SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

RAUL MENJURA MACHADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SITEMAS
BOGOTÁ, COLOMBIA
2020

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

RAUL MENJURA MACHADO

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR POR EL TITULO DE INGENIERO DE SISTEMAS

TUTOR

Ingeniero JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS E TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SITEMAS
BOGOTÁ, COLOMBIA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, Diciembre de 2020

DEDICATORIA

A mis padres Melany y Parmenio quienes con su paciencia, impulso y orientación me permitieron llegar a cumplir este sueño profesional cultivando la creencia en Dios y cómo enfrentar las dificultades y no decaer ante ellas.

A mi esposa Diana y mis hijos Daniela, Valentina y Juan Diego por su amor y compañía incondicional en todo el proceso académico de formación, agradecer porque con sus oraciones, consejos y palabras de aliento me motivaron para terminar este reto y afrontar los que están por venir.

AGRADECIMIENTOS

Al personal de docentes y directivos de Universidad Nacional Abierta y a Distancia - UNAD, por brindar un entorno de alta calidad educativa, aprovechando las herramientas de la última generación que permiten el adecuado uso de la tecnología enfocada a formar mejores profesionales con valores éticos y de pertenencia que se incorporan de manera exitosa al mundo laboral en pro de un mejor país.

CONTENIDO

GLOSARIO

DHCP

Protocolo que permite la configuración automática de red de los hosts de una red TCP/IP mediante un mecanismo de cliente-servidor.

Ethernet

Protocolo LAN ampliamente utilizado, inventado por Xerox Corporation y desarrollado por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y se ejecutan a través de una variedad de tipos de cables a 10 Mbps o 100 Mbps. Ethernet es similar a la serie de estándares IEEE 802.3.

Host

Equipo, como un PC u otro dispositivo informático como un servidor, asociado a una dirección IP individual y, opcionalmente, a un nombre. Nombre de cualquier dispositivo en una red TCP/IP que tenga una dirección IP. Asimismo, cualquier dispositivo de una red al que se pueda asignar una dirección. El término nodo incluye dispositivos como routers e impresoras que, normalmente, no se denominan hosts.

Interfaz

Conexión física entre una red determinada y el router. La interfaz de LAN del router se conecta con la red local a la que proporciona servicio el router. El router cuenta con una o varias interfaces WAN que se conectan con Internet.

IOS

Software del IOS de Cisco. Software del sistema Cisco que proporciona funciones comunes, escalabilidad y seguridad para todos los productos de la arquitectura Cisco Fusion. El IOS de Cisco permite una instalación automatizada, integrada y centralizada, así como la gestión de intrarredes. Por otro lado, permite asegurar la compatibilidad de una amplia variedad de protocolos, soportes, servicios y plataformas.

IP

Protocolo de Internet. Los protocolos de Internet son la familia de protocolos de sistema abierto (no de propiedad) más conocida del mundo ya que pueden utilizarse para establecer una comunicación entre cualquier conjunto de redes interconectadas y sirven tanto para comunicaciones WAN como LAN.

MÁSCARA DE SUBRED

Máscara de 32 bits que especifica cómo se deberá dividir una dirección de Internet en las partes correspondientes a red, subred y host. La máscara de red tiene unos (1) en las posiciones de los bits de la dirección de 32 bits que deben utilizarse para las partes de la red y de la subred, mientras que tiene ceros (0) para la parte correspondiente al host. La máscara debe contener como mínimo la porción de la red estándar (tal como determina la clase de dirección) y el campo subred debe estar al lado de la porción correspondiente a la red. La máscara se configura con el decimal equivalente del valor binario.

RESUMEN

En un mundo tan cambiante y que requiere más conectividad e interrelación del humano y la tecnología se hace necesario contar con profesionales ampliamente entrenados y capacitados para entender y plasmar las necesidades crecientes de diversos sectores en una solución practica de manejar encilla de implementar y que minimice el impacto de la tecnología en los procesos y que además por el contrario aporte beneficios y sea amigable con los usuarios, de allí surge la necesidad del adecuado uso de las herramientas tecnológicas con CISCO y su liderazgo mundial en el mundo del networking,

En este contexto se plasman unos escenarios hipotéticos con la debida resolución para poder ser aplicada en terreno real y con la orientación de profesionales capacitados para este fin.

Se abarcan componentes básicos de configuración hasta ambientes complejos en su estructura y dimensionamiento para probar que el egresado UNAD está en capacidad de afrontar este tipo de retos facilitando así convivir la tecnología de punta con todos sus elementos y características de manera simple y funcional

Palabras Clave: Conectividad, tecnología, amigable, networking, profesional, funcional.

