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

Víctor Mauricio Jaime Hernández

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERIA ELECTRONICA DUITAMA

2021

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

Víctor Mauricio Jaime Hernández

Diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN)

Director

NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERIA ELECTRONICA DUITAMA

2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DUITAMA, (Julio 18, 2021)

DEDICATORIA

En primer lugar, gracias a Dios y gracias a mi familia, han sido mi bastón incondicional de los hermosos y complejos momentos de mi sueño y meta de convertirme en ingeniero de electronica desde que comencé a aprender.

AGRADECIMIENTO

Agradecimiento en especial a mi familia que me ha brindado todo el apoyo incondicional en este proceso de formación profesional como ingeniero en electronica. De igual modo, agradezco a todos mis compañeros y mis tutores por el compromiso y acompañamiento oportuno.

Finalmente, mi agradecimiento a la Universidad Nacional Abierta a Distancia (UNAD) y a su extensos equipo de trabajo, sin este método de formación, muchas personas no podrían optar por una educación superior. Agradezco sinceramente todo el apoyo y espacio de formación, espero seguir perteneciendo a esta gran familia y ser parte de su futuro.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

En trabajo se realiza con el propósito de ejecutar de una forma práctica los conocimientos adquiridos a lo largo del Diplomado De Profundización CISCO (Diseño e Implementación de soluciones integradas LAN/WAN), aportando al estudiante las habilidades necesarias en el manejo de redes, enfrentándolo a dos escenarios, en donde para cada uno de ellos debe construir su topología.

En el escenario 1 se desarrolla los conocimientos en cuanto a la configuración de los equipos descritos en una topología y en una tabla la cual contiene el direccionamiento de cada uno de ellos, así como los servicios DHCP, RIPv2, enlaces troncales y la implementación de NAT.

En cuanto al escenario 2, se evalúa las competencias en la implementación del enrutamiento por OSPFv2, habilitar y deshabilitar DNS, al igual que NAT y VLAN.

GLOSARIO

Banda: Conjunto de las frecuencias comprendidas entre límites determinados y pertenecientes a un espectro o gama de mayor extensión. La clasificación adoptada internacionalmente está basada en bandas numeradas que van de la que se ubica de los 0.3 x 10n Hz a 3 x 10n Hz, en la cual n es el número de banda.

Dirección IP: Una dirección en la red asignada a una in-terfaz de un nodo de la red y usada para identificar (localizar) en forma única el nodo dentro de la Internet. Dos versiones están actualmente implementadas: IPv4 e IPv6.

Dirección IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

Dirección IPv6: Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2128 vs. 232). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación “punto”), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

ICPM (Internet Control Message Protocol, Protocolo de mensajes de control de Internet): Es un protocolo que permite administrar información relacionada con errores de los equipos en red

ISP (Internet Services Provider/Proveedor de Servicios de Internet): Una compañía que proporciona a sus clientes acceso a Internet.

LAN (del inglés Local Area Network, Red de Área Local): Una red local es la interconexión de varios computadores y periféricos. Su extensión esta limitada

físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de computadores personales y estaciones de trabajo en oficinas, fábricas, etc; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Network: Se le llama network o también red a aquellas series de ordenadores o dispositivos informáticos que se conectan por medio de cables, ondas, señales u otros mecanismos con el propósito de transmitir datos entre sí, además de recursos y servicios, con el fin de generar una experiencia de trabajo compartida, y ahorrar tiempo y dinero.

INTRODUCCIÓN

La rápida evolución a la que están sometidas las nuevas tecnologías en el mundo de las telecomunicaciones, provoca que en períodos cortos de tiempo se modifiquen los métodos que hasta ese momento se utilizaban, para obtener el máximo provecho de los servicios que ofrecen los mismos. El perfeccionamiento de las infraestructuras de telecomunicaciones, es una necesidad para optimizar las redes, promovido por su evolución tanto en tamaño como cantidad de prestaciones que demanda (Quiroz et al., 2013).

Las redes actualmente cumplen una función importante en facilitar la comunicación, colaboración e interacción de maneras totalmente novedosas a nivel mundial, proporcionando la plataforma para los servicios que permiten la conexión. A medida que la red global continúa ampliándose, también debe crecer la plataforma que la conecta y respalda.

Por medio de esta prueba de habilidades, se analizará, las maneras importantes que tienen que ver con la planificación e implementación de varias clases de Redes. Se ejecuta una práctica por medio del Software Packet Tracer. Donde se aprenderá la Configuración básica y de Seguridad tanto en switches, como Routers, se verán los tipos de Conectividad, con los tipos de cable requeridos, veremos el funcionamiento de herramientas de Protocolo, herramientas para permitir y denegar acceso de usuarios, se experimentará con las Conexiones remotas en Routers y Switches.

OBJETIVOS

General

Dominar conceptos y tecnologías de redes básicas, desarrollar planes e implementar las habilidades necesarias para redes pequeñas con diversas aplicaciones.

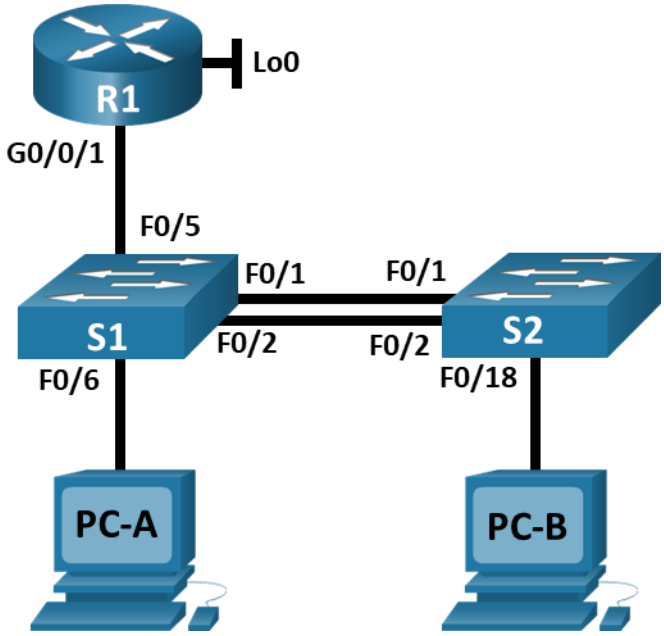
Específicos

- Desarrollar la actividad propuesta con el uso de la herramienta Cisco Packet Tracer.
- Configurar el direccionamiento IP para cada dispositivo en el esquema de acuerdo con la topología de la red.
- Verificar la conectividad de los dispositivos de red.

ESCENARIO 1

Topología

Figura 1 Topología de red escenario 1



Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

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 1. Tabla de VLAN

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

Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

Tabla 2. 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
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

Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

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

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

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

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

```
Router/Switchs #reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
```

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

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
Proceed with reload? [confirm]
```

Paso 2. Configurar R1

- Las tareas de configuración para R1 incluyen las siguientes:
- Desactivar la búsqueda DNS
- 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 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

- Configurar VTY solo aceptando SSH
- Cifrar las contraseñas de texto no cifrado
- Configure un MOTD Banner
- Habilitar el routing IPv6

```
Router>enable
Router#config terminal
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#ip domain name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin secret admin1pass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Unauthorized Acess is Prohibited#
R1(config)#ipv6 unicast-routing
```

- 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.

