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

MIGUEL ANGEL GÓMEZ DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

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

MIGUEL ANGEL GÓMEZ DIAZ

DIPLOMADO DE PROFUNDIZACIÓN CISCO DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WLAN

TUTOR
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
Bogotá octubre de 2020

CONTENIDO

Lista de imágenes

Lista de tablas

INTRODUCCIÓN

El presente trabajo muestra el paso a paso de la solución de dos estudios de caso bajo el uso de tecnología Cisco donde se evidencia lo aprendido en el curso 203092_11 diplomado de profundización cisco diseño e implementación de soluciones integradas LAN / WAN.

Como primer paso se utilizara el simulador de redes Packet Tracert el cual permite identificar diferentes formas de configuración de algunos dispositivos de red como routers, switches, servidores, etc mediante el uso de comandos en la interfaz de línea de comandos (CLI), para ambos escenarios se configura la red y se crearan VLAN, las cuales aíslan diferentes redes evitando problemas de seguridad, la conexión de estas diferentes redes se logra con la presencia de un router en cual realiza el enrutamiento entre la VLAN.

Igualmente se trabajaran comandos de configuración básica y de seguridad de router y switchs, servidores abordando temáticas de DHCP, EtherChannel y port-security, OSPF, NAT, ACL Y NTP.

OBJETIVOS

GENERAL

Demostrar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado de profundización cisco diseño e implementación de soluciones integradas LAN / WLAN de la universidad nacional Abierta y a Distancia, mediante la solución de dos problemas relacionados con aspectos de Networking acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

ESPECIFICOS

Configurar y administrar de forma segura dispositivos de una red pequeña router, switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados.

Configurar el enrutamiento entre VLAN, DHCP, EtherChannel y port-security para una red pequeña.

Configurar protocolo Open Shortest Path First (OSPF) en los routers de una red pequeña.

Configurar la traducción de direcciones de red a través Network Address Translation (NAT).

Configurar listas de control de acceso (ACL) en el router de una red pequeña.

Configurar la fecha y hora a través del protocolo de tiempo de red (NTP).

Verificar la conectividad de una red mediante el uso de comandos ping, traceroute y show ip route.

CASO DE ESTUDIO 1

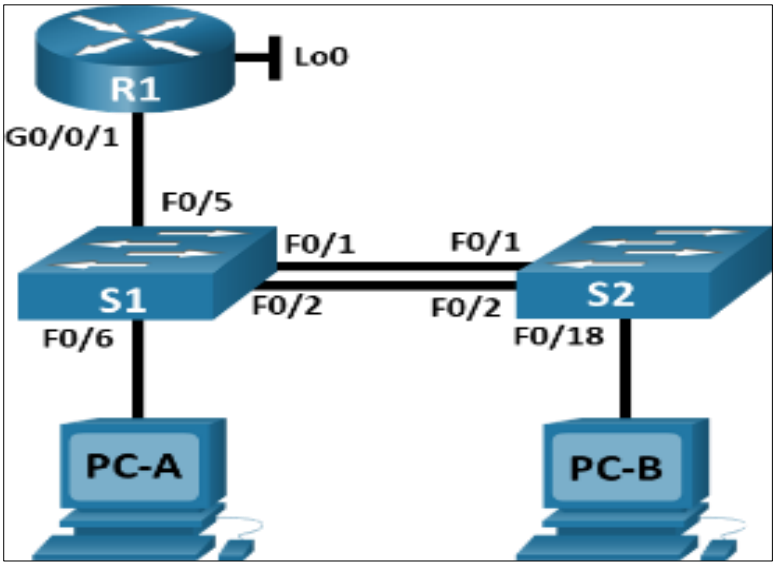


Imagen 1. Topología red caso de estudio 1.

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

Tabla 1. VLAN a crear para el caso de estudio 1.

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
	209.165.201.1 /27	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. Asignación de direcciones para el caso de estudio 1.

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

Parte 1: Inicializar y recargar y configurar aspectos básicos de los dispositivos

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

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

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Imagen 2. Borrado de la NVRAM del switch

```
Switch#delete vlan.data
Delete filename [vlan.data]?y
Delete flash:/y? [confirm]y%Error deleting flash:/y (No such file or
directory)
```

Imagen 3. Borrado VLAN del switch

```
Switch#reload
Proceed with reload? [confirm]yC3560 Boot Loader (C3560-HBOOT-M)
Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
3560-24PS starting...
Base ethernet MAC Address: 00D0.58EB.AB2B
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 3 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 8918011
flashfs[0]: Bytes available: 55098373
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c3560-advipservicesk9-mz.122-37.SE1.bin"...
################################################
```

Imagen 4. Cargue del switch

```
Router#delete vlan.data
Delete filename [vlan.data]?
Delete flash:/vlan.data? [confirm]
%Error deleting flash:/vlan.data (No such file or directory)

Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
Router#reload
Proceed with reload? [confirm]yInitializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly


System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018  by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory
```

Imagen 5. Borrado parámetros iniciales y cargue del router

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

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
Changes to the running SDM preferences have been stored, but cannot
take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

Imagen 6. Configuración Plantilla SDM IPV6 para el router

Paso 2: Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	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 con 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 privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)# line vty 0 4 R1(config-line)# login local
Configurar VTY solo aceptando SSH	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 #ACCESO NO AUTORIZADO#
Habilitar el routing IPv6	R1(config)# ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config)# interface g0/0/1 R1(config-if)# description conexión a S1 R1(config-if)# ipv6 address fe80::1 link-local R1(config-if)# no shutdown R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 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-if)# ipv6 address fe80::1 link-local R1(config)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 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-if)# ipv6 address fe80::1 link-local R1(config-subif)# interface g0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 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-if)# ipv6 address fe80::1 link-local R1(config-subif)# interface g0/0/1.6 R1(config-subif)#encapsulation dot1Q 6
Configure el Loopback0 interface	R1(config)# interface loopback 0 R1(config-if)# description interface loopback 0 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)# no shutdown R1(config-if)# exit R1(config)# ipv6 unicast-routing
Generar una clave de cifrado RSA	R1(config)# crypto key generate rsa general-key modulus 1024

Tabla 3. Configuración inicial router R1

```
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin privilege 15  secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #ACCESO NO AUTORIZADO#
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0/1
R1(config-if)#description conexin a S1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-subif)#exit
R1(config)#interface g0/0/1.3
R1(config-subif)#encapsulation dot1Q 3
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)#interface g0/0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#ip address 10.19.8.97  255.255.255.248
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#exit
R1(config)#interface g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#exit
R1(config)#interface loopback 0
R1(config-if)#description interface loopback 0
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)#no shutdown
R1(config-if)#exit
R1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:1:1.669: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
```

Imagen 7. Configuración inicial Router R1

Paso 3: configuración S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch #configure terminal Switch(config)# no ip domain-lookup
Nombre del switch	Switch (config)# hostname S1 Switch (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 con 0 S1(config-line)# password ciscoconpass S1(config-line)# login S2(config)# line con 0 4 S2(config-line)# password ciscoconpass S2(config-line)# login
Crear un usuario administrativo en la base de datos local	S1(config)# username admin privilege 15 secret admin1pass S2(config)# username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)# line vty 0 4 S1(config-line)# login local S2(config)# line vty 0 4 S2(config-line)# login local
Configurar las líneas VTY para que acepten únicamente conexiones SSH	S1(config-line)#trnsport input ssh S2(config-line)#trnsport 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 #ACCESO NO AUTORIZADO# S2(config)# banner motd #ACCESO NO AUTORIZADO#
Generar una clave de cifrado RSA	S1(config)# crypto key generate rsa general-key modulus 1024 S2(config)# crypto key generate rsa general-key modulus 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface 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 S1(config)#ipv6 unicast-routing S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.98 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 address fe80::98 link-local S2(config-if)#no shutdown S2(config-if)#exit S2(config)#ipv6 unicast-routing
Configuración del gateway predeterminado	S1(config)# ip default-gateway 10.19.8.97 S2(config)# ip default-gateway 10.19.8.97

Tabla 4. Configuración inicial switches S1 y S2

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line con 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15  secret adminlpass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #ACCESO NO AUTORIZADO#
S1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:0:24.83: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#interface 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
S1(config)#ipv6 unicast-routing
S1(config)#ip default-gateway 10.19.8.97
```

Imagen 8. Configuración inicial switch S1

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line con 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin privilege 15  secret adminlpass
S2(config)#line vty 0 4
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #ACCESO NO AUTORIZADO#
S2(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S2.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:1:42.488: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#interface 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
S2(config)#ipv6 unicast-routing
S2(config)#ip default-gateway 10.19.8.97
```

