DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNA

DAGNNER SUSAN CASTILLO LUCUMI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TENOLOGIA E INGENIERIA - ECBTI
INGENIERIA DE SISTEMAS
SANTIAGO DE CALI
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNA

DAGNNER SUSAN CASTILLO LUCUMI

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

DIRECTOR
PAULITA FLOR SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISTEMAS
SANTIAGO DE CALI
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Santiago de Cali, Noviembre 2020

Este trabajo es dedicado a todo el esfuerzo realizado durante el trascurso de la realización de esta carrera Ingeniería de Sistemas, ya que cuando se inicia un proyecto de vida como este. Se debe trabajar duro y no perder el enfoque.

AGRADECIMIENTOS

Primeramente totalmente a Dios por darme todo lo necesario para culminar este proyecto con éxito, después a mi hijo Gino Rodriguez por ser el motor para esforzarme cada día, aunque en muchos momentos me sentí agotada, cansada y sin fuerzas para continuar. A mi madre Yolanda Lucumi haber sembrado en mí esa persona que aunque este sin fuerzas y esperanzas no me doy por vencida.

También a todas esas personas que Dios coloco en mi camino para de una u otra manera aprender de ellas y darme una palabra de aliento y superación.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACION

LISTA DE ANEXOS

GLOSARIO

DHCP: Protocolo que asigna direcciones ip automáticamente a los hosts que se encuentran en una red local.

Ping: Este comando ayuda al diagnostico la conexión que existe entre los hosts tanto del origen como el de destino, mediante un comando.

Firewall: Este permite o bloquea el acceso de acuerdo a la configuracion que se realiza ya sea por hardware y software.

NAT: Sistema de protocolo IP que permite el intercambio de paquetes.

RESUMEN

Esta actividad está relacionada con todo aquello de direccionamiento tanto de direcciones ipv4 como ipv6, en donde se debe asignar y configurar direcciones, iniciando con la máscara de red y a cada uno de los equipos correspondientes con su respectiva configuración, donde se asigna un usuario como administrador con contraseña para ingresar al Router y para realizar las configuraciones pertinentes. También se logra entender y realizar sobre el enrutamiento y funcionamiento de redes y subredes, habilitando para funcionamiento la dirección ipv6 en las diferentes interfaces, generación clave de cifrado RSA. Entre otros funcionamientos relacionados con configuración y enrutamiento.

Cifrado de contraseñas.

En el segundo escenario se realizan diferentes configuraciones donde es utilizado un sistema para habilitar cantidades de direcciones el cual se sustituye la ip de origen dentro de un rango seleccionado en un grupo de direcciones.

Se utilizan contraseñas cifradas para garantizar la seguridad.

ABSTRACT

This activity is related to all that of addressing both IPv4 and IPv6 addresses, where addresses must be assigned and configured, starting with the network mask and each of the corresponding computers with their respective configuration, where a user is assigned as administrator with password to enter the Router and to make the pertinent configurations. It is also possible to understand and carry out the routing and operation of networks and subnets, enabling the IPv6 address to function in the different interfaces, generating the RSA encryption key. Among other operations related to configuration and routing.

Password encryption.

In the second scenario, different configurations are made where a system is used to inhabit quantities of addresses, which substitutes the source IP within a range selected in a group of addresses. Encrypted passwords are used to ensure security.

PALABRAS CLAVE: RSA, Cifrado, Enrutamiento, Configuración, Comando, NAT, Servidor, Internet.

Keywords: RSA, Encryption, Routing, Setting, Command, NAT, Server, Internet

1. INTRODUCCIÓN

A continuación se realiza el desarrollo con el fin de recibir la capacitación sobre resolución de conflictos de conectividad o todo aquello que tenga de ver con esta área. Ya que la universidad Nacional Abierta o A Distancia con este diplomado de profundización en redes teniendo como soporte la compañía cisco, tiene como finalidad ampliar este tipo de conocimientos de una forma ABE (Aprendizaje Basados en Escenarios). En este caso se presentan dos escenarios.

El primero con el objetivo de entender y realizar la configuración de dispositivos de una red pequeña, en donde se deben configurar 1 router, 1 switch, y equipo donde se logre la conectividad tanto e IPV4 como en IPV6, para los host presentados y tener en cuenta en forma segura.

En el segundo escenario se realiza las configuraciones de switches y router en donde se implementa y configura usuarios y contraseñas de acceso, además los host se configuran en protocolo dhcp, se realiza cifrado de contraseñas, configura hora y fecha. Tambien se implementa el sistema NAT el cual permite dinamizar las direcciones IP de origen dentro de un rango definido para dar respuesta.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Adquirir y demostrar el desarrollo de habilidades en el momento de implementar o actualizar una red, realizando las respectivas configuraciones de los diferentes dispositivos y verificar conectividad, comunicación entre estos dispositivos.

2.2 OBJETIVOS ESPECÍFICOS

Realizar la configuracion de router utilizando dirección IPV4 – IPV6.

Realizar la configuración de switch

Realizar la configuración de host utilizando DHCP, IPV4, IPV6

Realizar la configuracion de vlans y troncales

Realizar la configuracion de protocolo DHCP Y NAT.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

- ESCENARIO 1

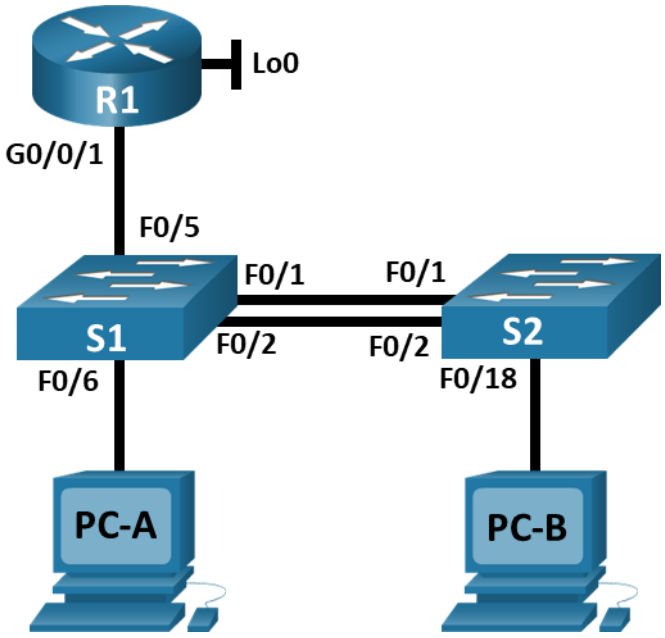


Ilustración 1A

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 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
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
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
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	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
PC-A NIC	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

Paso 1: En la parte 1: Se inicializa y recarga, donde se realiza la configuración de los aspectos básicos de los dispositivos, como lo es el Router, Swicht.

- Se realiza la configuración, en donde se utilizan los

  Comandos para la configuración de router, luego se procede a escribir la dirección ip 10.19.8.1 con una mascará de 255.255.255.0, después de realizar está configuración se da click en encender el router. Y se evidencia en el archivo pkt.

- Se realiza la configuración DHCP predeterminada, donde se ingresa a un servidor y se configura PC-A y PC-B, después de configurar el servidor se presiona en DHCP para que automáticamente asigne una dirección IP.
- También solicita configurar el swicht:

- Este comando es utilizado para configurar los PC-A y PC-B en ipv6.

```
Router#conf t

Enter configuration commands, one for line.  End with CNTL/Z
Router (config) #ipv6 unicast-routing
Router (config) #interface g0/0
Router (config-if) #iv6 address 2001:db8:acad:a::1/64
Router (config-if) #ipv6 address f80::1 link-local
Router (config-if) #no shutdown
Router (config-if) #exit
```

- Para borrar las configuraciones de inicio y las vlan del router, switch para luego volver a cargar los dispositivos. Se utiliza el siguiente comando:

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

- Después de borrar las configuraciones se realiza el cargue de la plantilla SDM en donde admite la dirección ipv6 que se establece con los siguientes comandos:

```
Router>enable                          Con este comando se ingresa a modo privilegiado
Router#configure terminal              ⇨ Modo de configuraciòn
Router(config)#interface Gig0/0        Ingreso a la interface
Router(config-if)#ipv6 address 2001:db8:acad:a::1/64
Router(config-if)#no shutdown
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2: Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router#conf term Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#ip ssh version 2 Please create RSA keys (of at least 768 bits size) to enable SSH v2. R1(config)#ip ssh authentication-retries 2 R1(config)#ip ssh time-out 120 R1(config)#exit
Cifrar las contraseñas de texto no cifrado	R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line console 0
Configure un MOTD Banner	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd #<Configuracion Router>#

Tarea	Especificación
Habilitar el routing IPv6	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ipv6 unicast-routing R1(config)#interface g0/0 R1(config-if)#ipv6 address 2001:db8:acad:a::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shutdown R1(config-if)#exit R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**
Generar una clave de cifrado RSA Módulo de 1024 bits	Password: R1>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name R1.ccna-lab.com R1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: R1.R1.ccna-lab.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *mar. 1 5:16:53.782: %SSH-5-ENABLED: SSH 2 has been enabled R1(config)#username admin secret admin1pass R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console

- Acontinuacion como lo indica la guia se genera la clave para ingreso y configuracion al Router.

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoenpass
R1(config-line)#login
R1(config-line)#line vty 0 10
R1(config-line)#password ciscoenpass
R1(config-line)#
```

- El siguiente comando se realiza con el fin de generar un usuario administrador con contraseña para el ingreso

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#username admin password admin1pass
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#configure terminal^

% Invalid input detected at '^' marker.
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Se procede a configurar el inicio de sesión con vty

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

- Se realiza la configuración de vty aceptando solo ssh como se muestra a continuación:

```
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R1(config)#ip ssh authentication-retries 2
R1(config)#ip ssh time-out 120
```

```
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip ssh
SSH Disabled - version 2
%Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 2
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#exit
```

- En los siguientes comandos se cifra las configuras de texto no cifradas y también se realiza la configuración de un MOTD Banner:

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console 0
R1(config)#service password-encryption
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#banner motd #<Configuracion Router>#
```

- A continuación se realizar la configuración del Router para direccionamiento de ipv6 donde se utilizan los siguientes comandos:

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int G0/0/1
R1(config-if)#IPV6 enable
```

```
R1(config-if)#int G0/0/1.2
R1(config-subif)#exit
R1(config)#int G0/0/1
R1(config-if)#ipv6 enable
R1(config-if)#int G0/0/1.2
R1(config-subif)#no shutdown
R1(config-subif)#encapsulation dot1Q2

% Invalid input detected at '^' marker.
R1(config-subif)#encapsullation dot1q 2

% Invalid input detected at '^' marker.
R1(config-subif)#exit
R1(config)#int g0/0/1
R1(config-if)#ipv6 enable
R1(config-if)#g0/0/1.2

% Invalid input detected at '^' marker.
R1(config-if)#int g0/0/1.2
R1(config-subif)#
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-subif)#no shutdown
R1(config-subif)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int 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)#no shut
R1(config-subif)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int 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:acasd:c::1/64
% Incomplete command.
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)#no shut
R1(config-subif)#exit
R1(config)#int g/0/1.6
```

Por ultimo en la configuración del Router se debe generar una clave de cifrado RSA de 1024 bits, como se muestra a continuación:

```
Password:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name R1.ccna-lab.com
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*mar. 1 5:16:53.782: %SSH-5-ENABLED: SSH 2 has been enabled
R1(config)#username admin secret admin1pass
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 3: Configure S1

Las tareas de configuración incluyen lo siguiente:

Para las siguientes configuraciones se utilizaron los switch 3560 ya que viene por defecto para visualizar la activación de direcciones ipv4 – ipv 6.

Pero para habilitar esta opción se debe antes utilizar los siguientes comandos:

```
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
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.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C3560 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: 0006.2A1D.20AE
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"...

###
########### [OK]

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#

Tarea	Especificación
Nombre del switch **S1 o S2, según proceda**	Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S1 S1(config)# S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Nombre de dominio **ccna-lab.com**	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado **Ciscoenpass**	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#enable secret ciscoenpass S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Contraseña de acceso a la consola **Ciscoconpass**	S1>enable Password: S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line console 0 S1(config-line)#login S1(config-line)#line vty 0 10 S1(config-line)#password ciscoconpass S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Crear un usuario administrativo en la base de datos local Nombre de usuario: **admin** Password: **admin1pass**	S1#enable S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#enable S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)# S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1>enable Password: Password: S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#service password-encryption S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console
Configurar un MOTD Banner	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#banner motd "Ingreso solo a personal autorizado" S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Generar una clave de cifrado RSA **Módulo de 1024 bits**	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (6), with S2 FastEthernet0/1 (1). %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (6), with S2 FastEthernet0/2 (1). % Incomplete command. S1(config)#ip domain-name S1.ccna-lab.com S1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S1.S1.ccna-lab.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *mar. 1 2:22:29.839: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)# %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (6), with S2 FastEthernet0/1 (1). %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (6), with S2 FastEthernet0/2 (1).

