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

WILLIAM ALBERTO ARTURO LEÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERIA DE TELECOMUNICACIONES

BOGOTÁ

2020

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

WILLIAM ALBERTO ARTURO LEÓN

Diplomado de opción de grado presentado para optar el título de INGENIERO DE TELECOMUNICACIONES

DIRECTOR:
JOSÉ IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA DE TELECOMUNICACIONES
BOGOTÁ
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

BOGOTÁ, 7 DE diciembre de 2020

AGRADECIMIENTOS

Les doy mis más sinceros agradecimientos a mi esposa y a mi hija que durante todo el tiempo me han brindado el apoyo para que pueda lograr este triunfo en mi vida, a pesar de no poder compartir durante muchos momentos especiales con ellas.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Etherchannel: Es una Tecnología desarrollada por Cisco mediante el estandar 802.3 Full Dúplex Fast Ethernet. Esta tecnología permite la agrupación lógica de varios enlaces físicos en un solo enlace troncal donde se suman las velocidades de cada uno de estos enlaces ampliando su velocidad total.

Subnetting: Se define como la subdivisión de una red en varias subredes. Este proceso tiene diferentes fines entre los cuales está un acceso más rápido, mejor organización lógica y un mayor grado de seguridad a la hora de aislar una subred afectada.

VLAN: corresponde al acrónimo Virtual LAN o red de área Local Virtual, y corresponde al método para crear redes lógicas independientes dentro de una misma red física. Son útiles en el proceso de administración de la red ya que se pueden segmentar las diferentes áreas de una empresa en diferentes Vlans dando un mejor manejo y organización.

NAT: Es un acrónimo que corresponde a su palabra en Ingles “Network Address Translation”**,** traducción de direcciones de red.

Red Interna: de acuerdo a la terminología NAT, corresponde al conjunto de redes sujetas a traducción.

RESUMEN

El presente documento corresponde al trabajo final “Diplomado de profundización CISCO, prueba de habilidades prácticas CCNA. Aquí encontraremos el desarrollo de los 2 escenarios propuestos, los cuales fueron desarrollados mediante la herramienta Packet Tracer. Se encontraran las configuraciones realizadas y sus respectivas evidencias mediante imágenes tomadas al momento de realizar el desarrollo en esta herramienta.
Realice las configuraciones básicas de seguridad para cada uno de los dispositivos y configuraciones tales como trunking, switching, routing mediante el uso de protocolos como OSPF y DHCPv4 entre otros.
Desarrolle las diferentes pruebas de conexión solicitadas para los diferentes eventos.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

This document corresponds to the final work "CISCO Deepening Diploma, CCNA Practical Skills Test. Here we will find the development of the 2 proposed scenarios, which were developed using the Packet Tracer tool. The configurations made and their respective evidences will be found by images taken at the time of the development in this tool.
Perform the basic security settings for each of the devices and configurations such as trunking, switching, routing by using protocols such as OSPF and DHCPv4 among others.
Develop the different connection tests requested for the different events.

Keywords: CISCO, CCNA, Switching, Routing, Networking, Electronics

INTRODUCCIÓN

Esta prueba de habilidades nos ha permitido poner en práctica los conocimientos obtenidos durante todas las unidades desarrolladas en el Diplomado de profundización Cisco.

Durante el desarrollo del escenario N° 1 he realizado los procesos de validación de vlans previamente configuradas y la inicialización de los routers y switches utilizados en el proceso con la finalidad de realizar las configuraciones desde cero, tales como la configuración básica de los mismos, habilitar restricciones de acceso y seguridad, configuración de direccionamiento IP en protocolos IPv4 e IPv6 en las diferentes interfaces y subinterfaces relacionadas.

He realizado la creación, configuración y direccionamiento de Vlans, definiendo los diferentes segmentos como accesos y troncales, de acuerdo a las disposición, mediante el protocolo 802.1Q, donde también se asignó la Vlan 6 como nativa.

En este proceso de configuración de vlans se observa la segmentación virtual de las redes para obtener una mejor calidad de comunicación y un mayor ancho de banda mediante la configuración de un canal EtherChannel a través del protocolo LACP entre los 2 switches utilizados.

Se realizó la configuración del default routing con la finalidad de dirigir el tráfico a la interfaz Loopback.

El uso del Router como servidor DHCP para la asignación de direcciones IPv4 a los dos PC conectadas en los switches S1 y S2 respectivamente.

Validación en los PC's de la asignación de direcciones IPv4 y su correcta asignación de acuerdo a los requerimientos solicitados.

Una vez realizada toda la configuración se procedió a la validación de las configuraciones y conectividad desde cada uno de los puntos solicitados.

En el Escenario 2, adicional a practicar las configuraciones básicas de los dispositivos, configuración de troncales y accesos, se experimentó la forma de realizar el routing tanto de forma manual como de forma automática mediante el uso del protocolo OSPFv2 y OSPFv3. También se realizaron prácticas de asignación automática de Ip's a través del protocolo DHCPv4.

Se propuso la configuración de un servidor WEB y conexión a internet lo cual no fue posible validarlo debido a que Packet tracer no soporta algunas configuraciones y por lo tanto es necesario hacerlas en dispositivos reales.

OBJETIVOS

Objetivo General

Aplicar los conocimientos adquiridos en cada uno de los capítulos y actividades realizadas durante el proceso de aprendizaje.

Objetivos Específicos

Conocer las sintaxis a utilizar en la configuración de los diferentes dispositivos que hacen parte de una red.

Lograr configurar una red sencilla y básica, mediante el uso de vlans, interfaces y subinterfaces, aplicación de los procesos de subnetting y direccionamiento mediante los protocolos IPv4 e IPv6.

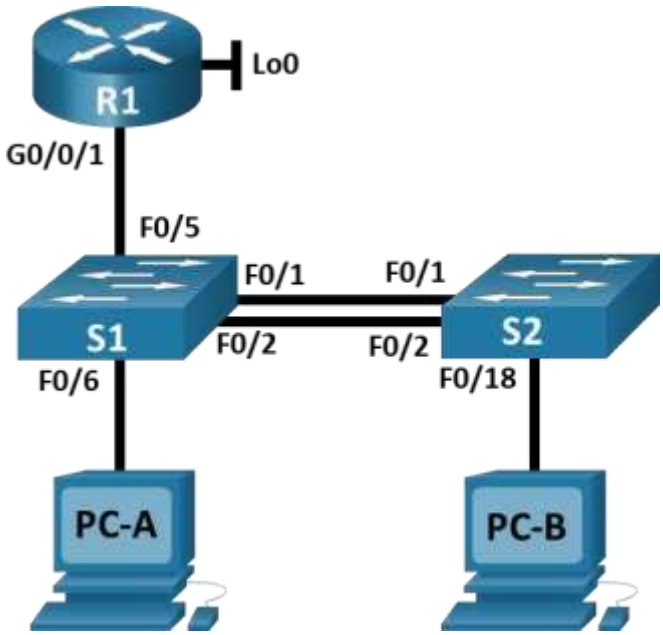
Aplicar los procesos básicos de seguridad para el acceso a los diferentes dispositivos de la red.

Conocer los diferentes protocolos de routing y sus alcances al momento de requerirlos dentro de una configuración de redes.

ESCENARIO 1

DESCRIPCIÓN Y DESARROLLO

Figura 1. Escenario 1



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

Tabla 1. Asignación VLANS con su respectivo nombre

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

Tabla 2. Asignación de Direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminado
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: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
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

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

Inicializar Recargar y Configurar aspectos básicos de los dispositivos

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.