Imagen 9. Configuración inicial switch S2

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

Paso 1: **Configurar S1**

Tarea	Especificación
Crear VLAN	S1(config)# vlan 4 S1(config-vlan)# name management S1(config)# vlan 2 S1(config-vlan)# name Bikes S1(config-vlan)# vlan 3 S1(config-vlan)# name Trikes S1(config-vlan)# vlan 5 S1(config-vlan)# name Parking S1(config-vlan)# vlan 6 S1(config-vlan)# name Native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)# interface f0/01 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)# interface f0/02 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)# interface f0/05 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
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range f0/1 – 2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#exit S1(config)#interface port-channel 1 S1(config-if)#switchport mode trunk
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface f0/6 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)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 S1(config-if)#switchport port-security violation shutdown S1(config-if)#switchport port-security mac-address sticky
Proteja todas las interfaces no utilizadas	S1(config)#interface range f0/3-4, f0/7-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description asegurar interfaces no utilizadas S1(config-if-range)#shutdown S1(config-if-range) #switchport port-security S1(config-if-range)#switchport port-security maximum 1 S1(config-if-range)#switchport port-security violation shutdown

Tabla 5. *Configuración de la infraestructura de red de S1*

Crear VLAN 2 nombre Bikes, VLAN 3 nombre Trikes, VLAN 4 name Management, VLAN 5 nombre Parking, VLAN 6 nombre Native

```
S1#show vlan brief

VLAN  Name                                      Status
----  ----------------------------------------  --------
--------------------------------
1     default                                   active
Fa0/8

Fa0/11, Fa0/12

Fa0/15, Fa0/16

Fa0/19, Fa0/20

Fa0/23, Fa0/24

2     Bikes                                     active
3     Trikes                                    active
4     management                                active
5     Parking                                   active
6     Native                                    active
```

Imagen 10. Configuración VLAN en S1

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

```
S1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
S1#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
S1#show interface f0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
```

Imagen 11. Configuración troncales 802.1Q con VLAN 6 nativa en S1

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#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+----------------------------------------

1      Po1(SU)         LACP      Fa0/1(P)  Fa0/2(P)
```

Imagen 12. Configuración EtherChannel de Capa 2 S1

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

```
2    Bikes                                active    Fa0/6
3    Trikes                               active
4    management                           active
5    Parking                              active
6    Native                               active
```

Imagen 13. Configuración puerto de acceso a host para VLAN 2 S1

Configurar la seguridad del puerto en los puertos de acceso, permitir 3 direcciones MAC

```
S1#show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.B0E9.14B8:2
Security Violation Count   : 0
```

Imagen 14. Configuración port-security en S1

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

```
S1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
          Fa0/3           1            0                  0         Shutdown
          Fa0/4           1            0                  0         Shutdown
          Fa0/6           3            1                  0         Shutdown
          Fa0/7           1            0                  0         Shutdown
          Fa0/8           1            0                  0         Shutdown
          Fa0/9           1            0                  0         Shutdown
         Fa0/10           1            0                  0         Shutdown
         Fa0/11           1            0                  0         Shutdown
         Fa0/12           1            0                  0         Shutdown
         Fa0/13           1            0                  0         Shutdown
         Fa0/14           1            0                  0         Shutdown
         Fa0/15           1            0                  0         Shutdown
         Fa0/16           1            0                  0         Shutdown
         Fa0/17           1            0                  0         Shutdown
         Fa0/18           1            0                  0         Shutdown
         Fa0/19           1            0                  0         Shutdown
         Fa0/20           1            0                  0         Shutdown
         Fa0/21           1            0                  0         Shutdown
         Fa0/22           1            0                  0         Shutdown
         Fa0/23           1            0                  0         Shutdown
         Fa0/24           1            0                  0         Shutdown
         Gig0/1           1            0                  0         Shutdown
         Gig0/2           1            0                  0         Shutdown
```

Imagen 15. Configuración interfaces no utilizadas en S1

Paso 5: configurar S2

Tarea	Especificación
Crear VLAN	S2(config)# vlan 4 S2(config-vlan)# name management S2(config)# vlan 2 S2(config-vlan)# name Bikes S2(config-vlan)# vlan 3 S2(config-vlan)# name Trikes S2(config-vlan)# vlan 5 S2(config-vlan)# name Parking S2(config-vlan)# vlan 6 S2(config-vlan)# name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)# interface f0/01 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)# interface f0/02 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
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface range f0/1 – 2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#exit S2(config)#interface port-channel 1 S2(config-if)#switchport mode trunk

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config)#interface f0/18 S2(config-if)#switchport mode Access S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#switchport port-security violation shutdown S2(config-if)#switchport port-security mac-address sticky
Asegure todas las interfaces no utilizadas.	S2(config)#interface range f0/3-4, f0/7-24, g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description asegurar interfaces no utilizadas S2(config-if-range)#shutdown S2(config-if-range) #switchport port-security S2(config-if-range)#switchport port-security maximum 1 S2(config-if-range)#switchport port-security violation shutdown

Tabla 6. *Configuración de la infraestructura de red de S2*

Crear VLAN 2 nombre Bikes, VLAN 3 nombre Trikes, VLAN 4 name Management, VLAN 5 nombre Parking, VLAN 6 nombre Native

```
S2#show vlan brief

VLAN Name                                      Status
---- --------------------------------- ---------
--------------------------------
1    default                                   active
Fa0/6

Fa0/10

Fa0/13, Fa0/14

Fa0/17, Fa0/19

Fa0/22, Fa0/23

Gig0/2
2    Bikes                                     active
3    Trikes                                    active
4    management                                active
5    Parking                                   active
6    Native                                    active
```

Imagen 16. Configuración VLAN en S2

Crear troncos 802.1Q que utilicen la VLAN 6 nativa, interfaces F0/1 y F0/2

```
S2#show interfaces f0/01 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)

S2#show interfaces f0/02 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
```

Imagen 17. Configuración troncales 802.1Q con VLAN 6 nativa en S2

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#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+----------------------------------------------

1      Po1(SU)         LACP      Fa0/1(P)  Fa0/2(P)
```

Imagen 18. Configuración EtherChannel de Capa 2 en S2

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

```
S2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5,
Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 Fa0/11, Fa0/12,
Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16,
Fa0/17, Fa0/19
                                                 Fa0/20, Fa0/21,
Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1,
Gig0/2
2    Bikes                             active
3    Trikes                            active    Fa0/18
4    management                        active
5    Parking                           active
6    Native                            active
```

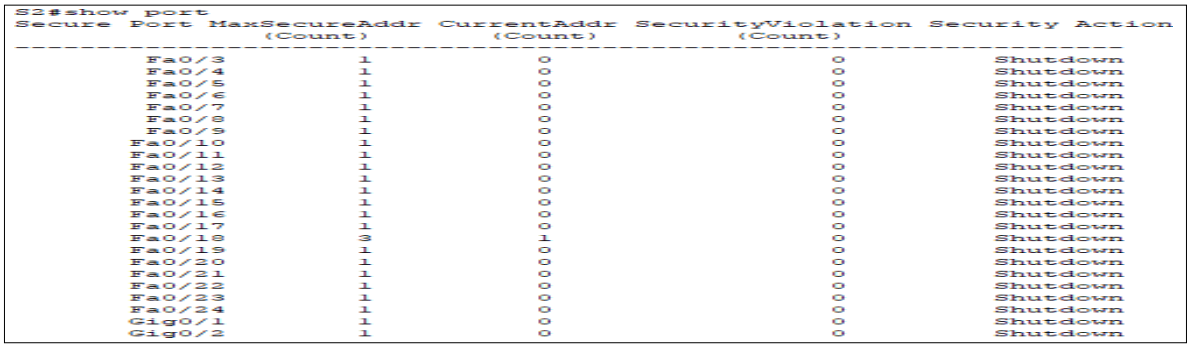
Imagen 19. Configuración puerto de acceso a host para VLAN 2 en S2

Configure port-security en los access ports, permitir 3 direcciones MAC

```
S2#show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00D0.BCD5.32C1:3
Security Violation Count   : 0
```

Imagen 20. Configuración port-security en S2

Asegure todas las interfaces no utilizadas, asignar a VLAN 5, establecer en modo de acceso, agregar una descripción y apagar



```
S2#show port
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)        (Count)
-----------------------------------------------------------------------------
          Fa0/3          1            0                  0         Shutdown
          Fa0/4          1            0                  0         Shutdown
          Fa0/5          1            0                  0         Shutdown
          Fa0/6          1            0                  0         Shutdown
          Fa0/7          1            0                  0         Shutdown
          Fa0/8          1            0                  0         Shutdown
          Fa0/9          1            0                  0         Shutdown
         Fa0/10          1            0                  0         Shutdown
         Fa0/11          1            0                  0         Shutdown
         Fa0/12          1            0                  0         Shutdown
         Fa0/13          1            0                  0         Shutdown
         Fa0/14          1            0                  0         Shutdown
         Fa0/15          1            0                  0         Shutdown
         Fa0/16          1            0                  0         Shutdown
         Fa0/17          1            0                  0         Shutdown
         Fa0/18          3            1                  0         Shutdown
         Fa0/19          1            0                  0         Shutdown
         Fa0/20          1            0                  0         Shutdown
         Fa0/21          1            0                  0         Shutdown
         Fa0/22          1            0                  0         Shutdown
         Fa0/23          1            0                  0         Shutdown
         Fa0/24          1            0                  0         Shutdown
         Gig0/1          1            0                  0         Shutdown
         Gig0/2          1            0                  0         Shutdown
```