Tarea	Especificación
pvConfigurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface vlan1 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#no shut S1(config-if)#end S1# %SYS-5-CONFIG_I: Configured from console by console S1#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] S1#enable S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface vlan1 S1(config-if)#ipv6 enable S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#no shut S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#no shut S1(config-if)# S1(config-if)#exit S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by consoleto up
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S1(config)#ip default-gateway 10.19.8.97 S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console

- Para realizar y configurar el nombre del domino se debe utilizar el siguiente comando:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#host name S1
^
% Invalid input detected at '^' marker.
Switch(config)#hostname S1
S1(config)#
```

- Luego nos pide la contraseña en modo privilegiado de modo EXEC

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret ciscoenpass
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#exit
```

- Después me solicita generar una contraseña para ingreso a la consola, a continuación se realiza con los siguientes comandos:

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
```

- El siguiente punto solicita crear un nombre de usuario con una contraseña, para ingresar al switch y se muestra a continuación los comandos utilizados para configurar en esta punto:

```
S1#enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#username admin password admin1pass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
```

```
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#username admin password admin1pass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#enable
S1#exit
S1 con0 is now available
Press RETURN to get started.
```

- El ejercicio siguiente solicita que se debe configurar en el S1 la interfaz de administración SVI, el cual se realiza con los siguientes comandos para ipv4 fueron utilizado estos:

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#banner motd "Ingreo solo a personal autorizado"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#no shutdown
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]? ok
%Error copying nvram:ok (Invalid argument)
```

- En esta parte de configuracion vamos a realizar la configuracion de generación una clave de cifrado RSA donde nos informan que se debe dejr la configuracion de modulo de 1024 bits, a continuacion se utilizan los siguientes comandos:

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip domain-name S1.ccna-lab.com
S1(config)#crypto key generate rsa general-keys modulus 1024
% You already have RSA keys defined named S1.ccna-lab.com
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*mar. 1 1:29:44.605: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#username admin secret admin1pass
ERROR: Can not have both a user password and a user secret.
Please choose one or the other.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Configurar S2:

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch **S1 o S2, según proceda**	Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S2 S2(config)# S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console
Nombre de dominio **ccna-lab.com**	S2(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado **ciscoenpass**	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#enable secret ciscoenpass S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console
Contraseña de acceso a la consola **ciscoconpass**	S2>enable Password: S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#line console 0 S2(config-line)#login S2(config-line)#line vty 0 10 S2(config-line)#password ciscoconpass S2(config-line)#exit S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Crear un usuario administrativo en la base de datos local Nombre de usuario: **admin** Password: **admin1pass**	S2#enable S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#username admin password admin1pass S2(config)#line console 0 S2(config-line)#login local S2(config-line)#exit S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console S2#enable S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#username admin password admin1pass S2(config)#line console 0 S2(config-line)#login local S2(config-line)#exit S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)# S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#exit S2(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2>enable Password: Password: S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#service password-encryption S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console
Configurar un MOTD Banner	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#banner motd "Ingreso solo a personal autorizado" S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console
Generar una clave de cifrado RSA **Módulo de 1024 bits**	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#ip domain-name S1.ccna-lab.com S2(config)#crypto key generate rsa general-keys modulus 1024 % You already have RSA keys defined named S1.ccna-lab.com % They will be replaced. % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *mar. 1 1:29:44.605: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config)#username admin secret admin1pass ERROR: Can not have both a user password and a user secret. Please choose one or the other. S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface vlan1 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#no shut S2(config-if)#end S2# %SYS-5-CONFIG_I: Configured from console by console S2#copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] S2#enable S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface vlan1 S2(config-if)#ipv6 enable S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#no shut S2(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed S1(config-if)#ipv6 address FE80::98 link-local S2(config-if)#no shut S2(config-if)# S2(config-if)#exit S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by consoleto up
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S2(config)#ip default-gateway 10.19.8.97 S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console

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

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1>enable Password: S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 2 S1(config-vlan)#name bikes S1(config-vlan)#exit S1(config)# S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface F0/1 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S1(config-if)#switchport trunk native vlan 6 S1(config-if)#end S1# %SYS-5-CONFIG_I: Configured from console by console S1(config)#interface F0/2 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S1(config-if)#switchport trunk native vlan 6 S1(config-if)#end S1# %SYS-5-CONFIG_I: Configured from console by console exit S1>enable Password: S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface F0/5 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S1(config-if)#switchport trunk native vlan 6 S1(config-if)#end S1# %SYS-5-CONFIG_I: Configured from console by console exit

Tarea	Especificación
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)#interface range FastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1) %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down %EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (native vlan of Fa0/2 is 6, Po1 id 1) S1(config-if-range)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S1(config-if-range)#switchport trunk allowed vlan 1,2,20 S1(config-if-range)# %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1) %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1)

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int f0/6 S1(config-if)#switchport access vlan 2 S1(config-if)#switchport mode access S1(config-if)#end S1(config-if)#no shu S1# %SYS-5-CONFIG_I: Configured from console by console S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	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)#no shu S1(config-if)#exit
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int 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 "interface no utilizables" S1(config-if-range)#shutdown

- En este paso la configuración es nombrar cada una de las vlan en el S, Como se observa en los siguientes comandos:

S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 2
S1(config-vlan)#name bikes
S1(config-vlan)#exit
S1(config)#

Continua realizándose con cada una de las vlan hasta nombre la numero 6.

- En el siguiente punto se debe crear troncos que se utilicen la vlan 6 nativa, según lo que se logra identificar es que al realizar la configuración de las vlan, estas tienen unas troncales las cuales transmiten tráficos a diferentes partes de la red configurada en una vlan. Con esto se entiende que están troncales forman una configuración de enlaces los cuales transmiten el tráfico. Se utiliza los siguientes comandos:

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface F0/1
S1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Se utiliza para configurar cada uno de las interface, luego se procede a verificar.