ABSTRACT

In a world, so changing and that requires more connectivity and interrelation of human and technology, it is necessary to have widely trained and qualified professionals to understand and translate the growing needs of various sectors into a practical solution to manage before implementing and that minimizes the impact of technology on processes and that also, on the contrary, provides benefits and is user-friendly, hence the need for the proper use of technological tools with CISCO and its world leadership in the world of networking,

In this context, some hypothetical scenarios are reflected with the proper resolution to be applied in real terrain and with the guidance of professionals trained for this purpose.

Basic configuration components are covered up to complex environments in their structure and dimensioning to prove that the UNAD graduate is able to face this type of challenge, thus facilitating the coexistence of cutting-edge technology with all its elements and characteristics in a simple and functional way.

Keywords: Connectivity, technology, friendly, networking, professional, functional.

INTRODUCCIÓN

Se aplica la parte teórica abarcada en las unidades vistas en orientación a darle resolución aun escenario hipotético planteado, vislumbrando lo aprendido en el avance del diplomado de profundización CISCO y la adecuada utilización de medios tecnológicos para tal fin dando uso a los diversos módulos estudiados CCNA1 y CCNA2.

DESARROLLO

Se plantean dos escenarios que se desarrollarán basados en los conocimientos adquiridos así: 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.

Para el escenario dos 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.

ESCENARIO 1

Topología

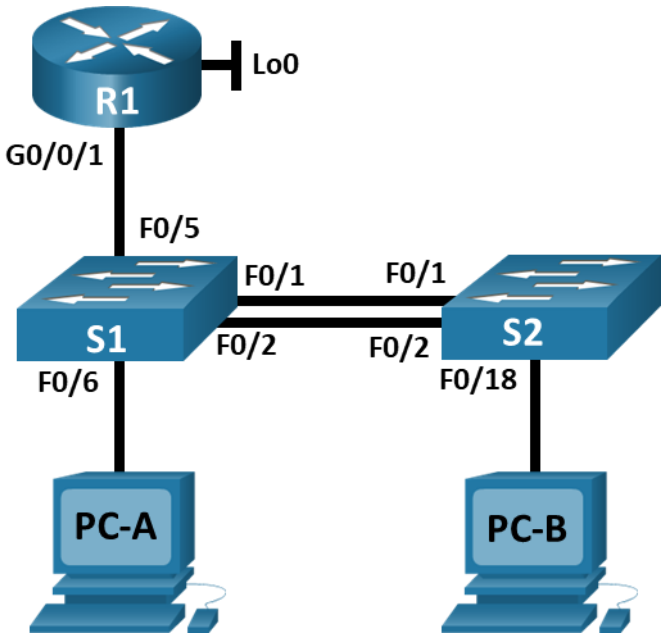


Tabla de VLAN

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

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

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

Instrucciones

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.

Mediante la consola nos conectamos a cada dispositivo R1, S1, S2 y ejecutamos
#**enable**
#**erase startup-config**
#**reload**

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

En este paso el objetivo primordial es el ajuste de los dispositivos para que sean accesibles con medidas de seguridad como password, incluyendo un password, si no se conoce la contraseña de acceso aparecerá el mensaje de acceso no permitido, sirviendo esto como método disuasivo para usuarios no autorizados.

También se asigna la información de red (dirección ip, mascara de red, Gateway) logrando que los dispositivos sean identificados y accedido en el entorno virtual de red.

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass

Tarea	Especificación
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Prohibido el Acceso No Autorizado#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	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

Tarea	Especificación
Configure el Loopback0 interface	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	R1(config)#crypto key generate rsa 1024

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación S1	Especificación S2
Desactivar la búsqueda DNS.	Switch1>enable Switch1#config terminal Switch1 (config)#no ip domain lookup	Switch2>enable Switch2#config terminal Switch2 (config)#no ip domain lookup
Nombre del switch	Switch1(config)#hostname S1	Switch2(config)#hostname S2
Nombre de dominio	S1(config)#ip domain name ccna-lab.com	S2(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass	S2(config)#username admin secret admin1pass

Tarea	Especificación S1	Especificación S2
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit	S2(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption	S2(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Prohibido el Acceso No Autorizado#	S2(config)#banner motd #Prohibido el Acceso No Autorizado#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa 1024	S2(config)#crypto key generate rsa 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management Interface S1(config-if)#no shutdown S1(config-if)#exit	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
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97	S1(config)#ip default-gateway 10.19.8.97

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

En esta parte realizaremos conexiones lógicas conocidas como VLAN, para tener la capacidad de mejorar el rendimiento de la red, segmentando la difusión logrando eficiencia y desempeño, seguridad, eficiencia y mejor utilización de los recursos humanos y físicos

Aplicaremos la configuración Trunking que lo podemos asimilar con el tronco de un árbol que lleva agua a cada rama y hoja, un trunking de red esencialmente transporta múltiples flujos de señales a las ubicaciones correctas, esto lo hace mediante el uso de un protocolo llamado IEEE 802.1Q, que lo que hace es agregar una etiqueta a la trama cada vez que pasa, marcándola como perteneciente a una VLAN específica. Esta etiqueta, que incluye la dirección MAC.