Imagen 21. Configuración interfaces no utilizadas en S2

Parte 3: Configurar soporte de host

Paso 1: Configure R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan2 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)#dns-server 209.165.200.225
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan2 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-a.net R1(dhcp-config)#dns-server 209.165.200.225

Tabla 7. Configuración DHCP en S1 VLAN2 y S2 VLAN 2

```
R1(config)#ip dhcp pool vlan2
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)#dns-server 209.165.200.225
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool vlan3
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)#dns-server 209.165.200.225
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
```

Imagen 22. Configuración DHCP en S1 VLAN2 y S2 VLAN 2

Paso 2: Configurar los servidores

PC-A Network Configuration	
Descripción	*Configuración PC-A*
Dirección física	*00E0.B0E9.14B8*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 8. Configuración PC-A

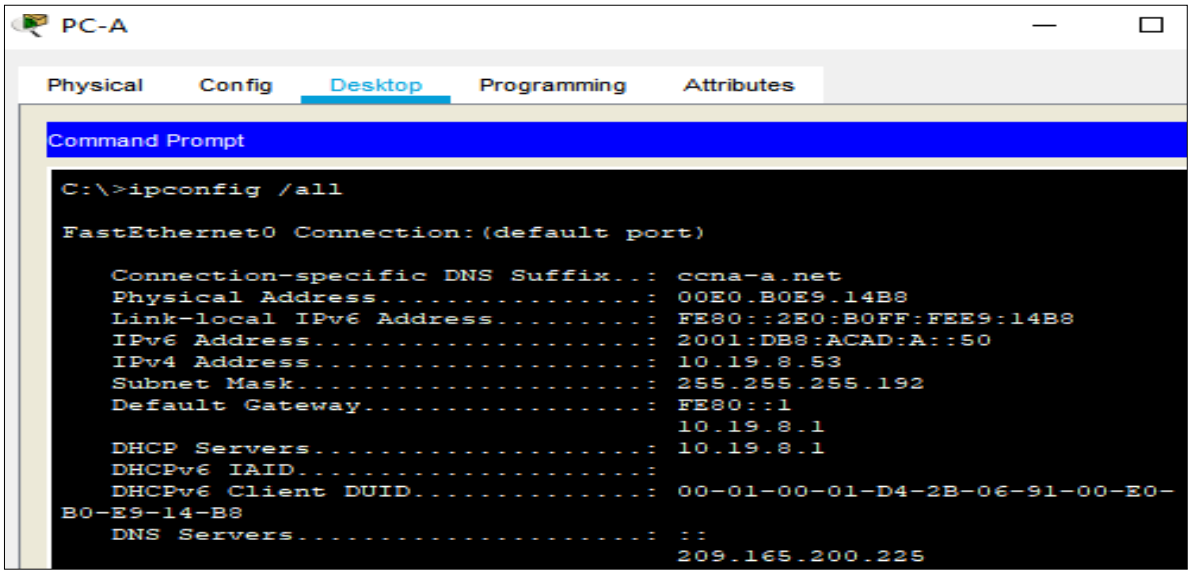


Imagen 23. Verificación configuración PC-A

Configuración de red de PC-B	
Descripción	*Configuración PC-A*
Dirección física	*00D0.BCD5.32C1*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.244*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

Tabla 9. Configuración PC-B

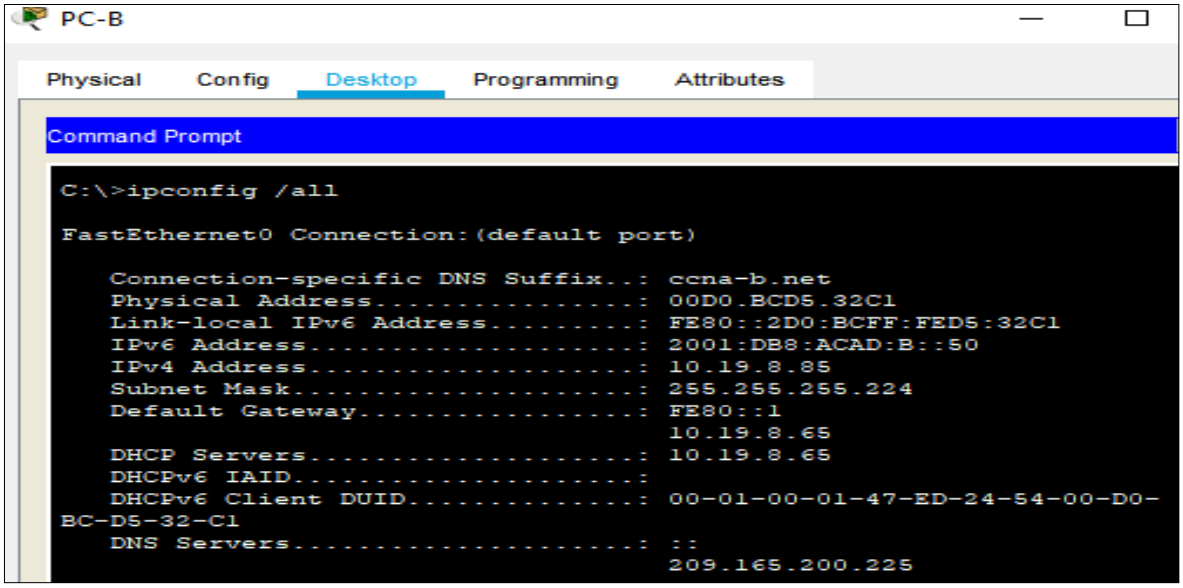


Imagen 24. Verificación configuración PC-B

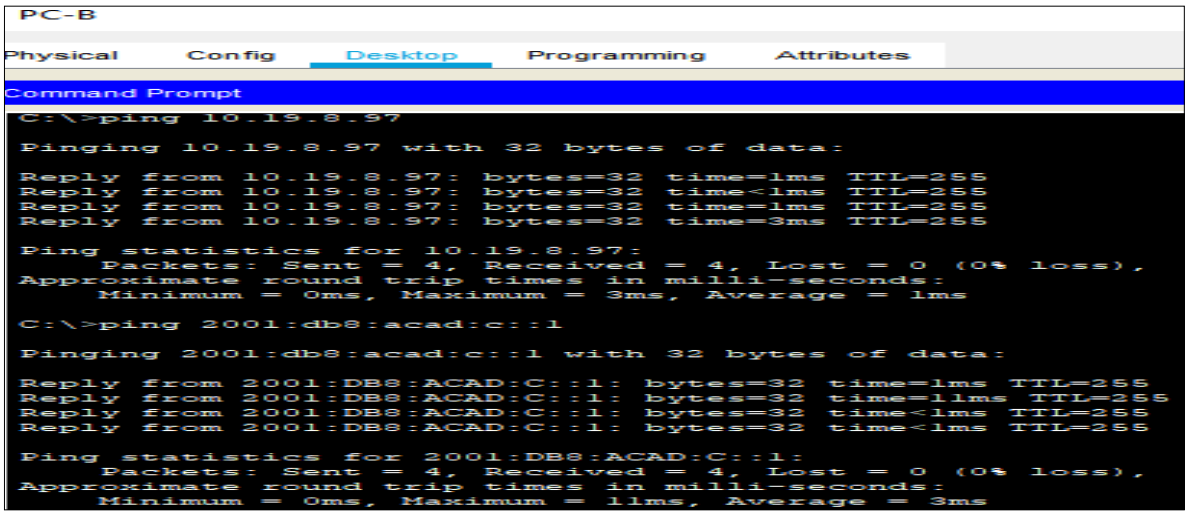


Imagen 25. Verificación con ping desde PC-B a interfaz G0/0/1.4

Parte 2: Probar y verificar la conectividad de extremo a extremo

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Conectado*
		IPv6	2001:db8:acad:a: :1	*Conectado*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Conectado*
		IPv6	2001:db8:acad:b: :1	*Conectado*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Conectado*
		IPv6	2001:db8:acad:c: :1	*Conectado*
	S1, VLAN 4	Dirección	10.19.8.98	*Conectado*
		IPv6	2001:db8:acad:c: :98	*No conectado*
	S2, VLAN 4	Dirección	10.19.8.99.	*Conectado*
		IPv6	2001:db8:acad:c: :99	*No conectado*
	PC-B	Dirección	10.19.8.85	*Conectado*
		IPv6	2001:db8:acad:b: :50	*Conectado*
	R1 Bucle 0	Dirección	209.165.201.1	*Conectado*
		IPv6	2001:db8:acad:209: :1	*Conectado*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Conectado*
		IPv6	2001:db8:acad:209: :1	*Conectado*
	R1, G0/0/1.2	Dirección	10.19.8.1	*Conectado*
		IPv6	2001:db8:acad:a: :1	*Conectado*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Conectado*
		IPv6	2001:db8:acad:b: :1	*Conectado*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Conectado*
		IPv6	2001:db8:acad:c: :1	*Conectado*
	S1, VLAN 4	Dirección	10.19.8.98	*Conectado*
		IPv6	2001:db8:acad:c: :98	*No conectado*
	S2, VLAN 4	Dirección	10.19.8.99.	*Conectado*
		IPv6	2001:db8:acad:c: :99	*No conectado*

Tabla 10. Verificación conectividad entre los dispositivos de red.