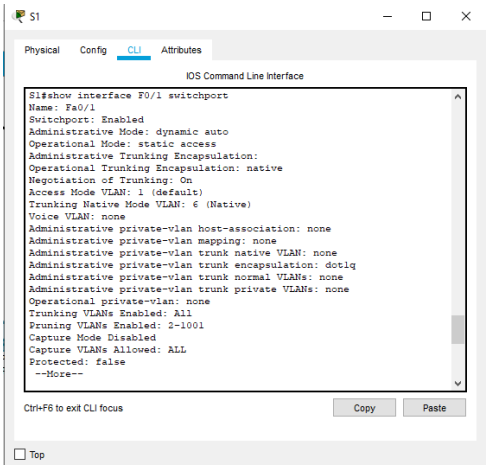


Ilustración 2A

- En este siguiente punto se realiza la configuración de ambos switch creando un grupo de puertos EthernetChannel de capa 2 que usa las interfaces F0/1, F0/2 con el protocolo LACP para negociación como se muestra en la siguiente configuración:

```
S1(config)#interface range FastEthernet 0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1)

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (native vlan of Fa0/2 is 6, Po1 id 1)
S1(config-if-range)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
S1(config-if-range)#switchport trunk allowed vlan 1,2,20
S1(config-if-range)#
%EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1)
%EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1)

- A continuación se realiza la respectiva configuración del puerto de acceso de host para la vlan2 en la interface F0/6 y se confirma:

S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range FastEthernet 0/6
S1(config-if-range)#switchport access vlan 2
S1(config-if-range)#switchport mode access
S1(config-if-range)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show running-config
Building configuration...

Current configuration : 1915 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!

!
enable secret 5 1mERr$EJnmB234UvJf9yoQMWYJK/
!
interface FastEthernet0/6
switchport access vlan 2
--More—

Paso 6: Configure el S2.

Se realiza los mismos comandos para las configuraciones en el S2 con algunos cambios en las interfaces y en las vlans

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2>enable Password: S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#name bikes S2(config)#vlan 2 S2(config-vlan)#name bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2#conf t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface F0/1 S2(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S2(config-if)#switchport trunk native vlan 6 S2(config-if)#end S2# %SYS-5-CONFIG_I: Configured from console by console exit
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 t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface F0/2 S2(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode. S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#end S2# %SYS-5-CONFIG_I: Configured from console by console
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int f0/18 S2(config-if)#switchport access vlan 3 S2(config-if)#switchport mode access S2(config-if)#end S2# %SYS-5-CONFIG_I: Configured from console by console

Tarea	Especificación
Configure port-security en los access ports permite 3 MAC addresses	S2# S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int range F0/1-3 S2(config-if-range)#switch mode access S2(config-if-range)#switchport port-security S2(config-if-range)#switch port-security maximum 3 S2(config-if-range)#switchport port-security violation shutdown S2(config-if-range)#switchport port-security mac-address sticky S2(config-if-range)#exit S2(config)#exit S2# %SYS-5-CONFIG_I: Configured from console by console
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2#config t Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int f0/18 S2(config-if)#no shu S2(config-if)#exit S2(config)#int range f0/3-17,f0/19-24,g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description "interfce no utilizables" S2(config-if-range)#shutdown

- En este ultimo punto de la configuracion nos solictan asignar a vlan 5 las interface no utilizadas y apagar se utiizan los comandos mencionados en la tabla de información:

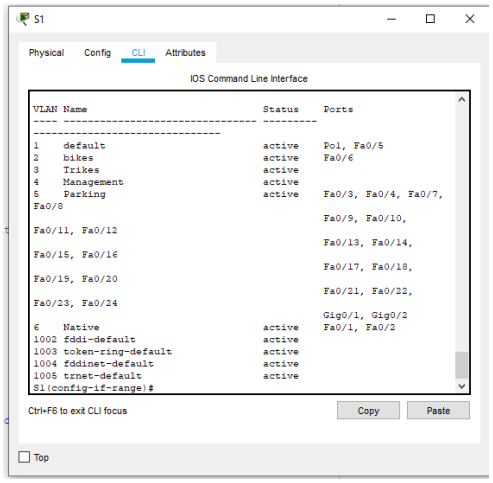


Ilustración 6A

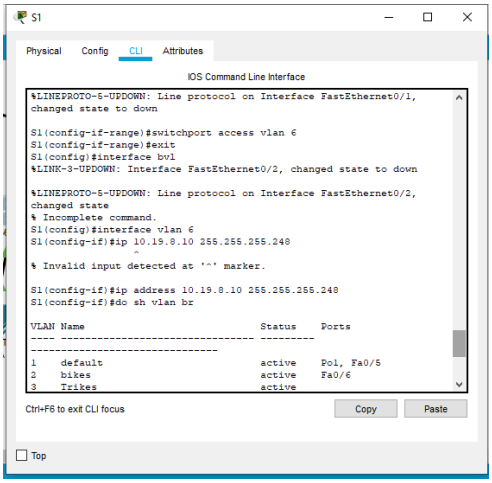


Ilustración 4A

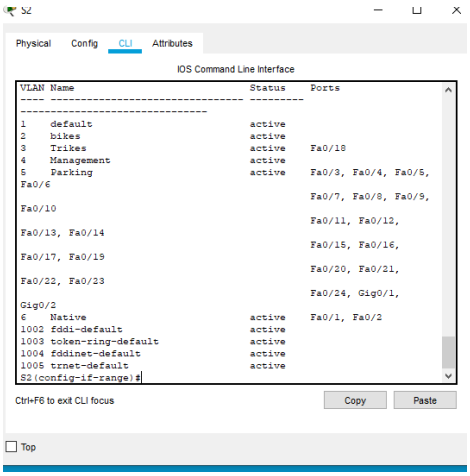


Ilustración 5A

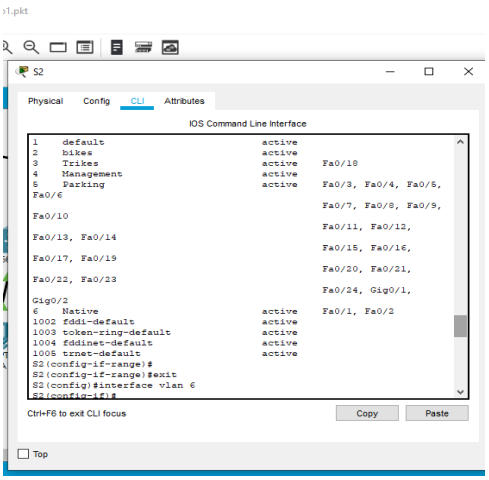


Ilustración 3A

En la siguiente imagen se observa, comando utilizado para Usar el protocolo LACP para la negociación:

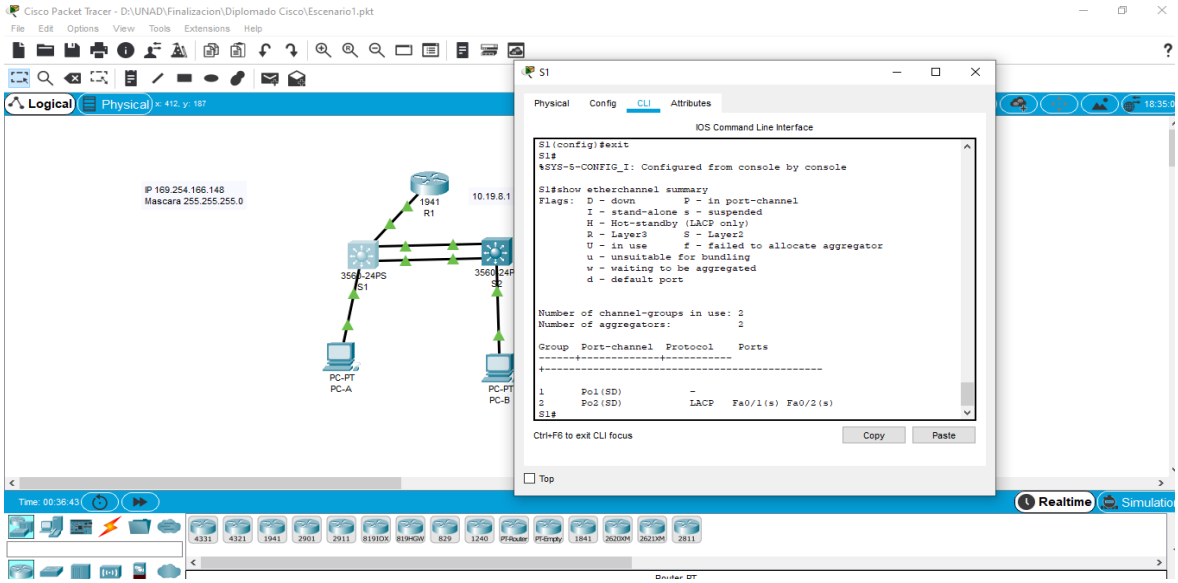


Ilustración 7A

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/0/1 R1(config-if)#ipv6 enable R1(config-if)#int g0/0/1.2 R1(config-subif)#no shutdown R1(config-subif)#encapsulation dot1q2 ^ % Invalid input detected at '^' marker. R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#exit R1(config)#int g0/0/1.2 R1(config-subif)#no shutdown 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::1/64 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#int 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)#n shutdown R1(config-subif)#exit R1(config)#int g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#10.19.8.97 255.255.255.248 ^ % Invalid input detected at '^' marker. 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)#no shutdown R1(config-subif)#exit R1(config)#int g0/0/1.6 R1(config-subif)#
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 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)#ip dhcp excluded-address 10.19.8.2 10.19.8.51 R1(config)#

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 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-a.net R1(dhcp-config)#ip dhcp excluded-address 10.19.8.66 10.19.8.83 R1(config)#

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	Se realiza la configuracion haciendo click en generación automática en DHCP
Dirección física	0001.9636.2509
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	2001:db8:acad:a::50/64

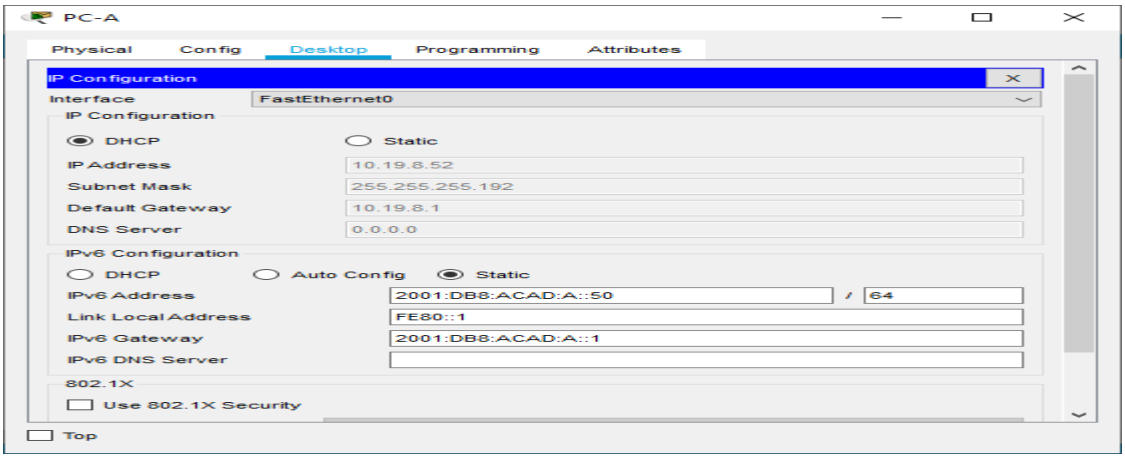


Ilustración 8A

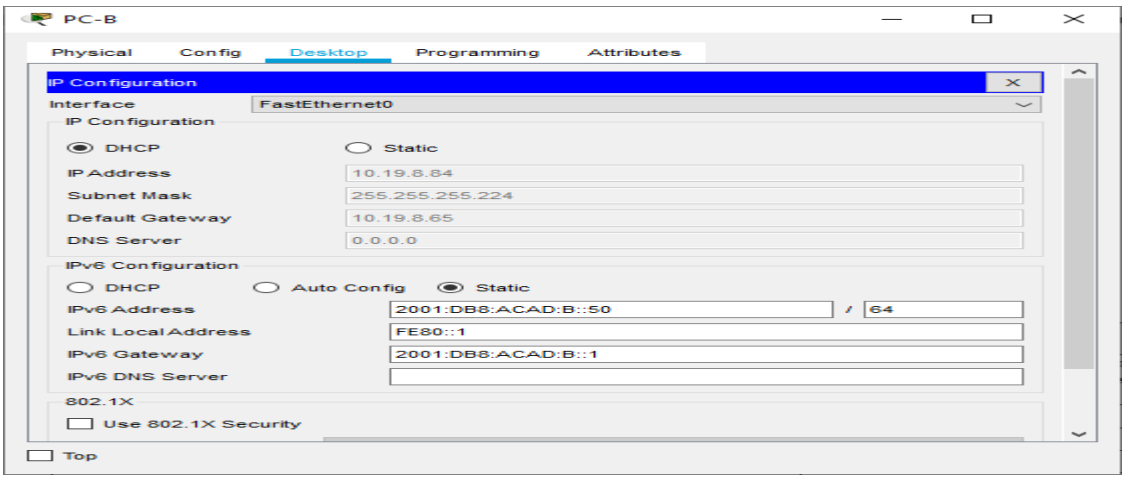
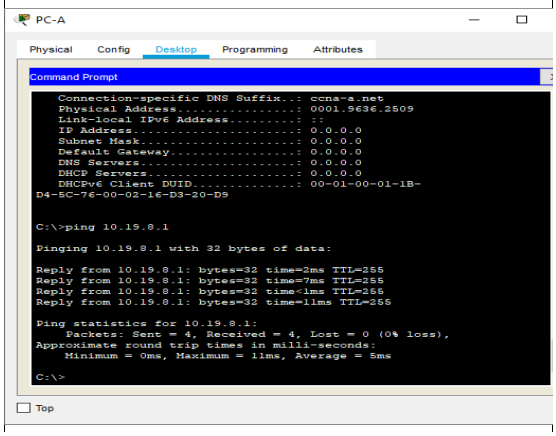
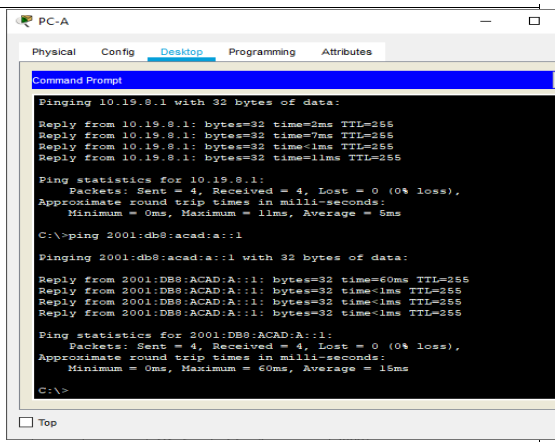


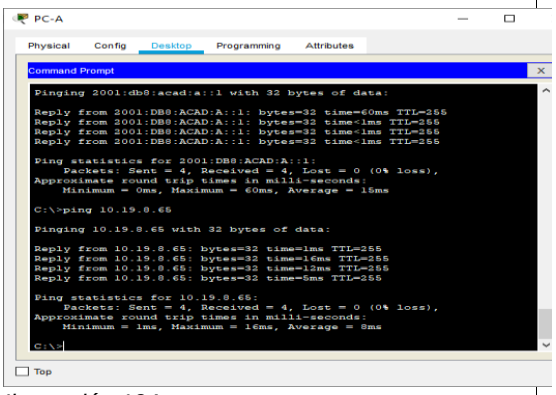
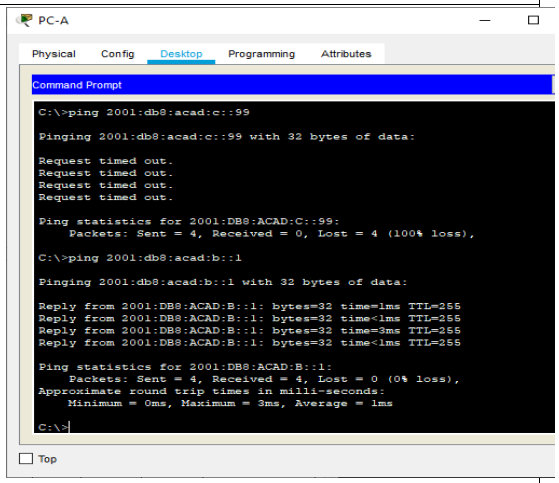
Ilustración 9A

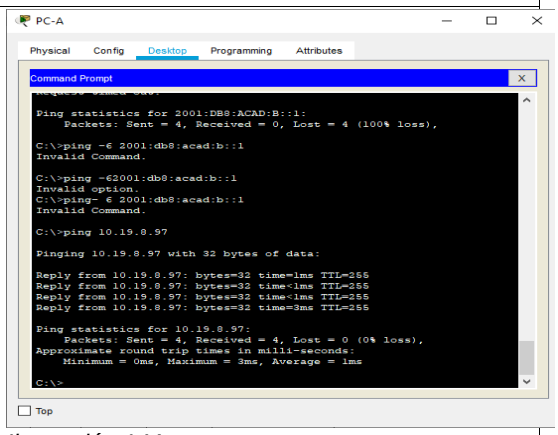
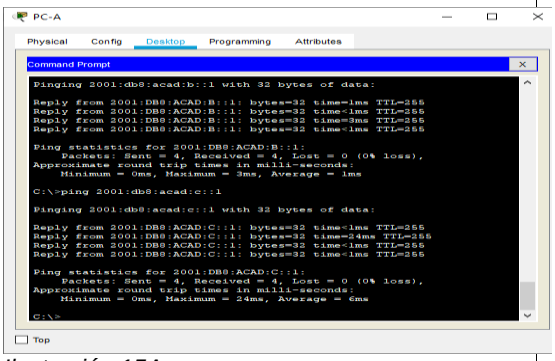
Configuración de red de PC-B	
Descripción	Se realiza la configuracion haciendo click en generación automática en DHCP
Dirección física	000A.41B8.4368
Dirección IP	10.19.8.84
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65

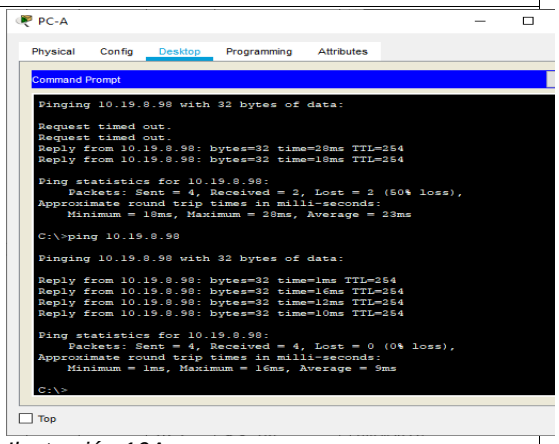
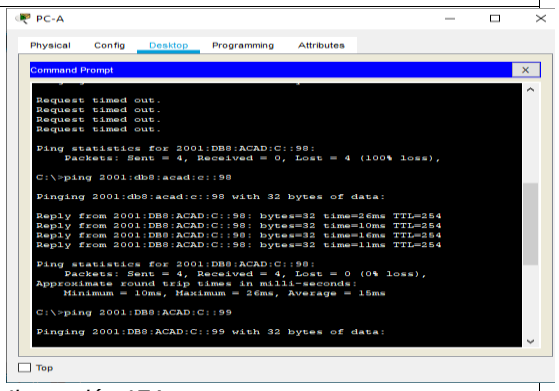
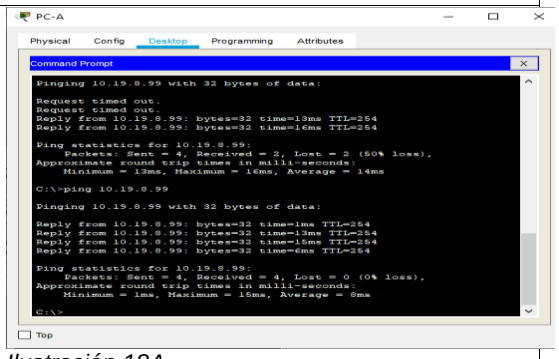
Configuración de red de PC-B	
Gateway predeterminado IPv6	2001:DB8:ACAD:B::50/64

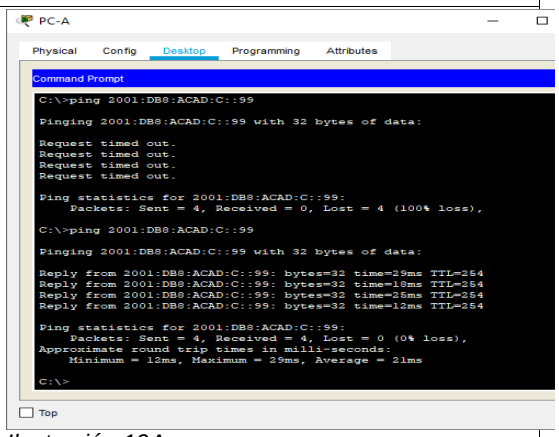
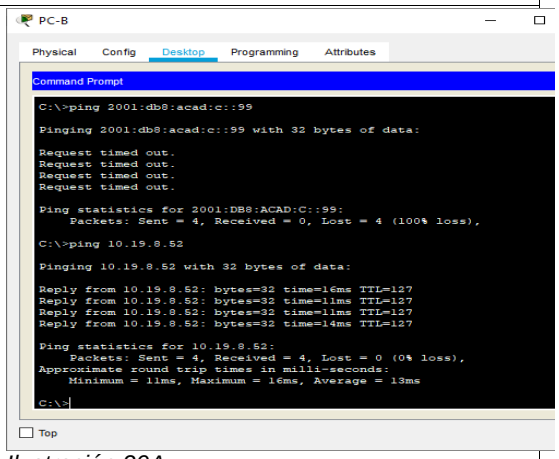