```
R1(config)#interface g0/0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#description Bikes
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#interface g0/0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#interface g0/0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#interface g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#description Native
R1(config)#interface g0/0/1
R1(config-if)#no shutdown
```

- 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**

```
R1(config-subif)#interface Loopback 0
R1(config-subif)#description Loopback
R1(config-subif)#ip address 209.165.201.1 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:209::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#description Native
R1(config-subif)#exit
```

- Generar una clave de cifrado RSA Módulo de 1024 bits

```
R1(config)#crypto key generate rsa 1024
```

Paso 3. Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

- Desactivar la búsqueda DNS.
- Nombre del switch **S1 o S2, según proceda**
- Nombre de dominio **ccna-lab.com**
- Contraseña cifrada para el modo EXEC privilegiado **ciscoenpass**
- Contraseña de acceso a la consola ciscoconpass
- 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
- Configurar las líneas VTY para que acepten únicamente las conexiones SSH
- Cifrar las contraseñas de texto no cifrado

- Configurar un MOTD Banner
- Generar una clave de cifrado RSA Módulo de 1024 bits

S1

```
Switch1>enable
Switch1#conf t
Switch1(config)#no ip domain lookup
Switch1(config)#hostname S1
S1(config)#ip domain name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin secret admin1pass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Unauthorized Access is Prohibitted!#
S1(config)#crypto key generate rsa 1024
S2
Switch2>enable
Switch2#conf t
Switch2(config)#no ip domain lookup
Switch2(config)#hostname S2
S2(config)#ip domain name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line console 0
```

```
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin secret admin1pass
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #Unauthorized Access is Prohibitted!#
S2(config)#crypto key generate rsa 1024
```

- 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
- Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

```
S1
S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#description Management Interface
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 10.19.8.97
S2
S2(config)#interface vlan 4
```

```
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#description Management Interface
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#ip default-gateway 10.19.8.97
```

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

Paso 4. Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

```
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
```

- Crear troncos 802.1Q que utilicen la VLAN 6 nativa

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

- Interfaces F0/1, F0/2 y F0/5

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

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

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

```
S1(config)#interface f0/6
S1(config-if)#switchport mode access
```

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

```
S1(config-if)#switchport access vlan 2
S1(config-if)#switchport port-security maximum 3
```

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

```
S1(config)#interface range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
S1(config)#interface range f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
S1(config)#interface range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
```

Paso 5. Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

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

```
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
```

```
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
```

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

```
S2(config)#interface range f0/1-2
S2(config-if-range)#switchport trunk encapsulation dot1q (#option)
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#switchport trunk allowed vlan 2 3 4 5 6
S2(config-if-range)#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)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#exit
```

- Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18

```
S2(config)#interface f0/18
S2(config-if)#switchport mode access
```

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

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

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

```
S2(config)#interface range f0/3-17
S2(config-if-range)#switchport mode access
```

```
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
S2(config)#interface range f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
S2(config)#interface range g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
```

Parte 2: 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)#ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
```

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

```
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool VLAN2-Bikes
```

```
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

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

```
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool VLAN3-Trikes
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#
```

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**.

Tabla 3. PC-A Network Configuration

PC-A Network Configuration	
Descripción	*PC-A*
Dirección física	*0030.A3DC.EB2B*
Dirección IP	*10.19.8.53*

Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 4. PC-B Network Configuration

Configuración de red de PC-B	
Descripción	*PC-B*
Dirección física	*00D0.585E.5B13*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

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

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

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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

Tabla 5 Conectividad con dispositivos de red

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

		IPv6	2001:db8:acad:c: :1	**EXITOSO**
	S1, VLAN 4	Dirección	10.19.8.98	**EXITOSO**
		IPv6	2001:db8:acad:c: :98	**EXITOSO**
	S2, VLAN 4	Dirección	10.19.8.99	**EXITOSO**
		IPv6	**2001:db8:acad:c: :99**	**EXITOSO**

Figura 2 verificación de conectividad

```
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 3 Verificación de conectividad

```
C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=2ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

PC A

Figura 4 Ping 10.19.8.99 PC-A

```
C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 5 ping 2001:db8:acad:c: :1 PC-A

```
C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 6 Ping 2001:db8:acad:a: :1 PC-A

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC B

Figura 7 Ping 209.165.201.1 PC-B

```
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=66ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=14ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 66ms, Average = 20ms
```

Figura 8 Ping 2001:db8:acad:a: :1 PC-B

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=22ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 5ms
```

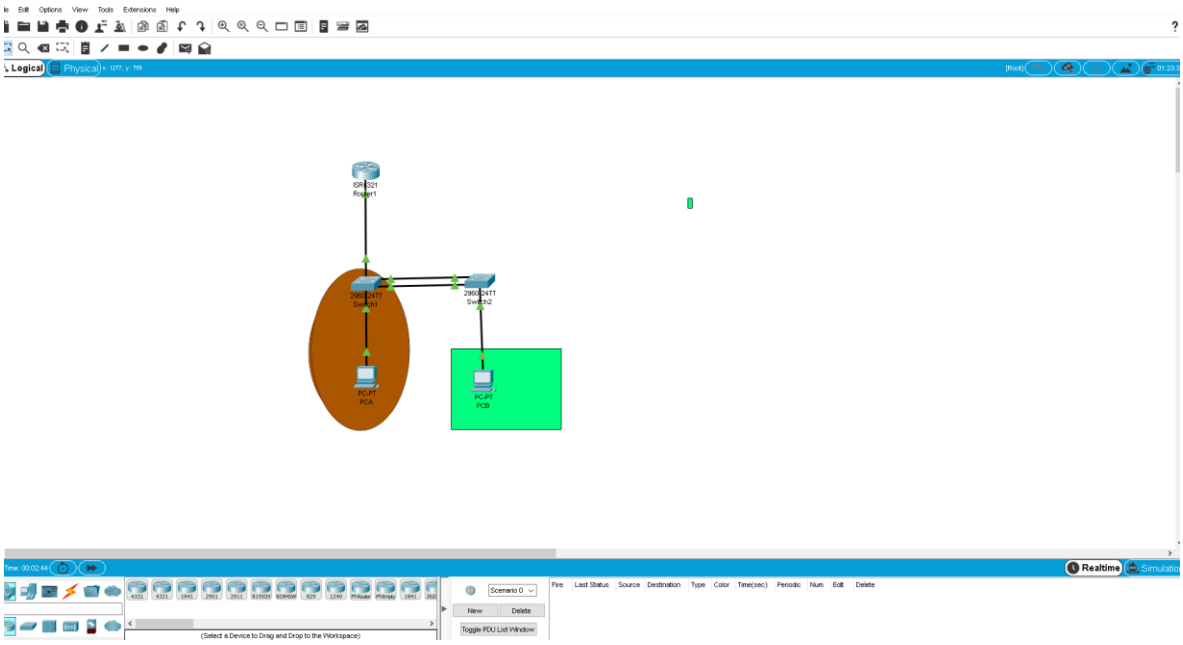
Figura 9 Ping 10.19.8.99 PC-B

```
C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Reply from 10.19.8.99: bytes=32 time=38ms TTL=254
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=14ms TTL=254
Reply from 10.19.8.99: bytes=32 time=12ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 38ms, Average = 16ms
```

Figura 10 Ping 10.19.8.97 PC-B

```
C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 11 Topología de red del escenario 1 - Cisco Packet Tracer

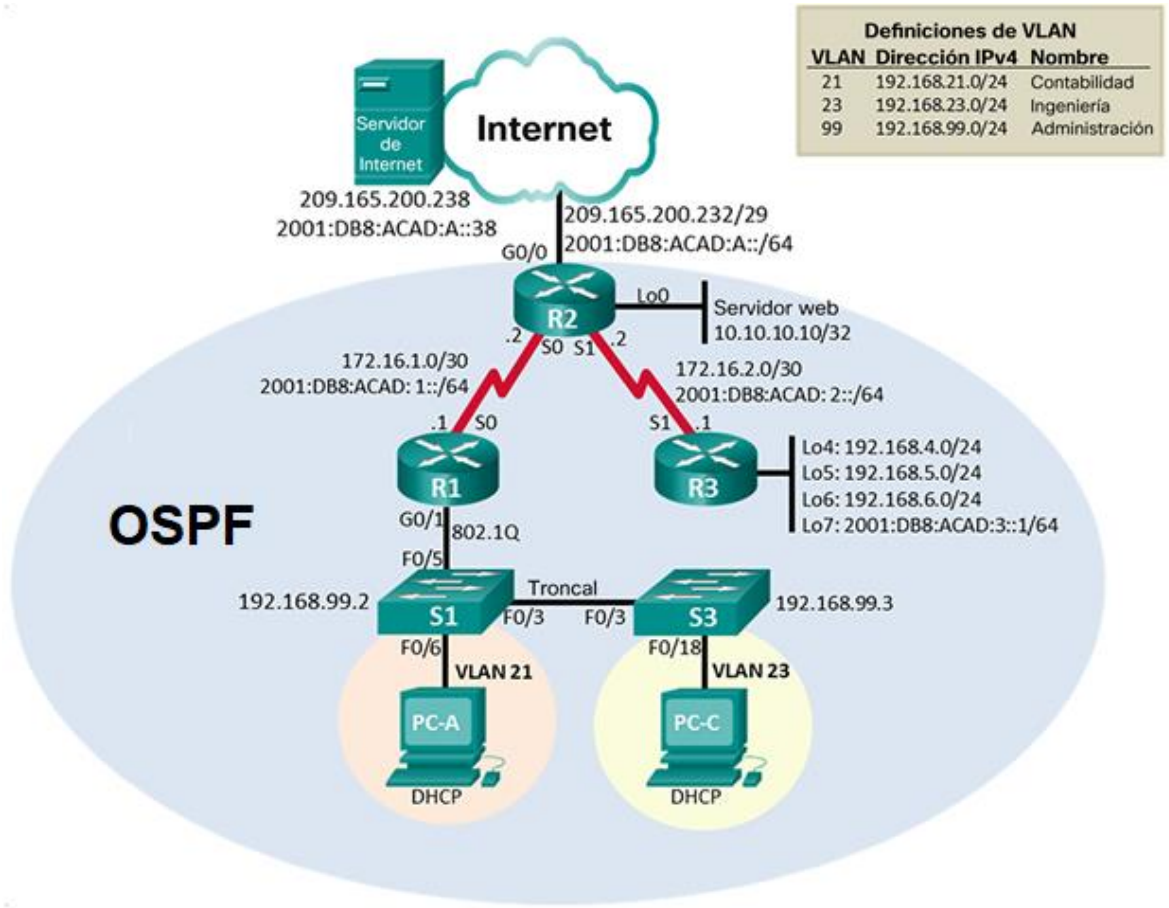


ESCENARIO 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología

Figura 12 Topología de red escenario 2.



Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

Parte 1: Inicializar dispositivos

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

- Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.
- 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
Router#

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
Router#

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
Router#
```