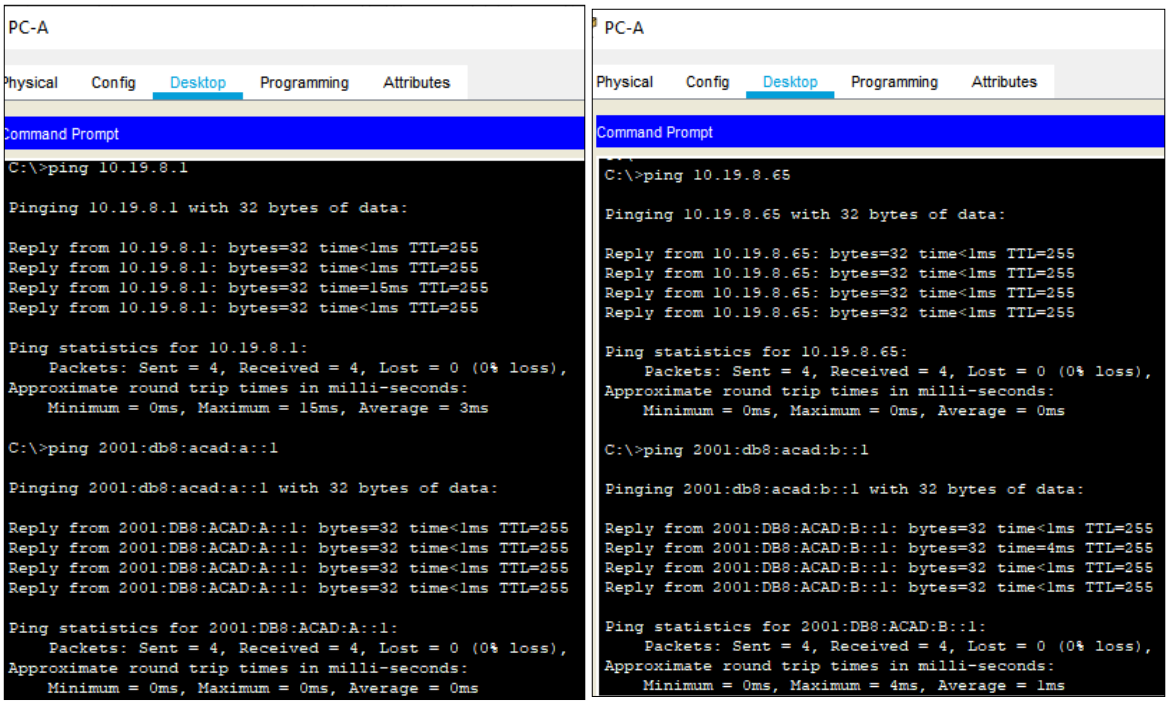


Imagen 26. Verificación con ping desde PC-A a interfaces G0/0/1.2 y G0/0/1.3

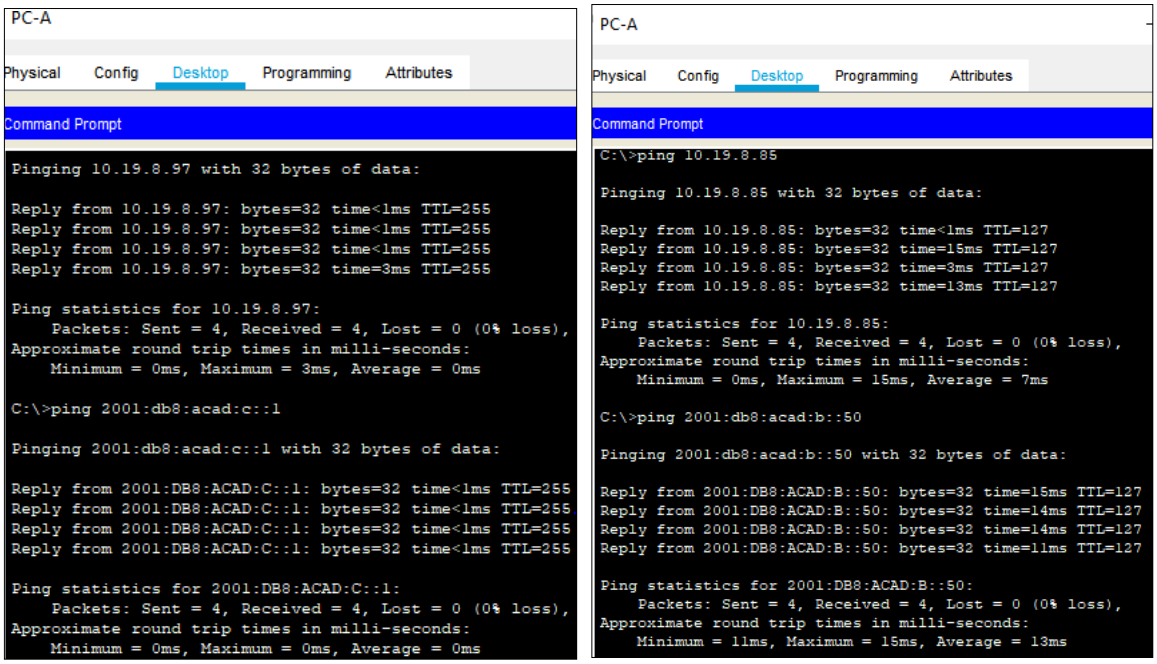


Imagen 27. Verificación con ping desde PC-A a interfaz G0/0/1.4 y PC-B

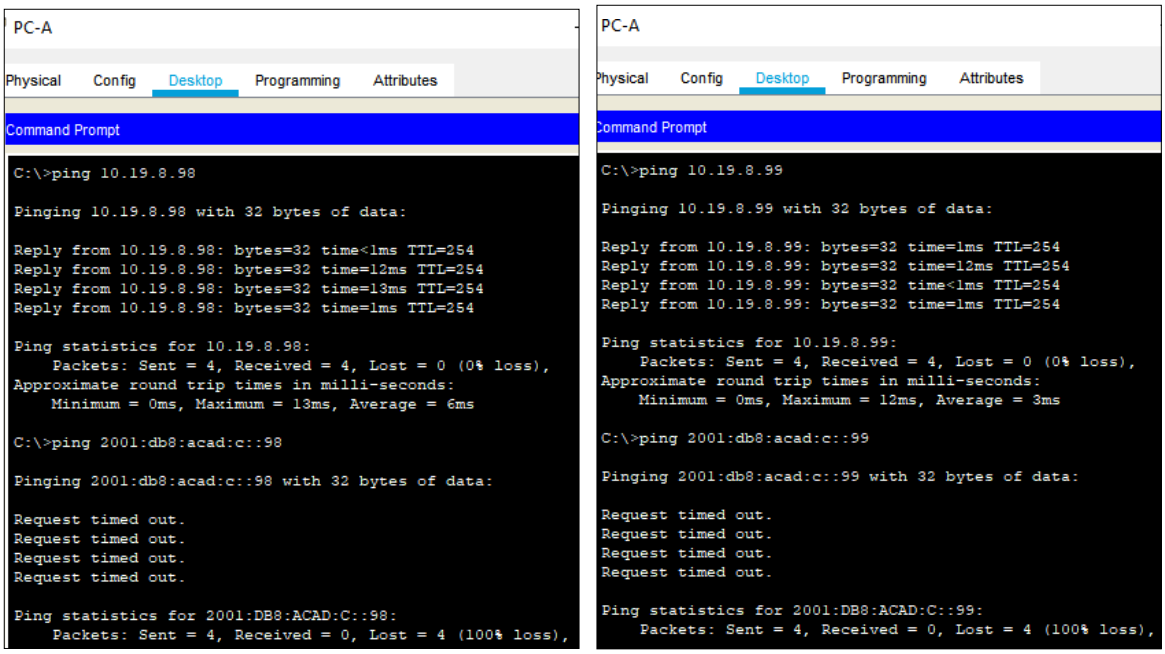


Imagen 28. Verificación con ping desde PC-A a VLAN 4 de S1 y S2

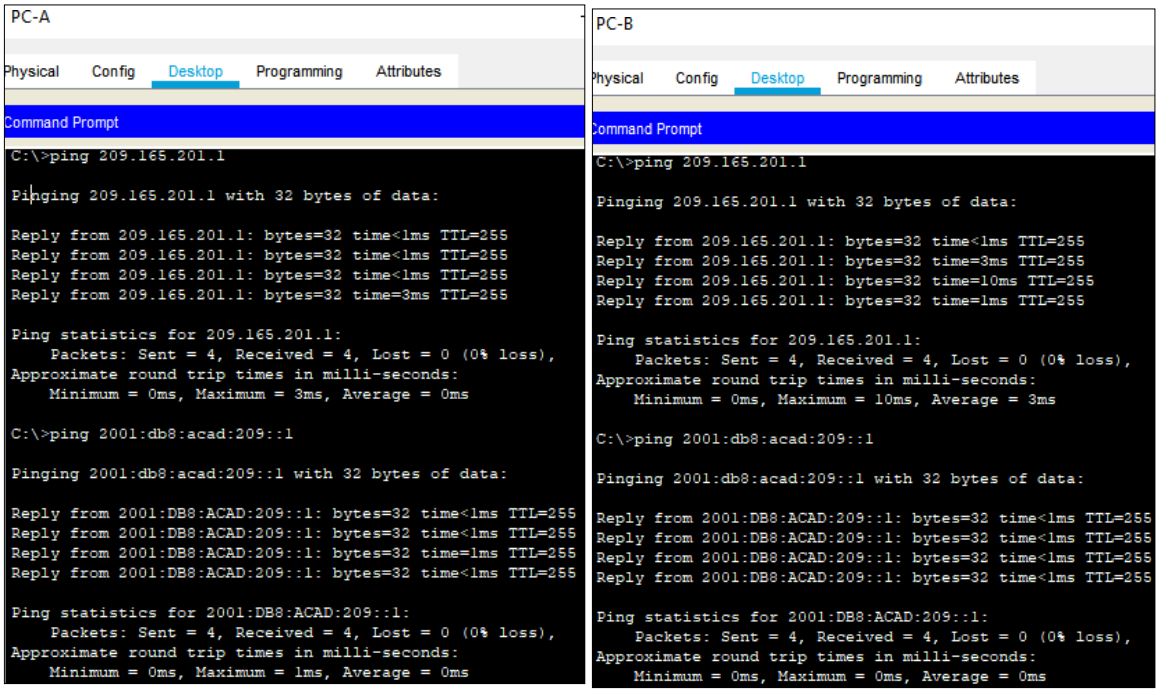


Imagen 29. Verificación con ping desde PC-A y PC-B a interfaz loopback 0

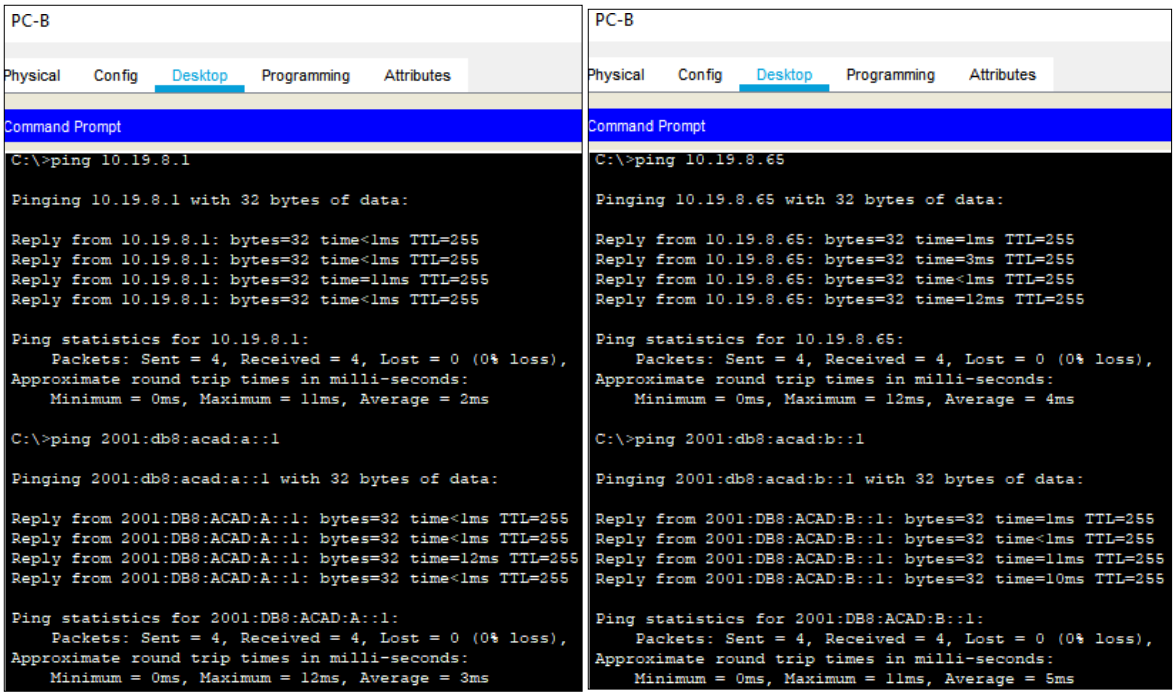


