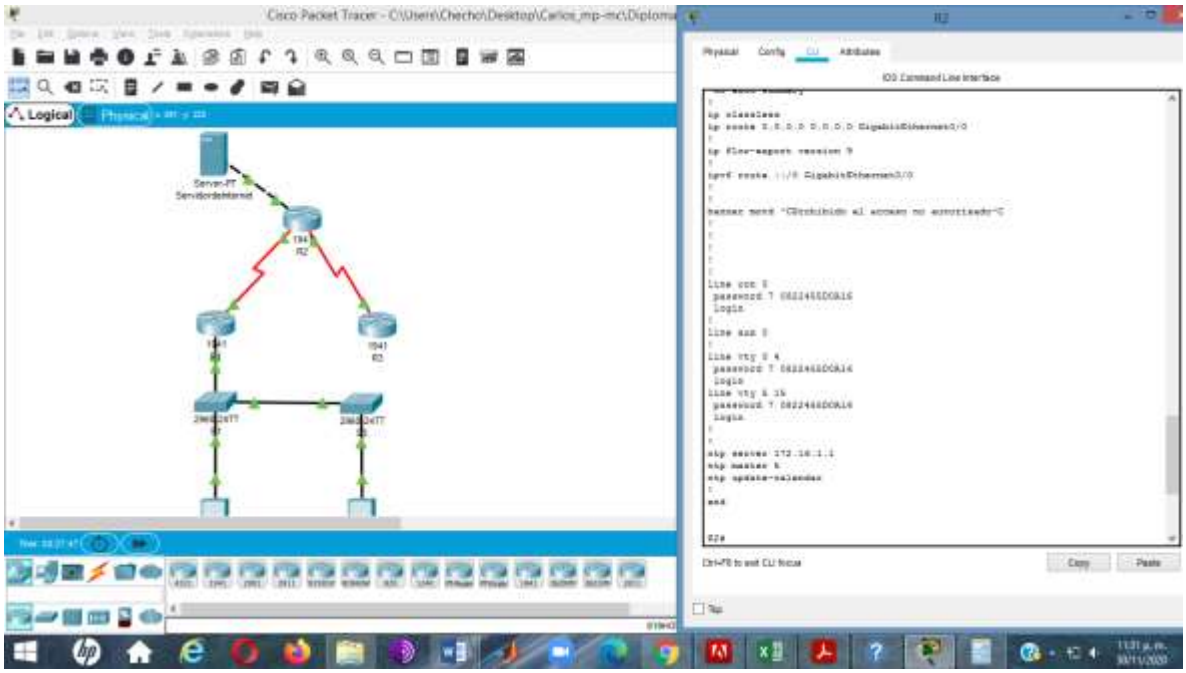
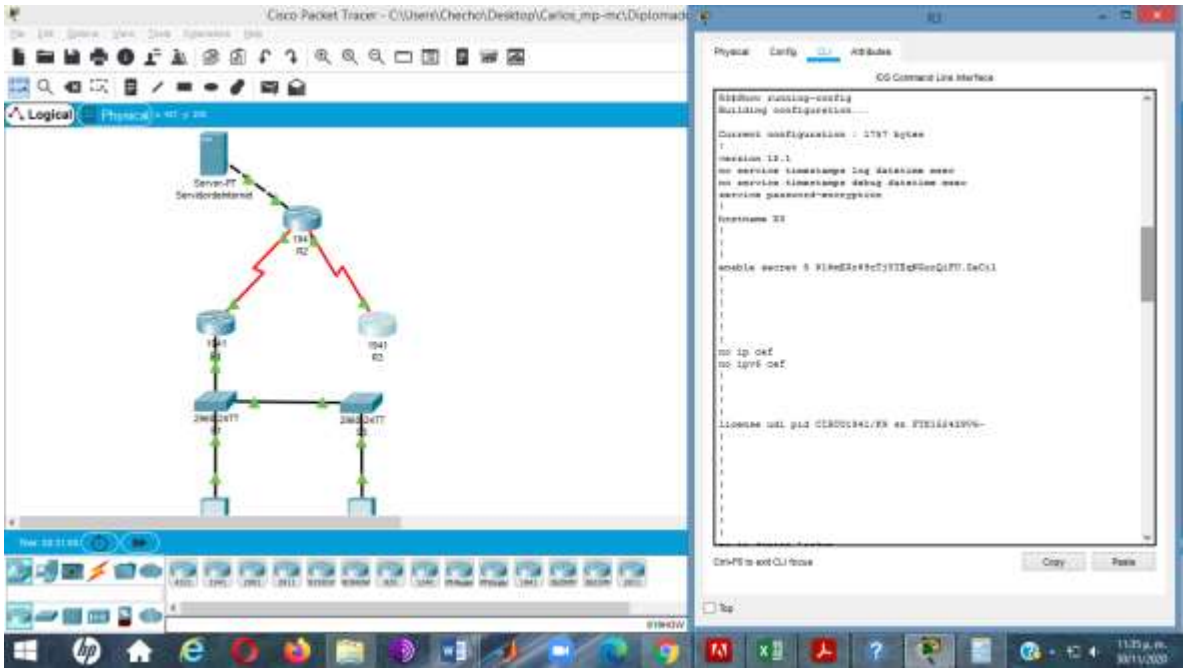