  Pasos para inicializar el 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#**reload**

  Proceed with reload? [confirm]
  Self decompressing the image :
  ##
  ####### [OK]
  Would you like to enter the initial configuration dialog? [yes/no]: n
  Press RETURN to get started!

  Router>

  Pasos para inicializar los switches
  Switch>**enable**
  No posee vlans configuradas procedemos a borrar la configuración de inicio:
  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#**reload**
  Proceed with reload? [confirm]
  Press RETURN to get started!
  Switch>

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

En mi caso primero actualice la versión de los switches 2960 a la versión **"c2960-lanbasek9-mz.150-2.SE4.bin"** la cual descargue por TFTP desde un server conectado al switch mediante los siguientes comandos:

Switch#**copy tftp flash**
Address or name of remote host [ ] ? **10.19.8.100**
Source filename [ ] ? **C2960-lanbasek9-mz.150-2.SE4.bin**
Switch#**conf t**
Switch (config)#**boot system c2960-lanbasek9-mz.150-2.SE4.bin**
Switch#**wr**
Switch#**reload**

Una vez actualice la versión del IOS configure la plantilla SDM para que el Sistema acepte IPv6 así:

Switch (config)#**sdm prefer dual-ipv4-and-ipv6 default**
Switch#**wr**
Switch#**reload**

Nota: El proceso de cargue de la plantilla se realizó para los 2 Switches S1 y S2

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

Configurar R1

Tabla 3. Tareas de configuración basica para R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	**Especificación**	Configuración **Router**
Desactivar la búsqueda DNS	no ip domain-lookup	Router>**enable** Router#**conf t** Router(config)#**no ip domain-lookup** Router(config)#**hostname R1** R1(config)#**ip domain-name ccna-lab.com** R1(config)#**enable secret ciscoenpass** R1(config)#**line con 0** R1(config-line)#**password ciscoconpass** R1(config-line)#**login** R1(config-line)#**exit** R1(config)#**security password min-length 10**
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	

Tarea	**Especificación**	Configuración **Router**
Establecer la longitud mínima para las contraseñas	10 caracteres	R1(config)#**username admin password 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 access is strictly prohibited#**
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		R1(config)#**ipv6 unicast-routing**

Tarea	Especificación	Configuración **Router**
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.	**Configuración interfaz-subif g0/1.2** R1(config)#**int g0/1.2** R1(config-subif)#**encapsulation dot1Q 2** R1(config-subif)#**ip addr 10.19.8.1 255.255.255.192** R1(config-subif)#**ipv6 addr 2001:db8:acad:a::1/64** R1(config-subif)#**ipv6 addr fe80::1 link-local** R1(config-subif)#**no shu** R1(config-subif)#**exit** **Configuración interfaz-subif g0/1.3** R1(config)#**int g0/1.3** R1(config-subif)#**encapsulation dot1Q 3** R1(config-subif)#**ip addr 10.19.8.65 255.255.255.224** R1(config-subif)#**ipv6 addr 2001:db8:acad:b::1/64** R1(config-subif)#**ipv6 addr fe80::1 link-local** R1(config-subif)#**no shu** R1(config-subif)#**exit** **Configuración interfaz-subif g0/1.4** R1(config)#**int g0/1.4** R1(config-subif)#**encapsulation dot1Q 4** R1(config-subif)#**ip addr 10.19.8.97 255.255.255.248** R1(config-subif)#**ipv6 addr 2001:db8:acad:c::1/64** R1(config-subif)#**ipv6 addr fe80::1 link-local** R1(config-subif)#**no shu** R1(config-subif)#**exit**

Tarea	Especificación	Configuración **Router**
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)#**int loopback 0** R1(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R1(config-if)#**ip addr 209.165.201.1 255.255.255.224** R1(config-if)#**ipv6 addr 2001:db8:acad:209::1/64** R1(config-if)#**ipv6 addr fe80::1 link-local** R1(config-if)#**no shu** R1(config-if)#**exit**
Generar una clave de cifrado RSA	Módulo de 1024 bits	R1(config)#**crypto key generate rsa** The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: **1024** % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Encapsulamiento de las subinterface	Validación de encendido de la interface y subinterfaces	R1#sh ip int br Interface IP-Address OK? Method Status Protocol GigabitEthernet0/0 unassigned YES NVRAM administratively down down GigabitEthernet0/1 unassigned YES NVRAM up up GigabitEthernet0/1.2 10.19.8.1 YES manual up up GigabitEthernet0/1.3 10.19.8.65 YES manual up up GigabitEthernet0/1.4 10.19.8.97 YES manual up up Loopback0 209.165.201.1 YES manual up up

Configure S1 y S2.

Tabla 4. Tareas de configuración básica Switches 1 y 2

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación	Configurar Switches S1 y S2
Desactivar la búsqueda DNS.		Switch>**en** Switch#**conf t** Switch(config)#**no ip domain-lookup** Switch(config)#**hostname S1** S1(config)#**ip domain-name ccna-lab.com** S1(config)#**enable secret ciscoenpass** S1(config)**#line con 0** S1(config-line)#**password ciscoconpass** S1(config-line)#**login** S1(config-line)#**exit** S1(config)#**username admin password 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 prohibited!#** S1(config)#**crypto key generate rsa** The name for the keys will be: S1.ccna-lab.com Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: **1024** % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
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	**Modulo de 1024 bits**	

Tarea	Especificación	Configurar Switches S1 y S2
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	S1(config)#**int vlan 4** *Mar 1 0:19:59.493: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#**ip addr 10.19.8.98 255.255.255.248** S1(config-if)#**ipv6 addr 2001:db8:acad:c::98/64** S1(config-if)#**ipv6 addr fe80::98 link-local**
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S1(config)#**ip default-gateway 10.19.8.97**
Salvar la Configuración de inicio		S1#**copy ru sta** Destination filename [startup-config]? Building configuration... [OK]

La configuración anterior se realizó para el Switch S2 teniendo en cuenta el direccionamiento dado.

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#ho S2
S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line con 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin password 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 prohibited!#
S2(config)#crypto key generat
S2(config)#crypto key generate rsa
The name for the keys will be: S2.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S2(config)#int vlan 4
*Mar 1 0:22:54.700: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config-if)#ip addr 10.19.8.99 255.255.255.248
S2(config-if)#ip default-gateway 10.19.8.97
S2(config-if)#ipv
S2(config-if)#ipv6 addr 2001:db8:acad:c::99/64
S2(config-if)#ipv6 addr fe80::99 link-local
S2(config-if)#exit
S2(config)#ip default-gateway 10.19.8.97
S2(config)#end
%SYS-5-CONFIG_I: Configured from console by console
S2#copy run sta
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Configurar S1

Tabla 5. Tareas de configuración VLANS, troncales y redundancia Etherchannel para S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación	Creación y Configuración VLANS S1
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1#conf t Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	S1(config)#int range f0/1-2 S1(config-if-range)# switchport mode trunk S1(config-if-range)# switchport trunk native vlan 6

Tarea	Especificación	Creación y Configuración VLANS S1
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación	S1(config)#int range f0/1-2 S1(config-if-range)# channel-group 2 mode active S1(config-if-range)#int port-channel 2 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)# S1(config-if)#end Luego de que los 2 switches quedan configurados con el Etherchannel se valida su conexión con el siguiente comando donde **SU** me confirma que está en uso: S1#sh etherchannel sum Group Port-channel Protocol Ports ------+-------------+-----------+----------------------------------- 2 Po2(**SU**) LACP Fa0/1(P) Fa0/2(P)
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6	S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC	S1(config-if)#switchport mode access S1(config-if)#switchport port-security maximum 3

Tarea	Especificación	Creación y Configuración VLANS S1
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#int range f0/3-4 S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description : "Interfaz de red no utilizada" S1(config-if-range)#shutdown **Este proceso se realizó para todas las interfaces no utilizadas y se validó verificando la configuración actual mediante el comando:** **show running-config**

Configure el S2.