Veremos también la diferencia con EtherChannel tecnología de cisco de agregación de enlaces de puertos en la que varios enlaces de puertos físicos se agrupan en un enlace lógico. Se utiliza para proporcionar redundancia y enlaces de alta velocidad.

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

Tarea	Especificación

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
	
	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	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	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security maximum 3

Tarea	Especificación
Proteja todas las interfaces no utilizadas	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 2: Configure el S2.

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

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	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	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	S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security maximum 3

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	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: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0

Tarea	Especificación
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-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	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Paso 2: Configurar los servidores

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

PC-A Network Configuration	
Descripción	
Dirección física	0010.113B.E818
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

PC-B Network Configuration	
Descripción	
Dirección física	00D0.BC5D.2404

PC-B Network Configuration	
Dirección IP	
Máscara de subred	
Gateway predeterminado	
Gateway predeterminado IPv6	

Parte 4: Probar y verificar la conectividad de extremo a extremo

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

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

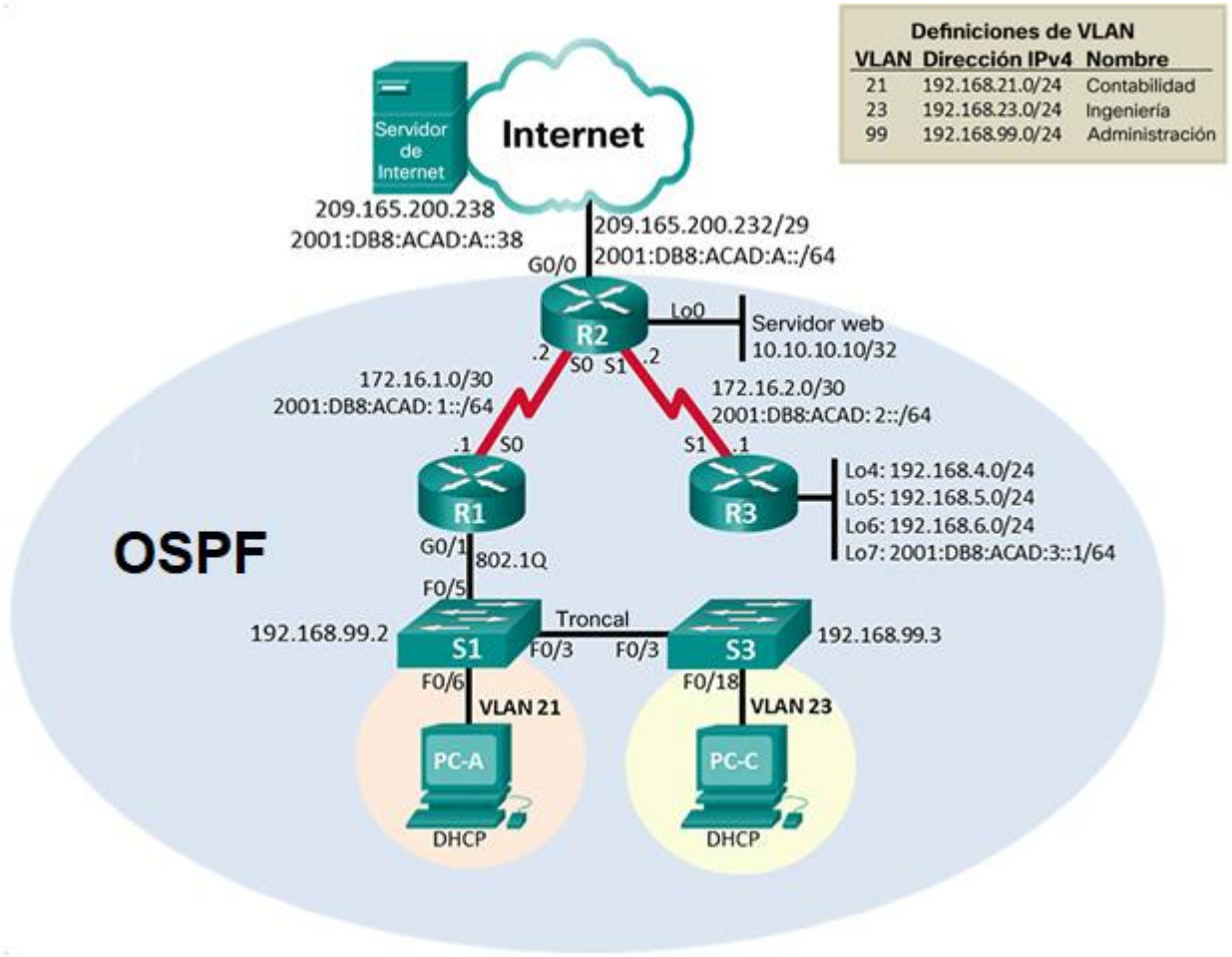
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	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