- 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

program load complete, entry point: 0x80803000, size:
0x1b340 program load complete, entry point: 0x80803000,
size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image:
################################################################################

[OK] Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 0 0x00200000 Onboard devices &
buffer pools 0x01E8F000
------------------------------------------------

TOTAL: 0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the
Government is subject to restrictions as set
forth in subparagraph (c) of the Commercial
Computer Software - Restricted Rights clause at
FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-
7013. cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
```

```
Technical                                   Support:
http://www.cisco.com/techsupport  Copyright (c)
1986-2012 by Cisco Systems, Inc. Compiled Thurs
5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply  third-party authority to import, export, distribute
or use encryption. Importers, exporters, distributors and users
are responsible for compliance with U.S. and local country
laws. By using this product you agree to comply with applicable
laws and regulations. If you are unable to comply with U.S. and
local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending
email to export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of
memory. Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
```

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
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or

directory) Switch#
```

Volver a cargar ambos switches

```
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0)
with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0001.C997.6CC1
Xmodem file system is
available. Initializing
Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned
directories flashfs[0]: Total bytes: 64016384

flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1
seconds.
...done Initializing Flash.

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

Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
############################################################################
## [OK] Restricted Rights Legend

Use, duplication, or disclosure by the
Government is subject to restrictions as set
forth in subparagraph (c) of the Commercial
Computer Software - Restricted Rights clause at
FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems,
Inc. Compiled Wed 12-Oct-05 22:05 by
pt_team
Image text-base: 0x80008098, data-base: 0x814129C4

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration
memory. Base ethernet MAC Address : 0001.C997.6CC1
Motherboard assembly number : 73-9832-06
Power supply part number : 341-0097-02
Motherboard serial number :
FOC103248MJ Power supply serial
number : DCA102133JA Model revision
number : B0
Motherboard revision number : C0
Model number : WS-C2960-24TT
System serial number : FOC1033Z1EY
Top Assembly Part Number : 800-26671-02

Top Assembly Revision Number : B0
Version ID : V02
CLEI Code Number : COM3K00BRA
Hardware Board Revision Number : 0x01


Switch Ports Model SW Version SW Image
------ ----- ----- ---------- ----------
* 1 26 WS-C2960-24TT 12.2 C2960-LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed
state to up
```

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

```
Switch>enable
Switch#show  flash
Directory      of
flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
64016384 bytes  total  (59601463  bytes
free) Switch#
Switch>enable
Switch#show  flash
Directory      of
flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
64016384 bytes  total  (59601463  bytes
free) Switch#
```

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1. Configurar la computadora de Internet

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

Tabla 6 configuracion del servidor

Elemento o tarea de configuración	Especificación
Dirección Ipv4	209.165.200.238
Máscaras de subred para Ipv4:	255.255.255.248
Gateway predeterminado:	209.165.200.233
Dirección Ipv6/subred:	201:db8:acad:a::38/64
Gateway prederminado Ipv6:	201:db8:acad:a::1

Fuente Elaboración propia

Tabla 7 IpV4 Subnet

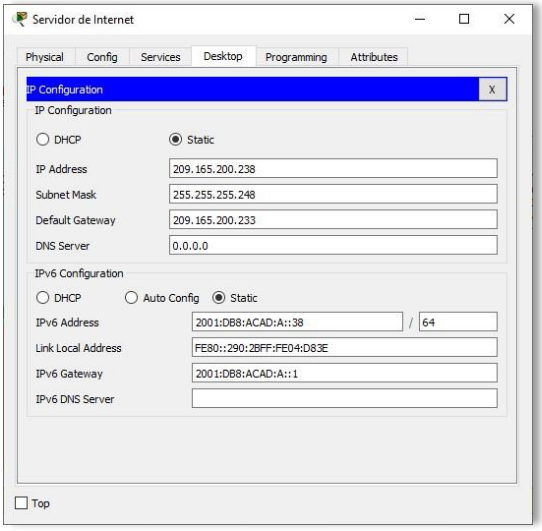
Id address:	**209.165.200.232**
Network Address:	209.165.200.232
Usable Host Ip Range:	209.165.200.233-209.165.200.238
Broadcast Address:	209.165.200.239
Total Number of Hosts:	8
Number of Usable:	6
Subnet mask:	255.255.255.248
Wildcard Mask:	0.0.0.7
Binary subnet Mask:	11111111.11111111.11111111.111110
Ip Type:	PUBLICIP-CLASS C

Tabla 8 IpV6 Subnet

Fuente: Elaboración propia

Ip Addres:	**2001.db8:a cad:a::38/64**
Full Ip Address:	2001:0db8:acad:000a:0000:0000:0000:0038
Total Ip Addresses:	18.446.744.073.709.551.616
Network:	2001:0db8:acad:000a:: /64 2001:0db8:acad:000a:0000:0000:0000:0000/
Ip Range	2001:db8:acad:a::1 2001:0db8:acad:000a:0000:0000:0000:0001 2001:db8:acad:a:ffff:ffff:ffff:ffff 2001:0db8:acad:000a:ffff:ffff:ffff:ffff
Ip Type:	GLOBAL UNICAST

Figura 13 Configuración IP del servidor



Fuente: Elaboración propia

Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

- Desactivar la búsqueda DNS
- Nombre del router R1
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD
- Se prohíbe el acceso no autorizado.

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
- Rutas predeterminadas
- Configurar una ruta IPv4 predeterminada de S0/0/0
- Configurar una ruta IPv6 predeterminada de S0/0/0

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
```

```
R1(config-line)#service password-encryption
R1(config)#banner motd %Se prohibe el acceso no
autorizado.% 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
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface,
may impact performance

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

Nota: Todavía no configure G0/1.

Paso 3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del router R2
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Habilitar el servidor HTTP
- Mensaje MOTD Se prohíbe el acceso no autorizado.

Interfaz S0/0/0

- 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

Interfaz S0/0/1

- Establecer la descripción
- Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
- Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
- Establecer la frecuencia de reloj en 128000.
- Activar la interfaz

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

Interfaz loopback 0 (servidor web simulado)

- Establecer la descripción.
- Establezca la dirección IPv4.