Imagen 30. Verificación con ping desde PC-B a interfaces G0/0/1.2 y G0/0/1.3

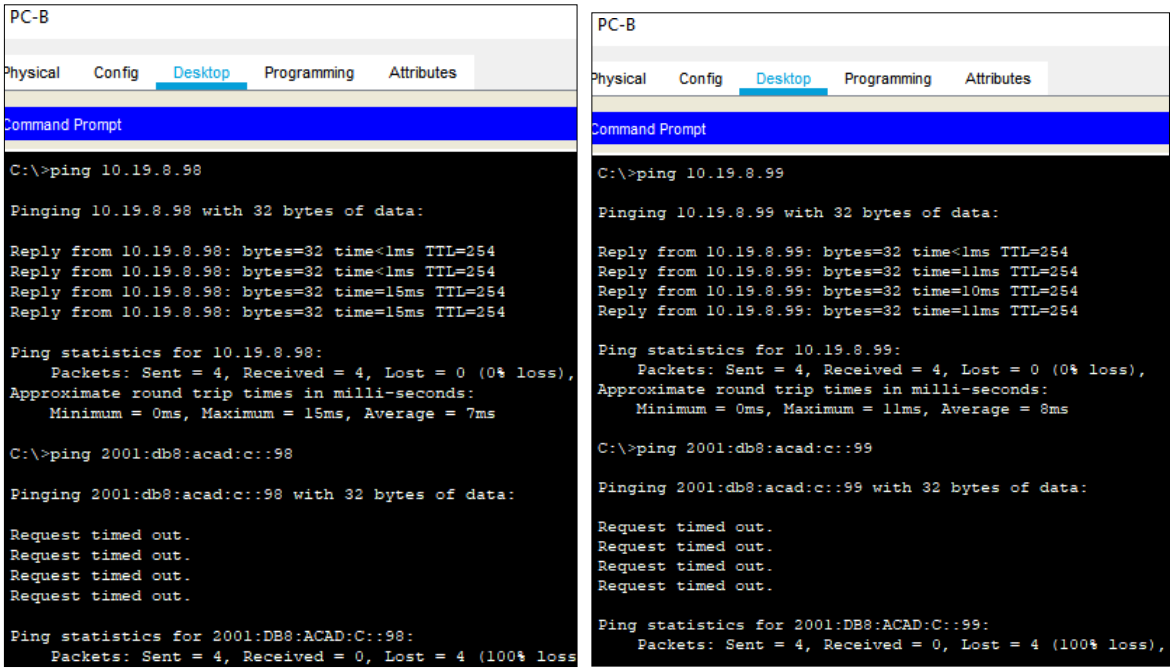


Imagen 31. Verificación con ping desde PC-A a VLAN 4 de S1 y S2

Con la conexión IPV4 e IPV6 se evidencia el correcto enrutamiento funcionamiento de la red, con la creación de las VLAN se aisló las diferentes redes evitando problemas de seguridad, mediante R1 conocido en esta topología como router-on-a-stick y con un con enlace troncal 802.1Q, se logro el enrutamiento entre las VLAN.

CASO DE ESTUDIO 2.