Desde	A	de Internet	Dirección IP	Resultados de ping
	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

ESCENARIO 2

Topología



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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	#erase startup-config
Volver a cargar todos los routers	#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	#erase startup-config #delete vlan.dat
Volver a cargar ambos switches	#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	#dir flash: Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225 es incorrecto la primera ip en la red 209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	#no ip domain-lookup
Nombre del router	#hostname R1
Contraseña de exec privilegiado cifrada	#enable secret class
Contraseña de acceso a la consola	#line console 0 #password cisco #login #service password-encryption
Contraseña de acceso Telnet	#line vty 0 15 #password cisco #login
Cifrar las contraseñas de texto no cifrado	#service password-encryption
Mensaje MOTD	# banner motd # Se prohíbe el acceso no autorizado. #
Interfaz S0/0/0	#int s0/0/0 #description Connection to R2 #ip address 172.16.1.1 255.255.255.252 #ipv6 address 2001:DB8:ACAD:1::1/64 #clock rate 128000 #no shutdown
Rutas predeterminadas	#ip route 0.0.0.0 0.0.0.0 s0/0/0 #ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	#no ip domain-lookup

Nombre del router	#hostname R2
Contraseña de exec privilegiado cifrada	#enable secret class
Contraseña de acceso a la consola	#line console 0 #password cisco #login
Contraseña de acceso Telnet	#line vty 0 15 #password cisco #login
Cifrar las contraseñas de texto no cifrado	#service password-encryption
Habilitar el servidor HTTP	Comando no soportado en Packet Tracer
Mensaje MOTD	# banner motd # Se prohíbe el acceso no autorizado. #
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#descripcion Connection to R1 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
Interfaz S0/0/1	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
Interfaz G0/0 (simulación de Internet)	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

Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	#no ip domain-lookup
Nombre del router	#hostname R3
Contraseña de exec privilegiado cifrada	#enable secret class
Contraseña de acceso a la consola	#line console 0 #password cisco #login
Contraseña de acceso Telnet	#line vty 0 15 #password cisco #login
Cifrar las contraseñas de texto no cifrado	#service password-encryption
Mensaje MOTD	# banner motd # Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	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
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	#no ip domain-lookup
Nombre del switch	#hostname S3
Contraseña de exec privilegiado cifrada	#enable secret class
Contraseña de acceso a la consola	#line console 0 #password cisco #login
Contraseña de acceso Telnet	#line vty 0 15 #password cisco #login
Cifrar las contraseñas de texto no cifrado	#service password-encryption
Mensaje MOTD	# banner motd # Se prohíbe el acceso no autorizado.

Paso 7: Verificar la conectividad de la red

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

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

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

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

```
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
```

```
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 = 1/2/9 ms
```

```
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
```

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:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0

Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

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

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

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

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
S1#ping 192.168.21.1

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

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	OSPF no sumariza automaticamente

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface g0/1

Desactive la sumarización automática.	OSPF no sumariza automaticamente

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.21.0 0.0.0.255 area 0 R3(config-router)#network 192.168.23.0 0.0.0.255 area 0 R3(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	OSPF no sumariza automaticamente

Paso 4: Verificar la información de OSPF

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

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#show ip protocols

¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show run

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:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#no ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