Tabla 6. Tareas de configuración VLANS, troncales y redundancia Etherchannel para S1

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

Tarea	Especificación	Creación y Configuración VLANS S2
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)#exit S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2	S2(config-vlan)#int range f0/1-2 range)#switchport mode trunk S2(config-if-range)#switchport trunk Native vlan 6

Tarea	Especificación	Creación y Configuración VLANS S2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación	S2(config-vlan)#int range f0/1-2 S2(config-if-range)#channel-group 2 mode active S2(config-if-range)#int port-channel 2 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)# S2(config-if)#end Luego de que los 2 switches quedan configurados con el Etherchannel se valida su conexión con el siguiente comando donde **SU** me confirma que está en uso: S2#sh etherchannel sum Group Port-channel Protocol Ports ------+-------------+-----------+-------------------------------- 2 Po2(**SU**) LACP Fa0/1(P) Fa0/2(P)
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18	S2(config)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	permite 3 MAC addresses	S2(config-if)#switchport port-security maximum 3

Tarea	Especificación	Creación y Configuración VLANS S2
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#int range f0/3-17 S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description : "Interfaz de red no utilizada" S2(config-if-range)#shutdown **Este proceso se realizó para todas las interfaces no utilizadas y se validó verificando la configuración actual mediante el comando:** **show running-config**

Configurar soporte de host

Configure R1

Tabla 7. Tareas de configuración Default Routing y DHCPV4

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
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 10.19.8.98	
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
DHCP VLAN 2 R1(config)# ip dhcp excluded-address 10.19.8.1 10.19.8.53 **(rango Ip´s Excluidas)** R1(config)#ip dhcp pool VLAN2 R1(config)#network 10.19.8.0 255.255.255.192 R1(config)#default-router 10.19.8.1	

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
DHCP VLAN 3 R1(config)# ip dhcp excluded-address 10.19.8.65 10.19.8.85 **(rango Ip's Excluidas)** R1(config)# ip dhcp pool VLAN3 R1(config)# network 10.19.8.64 255.255.255.224 R1(config)# default-router 10.19.8.65	

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 8. Configuración de red PC-A

PC-A Network Configuration	
Descripción	*FastEthernet0 Connection:(default port)*
Dirección física	*0001.43A8.00C7*
Dirección IP	*10.19.8.54*
Mascara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Figura 2. Configuración de red PC-A

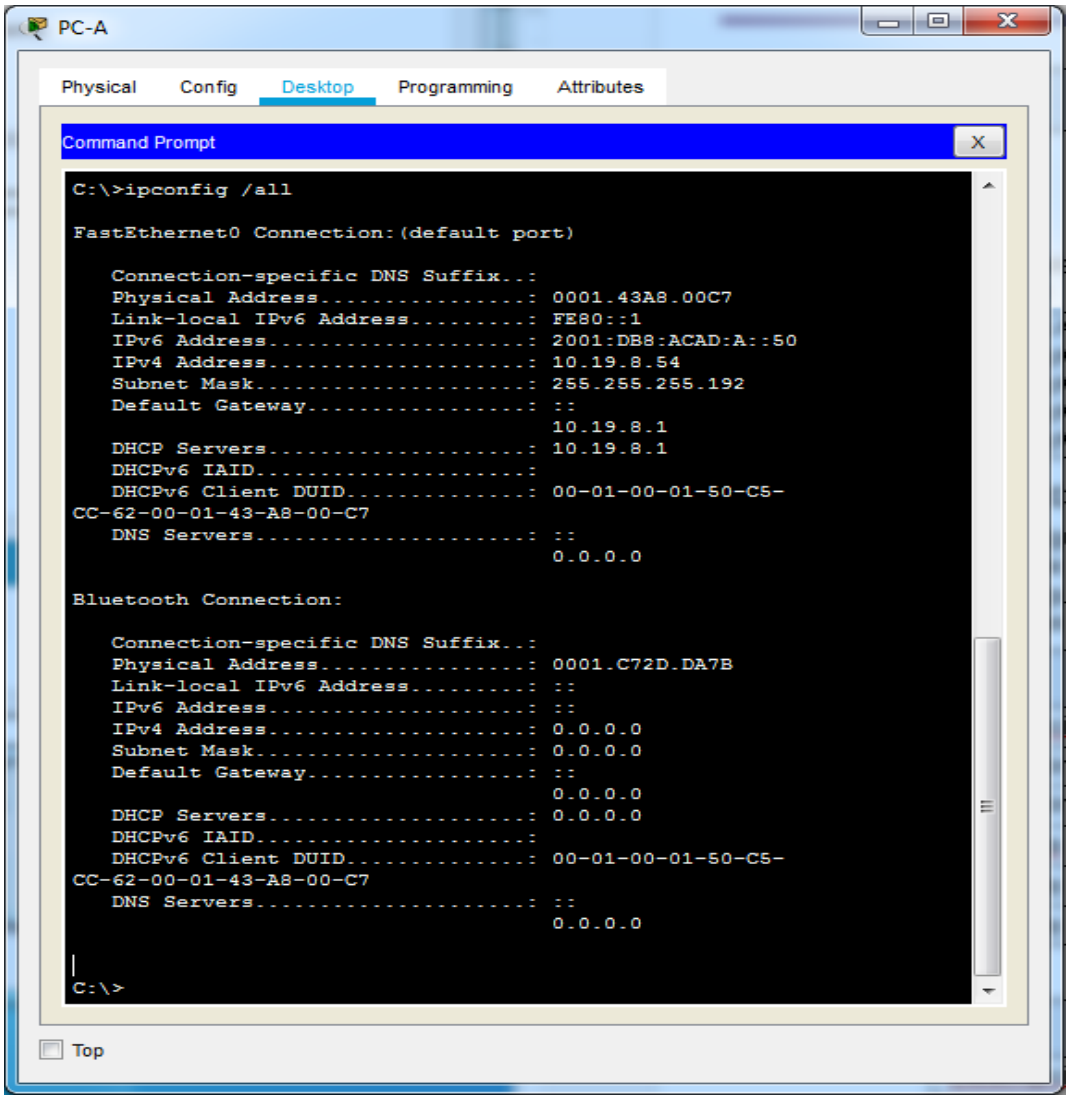
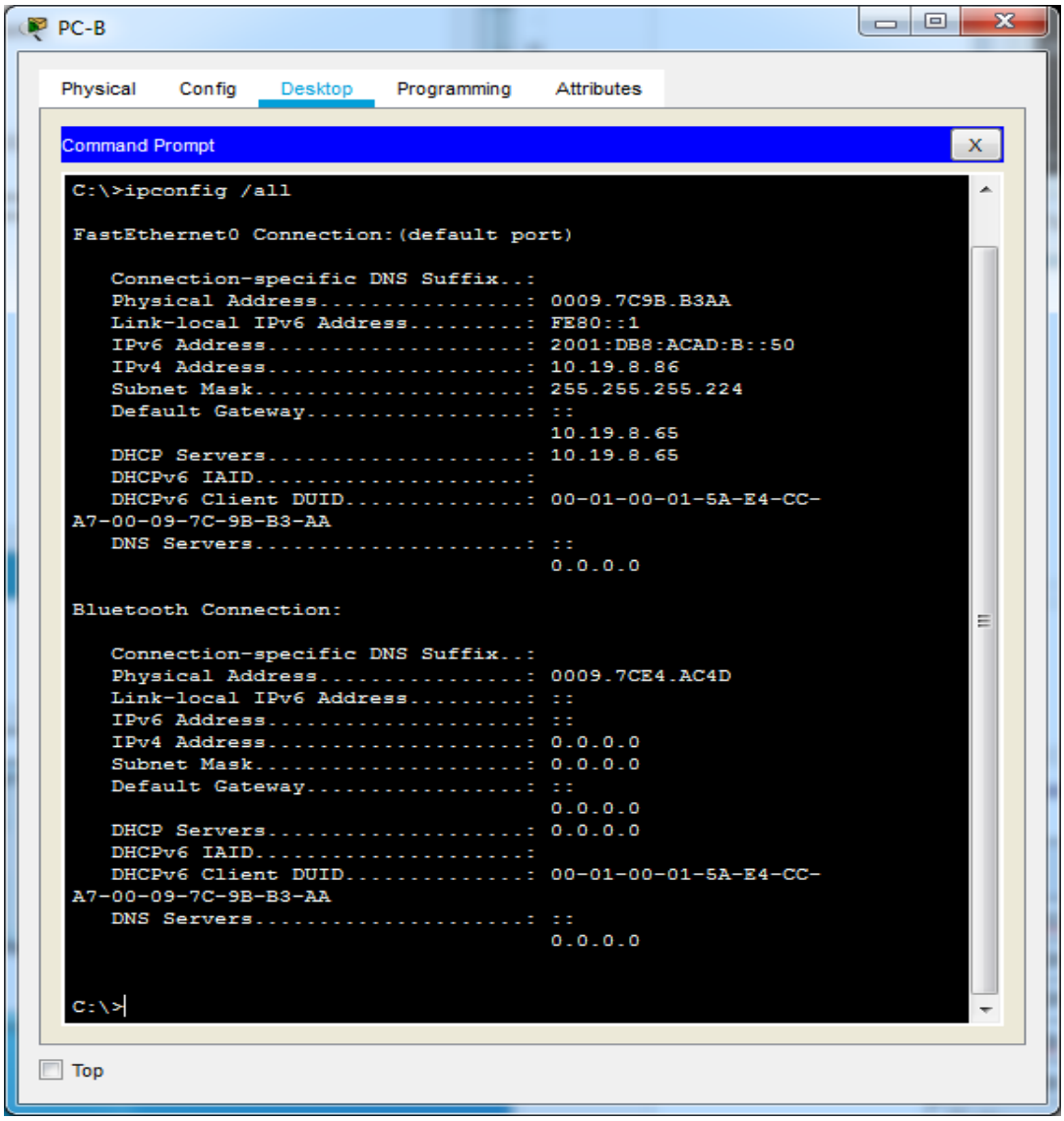