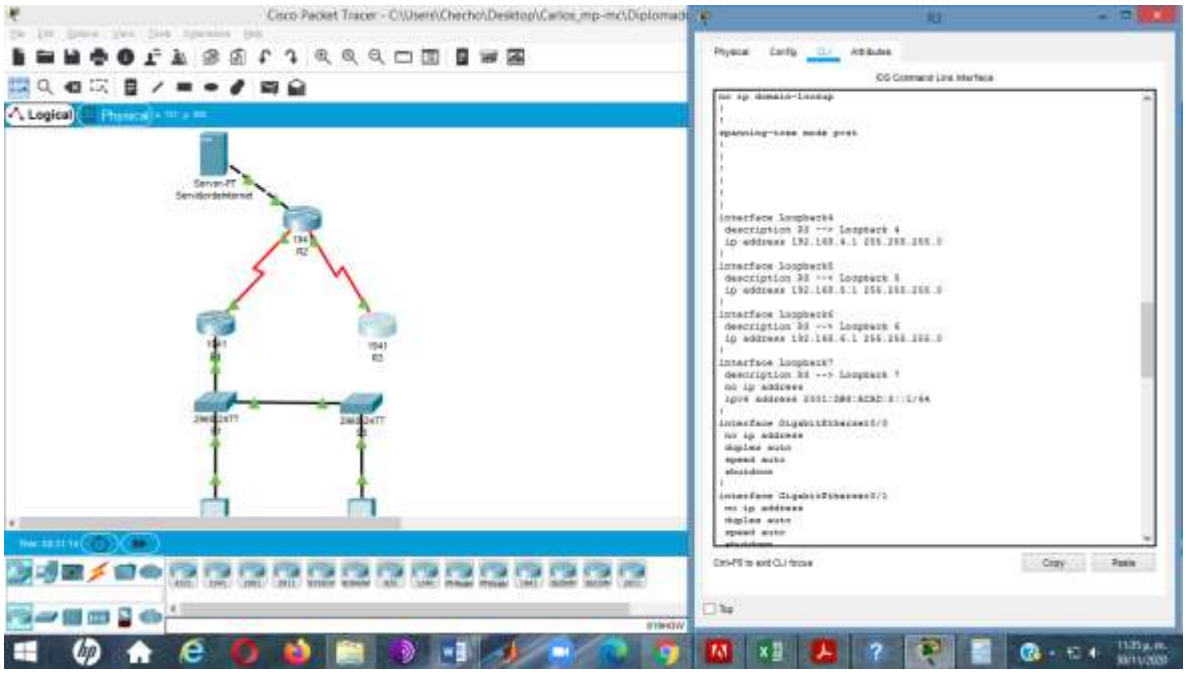