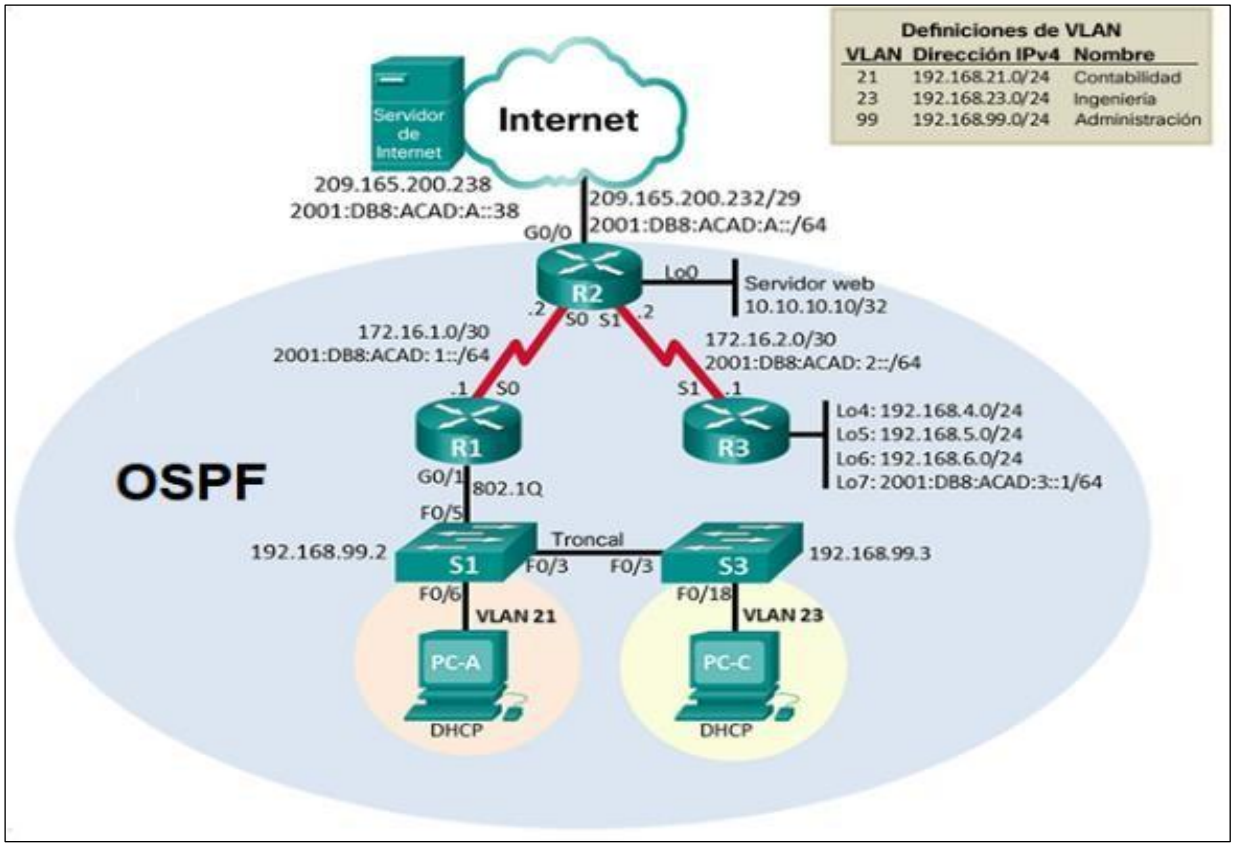


Imagen 32. Topología de red del caso 2

Parte 1: Inicializar dispositivos

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

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 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	Switch#show vlan

Tabla 11. Configuración inicial dispositivos de la red

Eliminar el archivo startup-config de todos los routers y volver a cargarlos

```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]yInitializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly


System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018  by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4331/K9 platform with 4194304 Kbytes of main mem
```

Imagen 33. Configuración inicial routers

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior y volver a cargar ambos switches

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0090.2150.1CBC
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
###########################################################################
```

Imagen 34. Configuración inicial switches

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

```
Switch#show vlan

VLAN  Name                                      Status
----  ----------------------------------------  ---------
1     default                                   active
Fa0/4
Fa0/8
Fa0/11, Fa0/12
Fa0/15, Fa0/16
Fa0/19, Fa0/20
Fa0/23, Fa0/24
1002  fddi-default                              active
1003  token-ring-default                        active
1004  fddinet-default                           active
1005  trnet-default                             active
```

Imagen 35. Verificación VLAN switches

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.226
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 12. Configuración computadora de internet

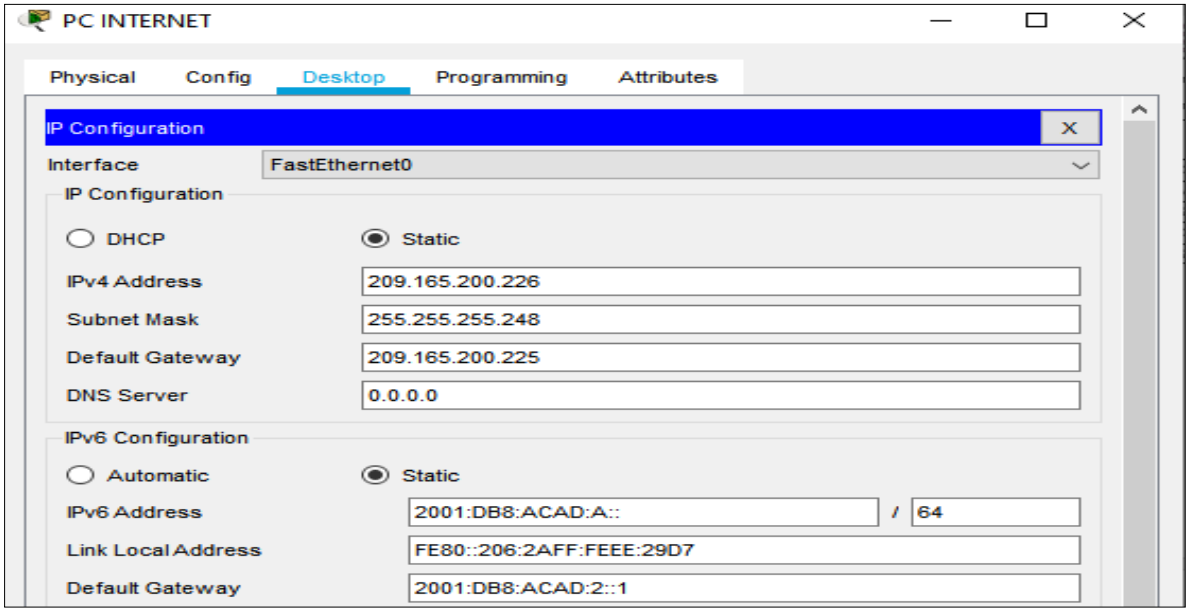


Imagen 36. Configuración computadora de internet

Paso 2: Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R1
Contraseña de exec privilegiado cifrada	R1(config)# enable secret class
Contraseña de acceso a la consola	R1(config)# line con 0 R1(config-line)# password cisco R1(config-line)# login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#pass cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption
Mensaje MOTD	R1(config)# banner motd # se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface S0/0/0 R1(config-if)#description conexión a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
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

Tabla 13. Configuración inicial R1

```
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
R1(config)#interface S0/0/0
R1(config-if)#description coneccion a R2
R1(config-if)#ip address 172.16.1.0 255.255.255.252
Bad mask /30 for address 172.16.1.0
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0
```

Imagen 37. Configuración parámetros básicos R1

Paso 3: Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	Router(config)# hostname R1
Contraseña de exec privilegiado cifrada	R2(config)# enable secret class
Contraseña de acceso a la consola	R2(config)# line con 0 R2(config-line)# password cisco R2(config-line)# login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#pass cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)# service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)# banner motd # se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface S0/0/0 R2(config-if)#description conexin a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface S0/0/1 R2(config-if)#description conexin a R1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface G0/0 R2(config-if)#description conexion a ISP R2(config-if)#ip address 209.165.200.224 255.255.255.248

	R2(config-if)#ipv6 address 2001:DB8:ACAD:A::/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#description conexin a servidor web simulado 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 G0/0 R2(config)#ipv6 route ::/0 G0/0

Tabla 14. Configuración inicial R2

```
R2(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
R2(config)#interface S0/0/0
R2(config-if)#description conexin a R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#exit
R2(config)#interface S0/0/1
R2(config-if)#description conexin a R3
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#interface G0/0
R2(config-if)#description conexin a ISP
R2(config-if)#ip address 209.165.200.225  255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface loopback 0
R2(config-if)#description conexin a servidor web simulado
R2(config-if)#ip address 10.10.10.10  255.255.255.0
R2(config-if)#exit
R2(config)#interface g0/1
R2(config-if)#description conexin a servidor web simulado
R2(config-if)#ip address 10.10.10.1  255.255.255.0
% 10.10.10.0 overlaps with Loopback0
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0
```

Imagen 38. Configuración parámetros básicos R2

Paso 4: 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 con 0 R3(config-line)# password cisco R3(config-line)# login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#pass cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)# service password-encryption
Mensaje MOTD	R3(config)# banner motd # se prohíbe el acceso no autorizado#
Interfaz S0/0/1	R3(config-if)#description conexion a R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::/64 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.000
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.000
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.000
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::/64

Tabla 15. Configuración inicial R3

```
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
R3(config)#interface S0/0/1
R3(config-if)#description conexin a R2
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::/64
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#exit
R3(config)#interface loopback 4

R3(config-if)#ip address 192.168.4.1  255.255.255.000
R3(config-if)#exit
R3(config)#interface loopback 5

R3(config-if)#ip address 192.168.5.1  255.255.255.000
R3(config-if)#exit
R3(config)#interface loopback 6