Ruta predeterminada

- Configure una ruta IPv4 predeterminada de G0/0.
- Configure una ruta IPv6 predeterminada de G0/0

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
```

```
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#ip http server
R2(config)#banner motd %Se prohibe el acceso no autorizado.%
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
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
R2(config-if)#int s0/0/1
R2(config-if)#description Connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

R2(config-if)#int g0/0
R2(config-if)#description Connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
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

R2(config-if)#int loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line Interface Loopback0, changed state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description Simulated Web Server
R2(config-if)#exit
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface,
may impact performance
R2(config)#ipv6 route ::/0 g0/0
R2(config)#
```

Nota: Este comando (ip http server) no es compatible con Packet Tracer.

Paso 4. Configurar R3

La configuración del R3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del router R3
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD Se prohíbe 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

Interfaz loopback 4

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 5

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 6

Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 7

Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

Rutas predeterminadas

```
Router>enable

Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd %Se prohibe el acceso no
autorizado.% 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
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up

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
R3(config-if)#ip address 192.168.4.1 255.255.255.0

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
R3(config-if)#ip address 192.168.5.1 255.255.255.0
```

```
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
R3(config-if)#ip address 192.168.6.1 255.255.255.0

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
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit

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

Paso 5. Configurar S1

La configuración del S1 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del switch S1
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD Se prohíbe el acceso no autorizado.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
```

```
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se Se prohíbe el acceso no autorizado.%
S1(config)#
```

Paso 6. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del switch S1
- Contraseña de exec privilegiado cifrada class
- Contraseña de acceso a la consola cisco
- Contraseña de acceso Telnet cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD Se prohíbe el acceso no autorizado.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd %Se Se prohíbe el acceso no autorizado.%
S3(config)#
```

Paso 7. Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

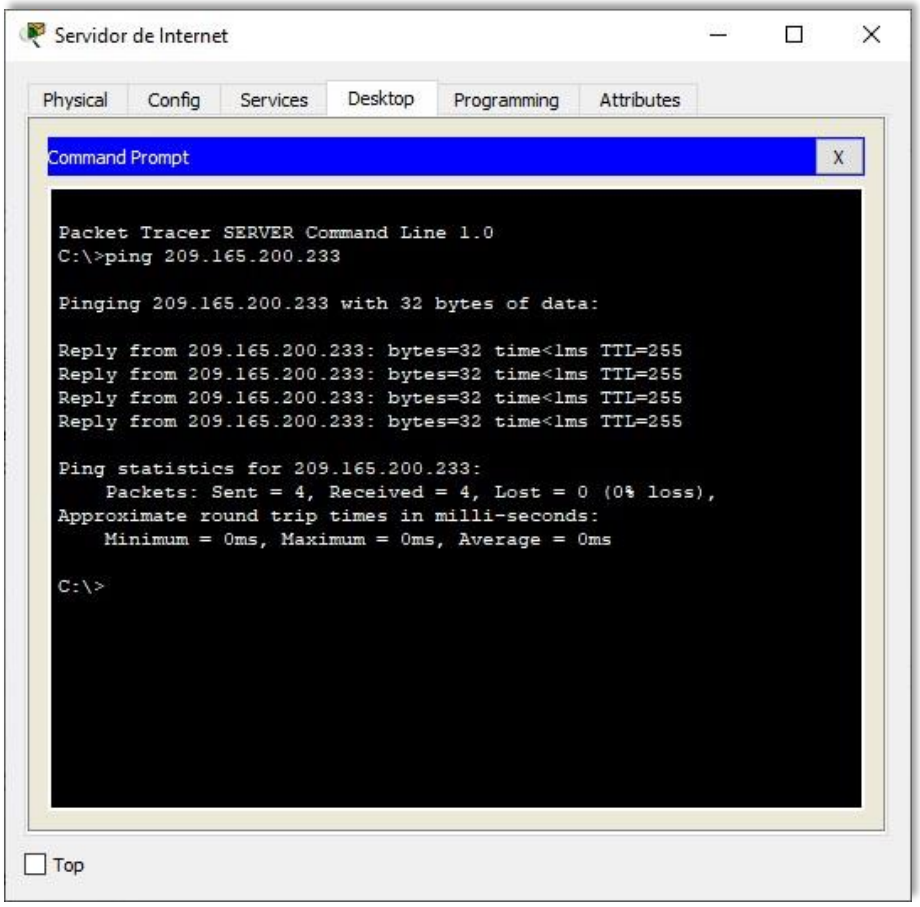
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

Tabla 9 Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de Ping
R1	R2, S0/0/0	172.16.1.2	Success
R2	R3, S0/0/1	172.16.2.1	Success
Servidor de internet	Gateway predetermi	209.165.200.233	Success

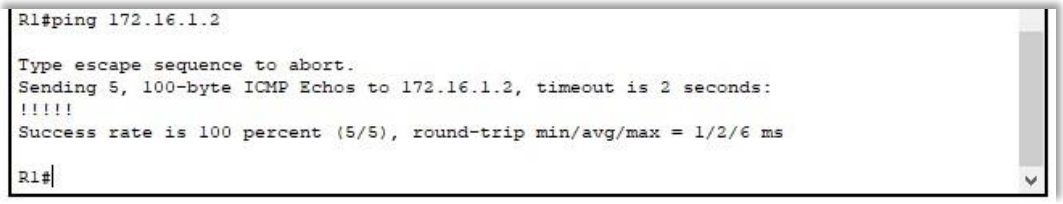
Fuente: Elaboración propia

Figura 14 Prueba de Ping desde R1 a R2



Fuente: Elaboración propia

Figura 15 Prueba de ping desde Servidor de Internet a Gateway predeterminado



Fuente: Elaboración propia

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

Paso 1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

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

Asignar el gateway predeterminado

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

Forzar el enlace troncal en la interfaz F0/3

- Utilizar la red VLAN 1 como VLAN nativa

Forzar el enlace troncal en la interfaz F0/5

- Utilizar la red VLAN 1 como VLAN nativa

Configurar el resto de los puertos como puertos de acceso

- Utilizar el comando interface range
- Asignar F0/6 a la VLAN 21
- Apagar todos los puertos sin usar

```
S1(config)#vlan 21
```

```
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to
up
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down
```

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

Paso 2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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.

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

Asignar el gateway predeterminado.

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

Forzar el enlace troncal en la interfaz F0/3

- Utilizar la red VLAN 1 como VLAN nativa

Configurar el resto de los puertos como puertos de acceso

- Utilizar el comando interface range
- Asignar F0/18 a la VLAN 21
- Apagar todos los puertos sin usar

```
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3


S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode Access
```

```
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

%LINK-5-CHANGED:   Interface   FastEthernet0/1,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/2,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/4,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/5,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/6,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/7,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/8,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/9,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/10,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/11,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/12,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/13,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/14,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/15,   changed   state   to
administratively down

%LINK-5-CHANGED:   Interface   FastEthernet0/16,   changed   state   to
administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S3(config-if-range)#
```

Paso 3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

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

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

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
- Activar la interfaz G0/1

```
R1(config)#int g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description LAN de 45suario45o n45ón
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface GigabitEthernet0/1,
changed state to up

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

%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface GigabitEthernet0/1.21,
changed state to up

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

%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface GigabitEthernet0/1.23,
changed state to up

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

%LINEPROTO-5-UPDOWN: Line 45suario45o n Interface GigabitEthernet0/1.99,
changed state to up

R1(config-if)#
```

Paso 4. Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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

Tabla 10 Verificar la conectividad de los dispositivos

Desde	A	Dirección Ip	Resultados de ping
S1	R1,dirección VLAN 99	192.168.99.1	Success
S3	R1,dirección VLAN 99	192.168.99.1	Success
S1	R1,dirección VLAN 21	192.168.21.1	Success
S3	R1,dirección VLAN 23	192.168.23.1	Success