Parte 3: En este punto s deben realizar los ping en el PC-A ingrea por la interface de command prompt digita ping numero ip, como se muestra a continuación:

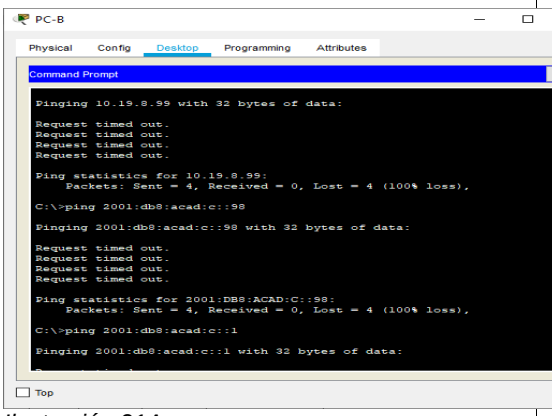
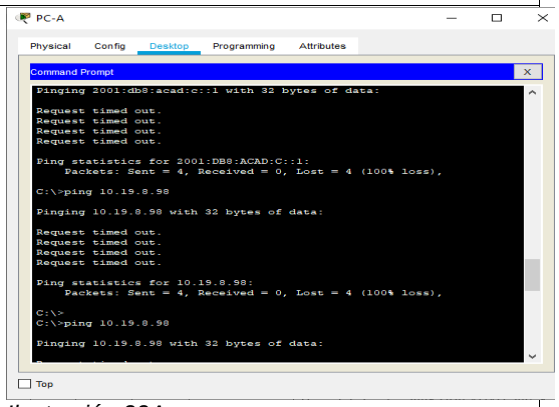
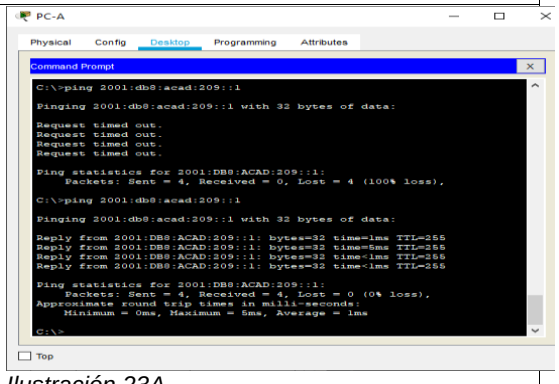
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	 *Ilustración 10A*
		IPv6	2001:db8:acad:a: :1	 *Ilustración 11A*

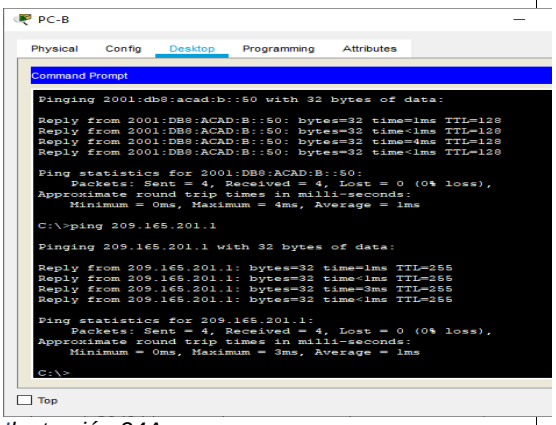
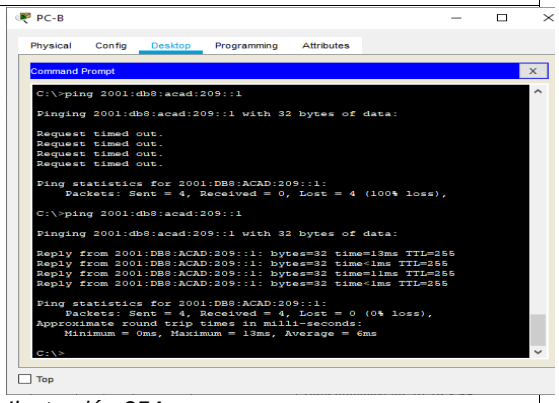
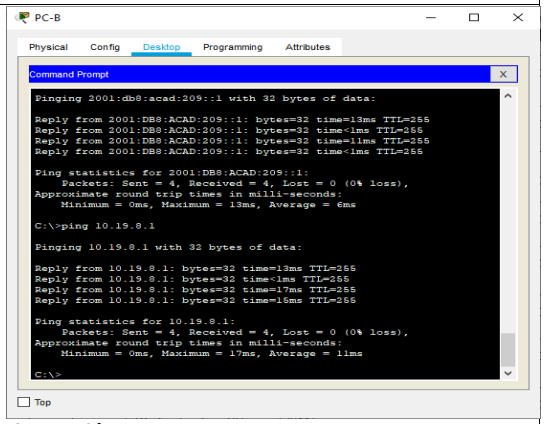
Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	 *Ilustración 12A*
		IPv6	2001:db8:acad:b: :1	 *Ilustración 13A*

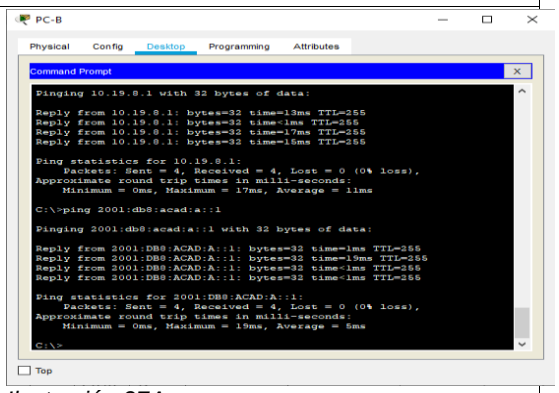
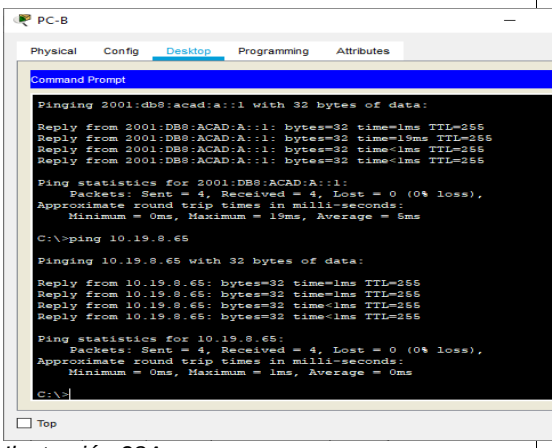
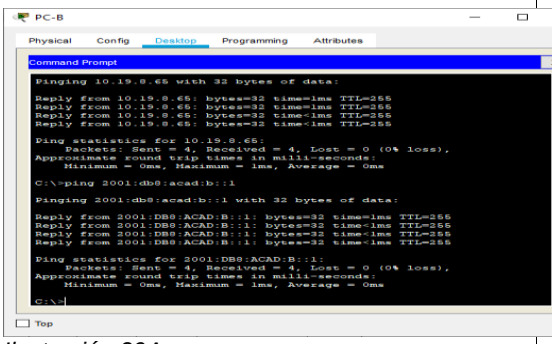
Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	 *Ilustración 14A*
		IPv6	2001:db8:acad:c: :1	 *Ilustración 15A*

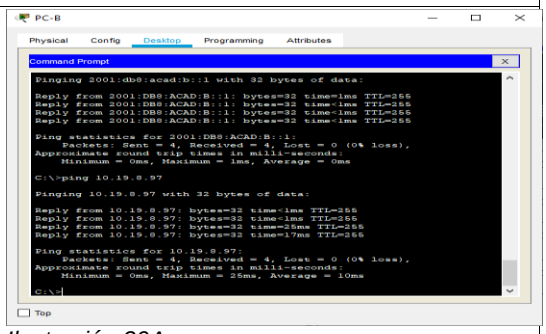
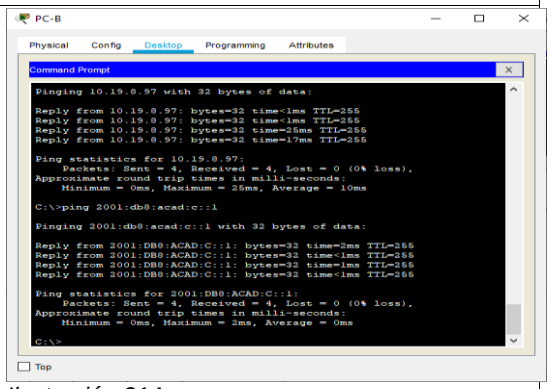
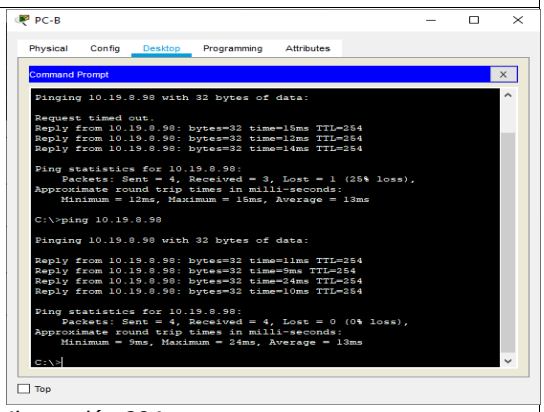
Desde	A	de Internet	Dirección IP	Resultados de ping
	S1, VLAN 4	Dirección	10.19.8.98	 *Ilustración 16A*
		IPv6	2001:db8:acad: c: :98	 *Ilustración 17A*
	S2, VLAN 4	Dirección	10.19.8.99	 *Ilustración 18A*

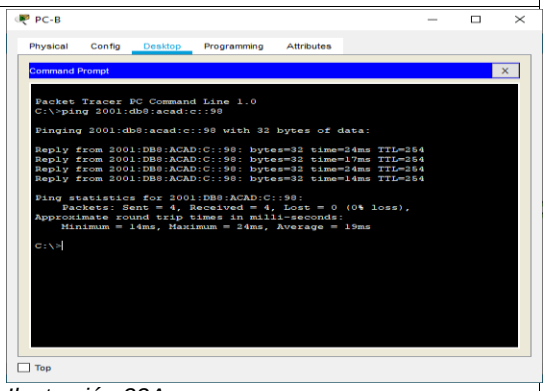
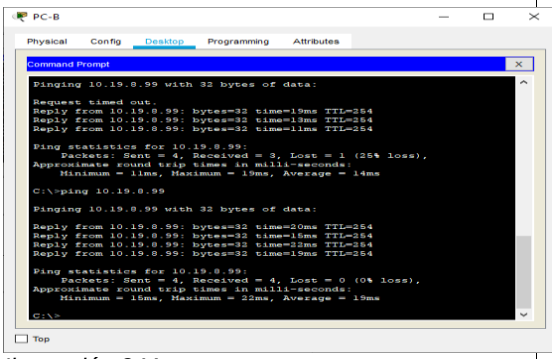
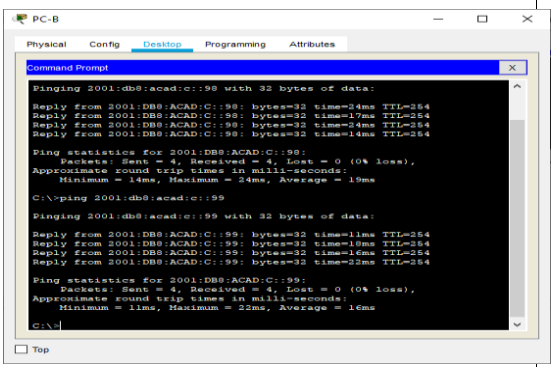
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c: :99	 *Ilustración 19A*
	PC-B	Dirección	*10.19.8.52*	 *Ilustración 20A*

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b: :50	 *Ilustración 21A*
	R1 Bucle 0	Dirección	209.165.201.1	 *Ilustración 22A*
		IPv6	2001:db8:acad:209: :1	 *Ilustración 23A*

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1 Bucle 0	Dirección	209.165.201.1	 *Ilustración 24A*
		IPv6	2001:db8:acad:209: :1	 *Ilustración 25A*
	R1, G0/0/1.2	Dirección	10.19.8.1	 *Ilustración 26A*

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:a: :1	 *Ilustración 27A*
	R1, G0/0/1.3	Dirección	10.19.8.65	 *Ilustración 28A*
		IPv6	2001:db8:acad:b: :1	 *Ilustración 29A*

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	 *Ilustración 30A*
		IPv6	2001:db8:acad:c: :1	 *Ilustración 31A*
	S1, VLAN 4	Dirección	10.19.8.98	 *Ilustración 32A*

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c: :98	 *Ilustración 33A*
	S2, VLAN 4	Dirección	10.19.8.99.	 *Ilustración 34A*
		IPv6	2001:db8:acad:c: :99	 *Ilustración 35A*

- ESCENARIO 2

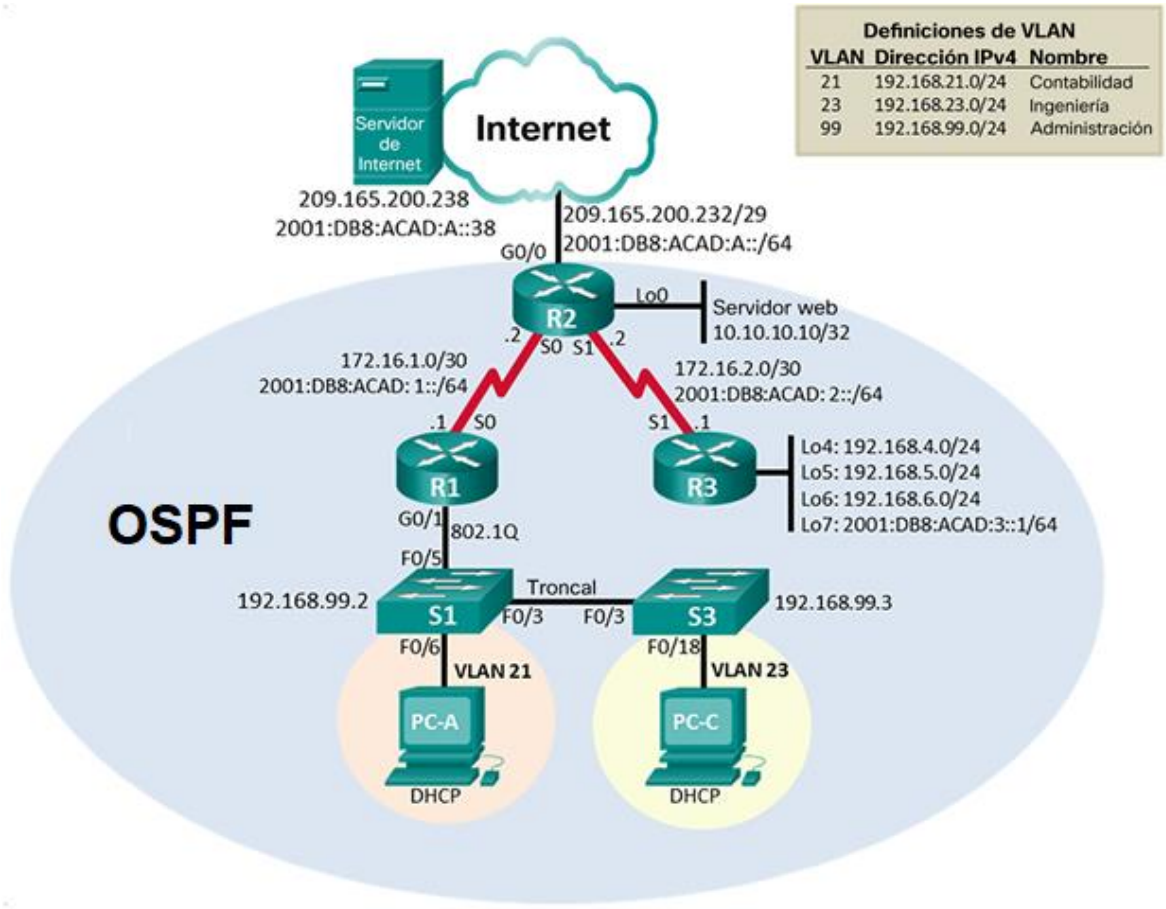


Ilustración 36A

Topologia Propuesta

- Parte 1: En esta parte solicita inicializar los dispositivos, en donde se vuelve a cargar los routers y switchs.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable 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

Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 2010 by cisco Systems, Inc. Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB CISCO1941/K9 platform with 524288 Kbytes of main memory Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled Readonly ROMMON initialized
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	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
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] C3560 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: 0001.64D9.0E01 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"... ## [OK]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash System flash directory: File Length Name/status 3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin 2 28282 sigdef-category.xml

	1 227537 sigdef-default.xml [8918011 bytes used, 55098373 available, 64016384 total] 63488K bytes of processor board System flash (Read/Write)

- **Parte 2:** En esta parte solicitan configurar los parametros basicos de los dispositivos.

Paso 1: Configurar la computadora de internet.

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
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: En Este paso solicitan configurar el R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(1)(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 console 0 R1(config-line)#password cisco
Contraseña de acceso Telnet	R1(config-line)#login R1(config-line)#line vty 0 15 R1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R1(config-line)#login R1(config-line)#service password-encryption R1(config)#
Mensaje MOTD	R1(config)#banner motd "Se pronibe el acceso no autorizado" R1(config)#

Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config)#int s0/0/0 R1(config-if)#description connection to 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 %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config-if)#exit R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Paso 3: Configurar R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco
Contraseña de acceso Telnet	R2(config-line)#login R2(config-line)#line vty 0 15 R2(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R2(config-line)#login R2(config-line)#serrvice password-encryption
Habilitar el servidor HTTP	

Mensaje MOTD	R2(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Interfaz S0/0/1 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config-if)#exit R2(config)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.1.2 255.255.255.252 % 172.16.1.0 overlaps with Serial0/0/0 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down R2(config-if)#
Interfaz G0/0 (simulación de Internet) Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config)#int g0/0 R2(config-if)#description connection to Internet R2(config-if)#ip address 209.165.200.238 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Interfaz loopback 0 (servidor web simulado) Establecer la descripción. Establezca la dirección IPv4.	R2(config)#interface loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#description server web R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#

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 console 0 R3(config-line)#password cisco
Contraseña de acceso Telnet	R3(config-line)#login R3(config-line)#line vty 0 15 R3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R3(config-line)#login R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Se prohibe el acceso no autorizado"

Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 4 R3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config-if)#int loopback 6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config-if)#int loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit

Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 %Default route without gateway, if not a point-to-point interface, may impact performanceR3(config)#ipv6 route ::/0 s0/0/1 R3(config)#

Paso 5: Configurar S1

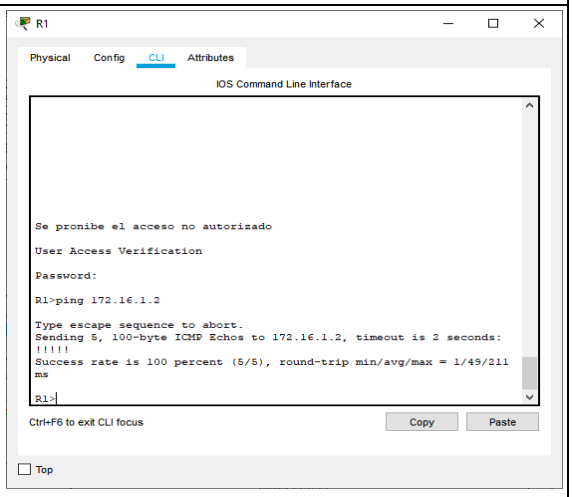
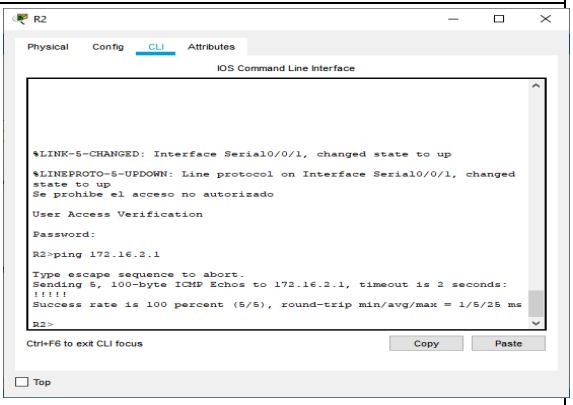
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco
Contraseña de acceso Telnet	S1(config-line)#login S1(config-line)#line vty 0 15 S1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S1(config-line)#login S1(config-line)#service password-Encryption
Mensaje MOTD	S1(config)#banner motd "Se prohibe el acceso no autorizado"

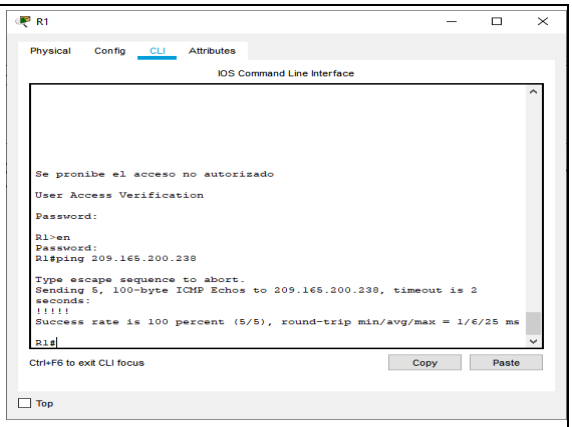
Pase 6: Cnfigurar el S3

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 console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	S3(config-line)#login S3(config-line)#line vty 0 15 S3(config-line)#password cisco

Cifrar las contraseñas de texto no cifrado	S3(config-line)#login S3(config-line)#service password-Encryption
Mensaje MOTD	S3(config)#banner motd "Se prohibe el acceso no autorizado"

Paso 7: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	 *Ilustración 37A*
R2	R3, S0/0/1	172.16.2.1	 *Ilustración 38A*

PC de Internet	Gateway predeterminado	209.165.200.238	 *Ilustración 39A*

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: Cnfigurar S1

Elemento o tarea de configuración	Especificación
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>enable Password: Password: Password: S1#config t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit S1(config)#

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)# %LINK-5-CHANGED: Interface Vlan99, changed state to up ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
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
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
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
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

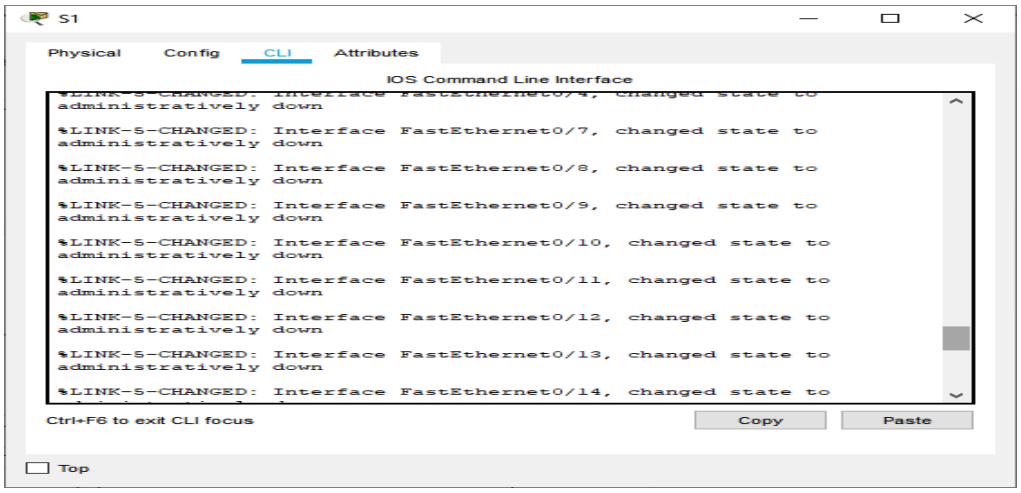


Ilustración 40A

Paso 2: Configurar el S3

Elemento o tarea de configuración	Especificación
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>enable Password: Password: S3#config t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
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)# %LINK-5-CHANGED: Interface Vlan99, changed state to up ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit

Asignar el gateway predeterminado. Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
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
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

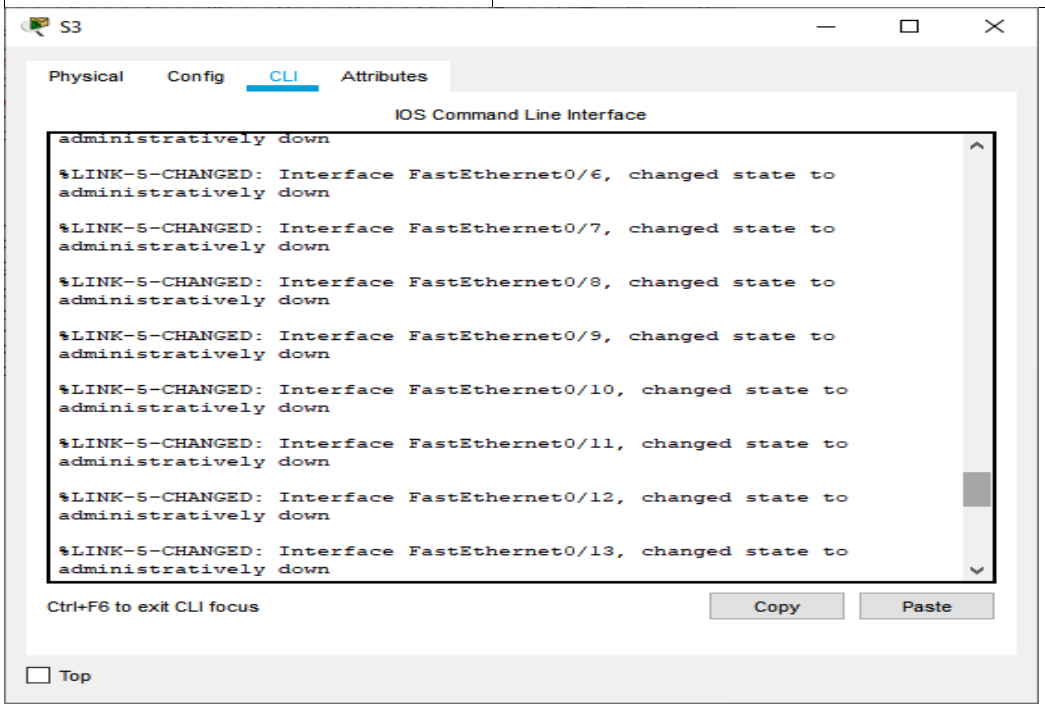


Ilustración 41A

Paso 3: Configurar R1

Elemento o tarea de configuración	Especificación
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>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
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)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 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)#description LAN de administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown

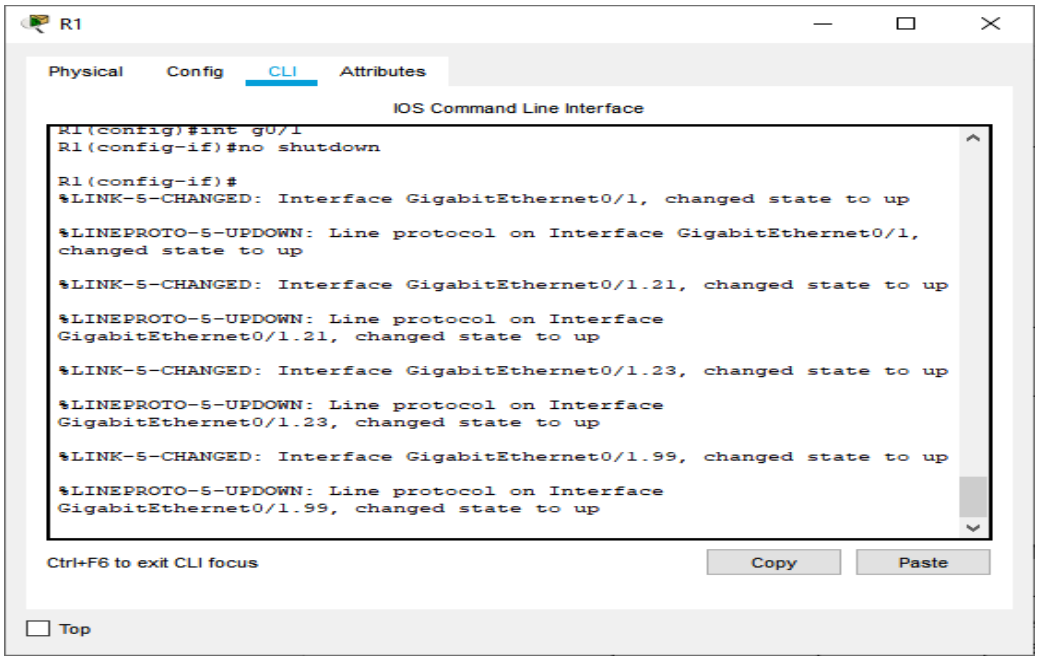


Ilustración 42A

Paso 4: Verificar la conectividad

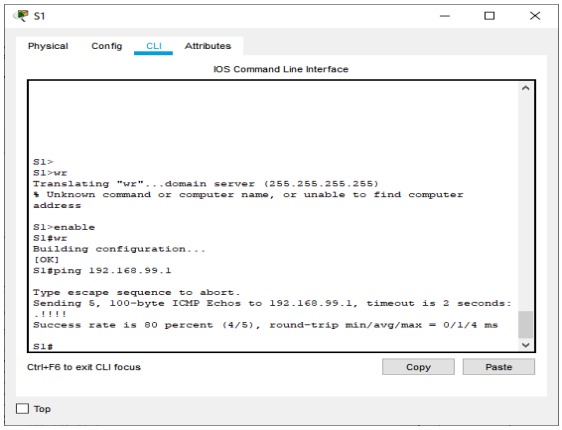
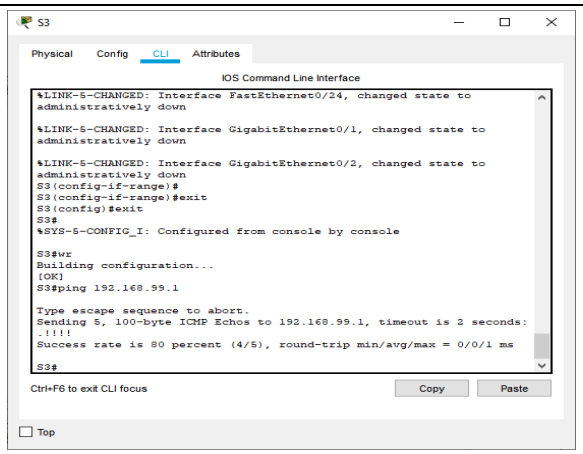
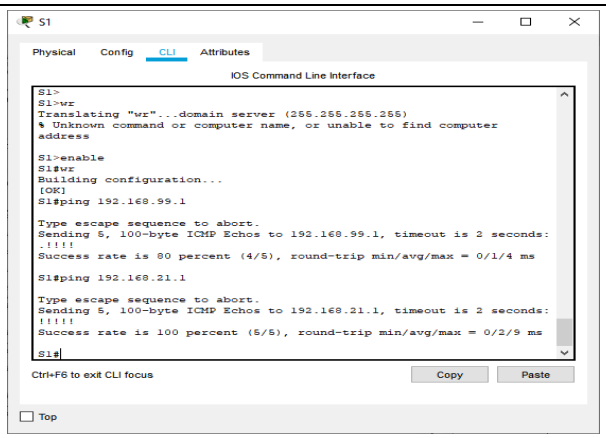
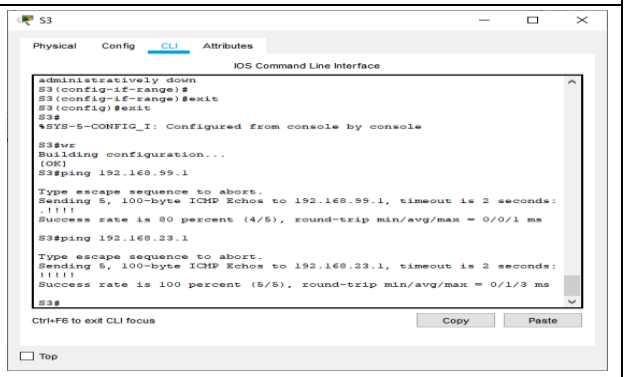
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	

Ilustración 43A

S3	R1, dirección VLAN 99	192.168.99.1	 *Ilustración 44A*
S1	R1, dirección VLAN 21	192.168.21.1	 *Ilustración 45A*
S3	R1, dirección VLAN 23	192.168.23.1	 *Ilustración 46A*

Parte 4: Configurar el protocolo de routing dinamico OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	R1(config-router)#network 192.168.99.1 0.0.0.0 area 0 R1(config-router)#network 192.168.23.1 0.0.0.0 area 0 R1(config-router)#network 192.168.21.1 0.0.0.0 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 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	No Aplica

Se realiza configuracion del OSPFv3 EN R1

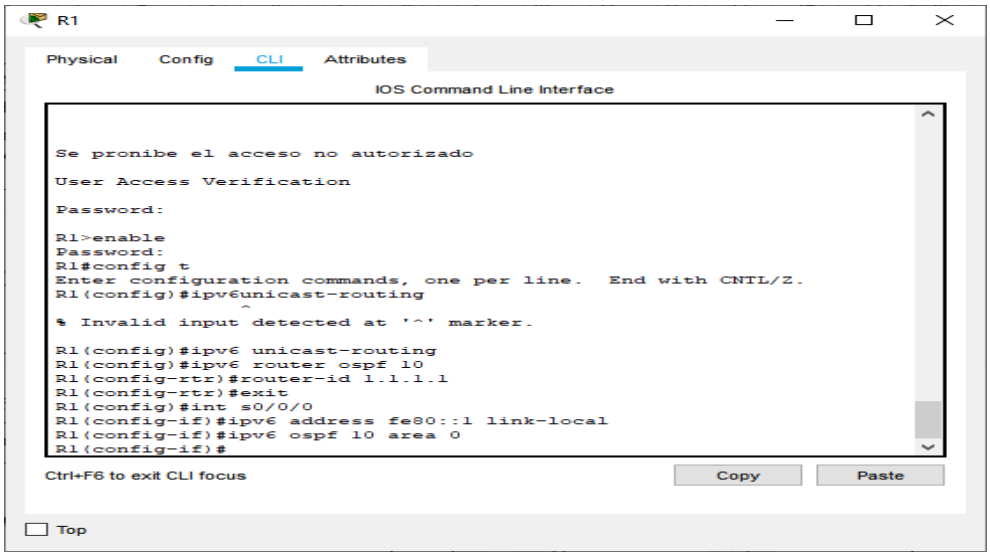


Ilustración 47A

Paso 2: Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2>enable Password: Password: R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2
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 18:17:45: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No Aplica

Paso 3: Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#ipv6 unicast-routing R2(config)#int g0/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#int s0/0/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#int s0/0/1 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#ipv6 router ospf 10 R2(config-rtr)#router-id 2.2.2.2 R2(config-rtr)#auto-cost reference-bandwidth 1000 % OSPF: Reference bandwidth is changed. Please ensure reference bandwidth is consistent across all routers.
Anunciar redes IPv4 conectadas directamente	R2(config)#interface g0/0 R2(config-if)#ipv6 ospf 10 % Incomplete command. R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#int s0/0/0 R2(config-if)#ipv6 ospf 10 area 0 18:32:32: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done R2(config-if)#int s0/0/1 R2(config-if)#ipv6 ospf 10 area 0 R2(config-if)#end R2# %SYS-5-CONFIG_I: Configured from console by console
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config)#router ospf 10 R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No Aplica

Se configura el SOPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3>EN R3#CONFIG T Enter configuration commands, one per line. End with CNTL/Z. R3(config)#router ospf 10 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)# 22:34:02: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/1/0 from LOADING to FULL, Loading Done R3(config-router)#network 192.168.4.1 0.0.0.0 area 0 R3(config-router)#network 192.168.5.1 0.0.0.0 area 0 R3(config-router)#network 192.168.6.1 0.0.0.0 area 0
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
Desactive la sumarización automática.	No Aplica

Se configura OSPFv3 en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 10 R3(config-rtr)#router-id 3.3.3.3