R3(config-if)#ip address 192.168.6.1  255.255.255.000
R3(config-if)#exit
R3(config)#interface loopback 7

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 G0/0
```

Imagen 39. Configuración parámetros básicos R3

Paso 5: Configurar S1

Elemento o tarea de configuración	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 con 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#pass cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#

Tabla 16. Configuración inicial S1

```
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
```

Imagen 40. Configuración parámetros básicos S1

Paso 6: Configurar el 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 con 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#pass cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#

Tabla 17. Configuración inicial S3

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #PROHIBIDO EL ACCESO NO AUTORIZADO#
```

Imagen 41. Configuración parámetros básicos S3

Paso 7: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Conectado
R2	R3, S0/0/1	172.16.2.2	Conectado
PC de Internet	Gateway predeterminado	209.165.200.225	Conectado

Tabla 18. Verificación de la conectividad de la red

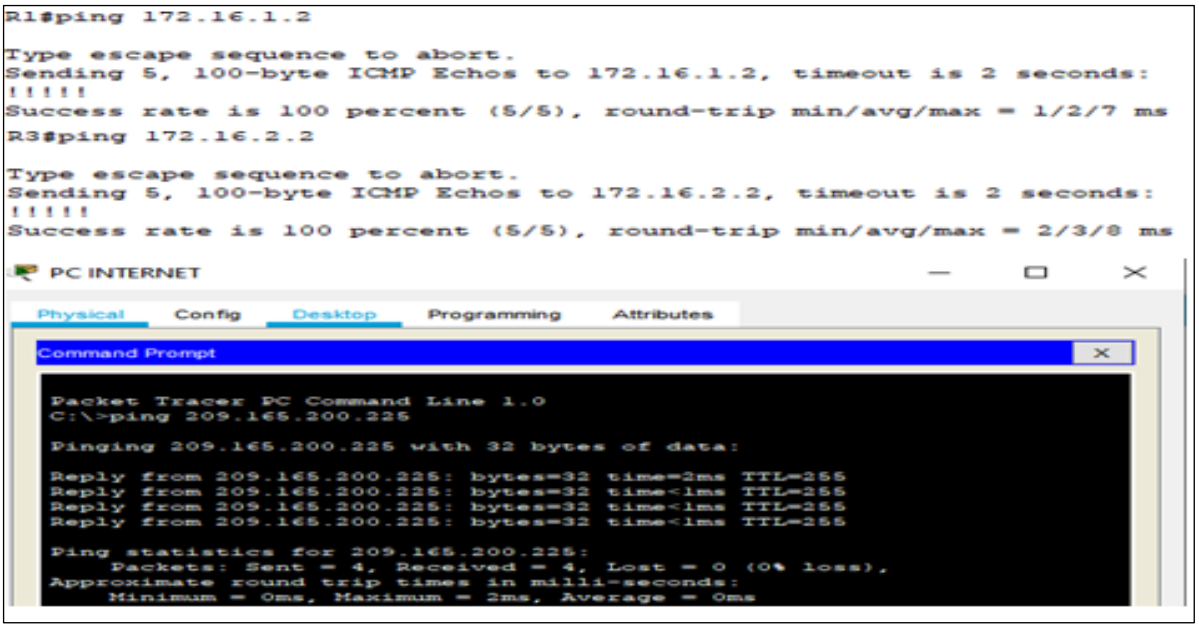


Imagen 42. Verificación de la conectividad de la red con ping.

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

Paso 1: 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)#vlan 23 S1(config-vlan)#name Ingeniera S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.000

Asignar el gateway predeterminado	S1(config-if)#ip default-gateway 199.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switchport trunk allowed vlan 21,23,99
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switchport trunk allowed vlan 21,23,99
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface range f0/6 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)# interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 19. Configuración VLAN y seguridad en S1

```
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingeniera
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracin
S3(config-vlan)#exit
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.000
S3(config-if)#ip default-gateway 199.168.99.1
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#switchport trunk allowed vlan 21,23,99
S3(config-if)#exit
S3(config)#interface range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#interface range f0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 23
S3(config-if-range)#exit
S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

Imagen 43. Configuración VLAN y seguridad en S1

Paso 2: Configurar el 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)#vlan 23 S3(config-vlan)#name Ingeniera S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.000
Asignar el gateway predeterminado.	S3(config-if)#ip default-gateway 199.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#switchport trunk allowed vlan 21,23,99
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#interface range f0/18 S3(config-if-range)#switchport mode access S3(config-if-range)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 20. Configuración VLAN y seguridad en S3

```
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingeniera
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracin
S3(config-vlan)#exit
S3(config)#interface vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.000
S3(config-if)#ip default-gateway 199.168.99.1
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#switchport trunk allowed vlan 21,23,99
S3(config-if)#exit
S3(config)#interface range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#interface range f0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 23
S3(config-if-range)#exit
S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

Imagen 44. Configuración VLAN y seguridad en S3

Paso 2: Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description LAN de contabilidad R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.000
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#description LAN de Ingeniera R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.000
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface g0/1.99 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.000
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shutdown

Tabla 21. Configuración Subinterfaces en R1

```
R1(config)#interface g0/1.21
R1(config-subif)#description LAN de contabilidad
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1  255.255.255.000
R1(config-subif)#exit
R1(config)#interface g0/1.23
R1(config-subif)#description LAN de Ingeniera
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1  255.255.255.000
R1(config-subif)#exit
R1(config)#interface g0/1.99
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1  255.255.255.000
```

Imagen 45. Configuración Subinterfaces en R1

Paso 3: 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	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Tabla 22. Verificación de la conectividad de la red

```
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 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/16 ms

S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/15 ms
```

Imagen 46. Verificación de la conectividad de la red

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar 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 0.0.0.3 area 0 R1(config-router)#network 192.168.23.0 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 g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config)# area 0 stub no-summary

Tabla 23. Configuración OSPF en R1

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.3 area 0
    192.168.23.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:19:05
    2.2.2.2              110      00:08:03
    3.3.3.3              110      00:10:17
  Distance: (default is 110)

R1#show ip ospf border-routers
OSPF Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 2.2.2.2 [64] via 172.16.1.2, Serial0/0/0, ABR, Area 0, SPF 64
i 3.3.3.3 [128] via 172.16.1.2, Serial0/0/0, ABR, Area 0, SPF 128

R1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
1.1.1.1         1.1.1.1         1567        0x80000005 0x00201a 5
3.3.3.3         3.3.3.3         1039        0x80000004 0x00c3e2 3
2.2.2.2         2.2.2.2         905         0x80000007 0x008e7c 4
```

Imagen 47. Comprobación OSPF en R1

Paso 2: 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 2.2.2.2
Anunciar las redes conectadas directamente	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 255
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface g0/1
Desactive la sumarización automática.	R2(config)# area 0 stub no-summary

Tabla 24. Configuración OSPF en R2

```
R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 255
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:27:05
    2.2.2.2              110      00:16:02
    3.3.3.3              110      00:18:16
  Distance: (default is 110)

R2#show ip ospf border-routers
OSPF Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 3.3.3.3 [64] via 172.16.2.2, Serial0/0/1, ABR, Area 0, SPF 64
R2#
```

Imagen 48. Comprobación OSPF en R2

```
R2#show ip ospf database
            OSPF Router with ID (2.2.2.2) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
2.2.2.2         2.2.2.2         1118        0x80000008 0x008c7d 4
1.1.1.1         1.1.1.1         1780        0x80000006 0x001e1b 5
3.3.3.3         3.3.3.3         1251        0x80000005 0x00cle3 3

                Router Link States (Area 255)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
2.2.2.2         2.2.2.2         1117        0x80000002 0x00064d 0

                Summary Net Link States (Area 255)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.0      2.2.2.2         257         0x8000000d 0x000a45
172.16.1.0      2.2.2.2         247         0x8000000e 0x00133c
192.168.21.0    2.2.2.2         1774        0x80000009 0x00305f
192.168.23.0    2.2.2.2         1774        0x8000000a 0x001874
192.168.99.0    2.2.2.2         1774        0x8000000b 0x00ce70
192.168.4.1     2.2.2.2         1112        0x8000000c 0x00dbc0
```

Imagen 49. Comprobación OSPF en R2

Paso 3: Configurar OSPFv3 en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 2.2.2.2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.1.0 0.0.0.3 area 0 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 10.10.10.0 0.0.0.255 area 255
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface g0/1
Desactive la sumarización automática.	R3(config)# area 0 stub no-summary

Tabla 25. Configuración OSPF en R3

```
R3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    192.168.4.0 0.0.0.255 area 0
    10.10.10.0 0.0.0.255 area 255
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:04:19
    2.2.2.2              110      00:23:20
    3.3.3.3              110      00:25:32
  Distance: (default is 110)

R3#show ip ospf database
            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
3.3.3.3         3.3.3.3         1724        0x80000005 0x00c1e3 3
2.2.2.2         2.2.2.2         1592        0x80000008 0x008c7d 4
1.1.1.1         1.1.1.1         451         0x80000007 0x001c1c 5