Ilustración 16



R3 - Show running-config





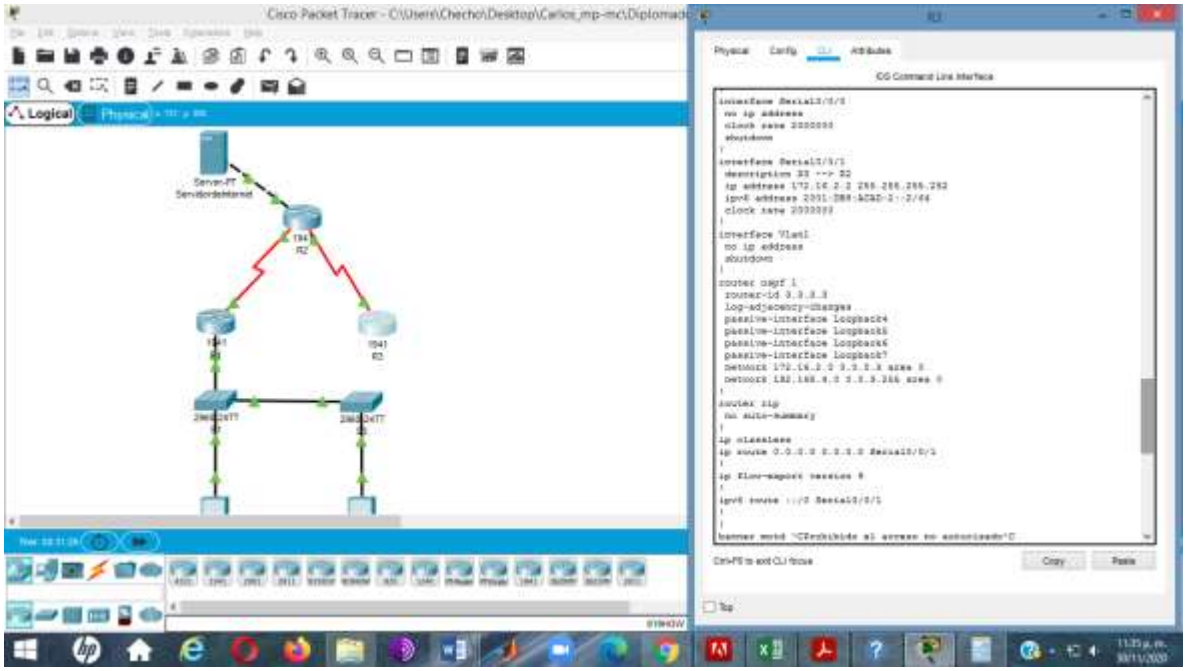


Ilustración 17

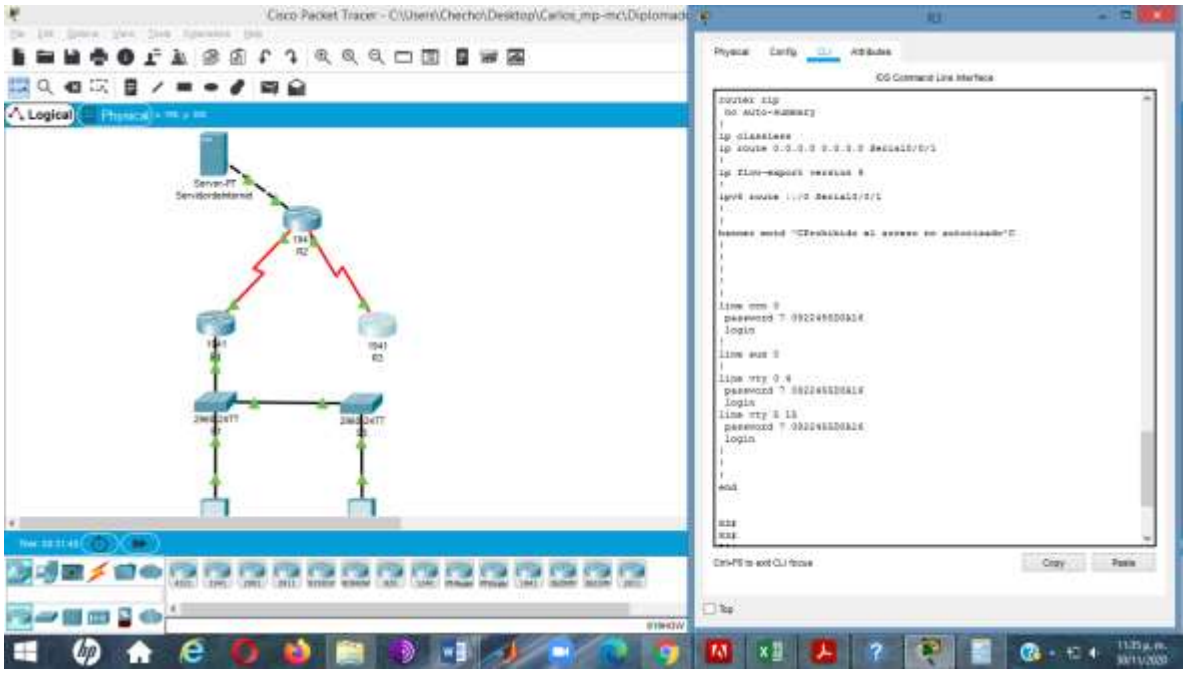


Ilustración 18

CONCLUSIONES

- ✓ Este trabajo tiene como objetivos obtener la capacidad intelectual y el conocimiento para realizar los ejercicios a desarrollar durante la actividad buscando alternativas funcionales y propias en el desarrollo de la actividad como base para el desempeño de nuestra Carrera profesional y laboral con el fin de mostrar resultados positivos a través de la guías y las unidades tratadas en el curso.

- ✓ Mediante la aplicación y enrutamiento de programas a través de comandos, podemos conectar dispositivos aleatoriamente con un funcionamiento eficaz y controlado obteniendo resultados que permitan avanzar en el desarrollo de ejercicios y trabajos que a diario son frecuentes en nuestra Carrera, para así, de esta manera estar preparado para los nuevos avances que día a día se presentan con el cambio de tecnología

REFERENCIAS BIBLIOGRÁFICAS

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

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

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

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

ANEXOS

Anexo 1. Link de descarga Escenario 1.

https://drive.google.com/file/d/1AWjWmqUFDLclwr5bJia36jHZTDCxtvtK/view?usp=sharing

Anexo 2. Link de descarga Escenario 2.

https://drive.google.com/file/d/1a62TcYFb2LJlEyxi96IIekqkBSJqRCKB/view?usp=sharing

Anexo 3. Pantallazos 3

https://docs.google.com/document/d/1U-xBpFtq0xQrMNq5sm_1yERQOW4E1RjU/edit