Fuente: Elaboración propia

Figura 16 Prueba de ping desde S1 a R1, dirección VLAN 99

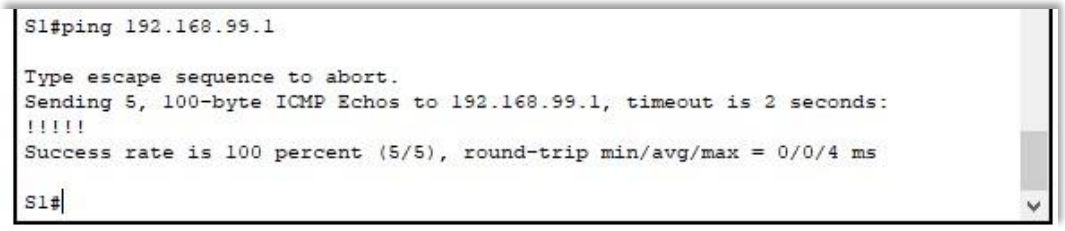
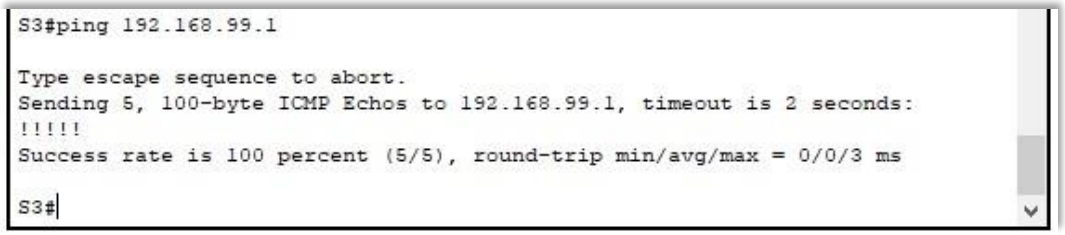
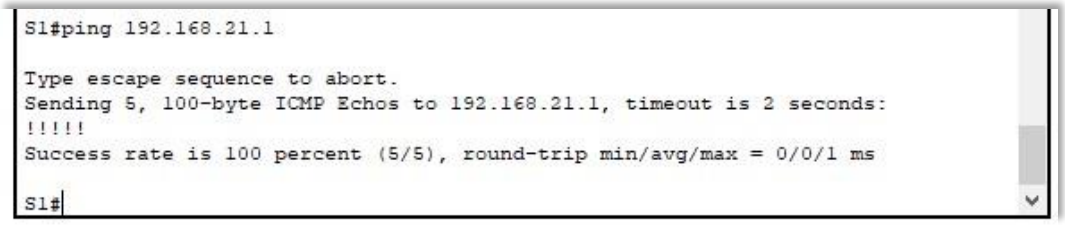


Figura 17 Prueba de ping desde S3 a R1, dirección VLAN 99.



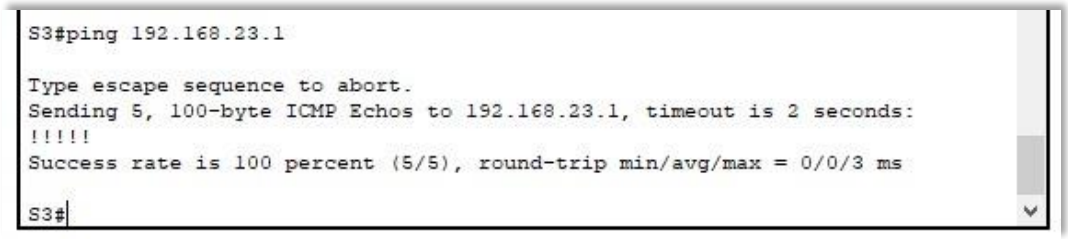
Fuente: Elaboración propia

Figura 18 Prueba de ping desde S1 a R1, dirección VLAN 21



Fuente: Elaboración propia

Figura 19 Prueba de ping desde S3 a R1, dirección VLAN 23.



Fuente: Elaboración propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1. Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente
- Asigne todas las redes conectadas directamente.
- Establecer todas las interfaces LAN como pasivas
- Desactive la sumarización automática

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#
```

Paso 2. Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente
- Establecer la interfaz LAN (loopback) como pasiva
- Desactive la sumarización automática.

```
R2(config)#router ospf 1
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#passive-interface loopback 0
R2(config-router)#
```

Paso 3. Configurar OSPFv3 en el R3

La configuración del R2 incluye las siguientes tareas:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente
- Establecer la interfaz LAN (loopback) como pasiva
- Desactive la sumarización automática.

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
```

Paso 4. Verificar la información de OSPF

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

¿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?

Sh ip protocols

¿Qué comando muestra solo las rutas OSPF?

Sh ip route

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

Sh run begin | ospf

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

- Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas
- Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

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

Crear un pool de DHCP para la VLAN 23

- Nombre: ENGNR
- Servidor DNS: 10.10.10.10
- Nombre de dominio: ccna-sa.com
- Establecer el gateway predeterminado

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
```

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

R1(config)#
```

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

La configuración del R2 incluye las siguientes tareas:

Crear una base de datos local con una cuenta de usuario

- Nombre de usuario: **webuser**
- Contraseña: **cisco12345**
- Nivel de privilegio: **15**
- Habilitar el servicio del servidor HTTP
- Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

Crear una NAT estática al servidor web.

- Dirección global interna: **209.165.200.229**
- Asignar la interfaz interna y externa para la NAT estática
- 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
- 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**
- Definir la traducción de NAT dinámica

```
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
^
% Invalid input detected at ‘^’ marker.
```

```
R2(config)#ip http authentication local

% Invalid input detected at ‘^’
marker.
R2(config)#ip http secure-
server
^
% Invalid input detected at ‘^’
marker.

R2(config)#ip nat inside source static 10.10.10.10
209.165.200.237
R2(config)#intg0
/0
R2(config-if)#ip
natoutside
R2(config-
if)#ints0/0/0
R2(config-if)#ipnat
inside
R2(config-
if)#ints0/0/1
R2(config-if)#ipnat
inside
R2(configif)#ex
it
R2(config)#access-list 1 permit 192.168.21.0
0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0
0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0
0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236
netmask
255.255.255.
28
R2(config)#ip nat inside source list 1 pool
INTERNET
R2(config
#
```

Nota: Los siguientes comandos no son compatibles con Packet Tracer.

- ip http server
- ip http authentication local
- ip http secure-server

Paso 3. Verificar el protocolo DHCP y la NAT estática

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

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

Figura 20 Información de IP del servidor de DHCP en el PC-A.

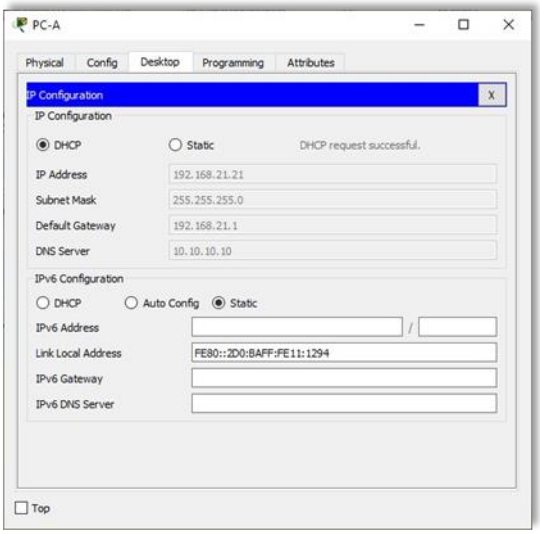
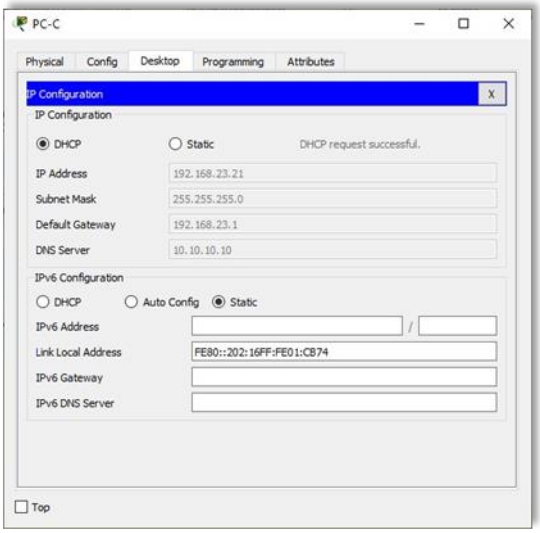