Tabla 9. Configuración de red PC-B

PC-B Network Configuration	
Descripción	*FastEthernet0 Connection:(default port)*
Dirección física	*0009.7C9B.B3AA*
Dirección IP	*10.19.8.86*
Mascara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

Figura 3. Configuración de red PC-B



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 10. Verificación de conectividad mediante el comando ping desde los PC-A y PC-B

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

Command Prompt

```
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=235ms 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 = 235ms, Average = 58ms

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=97ms 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 = 97ms, Average = 24ms

C:\>
```

PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	*Ok*
PC-A	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	

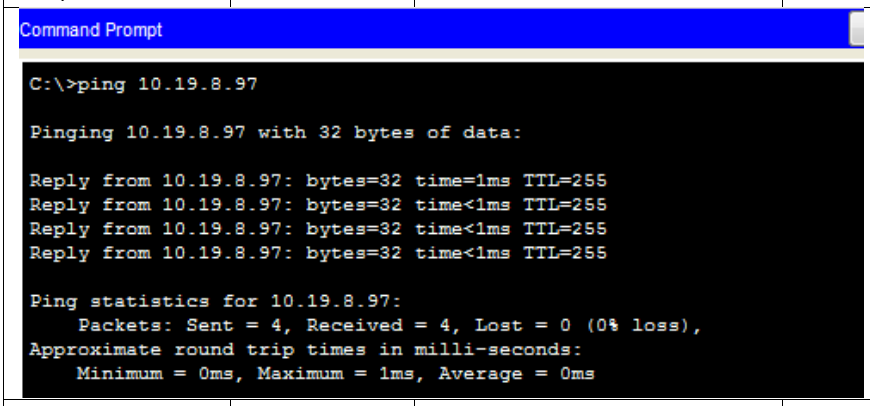
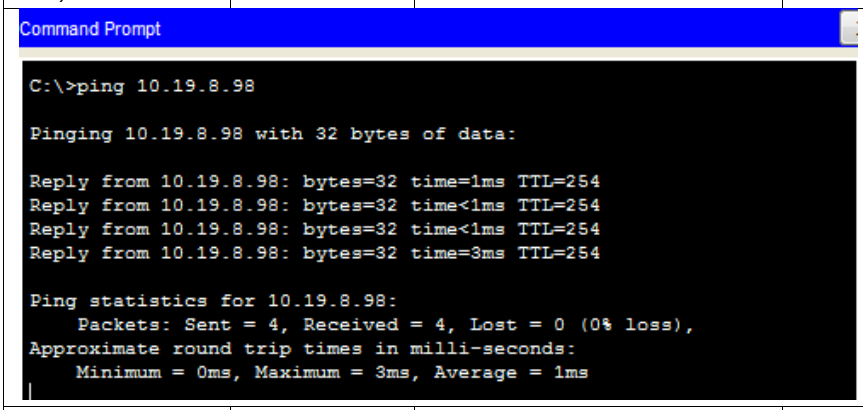
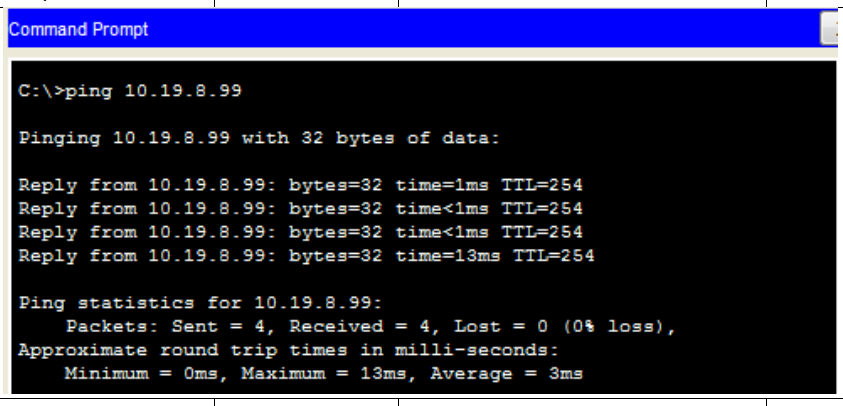
Command Prompt

```
C:\>ping 10.19.8.65

Pinging 10.19.8.65 with 32 bytes of data:

Reply from 10.19.8.65: bytes=32 time=2ms TTL=255
Reply from 10.19.8.65: bytes=32 time=3ms TTL=255
Reply from 10.19.8.65: bytes=32 time<1ms TTL=255
Reply from 10.19.8.65: bytes=32 time=1ms TTL=255

Ping statistics for 10.19.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	*Ok*
PC-A	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	*en blanco*
				
PC-A	S1, VLAN 4	Dirección	10.19.8.98	*Ok*
PC-A	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	*en blanco*
				
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	*Ok*
PC-A	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	*en blanco*
				
PC-A	PC-B	Dirección	IP address will vary.	*Ok*

<table>
<tr><th>Desde</th><th>A</th><th>de Internet</th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td rowspan="3">PC-A</td><td>PC-B</td><td>IPv6</td><td>2001:db8:acad:b: :50</td><td>en blanco</td></tr>
<tr><td colspan="4">Command Prompt

C:\>ping 10.19.8.86

Pinging 10.19.8.86 with 32 bytes of data:

Reply from 10.19.8.86: bytes=32 time=1ms TTL=127
Reply from 10.19.8.86: bytes=32 time=11ms TTL=127
Reply from 10.19.8.86: bytes=32 time=13ms TTL=127
Reply from 10.19.8.86: bytes=32 time<1ms TTL=127

Ping statistics for 10.19.8.86:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 6ms</td></tr>
<tr><td>R1 Bucle 0</td><td>Dirección</td><td>209.165.201.1</td><td>Ok</td></tr>
<tr><td>PC-A</td><td>R1 Bucle 0</td><td>IPv6</td><td>2001:db8:acad:209: :1</td><td>en blanco</td></tr>
<tr><td>PC-A</td><td colspan="4">Command Prompt

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=1ms 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<1ms 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 = 0ms, Maximum = 1ms, Average = 0ms</td></tr>
<tr><td>PC-B</td><td>R1 Bucle 0</td><td>Dirección</td><td>209.165.201.1</td><td>Ok</td></tr>
<tr><td rowspan="2">PC-B</td><td>R1 Bucle 0</td><td>IPv6</td><td>2001:db8:acad:209: :1</td><td>en blanco</td></tr>
<tr><td colspan="4">Command Prompt

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=1ms 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=3ms 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 = 0ms, Maximum = 3ms, Average = 1ms</td></tr>
<tr><td>PC-B</td><td>R1, G0/0/1.2</td><td>Dirección</td><td>10.19.8.1</td><td>Ok</td></tr>
</table>

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	*R1, G0/0/1.2*	IPv6	2001:db8:acad:a: :1	*en blanco*
	Command Prompt 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			
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	*Ok*
PC-B	*R1, G0/0/1.3*	IPv6	2001:db8:acad:b: :1	*Ok*
	Command Prompt C:\>ping 10.19.8.65 Pinging 10.19.8.65 with 32 bytes of data: Reply from 10.19.8.65: bytes=32 time=1ms TTL=255 Reply from 10.19.8.65: bytes=32 time=4ms TTL=255 Reply from 10.19.8.65: bytes=32 time=1ms TTL=255 Reply from 10.19.8.65: bytes=32 time=1ms TTL=255 Ping statistics for 10.19.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 4ms, Average = 1ms C:\>ping 2001:db8:acad:b::1 Pinging 2001:db8:acad:b::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:B::1: bytes=32 time=47ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 47ms, Average = 11ms			
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	*Ok*
PC-B	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	*en blanco*

Desde	A	de Internet	Dirección IP	Resultados de ping
	Command Prompt 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=11ms 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 = 11ms, Average = 2ms			
PC-B	S1, VLAN 4	Dirección	10.19.8.98	*Ok*
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	*en blanco*
	Command Prompt C:\>ping 10.19.8.98 Pinging 10.19.8.98 with 32 bytes of data: Reply from 10.19.8.98: bytes=32 time=1ms TTL=254 Reply from 10.19.8.98: bytes=32 time=14ms TTL=254 Reply from 10.19.8.98: bytes=32 time<1ms TTL=254 Reply from 10.19.8.98: bytes=32 time<1ms TTL=254 Ping statistics for 10.19.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 14ms, Average = 3ms			
PC-B	S2, VLAN 4	Dirección	10.19.8.99	*Ok*
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	*en blanco*