Anunciar redes IPv6 conectadas directamente	R3(config)#int s0/0/1 R3(config-if)#ipv6 ospf 10 area 0 R3(config-if)# 23:03:43: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/1/0 from LOADING to FULL, Loading Done R3(config-if)#ipv6 address fe80::3 link-local R3(config-if)# 23:04:04: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/1/0 from LOADING to FULL, Loading Done R3(config)#interface loopback 7 R3(config-if)#ipv6 address fe80::3 link-local R3(config-if)#ipv6 ospf 10 area 0
Establecer todas las interfaces de LAN IPv6 (Loopback) como pasivas	R3(config)#ipv6 router ospf 10 R3(config-rtr)#passive-interface loopback 7
Desactive la sumarización automática.	No Aplica

Paso 4: Verificar la información de OSPF R1

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?	Password: R1>enable Password: R1#show ip protocols Routing Protocol is "ospf 10" 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: 192.168.99.1 0.0.0.0 area 0 192.168.23.1 0.0.0.0 area 0 192.168.21.1 0.0.0.0 area 0 172.16.1.0 0.0.0.3 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 00:10:28 2.2.2.2 110 00:13:25 3.3.3.3 110 00:12:10 Distance: (default is 110)
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf 10.0.0.0/32 is subnetted, 1 subnets O 10.10.10.10 [110/65] via 172.16.1.2, 00:40:14, Serial0/0/0 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks O 172.16.2.0 [110/128] via 172.16.1.2, 00:40:41, Serial0/0/0 192.168.4.0/32 is subnetted, 1 subnets O 192.168.4.1 [110/129] via 172.16.1.2, 00:14:06, Serial0/0/0 192.168.5.0/32 is subnetted, 1 subnets O 192.168.5.1 [110/129] via 172.16.1.2, 00:13:46, Serial0/0/0 192.168.6.0/32 is subnetted, 1 subnets O 192.168.6.1 [110/129] via 172.16.1.2, 00:13:24, Serial0/0/0
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip ospf Routing Process "ospf 10" with ID 1.1.1.1 Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 1. 1 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 3 Area has no authentication SPF algorithm executed 11 times Area ranges are Number of LSA 3. Checksum Sum 0x00a59f Number of opaque link LSA 0. Checksum Sum 0x000000 Number of DCbitless LSA 0 Number of indication LSA 0 Number of DoNotAge LSA 0

	Flood list length 0

Verificar OSPF R2

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?	R2#show ip protocols Routing Protocol is "ospf 10" 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 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 172.16.1.0 0.0.0.3 area 0 172.16.2.0 0.0.0.3 area 0 10.10.10.10 0.0.0.0 area 0 Passive Interface(s): Loopback0 Routing Information Sources: Gateway Distance Last Update 1.1.1.1 110 00:19:09 2.2.2.2 110 00:22:06 3.3.3.3 110 00:20:51 Distance: (default is 110)
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf 192.168.4.0/32 is subnetted, 1 subnets O 192.168.4.1 [110/65] via 172.16.2.1, 00:22:28, Serial0/0/1 192.168.5.0/32 is subnetted, 1 subnets O 192.168.5.1 [110/65] via 172.16.2.1, 00:22:08, Serial0/0/1 192.168.6.0/32 is subnetted, 1 subnets O 192.168.6.1 [110/65] via 172.16.2.1, 00:21:46, Serial0/0/1 O 192.168.21.0 [110/65] via 172.16.1.1, 00:50:10, Serial0/0/0 O 192.168.99.0 [110/65] via 172.16.1.1, 00:50:10, Serial0/0/0
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show ip ospf Routing Process "ospf 10" with ID 2.2.2.2 Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs

	Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 1. 1 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 3 Area has no authentication SPF algorithm executed 9 times Area ranges are Number of LSA 3. Checksum Sum 0x00a59f Number of opaque link LSA 0. Checksum Sum 0x000000 Number of DCbitless LSA 0 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0

Verifcar OSPF 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?	R3#show ip protocols Routing Protocol is "ospf 10" 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 1. 1 normal 0 stub 0 nssa Maximum path: 4 Routing for Networks: 172.16.2.0 0.0.0.3 area 0 192.168.4.1 0.0.0.0 area 0 192.168.5.1 0.0.0.0 area 0 192.168.6.1 0.0.0.0 area 0 Passive Interface(s): Loopback4 Loopback5 Loopback6 Routing Information Sources: Gateway Distance Last Update 1.1.1.1 110 00:22:53 2.2.2.2 110 00:25:50 3.3.3.3 110 00:24:35

	Distance: (default is 110)
¿Qué comando muestra solo las rutas OSPF?	R3#show ip route ospf 10.0.0.0/32 is subnetted, 1 subnets O 10.10.10.10 [110/65] via 172.16.2.2, 00:26:55, Serial0/0/1 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks O 172.16.1.0 [110/128] via 172.16.2.2, 00:26:55, Serial0/0/1 O 192.168.21.0 [110/129] via 172.16.2.2, 00:26:55, Serial0/0/1 O 192.168.99.0 [110/129] via 172.16.2.2, 00:26:55, Serial0/0/1
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#show ip ospf Routing Process "ospf 10" with ID 3.3.3.3 Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of DCbitless external and opaque AS LSA 0 Number of DoNotAge external and opaque AS LSA 0 Number of areas in this router is 1. 1 normal 0 stub 0 nssa External flood list length 0 Area BACKBONE(0) Number of interfaces in this area is 4 Area has no authentication SPF algorithm executed 5 times Area ranges are Number of LSA 3. Checksum Sum 0x00a59f Number of opaque link LSA 0. Checksum Sum 0x000000 Number of DCbitless LSA 0 Number of indication LSA 0 Number of DoNotAge LSA 0 Flood list length 0

Parte 5: Implementar DHCP y NAT para ipv4

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

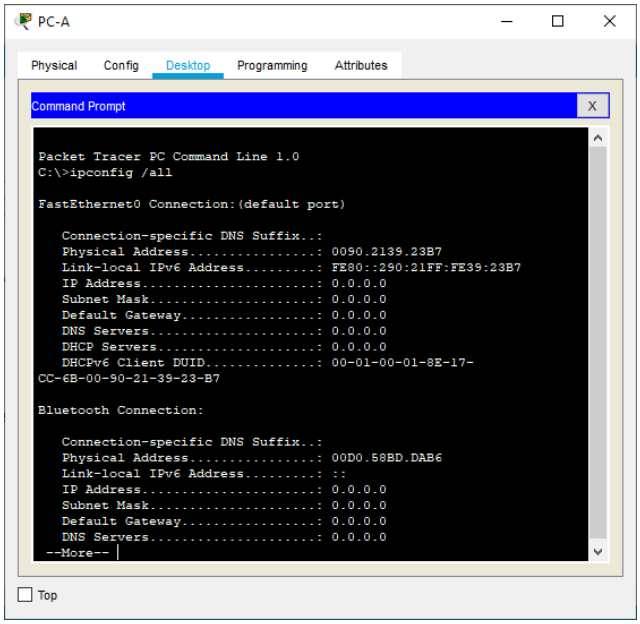
Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Password: Password: R1>enable Password: R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.231.1 192.168.23.20
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)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 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)#end R1# %SYS-5-CONFIG_I: Configured from console by console
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 t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#end R1# %SYS-5-CONFIG_I: Configured from console by console

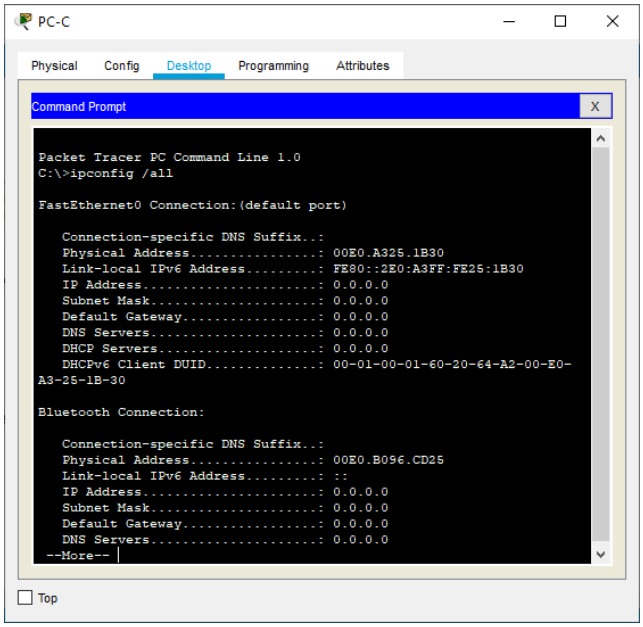
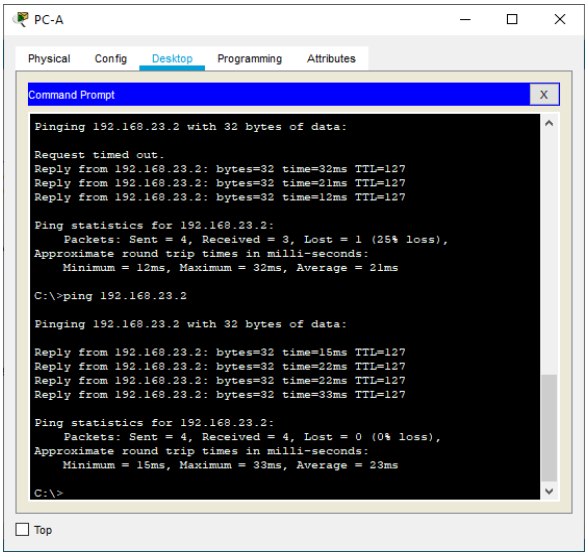
Paso 2: Configurar la NAT estatica y dinámica en el R2

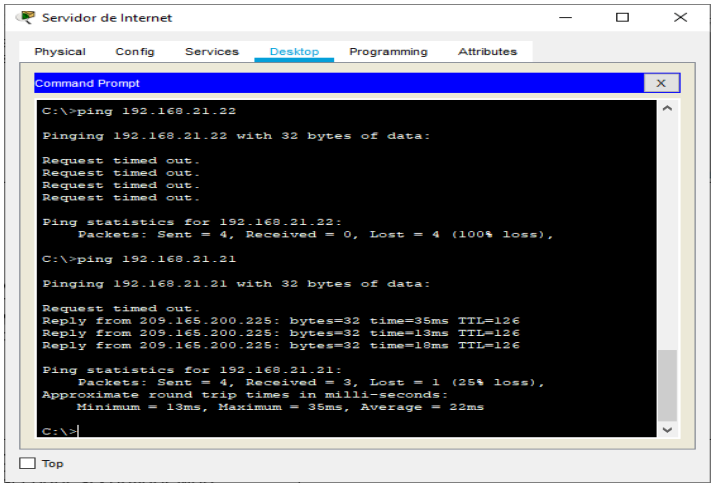
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	Password: R2>enable Password: R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#username webuser privilege 15 secret cisco12345 R2(config)#