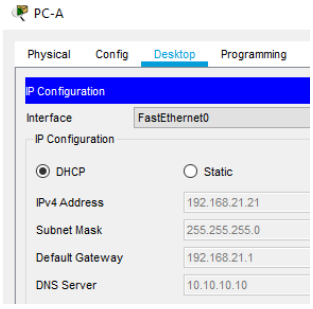
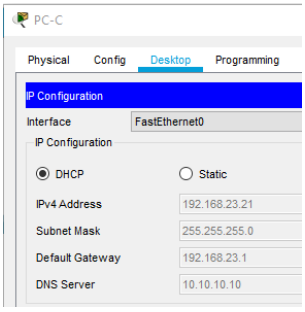
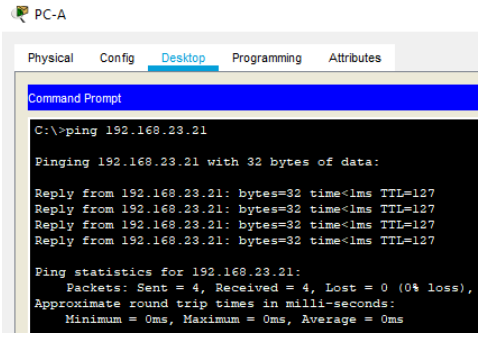
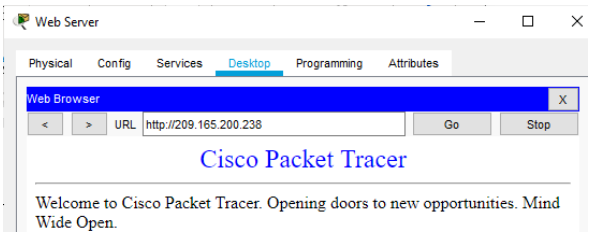
La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP	R2(config)#ip http server, Packet Tracer no soporta este comando
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local, Packet Tracer no soporta este comando
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#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)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

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 (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 8 16 37 8.00 726200685674.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Open Se prohbe el acceso no autorizado. User Access Verification Password: R2>exit [Connection to 172.16.1.2 closed by foreign host] R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists 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))
Restablecer los contadores de una lista de acceso	R2#clear ip access-lists counters NO SOPORTADO EN PACKET TRACER
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface Outgoing access list is not set Inbound access list is not set
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside global Inside local Outside local Outside global icmp 209.165.200.233:13192.168.21.21:13 209.165.200.238:13 209.165.200.238:13 icmp 209.165.200.233:14192.168.21.21:14 209.165.200.238:14 209.165.200.238:14 icmp 209.165.200.233:15192.168.21.21:15 209.165.200.238:15 209.165.200.238:15 icmp 209.165.200.233:16192.168.21.21:16 209.165.200.238:16 209.165.200.238:16 icmp 209.165.200.233:17192.168.21.21:17 209.165.200.238:17 209.165.200.238:17 icmp 209.165.200.233:18192.168.21.21:18 209.165.200.238:18 209.165.200.238:18 icmp 209.165.200.233:19192.168.21.21:19 209.165.200.238:19 209.165.200.238:19 icmp 209.165.200.233:20192.168.21.21:20 209.165.200.238:20 209.165.200.238:20 --- 209.165.200.229 209.165.200.238 --- --- --- 209.165.200.238 10.10.10.10 --- ---

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

CONCLUSIÓNES

Con el desarrollo del escenario uno, se plasma la capacidad cognitiva adquirida en el desarrollo de los módulos CISCO, partiendo de la configuración básica de los dispositivos Router y Switches y las conexiones que se realizan para el adecuado uso de las redes con eficiencia y seguridad, facilitando al realizarse en un ambiente de simulación tomar los correctivos necesarios para cuando se requiera llevar a la vida real su impacto va a ser mínimo y su implementación satisfactoria.

En el segundo escenario basados en la parte teórica proporcionada por CISCO se logra configurar la pequeña red con conectividad, seguridad, segmentación por Vlans, soportando protocolos IPv4 e IPv6, aplicando un routing dinámico que proporciona mejor desempeño a esta, con características orientadas a buenas prácticas de la industria como lo es 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, todo lo anterior funcional y operativo con adecuado uso del entorno CLI de cada dispositivo de red.

BIBLIOGRAFIA

CISCO NETWORKING ACADEMY. CCNA Exploration 4.0 - Módulo del curso de profundización CISCO Aspectos básicos del Networking. CISCO. 2013. 426 páginas.

CISCO NETWORKING ACADEMY. CCNA Exploration 4.0 - Guías de prácticas del curso de profundización CISCO Aspectos básicos del Networking. CISCO. 2013.

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

Temática: VLANs

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). 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. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.

ANEXO 1 ENLACE DE DESCARGA ARCHIVO DE SIMULACION

https://drive.google.com/drive/folders/1pFtudBQ2h0x9NdCg3tcQIKjcqkmFVqwA?usp=sharing

ANEXO 2 ARTICULO CIENTIFICO ENLACE DE DESCARGA

https://drive.google.com/file/d/1ZqvWne0zS4Cjj5hU6qlneJMyuKUAGsnK/view?usp=sharing