	Command Prompt 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=1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 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 = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms			

ESCENARIO 2

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.

Figura 4. Topología Escenario2

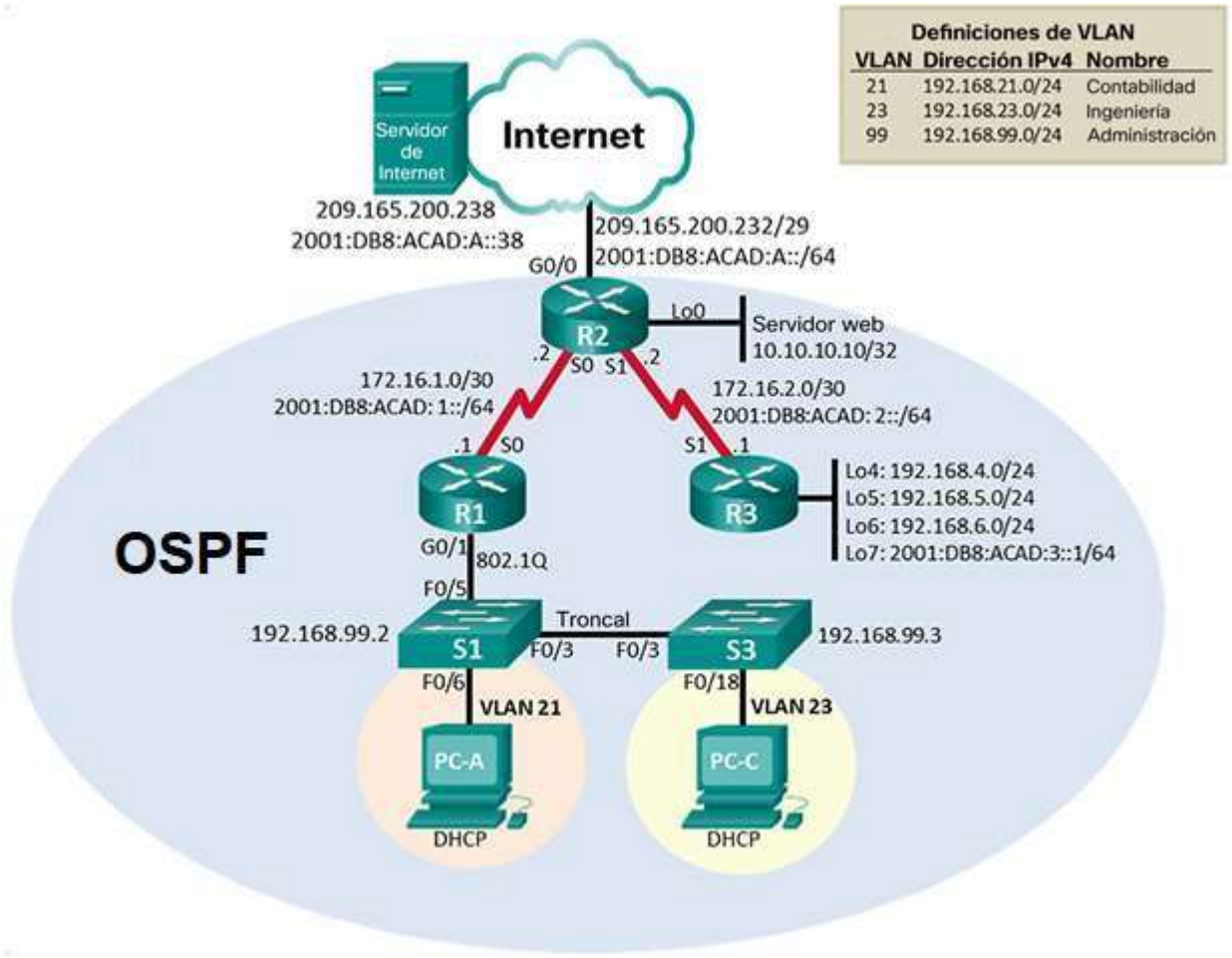


Tabla 11. Asignación de direcciones de acuerdo al diagrama de Topología Escenario2

	Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminado
Server Internet	Fa 0	209.165.200.238 /29	
		2001:DB8:ACAD:A::38 /64	
R1	G0/1.21 VLAN Contabilidad	192.168.21.1 /24	
	G0/1.23 VLAN Ingenieria	192.168.23.1 /24	
	G0/1.99 VLAN Administración	192.168.99.1 /24	
	S0/0/0	172.16.1.1 /30	
R2	Loopback (Servidor Web simulado)	10.10.10.10 /32	
	G0/0(simulación de internet)	209.165.200.233	
		2001:DB8:ACAD:A::1 /64	
	S0/0/0	172.16.1.2 /30	
		2001:DB8:ACAD:1::2 /64	
	S0/0/1	172.16.2.2 /30	
		2001:DB8:ACAD:2::2 /64	
R3	S0/0/1	172.16.2.1 /30	
		2001:DB8:ACAD:2::1 /64	
	Lo4 Lo5 Lo6 Lo7	192.168.4.1 /24 192.168.5.1 /24 192.168.6.1 /24 2001:DB8:ACAD:3::1 /64	
S1	INT VLAN 99	192.168.99.2	192.168.99.1
	F0/3	Trunk VLAN 1 como Nativa	
	F0/5	Trunk VLAN 1 como Nativa	

	Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminado
	F0/6	Mode access VLAN 21	
S3	F0/3	Trunk VLAN 1 como Nativa	
	F0/18	Mode access Vlan 23	
PC-A	VLAN 21	DHCPv4	
PC-B	VLAN 23	DHCPv4	

Inicializar Recargar y Configurar aspectos básicos de los dispositivos

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.

Tabla 12. Tareas de inicialización y carga de los Routers R1, R2, R3 y Switches S1 y S3

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#dir Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 3 -rw- 4670455 <no date> c2960-lanbasek9-mz.150-2.SE4.bin 2 -rw- 1093 <no date> config.text 64016384 bytes total (54929915 bytes free)

Configurar los parámetros básicos de los dispositivos

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 13. Tareas de configuración del Servidor de Internet

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

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

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Tareas de configuración básica R1 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router(config)#ho 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	R1(config)#service password-encryption
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

Nota: Todavía no configure G0/1.

Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 15. Tareas de configuración básica R2 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
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	R2(config)#service password-encryption
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.

Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 16. Tareas de configuración básica R3 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup
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	R3(config)#service password-encryption
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	

Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 17. Tareas de configuración básica S1 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
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	S1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 18. Tareas de configuración básica S3 Escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del switch	S3
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	S3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

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 19 Tabla de verificación de conectividad de la red entre R1 R2 y R3

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms R1#

R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms R2#
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time=1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>

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

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

Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 20. Configuración de las VLAN, Routing entre ellas y Seguridad de los Puertos de S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
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	S1(config)#int F0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2 S1(config-if-range)#switchport port-security S1(config-if-range)#int range f0/4-5 S1(config-if-range)#switchport port-security S1(config-if-range)#int range f0/7-24 S1(config-if-range)#switchport port-security S1(config-if-range)#int range g0/1-2 S1(config-if-range)#switchport port-security

Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 21. Configuración de las VLAN, Routing entre ellas y Seguridad de los Puertos de S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
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 23	S3(config)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23

Apagar todos los puertos sin usar	S3(config)#int range f0/1-2 S3(config-if-range)#switchport port-security S3(config-if-range)#int range f0/4-17 S3(config-if-range)#switchport port-security S3(config-if-range)#int range f0/19-24 S3(config-if-range)#switchport port-security S3(config-if-range)#int range g0/1-2 S3(config-if-range)#switchport port-security