Habilitar el servicio del servidor HTTP	Comando ip http server con es compatible con el simulador Packet Tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Comando ip http authentication local server con es compatible con el simulador Packet Tracer
Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.229**	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	Password: R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#int lo 0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#
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	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 R2(config)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#

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**	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 R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#

Paso 3: Verificar el protocolo DHCP y la NAT estática

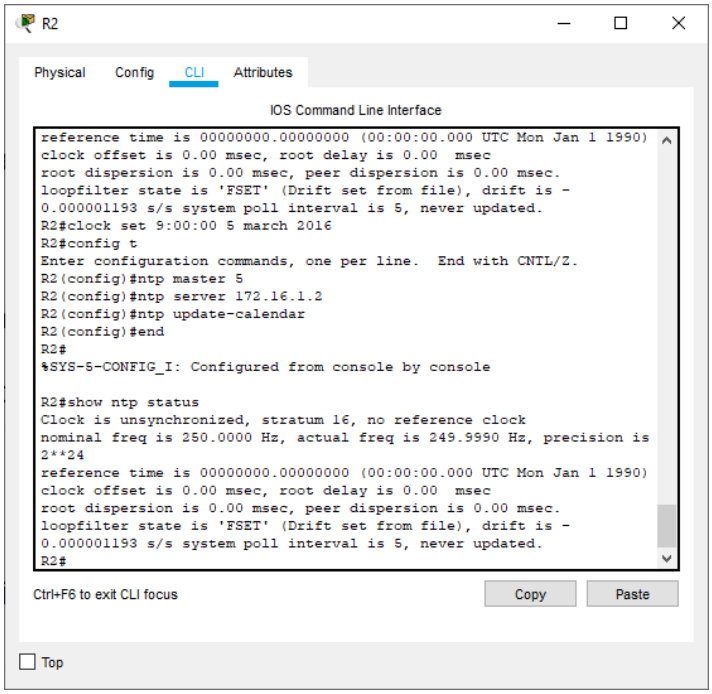
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 *Ilustración 48A*

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 *Ilustración 49A*
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 *Ilustración 50A*

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**	 *Ilustración 51A*

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. 5 de marzo de 2016, 9 a. m.	R2>enable Password: R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP. Nivel de estrato: **5**	R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: **R2**	R2(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#ntp update-calendar

Verifique la configuración de NTP en R1.	 *Ilustración 52A*

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

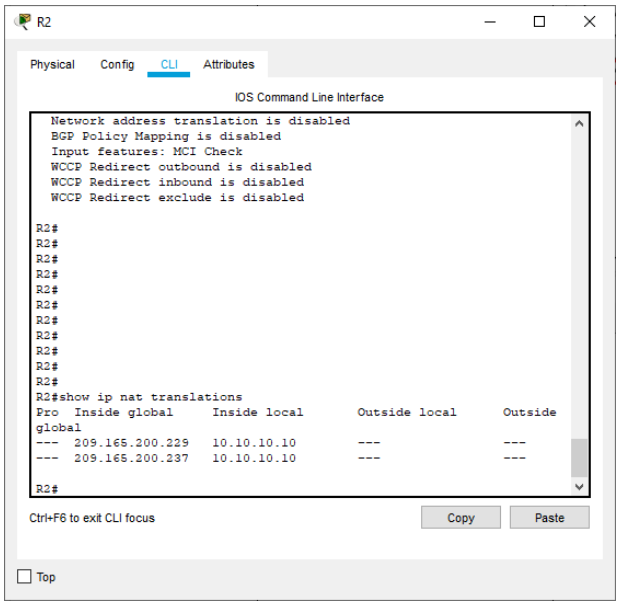
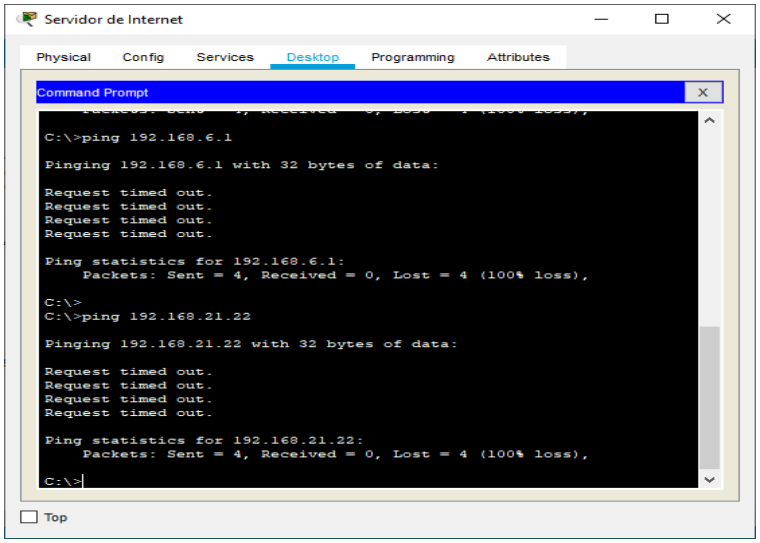
Paso 1: Restringir el acceso líneas vty en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: **ADMIN-MGT**	R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#end R2# %SYS-5-CONFIG_I: Configured from console by console
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in

Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1>enable Password: R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohibe el acceso no autorizado User Access Verification R2#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host

Paso 2: Introducir el comando de CLI adecuado:

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.5.0 0.0.0.255 30 permit 192.168.6.0 0.0.0.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es))
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface Nombre de interface Ejemplo: R2#show ip interface g0/0 GigabitEthernet0/0 is up, line protocol is up (connected) Internet address is 209.165.200.238/29 Broadcast address is 255.255.255.255 Address determined by setup command

¿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.	 *Ilustración 53A*  *Ilustración 54A*
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

2 CONCLUSION

En el primer escenario se desarrolla la parametrización de los switchs administrables para asigancion de las diferentes Vlans, y configuracion de los dispositivos de una red, desactivar aquellas interfaces no utilizables. Se realiza la configuracion de establecer privilegios en las ejecuciones de comandos, también se establecio usuario y contraseña para el ingreso y configuracion de los dispositivos como el router y los switch. Se implementa el uso de troncales para una adecuada conectividad y un mejor funcionamiento en la red.

En el segundo escenario tuvo un desarrollo parecido al primero ya que también hay parametrización de los switchs administrables, asignación de las diferentes Vlans, también se implementaron protocolos como son DHCP y NAT. Se desactivan aquellas interfaces no utilizables y se realiza configuracion de contraseña para ingreso a los diferentes dispositivos. Para lograr el buen funcionamiento de la red implementando una buena conectividad y comunicación entre los equipos de esta red, garantizando la seguridad de la información manejada en la red.

Aunque se recibió un acompañamiento por parte del tutor, se puede mejorar propiciando más encuentros el cual brinde mejor herramientas para desarrollar este tipo de escenarios ya que se maneja una complejidad que requiere explicaciones más minuciosas.

BIBLIOGRAFÍA

GARCIA FRANKLIN, Diseño de una Red en Packet Tracer con Switch y PC [En línea] Disponible en:
https://www.youtube.com/watch?v=2zayjJcIQmE

NARVAEZ, Networking Colombia Configurar DHCP con Vlans, Router on Stick CISCO [En línea] Disponible en:
https://www.youtube.com/watch?v=WucmiYGduv4

CARDONA JOSE, Prueba de Habilidades Diplomado CISCO [En línea] 16 Octubre Dsiponible en:
2020https://drive.google.com/file/d/1XTTmvwmU_Z-4SDMoRom6HeJSAJiqj_Q6/view

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

LOBATO CLARA GUSTAVO, Explicacion de NAT dinamico [En línea] Disponible en:
https://www.youtube.com/watch?v=Ir8ccfaeMro

MASTERING IT, ¿Cómo configurar NAT estatico en router CISCO? [En línea] Disponible:
https://www.youtube.com/watch?v=l4SEQHDfXf8

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de
https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

ANEXOS

Anexo A.Escenario uno funcional
https://1drv.ms/u/s!AvJGBYKryCsOg1qA6WCHWb_D3ZLk?e=3TfTOw

Anexo B. Escenario dos funcional
https://1drv.ms/u/s!AvJGBYKryCsOg1lVYAha5Ngqamrg?e=g7j6S7

Articulo C.

https://1drv.ms/w/s!AvJGBYKryCsOg18mZiHwA3GCMcDi?e=ApBkfF

Diseño de una red

Dagnner Susan Castillo Lucumi
Universidad Nacional, Abierta y A Distancia (UNAD), dagnnerscastillo@hotmail.com

Resumen

Este artículo se basa en el desarrollo de la actividad de profundización cisco, donde se presentan dos escenarios algo similares, en este artículo se nombrara el escenario dos donde se debe de realizar la configuración de los dispositivos de una red, garantizando la seguridad para esto se implementa validación de ingreso utilizando contraseña, también se realiza la utilización y nombramiento de vlan que se define como una red de área local y virtual con el objetivo de tener el aprovechamiento ya que este permite crear redes lógicas independientes estando dentro de una misma red física. También se realiza la configuración utilizando los comandos y métodos de encapsulamiento donde busca proteger la información de la red y minimiza los posibles ataques o amenazas que se puedan llegar a presentar en una red.