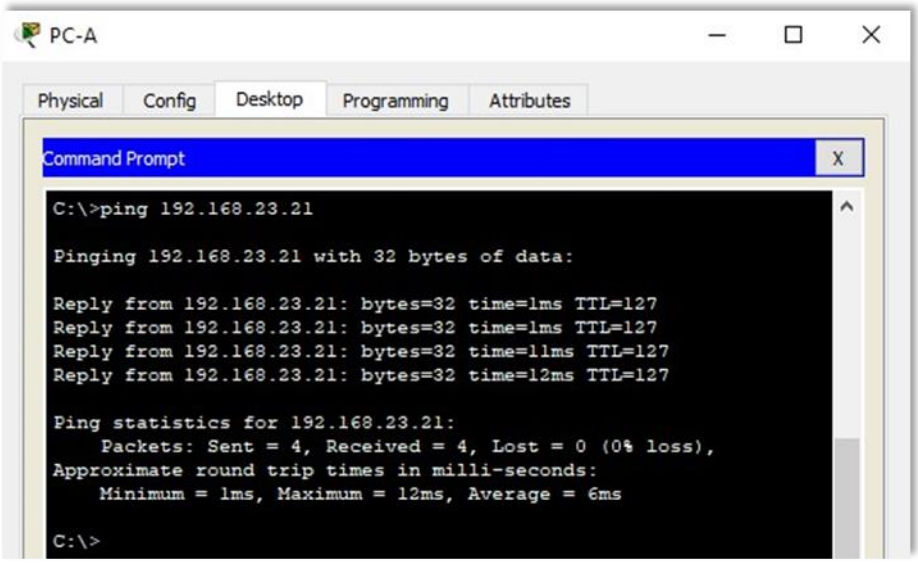
Figura 21 Información de IP del servidor de DHCP en el PC-C



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

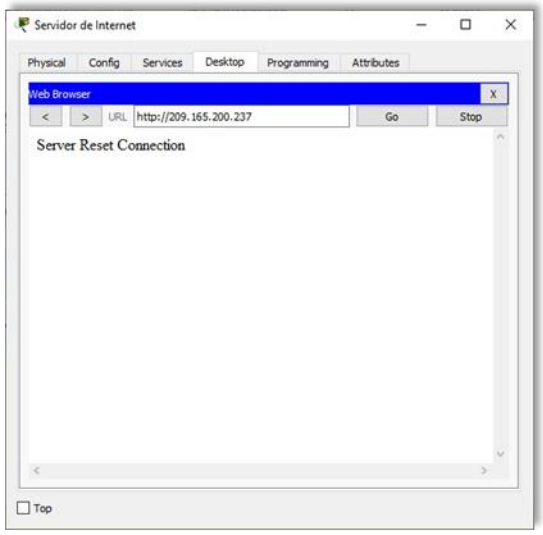
- Verificar que la PC-A pueda hacer ping a la PC-C

Figura 22 Verificación de ping PC-A a la PC-C



- 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**

Figura 23 Acceso Servidor Web desde el Servidor de Internet



Parte 6: Configurar NTP

- Ajuste la fecha y hora en R2.

```
R2#clock set 00:40:00 30 April 2020
```

- Configure R2 como un maestro NTP.

```
R2(config)#ntp master 5
^% Invalid input detected at ‘^’ marker. R2(config)#
```

Nota: Packet tracer no soporta este comando.

- Configurar R1 como un cliente NTP. Servidor: R2

```
R1(config)#ntp server 172.16.1.2
R1(config)#
```

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

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

- Verifique la configuración de NTP en R1.

```
R1#show ntp associations
% This command is not supported by Packet
Tracer. R1#
```

Nota: Este comando no es compatible con Packet Tracer.

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

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

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

- Nombre de la ACL: **ADMIN-MGT**

- Aplicar la ACL con nombre a las líneas VTY
- Permitir acceso por Telnet a las líneas de VTY
- Verificar que la ACL funcione como se espera

```
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
```

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 …OpenSe prohibe el acceso no Elaboración propiaizado.

User Access Verification

Password:
R2>exit

[Connection to 172.16.1.2 closed by foreign host]
R1#

R3#telnet 172.16.1.2
Trying 172.16.1.2 …
% Connection refused by remote host
R3#
```

Figura 24 Prueba de Telnet de R1 a R2.

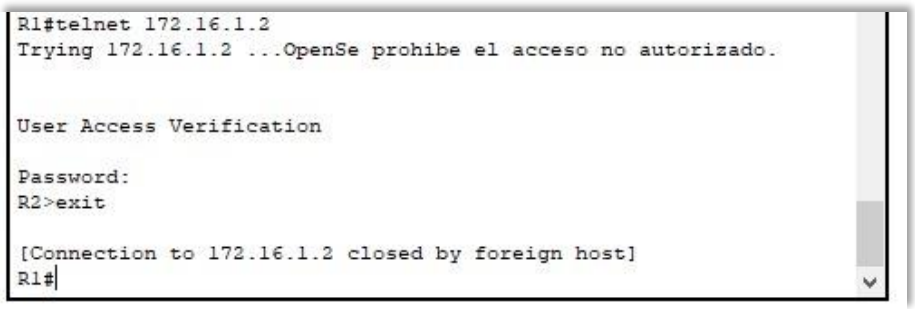
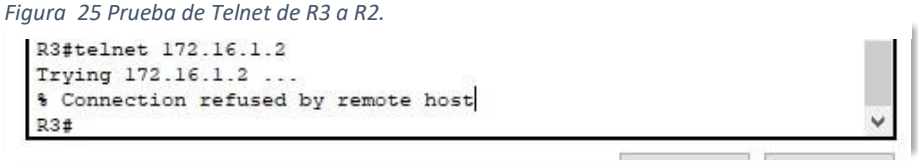


Figura 25 Prueba de Telnet de R3 a R2.



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

- Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

```
R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
R2#
```

- Restablecer los contadores de una lista de acceso

```
R2#clear ip access-list counters
R2#clear ip
bgp Clear BGP connections
dhcp Delete items from the DHCP database
nat Clear NAT
ospf OSPF clear commands
route Delete route table entries

      R2#
```

- ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up
(connected) Internet address is 209.165.200.233/29
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not
set Inbound access list is
not set Proxy ARP is
enabled
Security level is default
Split horizon is enabled
```

```
ICMP redirects are always
sent ICMP unreachables are
always sent ICMP mask replies
are never sent IP fast
switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is
disabled TCP/IP header compression is
disabled RTP/IP header compression is
disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
GigabitEthernet0/1 is administratively down, line protocol is down
(disabled)
Internet protocol processing disabled
Serial0/0/0 is up, line protocol is up (connected)
Internet address is 172.16.1.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled

Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent IP
fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
```

```
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected)
Internet address is 172.16.2.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent ICMP
unreachables are always sent ICMP
mask replies are never sent IP fast
switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled

BGP Policy Mapping is disabled
```

```
Loopback0 is up, line protocol is up
(connected) Internet address is
10.10.10.10/32
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1514bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not
set Inbound access list is
not set Proxy ARP is
enabled
Security level is default
Split horizon is enabled
ICMP redirects are always
sent ICMP unreachables are
always sent ICMP mask replies
are never sent IP fast
switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is
disabled RTP/IP header
compression is disabled Probe
proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is
disabled WCCP Redirect inbound
is disabled WCCP Redirect
exclude is disabled
Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled
R2#
```

- ¿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.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
Tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1033209.165.200.238:1033