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Tabla de configuración de las Subinterfaces y las Respectivas VLAN de acuerdo al direccionamiento de la figura correspondiente al escenario 2.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
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 R1(config-if)#no shu

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 23. Validación de conectividad entre las troncales configuradas entre R1, S1 y S3 escenario 2

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/6 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms S3#

Configurar el protocolo de routing dinámico OSPF

Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Configuración del protocolo re routing OSPF en R1 Escenario2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1 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
Anunciar las redes conectadas directamente	
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface default Luego activamos las interfaces WAN en este caso S0/0/0 R1(config-router)#no passive-interface S0/0/0
Desactive la sumarización automática	R1(config-router)#no auto-summary **N/A**

Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Configuración del protocolo re routing OSPF en R2 Escenario2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2 R2(config-router)#net R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)# 05:10:09: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	**N/A**

Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 26. Configuración del protocolo re routing OSPFv3 en R2 Escenario2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#ipv6 router ospf 1 % IPv6 routing not enabled R2(config)#ipv6 unicast-routing R2(config)#ipv6 router ospf 1 R2(config-rtr)#router-id 4.4.4.4
Anunciar redes IPv4 conectadas directamente	R2(config)#int s0/0/0 R2(config-if)#ipv6 ospf 1 area 0 R2(config-if)#int s0/0/1 R2(config-if)#ipv6 ospf 1 area 0 R2(config-if)#int g0/0 R2(config-if)#ipv6 ospf 1 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config-rtr)#passive-interface lo0
Desactive la sumarización automática.	**N/A**

Verificar la información de OSPF

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

Tabla 27. Verificación de las rutas creadas a partir de protocolo OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#sh ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2#sh ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#sh ip ospf

Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 28. Configuración de R1 como servidor DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado **R1(config)#ip dhcp pool ACCT** **R1(dhcp-config)#network 192.168.21.0 255.255.255.0** **R1(dhcp-config)#dns-server 10.10.10.10** **R1(dhcp-config)#domain-name ccna-sa.com** **R1(dhcp-config)#default-router 192.168.21.1**
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado **R1(config)#ip dhcp pool ENGNR** **R1(dhcp-config)#network 192.168.23.0 255.255.255.0** **R1(dhcp-config)#dns-server 10.10.10.10** **R1(dhcp-config)#domain-name ccna-sa.com** **R1(dhcp-config)#default-router 192.168.23.1**

Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 29. Configuración Base de datos Local y Servicio de Web en R2, Configuración de NAT estático y dinámico.

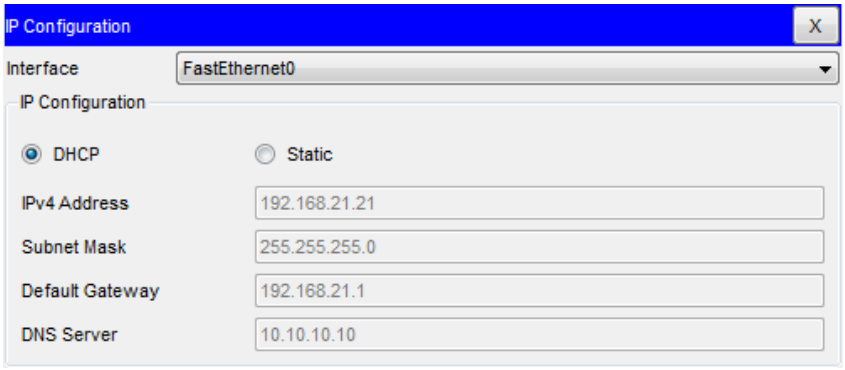
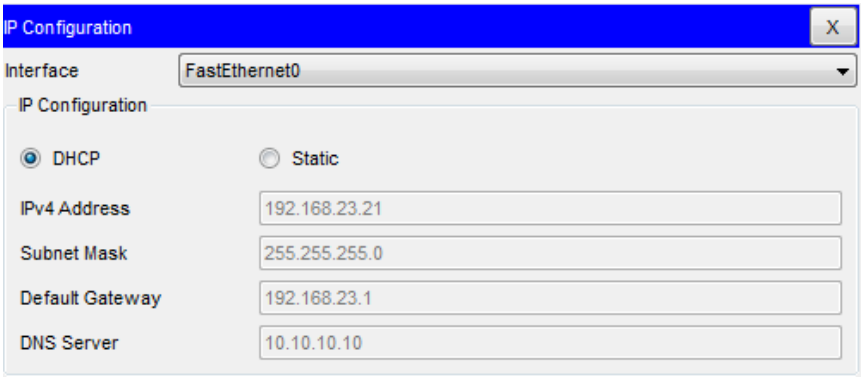
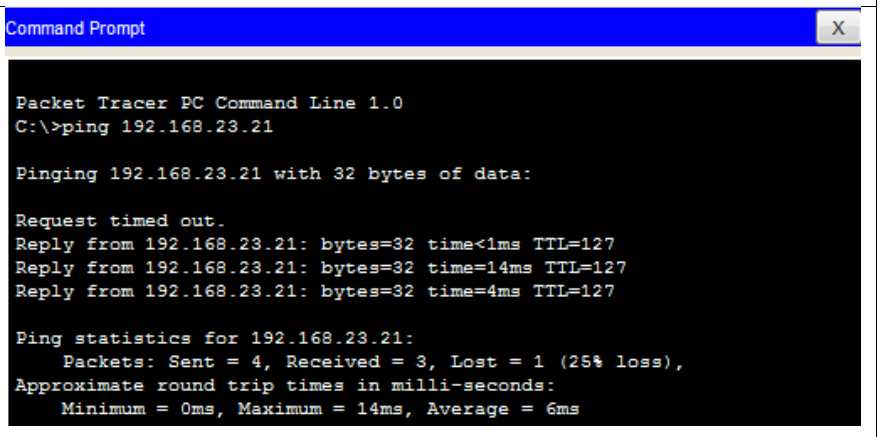
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	**Packet Tracer no soporta esta configuración a pesar de haber actualizado el IOS a la 15.5 Universalk9**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**Packet Tracer no soporta esta configuración a pesar de haber actualizado el IOS a la 15.5 Universalk9**

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
R2(config)#**ip nat inside source static 10.10.10.10 209.165.200.229**	
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int lo0 R2(config-if)#ip nat inside R2(config-if)#int g0/0 R2(config-if)#ip nat outside
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** con el siguiente comando cree el pool de las IPS públicas con las cuales podremos realizar el NAT dinámico R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#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 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#int g0/0 R2(config-if)#ip nat outside

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.

Tabla 30. Verificación del servicio DHCPV4 en R1 para asignación de IP´s dinámicas a PC-A y PC-C. Validación NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
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 **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	No Fue posible configurarlo.

Configurar NTP

Tabla 31. Configuración protocolo NTP para sincronización de fecha y Hora.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** Aquí asignamos la hora y fecha de manera manual.
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

Tabla 32. Tareas de configuración ACL para restricción de líneas VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
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	

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	
Restablecer los contadores de una lista de acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	

CONCLUSIONES

Se logra conocer los comandos básicos y sus diferentes sintaxis para la configuración de los dispositivos intermedios.

Se logra aplicar la configuración básica de una red compuesta por un router, 2 switches y dos estaciones enrutadas cada una por una Vlan, donde adicional se puso en práctica la configuración de las troncales, medios de acceso y un etherchannel compuesto por 2 enlaces.

Se puso en práctica las diferentes sintaxis para la aplicación de seguridad de acceso a los diferentes dispositivos de la red.

Este trabajo me ha permitido aprender sobre las diferentes configuraciones que me permitirán administrador y controlar una red a partir de herramientas con las listas de Acceso, los NATS.

También me ha permitido comprobar el protocolo de enrutamiento OSPF, lo cual de cierta manera nos da ciertas ventajas al descubrir rutas de forma automática, pero también tiene la desventaja de exponer mensajes que puede ser perjudiciales en la seguridad de la red.

BIBLIOGRAFÍA

CCNA Routing and Switching: Introducción a las redes. CP CCNA1 II- 2020 16-04. Cap. 6-8, 11. https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

Routing y switching de CCNA: Principios básicos de routing y switching. CP CCNA2 II- 2020 16-04. Caps. 1-3. https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#1.1.1.1

VLANS. Routing y switching de CCNA: Principios básicos de routing y switching. CP CCNA2 II- 2020 16-04. Cap. 6 https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#6.1.1.1

Configuración de ACL de IPv4 estándar. Routing y switching de CCNA: Principios básicos de routing y switching. CP CCNA2 II- 2020 16-04. Cap. 7 https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#7.2.1

Configurar NAT. Routing y switching de CCNA: Principios básicos de routing y switching. CP CCNA2 II- 2020 16-04. Cap. 9 https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#9.2

Ethernet Channel y Port Channel. Posted on 7 septiembre, 2017 actualizado el 15 septiembre, 2017, disponible en: https://todopacketracer.com/2017/09/07/ethernet-channel-y-port-channel/

De Leon, E. (16 de Oct. De 2016). SUBNETEO DE REDES [CAPITULO I] {Teoría, Dirección IP, Clases de IP}. Obtenido de: https://www.youtube.com/watch?v=kceWXMaJsew

De Leon, E. (22 de Oct. De 2016). SUBNETEO DE REDES [CAPITULO II] {Dirección IP, Mascara de red}. Obtenido de: https://www.youtube.com/watch?v=YTdmzlYM-u0

De Leon, E. (30 de Oct de 2016). SUBNETEO DE REDES [CAPITULO III] {Conversiones, Fórmulas Subredes y Hosts, Salto de Red}. Obtenido de: https://www.youtube.com/watch?v=NVBYx8iHpwQ

De Leon, E. (20 de Sep. de 2015). *Subneteo VLSM (VLSM Subnetting)* Como crear subredes con el método de VLSM. Obtenido de: https://www.youtube.com/watch?v=KsMXVnqQ3sg

Reyes, B (26 de Jul de 2019). Cómo escribir referencias bibliográficas en ICONTEC por número de autores. Disponible en: https://www.youtube.com/watch?v=qIBCZPdXbTY

Diplomado CP CCNA1 II- 2020 16-04. Cap. 1-11, disponible en: https://www.netacad.com/portal/learning

Thaheem, Suhrab. How to enable / Configure IPv6 on Cisco 2960 switch using packet tracer and how to upgrade IOS v15 on cisco 2960 swich from tftp server in packet tracer. 10 abr. 2020. 7:59 minutos. Disponible en: https://www.youtube.com/watch?v=PhuI895gUOY

CIPA 2 Prueba de Habilidades Diplomado Cisco. 16/16/2020 16:04. Disponible en: https://drive.google.com/file/d/1XTTmvwmU_Z-4SDMoRom6HeJSAJiqj_Q6/view

Diplomado CP CCNA2 II- 2020 16-04. Caps. 1-11 disponible en: https://lms.netacad.com/course/view.php?id=91200

Tipos de NAT y configuración en Cisco. 06 de junio de 2010 Leandro Di Tommaso, disponible en: https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/

ANEXOS

Anexo 1: Vinculo de descarga archivos de Simulación

https://drive.google.com/file/d/10_Id-dZMuuh4t8AL65fnp3tS9JuwD2i8/view?usp=sharing
https://drive.google.com/file/d/1BmFTYNZUtguphk_sS1KNBRSXPLM0oHXP/view?usp=sharing

Anexo 2: Artículo Científico IEEE

Solución de dos escenarios presentes en entornos corporativos bajo el uso de tecnología CISCO

Solution of two scenarios present in corporate environments using CISCO technology

Autor: William Arturo

Código 79667309
(Diciembre de 2020

RESUMEN

El presente documento corresponde al trabajo final "Diplomado de profundización CISCO, prueba de habilidades prácticas CCNA. Aquí encontraremos el desarrollo de los 2 escenarios propuestos, los cuales fueron desarrollados mediante la herramienta Packet Tracer. Se encontraran las configuraciones realizadas y sus respectivas evidencias mediante imágenes tomadas al momento de realizar el desarrollo en esta herramienta.

Realice las configuraciones básicas de seguridad para cada uno de los dispositivos y configuraciones tales como trunking, switching, routing mediante el uso de protocolos como OSPF y DHCPv4 entre otros.

Desarrolle las diferentes pruebas de conexión solicitadas para los diferentes eventos.