                Router Link States (Area 255)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
3.3.3.3         3.3.3.3         1724        0x80000002 0x00b991 0

                Summary Net Link States (Area 255)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.0      3.3.3.3         1720        0x80000007 0x00f759
192.168.4.1     3.3.3.3         1720        0x80000008 0x004399
172.16.1.0      3.3.3.3         1585        0x80000009 0x00818e
192.168.21.0    3.3.3.3         1585        0x8000000a 0x0092b7
192.168.23.0    3.3.3.3         1585        0x8000000b 0x007acc
192.168.99.0    3.3.3.3         1585        0x8000000c 0x0031c8
```

Imagen 50. Comprobación OSPF en R3

Paso 4: Verificar la información de OSPF

```
R1#show ip route ospf
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.2.0 [110/128] via 172.16.1.2, 00:21:45, Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/129] via 172.16.1.2, 00:10:40, Serial0/0/0
R2#show ip route ospf
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/65] via 172.16.2.2, 00:47:35, Serial0/0/1
O    192.168.21.0 [110/65] via 172.16.1.1, 00:58:40, Serial0/0/0
O    192.168.23.0 [110/65] via 172.16.1.1, 00:58:40, Serial0/0/0
O    192.168.99.0 [110/65] via 172.16.1.1, 00:58:40, Serial0/0/0
R3#show ip route ospf
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.1.0 [110/128] via 172.16.2.1, 00:54:51, Serial0/0/1
O    192.168.21.0 [110/129] via 172.16.2.1, 00:54:51, Serial0/0/1
O    192.168.23.0 [110/129] via 172.16.2.1, 00:54:51, Serial0/0/1
O    192.168.99.0 [110/129] via 172.16.2.1, 00:54:51, Serial0/0/1
```

Imagen 51. Comprobación OSPF en R1, R2 R3.

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 ip ospf database

Tabla 26. Respuestas a interrogantes de OSPF

Parte 5: Implementar DHCP y NAT para IPv4

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

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.000 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.23.0 255.255.255.000 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.21.1

Tabla 27.Configuración R1 como servidor de DHCP para las VLAN 21 y 23

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.000
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGR
R1(dhcp-config)#network 192.168.23.0 255.255.255.000
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#default-router 192.168.23.1
```

Imagen 52. Configuración R1 como servidor de DHCP para las VLAN 21 y 23

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

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface loopback 0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/0/1 R2(config-if)#ip nat inside R2(config-if)#interface g0/0 R2(config-if)#ip nat outside
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)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 28. Configuración NAT estática y dinámica en R2

```
R2(config)#username webuser privilege 15  secret ciscol2345
R2(config)#ip http server
                ^
% Invalid input detected at '^' marker.

R2(config)#ip http authentication local
                ^
% Invalid input detected at '^' marker.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface loopback 0
R2(config-if)#ip nat inside
R2(config-if)#interface s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET
% Incomplete command.
R2(config)#ip nat pool INTERNET 209.165.200.225  209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
```

Imagen 53. Configuración NAT estática y dinámica en R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Connection-specific DNS Suffix..: ccna-a.net Link-local IPv6 Address.....: FE80::201:97FF:FEC6:A827 IPv6 Address.....: :: IPv4 Address.....: 192.168.21.21 Subnet Mask.....: 255.255.255.0 Default Gateway.....: :: 192.168.21.1
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Connection-specific DNS Suffix..: ccna-sa.com Link-local IPv6 Address.....: FE80::2D0:BAFF:FE09:E91E IPv6 Address.....: :: IPv4 Address.....: 192.168.23.21 Subnet Mask.....: 255.255.255.0 Default Gateway.....: :: 192.168.23.1
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	C:\>ping 192.168.23.21 Pinging 192.168.23.21 with 32 bytes of data: Reply from 192.168.23.21: bytes=32 time=2ms TTL=127 Reply from 192.168.23.21: bytes=32 time=16ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time=12ms TTL=127 Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 16ms, Average = 7ms

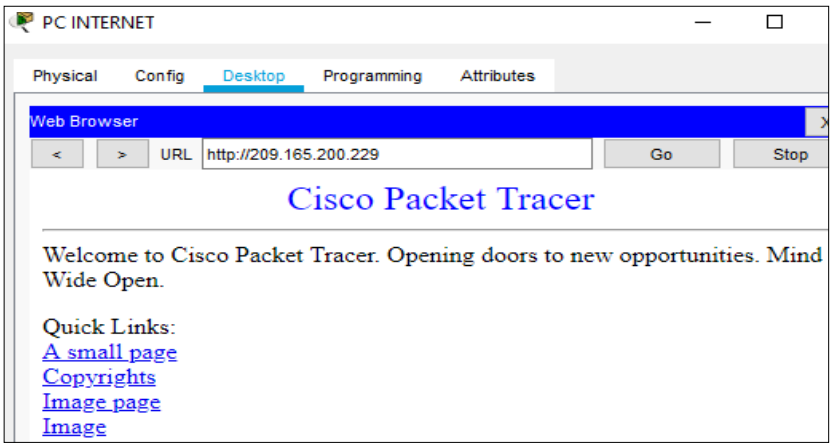
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

Tabla 29. Verificación el protocolo DHCP y NAT estática

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 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

Tabla 30. Configuración NTP

```
R2#clock set 09:00:00 05 march 2016
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp  master 5

R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#exit
R1#show ntp associations

address         ref clock       st   when      poll     reach   delay
offset           disp
 ~172.16.1.2     .INIT.          16   -         64       0       0.00
0.00             0.01
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

Imagen 54. Comprobación configuración NTP

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 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	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenPROHIBIDO EL ACCESO NO AUTORIZADO User Access Verification Password: R2>enable Password: R2# R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host

Tabla 31. Configuración y verificación listas de control de acceso

```
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#exit
R2#show access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
```

Imagen 55. Configuración y verificación listas de control de acceso

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-list
Restablecer los contadores de una lista de acceso	Clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translations

Tabla 32. Respuestas a preguntas sobre listas de acceso.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:13192.168.21.21:13   209.165.200.226:13 209.165.200.226:13
```

Imagen 56. Verificación lista de acceso en R2.

Para este segundo caso igual que el primer caso la creación de las VLAN ayudaron a mejorar la seguridad de la red, de igual forma se establecieron parámetros de configuración con el protocolo OSPF

CONCLUSIONES

- La solución de dos estudios de caso bajo el uso de tecnología cisco permitió afianzar los conocimientos teóricos adquiridos durante las 10 unidades del diplomado de profundización cisco diseño e implementación de soluciones integradas LAN / WLAN, profundizando en la configuración de parámetros básicos y de seguridad en switchs, routers, principios de enrutamiento y conmutación, VLAN, troncales utilizando protocolo 802.1Q, implementación EtherChannel, port security, routing dinámico a través del protocolo Open Shortest Path First (OSPF), Protocolo de configuración hosts dinámico (DHCP), traducción de direcciones de red a través Network Address Translation (NAT), listas de control de acceso (ACL) y configuración de fecha y hora en router a través del protocolo te tiempo de red (NTP)

Se logro simular en el programa Packet Tracert la red del caso uno configurando a través de la interfaz de línea de comandos (CLI) dispositivos como el router y los dos switchs limitando el acceso a su configuración. Se establecieron en los switchs puertos de acceso y troncales para VLAN, se implementó también en ambos EtherChannel y port security. En el router se configuro el protocolo de configuración hosts dinámico (DHCP) creando pool para las VLAN 21 y 23, por último, se verifico la conectividad mediante el uso de comandos ping, traceroute y show ip route.

El Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch, las cuales pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch, en el caso de estudio uno se seleccionó la SDM dual-ipv4-and-ipv6 routing en un switch 3560 para habilitar tanto el direccionamiento IPV4 como IPV6.

Se logro simular en el programa Packet Tracert la red del caso dos configurando a través de la interfaz de línea de comandos (CLI) dispositivos como el routers y switchs limitando el acceso a su configuración. Se establecieron en los switchs puertos de acceso y troncales para VLAN. En lo routers se implementó routing dinámico a través del protocolo Open Shortest Path First (OSPF),en el router R2 se estableció el protocolo de configuración hosts dinámico (DHCP), traducción de direcciones de red a través Network Address Translation (NAT), listas de control de acceso (ACL) y configuración de fecha y hora a través del protocolo te tiempo de red (NTP), por último se verifico la conectividad mediante el uso de comandos ping, traceroute y show ip route.

Las listas de control de acceso (ACL) se pueden implementar en routers para aumentar la seguridad de una red o implementar políticas de entrada y salida de paquetes para ciertos equipos específicos.

BIBLIOGRAFÍA

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

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

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

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-asset.s3.amazonaws.com/RSE6/es/index.html#3

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

Router-on-a-Stick Inter-VLAN Routing (4.2) > Inter-VLAN Routing | Cisco Press. Recuperado de: https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=5