R2#
```

Figura 26 Ver las traducciones NAT en el R3.

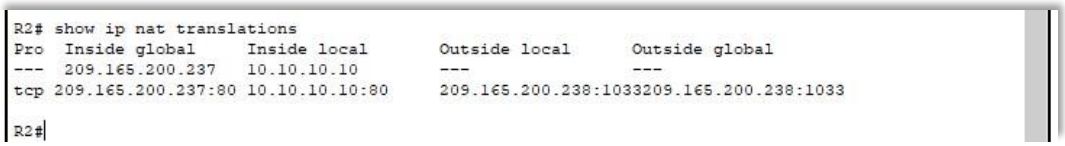


Figura 27 Prueba de ping al Servidor de Internet desde la PC-A.

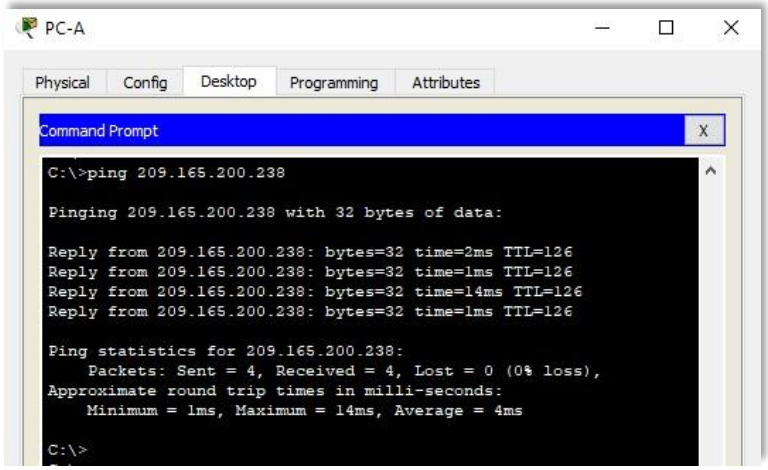


Figura 29 Prueba de ping al Servidor de Internet desde la PC-C.

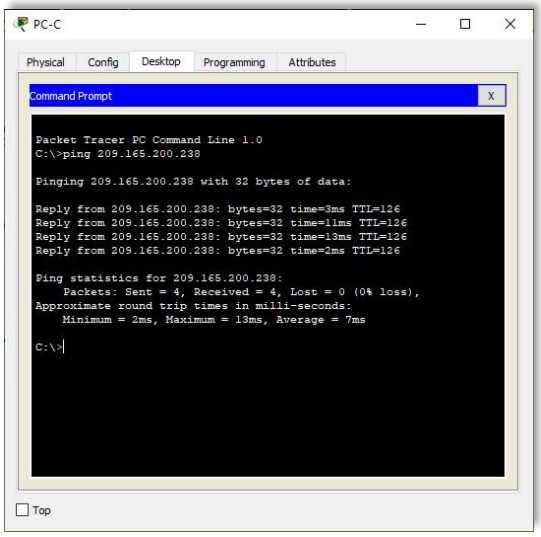
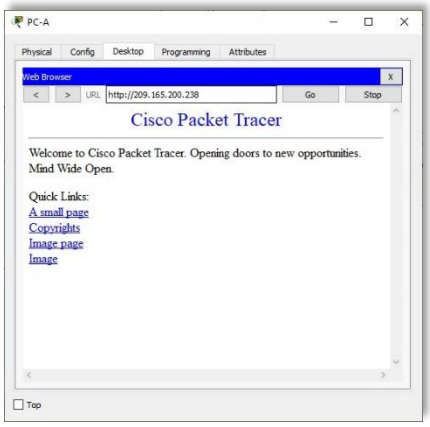


Figura 28 Prueba de acceso al Servidor de Web desde PC-A.



¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas

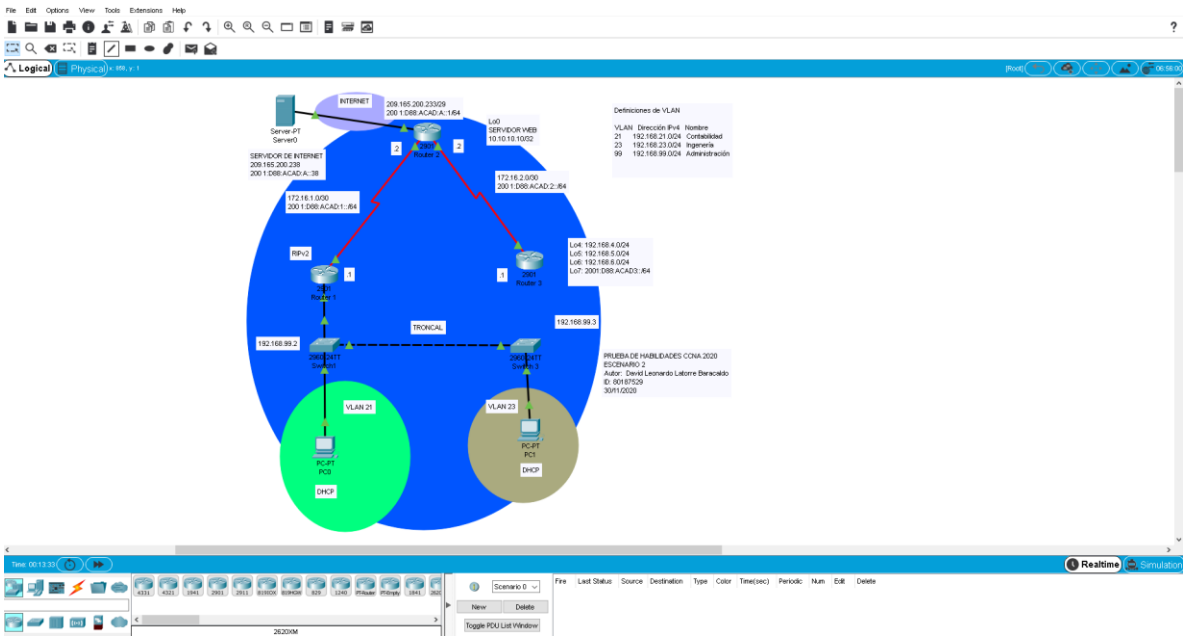
```
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.233:1025192.168.23.21:1025 209.165.200.238:80
209.165.200.238:80
tcp 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80
209.165.200.238:80 tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1033209.165.200.238:1033

R2#clear ip nat translation * R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
```

```
--- 209.165.200.237 10.10.10.10 --- --- R2#
```

Figura 30 Eliminar las traducciones de NAT dinámicas.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---
tcp 209.165.200.233:1025192.168.23.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.237:80 10.10.10.10:80     209.165.200.238:1033209.165.200.238:1033

R2#clear ip nat translation *
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---

R2#
```

Figura 31 Topología de red escenario 2 - Cisco Packet Tracer.



Fuente: Elaboración propia

CONCLUSIONES

El diseño e implementación de escenarios en Cisco Packet Tracer Student ofrece visualización, creación, evaluación y capacidades de colaboración, y facilita a los estudiantes la comprensión de conceptos tecnológicos complejos

La implementación de los elementos abordados proporciona un mejor rendimiento de la red pues los mismos garantizan seguridad, fácil administración, redundancia óptimae incremento del ancho de banda, entre otras ventajas.

La verificación de las configuraciones desarrolladas y la realización de pruebas de conectividad entre los dipositivos, se torna una necesidad para el administrador, pues en caso de fallos en la red es importante descubrir el origen del problema para su solución inmediata.

BIBLIOGRAFÍA

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

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

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

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

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). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

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

Víctor Mauricio Jaime Hernández
Universidad Nacional Abierta y a Distancia, vi74jai820@unadvirtual.edu.co

Resumen

Las redes presentan un papel protagónico en el desarrollo de la sociedad. Actualmente Cisco constituye uno de los más grandes proveedores de equipos de redes en el mercado mundial, y ofrece una amplia variedad de certificaciones que garantizan altos niveles de conocimiento. Es necesario profundizar en este contenido, por su amplitud e importancia.

En el presente trabajo se caracterizan algunas temáticas relacionadas con switching entre las que destacan VLAN, STP y Etherchannel. Para una mejor comprensión, se analizan sus principales comandos de configuración y verificación mediante el diseño e implementación de escenarios que mejoran notablemente el desempeño de la red, pues garantizan seguridad, fácil administración, redundancia y aumento del ancho de banda, entre otras ventajas. Este trabajo permite enriquecer dicha asignatura a través de la memoria escrita, la cual puede ser utilizada como material complementario para el estudio y profundización de los tópicos de switching y servir de guía para la elaboración de futuras prácticas de laboratorio virtuales

Palabras clave: Switching, Vlan, DHCP, Port-security, IPV4, IPV6.

Abstract:

Networks play a leading role in the development of society. Cisco is currently one of the largest suppliers of networking equipment in the world market, and offers a wide variety of certifications that guarantee high levels of expertise. It is necessary to deepen in this content, because of its amplitude and importance.

In the present work, some topics related to switching are characterized, among which VLAN, STP and Etherchannel stand out. For a better understanding, its main configuration and verification commands are analyzed through the design and implementation of scenarios that significantly improve network performance, since they guarantee security, easy administration, redundancy and increased bandwidth, among other advantages. This work allows enriching this subject through the written memory, which can be used as complementary material for the study and deepening of the switching topics and serve as a guide for the elaboration of future virtual laboratory practices.

Keywords— Switching, Vlan, DHCP, Port-security, IPV4, IPV6.