PALABRAS CLAVE

CCNA; CISCO; Conmutación; Electrónica; Enrutamiento; Redes.

ABSTRACT

This document corresponds to the final work "CISCO Deepening Diploma, CCNA Practical Skills Test. Here we will find the development of the 2 proposed scenarios, which were developed using the Packet Tracer tool. The configurations made and their respective evidences will be found by images taken at the time of the development in this tool.

Perform the basic security settings for each of the devices and configurations such as trunking, switching, routing by using protocols such as OSPF and DHCPv4 among others.

Develop the different connection tests requested for the different events.

KEYWORDS

CCNA; CISCO; Switching; Electronics; Routing; Networking.

1. INTRODUCCIÓN

Esta prueba de habilidades nos ha permitido poner en práctica los conocimientos obtenidos durante todas las unidades desarrolladas en el Diplomado de profundización Cisco.

Durante el desarrollo de los dos escenarios se pusieron en práctica los procesos de configuración y de seguridad básicos de los dispositivos intermedios como fueron routers y Switches, sin embargo previo a estas configuraciones se han realizado los procesos de validación de vlans previamente configuradas y la inicialización de los routers y switches utilizados en el proceso con la finalidad de realizar las configuraciones desde cero.

He realizado la creación, configuración y direccionamiento de Vlans, definiendo los diferentes segmentos como accesos y troncales, de acuerdo a las disposición, mediante el protocolo 802.1Q, donde también se asignó la Vlan 6 como nativa.

En este proceso de configuración de vlans se observa la segmentación virtual de las redes para obtener una mejor calidad de comunicación y un mayor ancho de banda mediante la configuración de un canal EtherChannel a través del protocolo LACP entre los 2 switches utilizados.

Se realizó la configuración del default routing con la finalidad de dirigir el tráfico a la interfaz Loopback.

Se hizo uso de un router como servidor de DHCPv4 permitiendo asignar direcciones IP de forma automática.

Una vez realizada toda la configuración se procedió a la validación de las configuraciones y conectividad desde cada uno de los puntos solicitados.

Se experimentó la forma de realizar el routing tanto de forma manual como de forma automática mediante el uso del protocolo OSPFv2 y OSPFv3.

Se propuso la configuración de un servidor WEB y conexión a internet lo cual no fue posible validarlo debido a que Packet tracer no soporta algunas configuraciones y por lo tanto es necesario hacerlas en dispositivos reales.

2. METODOLOGÍA

Dentro del proceso de simulación de los respectivos escenarios, se utilizó la herramienta Packet Tracer, la cual nos aportó en un 98% para la realización del laboratorio, ya que algunas de las actividades solicitadas no eran soportadas por la herramienta.

Se siguió la guía propuesta en cada uno de los escenarios paso a paso, buscando obtener los mejores resultados, los cuales fueron validados y puestos en evidencia mediante la captura de pantallas.

3. RESULTADOS

Se pueden destacar dentro del proceso la configuración básica y de seguridad de los dispositivos los cuales fueron inicializados y configurados desde cero de forma satisfactoria, aunque en algunas ocasiones fue necesario descargar y actualizar algunas versiones de los dispositivos para realizar las tareas solicitadas. Esto nos permitió fortalecer los procesos tanto de generación de backup como el poder restaurar algunos de ellos.

4. CONCLUSIONES

En general el desarrollo de estos dos escenarios nos permitió conocer y aplicar los diferentes comandos IOS para la configuración de dispositivos intermedios logrando realizar una conexión de red con las condiciones de seguridad básica y permitiéndonos desarrollar procesos de enrutamiento tanto manuales como automáticos a través de los diferentes protocolos de enrutamiento, especialmente OSPF.

5. AGRADECIMIENTOS

Un gran agradecimiento a nuestro tutor José Ignacio Cardona, quien siempre estuvo pendiente de los avances y posibles falencias que pudiéramos tener durante el proceso de configuración y optimización de los dos escenarios.

8. REFERENCIAS

Ethernet Channel y Port Channel. Posted on 7 septiembre, 2017 actualizado el 15 septiembre, 2017, disponible en: https://todopacketracer.com/2017/09/07/ethernet-channel-y-port-channel/

Diplomado CP CCNA1 II- 2020 16-04. Cap. 1-11, disponible en: https://www.netacad.com/portal/learning

Thaheem, Suhrab. How to enable / Configure IPv6 on Cisco 2960 switch using packet tracer and how to upgrade IOS v15 on cisco 2960 swich from tftp server in packet tracer. 10 abr. 2020. 7:59 minutos. Disponible en: https://www.youtube.com/watch?v=PhuI895gUOY

CIPA 2 Prueba de Habilidades Diplomado Cisco. 16/16/2020 16:04. Disponible en: https://drive.google.com/file/d/1XTTmvwmU_Z-4SDMoRom6HeJSAJiqj_Q6/view

Diplomado CP CCNA2 II- 2020 16-04. Caps. 1-11 disponible en: https://lms.netacad.com/course/view.php?id=91200

Tipos de NAT y configuración en Cisco. 06 de junio de 2010 Leandro Di Tommaso, disponible en: https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/