También se implementa y configura el protocolo, DHCP y NAT el cual permite de una forma dinámica y/o es táctica donde hay un intercambio o se puede decir variación de las direcciones IP de origen dentro de un rango de direcciones definidas y configuradas.

Palabras clave:
DHCP, Enrutamiento, NAT, Red lógica, VLAN.

Abstract:

This article is based on the development of the deepening activity cisco, where two somewhat similar scenarios are presented, in this article scenario two will be named where the configuration of the devices of a network must be carried out, guaranteeing security for this. implements login validation using password, the use and naming of vlan is also

carried out, which is defined as a local and virtual area network with the aim of having the use of it, since it allows creating independent logical networks while being within the same physical network. The configuration is also carried out using encapsulation commands and methods where it seeks to protect network information and minimize possible attacks or threats that may occur in a network.
The protocol, DHCP and NAT are also implemented and configured, which allows in a dynamic and / or tactical way and there is an exchange or variation of the source IP addresses within a range of defined and configured addresses.

Keywords— DHCP, Enrutamiento, NAT, Red lógica, VLAN.

Introducción

A continuación se realiza el desarrollo con el fin de recibir la capacitación sobre resolución de conflictos de conectividad y/o todo aquello que esté relacionado con esta área. Ya que la Universidad Nacional Abierta y/o A Distancia (UNAD) con este diplomado de profundización en redes teniendo en soporte de la compañía cisco, tiene como finalidad este tipo de conocimientos de una forma ABE (Aprendizaje Basado en Escenarios). En este caso se presentan dos tipos de escenarios.
El cual en este artículo se menciona el escenario dos, teniendo en cuenta que se debe realizar las respectivas configuraciones de switchs y router el cual se implementa protocolo de autenticación para ingresar solicita contraseña. A demás en los host se realiza configuración del protocolo dhcp y NAT, el cual permite dinamizar direcciones ip de origen dentro de un pool de direcciones definida. Se utilizan los comandos para configuración de fecha y hora. Hay nombramiento de vlan asignadas a las diferentes interfaces y sub interfaces para aprovechamiento de la red.

Metodología:

Diseño de redes: Se realiza la configuración de una red el cual cuenta con diferentes dispositivos, implementando proceso de autenticación para el ingreso a estos dispositivos, utilización de contraseña, se nombran vlan y se relacionan a la interfaces y puertos.

Diseño de una red

Dagnner Susan Castillo Lucumi
Universidad Nacional, Abierta y A Distancia (UNAD), dagnnerscastillo@hotmail.com

Utilizando encapsulamiento el cual garantiza una mejor seguridad de la red.

Implementación:

Se presenta un escenario donde se requiere realizar la configuración de los dispositivos de una red.

Este se realiza utilizando un simulador dinámico el cual brinda todas las herramientas necesarias en el momento de realizar configuraciones como si fuera en la vida real, se escogen los dispositivos adecuados según sea el caso de lo que se requiere obtener de cada uno de los dispositivos dependiente de la red. Permite brindar solución a problemas de interconexión y conectividad.

En el escenario se desarrolla utilizando los siguientes dispositivos, 1 servidor con acceso a internet, 3 router, 2 switchs, 2 PC. En este escenario se utiliza la autenticación por medio de contraseña, se debe realizar la configuración del servidor para acceder a internet, en los router se debe nombrar las vlan y asignarles los puertos e interfaces dejando activas las utilizables y apagadas las que no se están utilizando. Se implementa el protocolo DHCP el cual permite de una forma automática generar una dirección IP a los Pcs y el protocolo NAT que permite tomar cualquier dirección IP definiendo un rango para mostrar como dirección IP de origen, donde se evidencia realizando ping la conectividad y la configuración sin errores.

Identificar la mejor forma de tener un enrutamiento y direccionamiento en el manejo de la información.

Conclusiones:

Desarrollando este tipo de escenarios se adquiere conocimiento de cómo parametrizar los switchs administrables para nombrar y asignar las diferentes vlan, desactivar los puertos y/o interfaces que no se requieren. Se establecieron privilegios y autenticación para ejecución de comandos en los dispositivos de red, mostrando una advertencia sobre el ingreso solo a personal autorizado. Se implementó el protocolo de DHCP y NAT. Por último se realizaron todas las pruebas de conectividad corroborando la funcionalidad adecuada de los dispositivos.

Pruebas de funcionalidad

1. Escenario

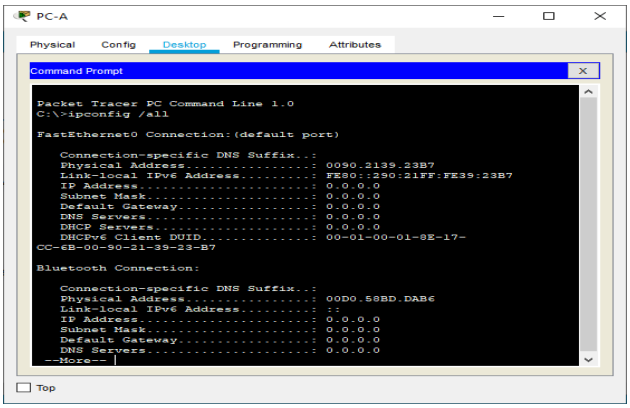


Ilustración 55

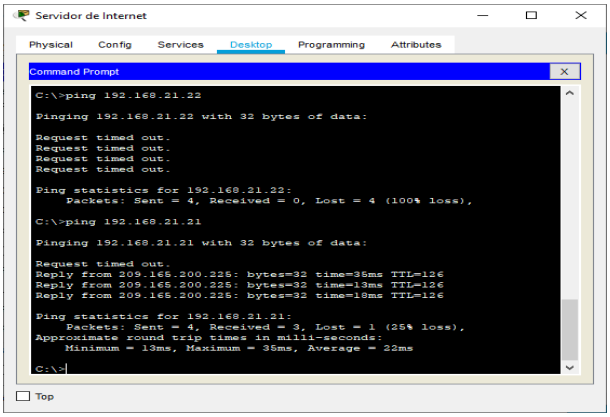


Ilustración 56

1.2 Escenario:

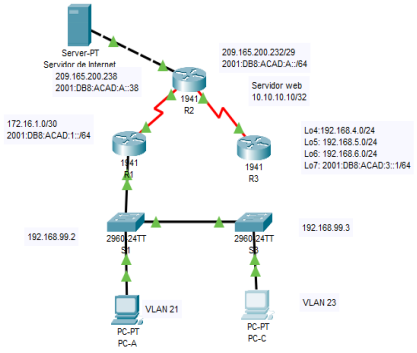


Ilustración 57

Resultados:

Se obtienen exitosamente los ping solicitados en los difernetes dispositivos del escenario propuesto, como se muestran en algunas imágenes mostradas en los anteriores puntos.

El cual se realizó de manera correcta la configuración de los dispositivos de esta red, y brinda seguridad de la información.

Dagnner Susan Castillo Lucumi
Universidad Nacional, Abierta y A Distancia (UNAD), dagnnerscastillo@hotmail.com

Minimizando amenazas o posibles riesgos que pueda llegar a sufrir la información de esta red.
Implementando las diferentes metodologías de configuración para garantizar las buenas prácticas de una red mejorando la seguridad para el ingreso de esta.

Referencias

https://www.youtube.com/watch?v=2zayjJcIQmE
NARVAEZ, Networking Colombia Configurar DHCP con Vlans, Router on Stick CISCO [En línea] Disponible en: https://www.youtube.com/watch?v=WucmiYGduv4
CARDONA JOSE, Prueba de Habilidades Diplomado CISCO [En línea] 16 Octubre Dsiponible en: 2020https://drive.google.com/file/d/1XTTmvwmU_Z-4SDMoRom6HeJSAJiqj_Q6/view
CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1
LOBATO CLARA GUSTAVO, Explicacion de NAT dinamico [En línea] Disponible en: https://www.youtube.com/watch?v=Ir8ccfaeMro