I. INTRODUCCIÓN

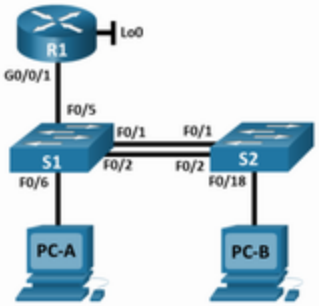
La rápida evolución a la que están sometidas las nuevas tecnologías en el mundo de las telecomunicaciones, provoca que en períodos cortos de tiempo se modifiquen los métodos que hasta ese momento se utilizaban, para obtener el máximo provecho de los servicios que ofrecen los mismos. El perfeccionamiento de las infraestructuras de telecomunicaciones, es una necesidad para optimizar las redes, promovido por su evolución tanto en tamaño como cantidad de prestaciones que demanda (Quiroz et al., 2013).

Las redes actualmente cumplen una función importante en facilitar la comunicación, colaboración e interacción de maneras totalmente novedosas a nivel mundial, proporcionando la plataforma para los servicios que permiten la conexión. A medida que la red global continúa ampliándose, también debe crecer la plataforma que la conecta y respalda.

Por medio de esta prueba de habilidades, se analizará, las maneras importantes que tienen que ver con la planificación e implementación de varias clases de Redes. Se ejecuta una práctica por medio del Software Packet Tracer. Donde se aprenderá la Configuración básica y de Seguridad tanto en switches, como Routers, se verán los tipos de Conectividad, con los tipos de cable requeridos, veremos el funcionamiento de herramientas de Protocolo, herramientas para permitir y denegar acceso de usuarios, se experimentará con las Conexiones remotas en Routers y Switches.

II. Parte Técnica del Artículo

Diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN).



Configuracion de etherchannel escenario 1

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	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
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	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
R1 Loopback0	2001:db8:acad:20 9: :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
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	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
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

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

Paso 4. Configurar S1

La configuración del S1 incluye las siguientes tareas:

• Crear VLAN

o VLAN 2, nombre Bikes

o VLAN 3, nombre Trikes

o VLAN 4, name Management

o VLAN 5, nombre Parking

o VLAN 6, nombre Native

S1(config)#vlan 2

S1(config-vlan)#name Bikes

S1(config-vlan)#vlan 3

S1(config-vlan)#name Trikes

S1(config-vlan)#vlan 4

S1(config-vlan)#name Management

S1(config-vlan)#vlan 5

S1(config-vlan)#name Parking

S1(config-vlan)#vlan 6

S1(config-vlan)#name Native

• Crear troncales 802.1Q que utilicen la VLAN 6 nativa

S1(config)#interface range f0/1-2

S1(config-if-range)#switchport trunk encapsulation dot1q (#option)

S1(config-if-range)#switchport mode trunk

S1(config-if-range)#switchport trunk native vlan 6

S1(config-if-range)#switchport trunk allowed vlan 2 3 4 5 6

S1(config-if-range)#exit

• Interfaces F0/1, F0/2 y F0/5

S1(config)#interface f0/5

S1(config-if)#switchport trunk encapsulation dot1q (#option)

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 6

S1(config-if)#switchport trunk allowed vlan 2 3 4 5 6

S1(config-if)#exit

• 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 f0/1-2

S1(config-if-range)#channel-group 1 mode active

S1(config-if-range)#exit

• Configurar el puerto de acceso de host para VLAN 2

interface F0/6

S1(config)#interface f0/6

S1(config-if)#switchport mode access

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

S1(config-if)#switchport access vlan 2

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

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

S1(config)#interface range f0/3-4

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 5

S1(config-if-range)#description Unused Interfaces

S1(config-if-range)#shutdown

S1(config)#interface range f0/7-24

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 5

S1(config-if-range)#description Unused Interfaces

S1(config-if-range)#shutdown

S1(config)#interface range g0/1-2

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 5

S1(config-if-range)#description Unused Interfaces

S1(config-if-range)#shutdown

Paso 5. Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

• Crear VLAN

o VLAN 2, name Bikes

o VLAN 3, name Trikes

o VLAN 4, name Management

o VLAN 5, nombre Parking

o VLAN 6, nombre Native

S2(config)#vlan 2

S2(config-vlan)#name Bikes

S2(config-vlan)#vlan 3

S2(config-vlan)#name Trikes

S2(config-vlan)#vlan 4

S2(config-vlan)#name Management

S2(config-vlan)#vlan 5

S2(config-vlan)#name Parking

S2(config-vlan)#vlan 6

S2(config-vlan)#name Native

• Crear troncales 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2

S2(config)#interface range f0/1-2

S2(config-if-range)#switchport trunk encapsulation dot1q (#option)

S2(config-if-range)#switchport mode trunk

S2(config-if-range)#switchport trunk native vlan 6

S2(config-if-range)#switchport trunk allowed vlan 2 3 4 5 6

S2(config-if-range)#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)#interface range f0/1-2

S2(config-if-range)#channel-group 1 mode active

S2(config-if-range)#exit

• Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18

S2(config)#interface f0/18

S2(config-if)#switchport mode access

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

S2(config-if)#switchport access vlan 3

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

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

S2(config)#interface range f0/3-17

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 5

S2(config-if-range)#description Unused Interfaces

S2(config-if-range)#shutdown

S2(config)#interface range f0/19-24

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 5

S2(config-if-range)#description Unused Interfaces

S2(config-if-range)#shutdown

S2(config)#interface range g0/1-2

S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 5

S2(config-if-range)#description Unused Interfaces

S2(config-if-range)#shutdown

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

Conectividad con dispositivos de red

c	**A**	**de Internet**	**Dirección IP**	**Result ados de ping**
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	**EXITOSO**
PC-A	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	**EXITOSO**
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	**EXITOSO**
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	**EXITOSO**
PC-A	R1, G0/0/	Dirección	10.19.8.97	**EXITOSO**

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

Verificación de conectividad

```
C:\>ping 10.19.8.1

Pinging 10.19.8.1 with 32 bytes of data:

Reply from 10.19.8.1: bytes=32 time=1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255
Reply from 10.19.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Verificación de conectividad

```
C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=2ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

PC A

Ping 10.19.8.99 PC-A

```
C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=1ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping 2001:db8:acad:c: :1 PC-A

```
C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping 2001:db8: acad:a:1 PC-A

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC B

Ping 209.165.201.1 PC-B

```
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=66ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=14ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 66ms, Average = 20ms
```

Ping 2001:db8: acad:a:1 PC-B

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=22ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 5ms
```

Ping 10.19.8.99 PC-B

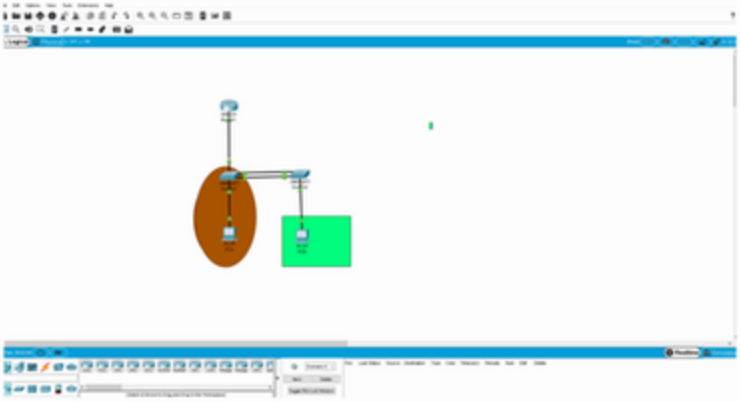
```
C:\>ping 10.19.8.99

Pinging 10.19.8.99 with 32 bytes of data:

Reply from 10.19.8.99: bytes=32 time=38ms TTL=254
Reply from 10.19.8.99: bytes=32 time<1ms TTL=254
Reply from 10.19.8.99: bytes=32 time=14ms TTL=254
Reply from 10.19.8.99: bytes=32 time=12ms TTL=254

Ping statistics for 10.19.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 38ms, Average = 16ms
```

Ping 10.19.8.97 PC-B

```
C:\>ping 10.19.8.97

Pinging 10.19.8.97 with 32 bytes of data:

Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time=1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255
Reply from 10.19.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.19.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pone de ultimo la imagen de la topología montada.

Topología de red del escenario 1 - Cisco Packet Tracer



III. Referencias

Las referencias son muy importantes, y se debe seguir el siguiente formato. El tamaño de letra es de 10 puntos:

Para articulos en revistas:

[1] CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

[2] CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de

https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

[3] CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

[4] CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

[5] CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

[6] CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

[7] CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

[8] CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

[9] CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

[10] CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

[11] CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

[12] 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

[13] CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

[14] 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

[15] CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

[16] UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm