

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

DEISY YOLIMA CUEVAS MENDIVELSO

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

TUNJA
2020

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

DEISY YOLIMA CUEVAS MENDIVELSO

Diplomado De Opción De Grado Presentado Para Obtener El Título De Ingeniería
De Sistemas

TUTOR

Ingeniera. PAULITA FLOR SALAZAR

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

INGENIERÍA *SISTEMAS*

TUNJA

2020

NOTA DE ACEPTACIÓN

FIRMA DEL PRESIDENTE DEL JURADO

FIRMA DEL JURADO

FIRMA DEL JURADO

FIRMA DEL ASESOR

TUNJA, 30 NOVIEMBRE 2020

AGRADECIMIENTOS

Dedico este trabajo primeramente a Dios, por permitirme alcanzar una meta más en mi vida, a mi familia; por su apoyo y amor incondicional a lo largo de esta carrera y de mi vida.

Este trabajo es dedicado a todo el esfuerzo y dedicación durante la carrera de ingeniería de sistemas ya que cuando nos proponemos algo en la vida es fundamental cumplirlo a pesar de las adversidades que se puedan presentar.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN.....	11
DESARROLLO.....	12
Escenario 1.....	12
Escenario 2.....	39
CONCLUSIONES.....	71
BIBLIOGRAFÍA.....	72
ANEXOS.....	73

LISTA DE TABLAS

Tabla 1. VLAN.....	12
Tabla 2. asignación de direcciones.....	13
Tabla 3 configuración R1	14
Tabla 4. Configuración S1	16
Tabla 5 configuración S2.....	18
Tabla 6 configuración S1 Vlan.....	20
Tabla 7 creación Vlan S2	25
Tabla 8. configuración R1 con DHCP.....	29
Tabla 9. Direccionamiento Pc-A.....	30
Tabla 9.1 direccionamiento Pc—B.....	30
Tabla10. conectividad	31
Tabla 11. Inicialización R1.....	40
Tabla12. direccionamiento servidor	44
Tabla 13 configuración inicial R1.....	44
Tabla 14 configuración R2	46
Tabla 15. configuración inicial R3.....	49
Tabla 16. configuración inicial del S1	52
Tabla 17 configuración inicial S3	53
Tabla 18 conectividad	54
Tabla 19 configuración vlan en S1	55
Tabla 20 configuración Vlan S3	62
Tabla 21 configuración R1 interfaz	68
Tabla 22 conectividad	69

LISTA DE FIGURAS

Figura 1. Escenario 1.....	11
Figura 2. Simulación de escenario 1.....	12
Figura 3. Aplicando código R1.....	13
Figura 4. Aplicando código R2.....	14
Figura 5. Aplicando código R3.....	15
Figura 6. Aplicando código R4.....	16
Figura 7. Aplicando código R5.....	17
Figura 8. Interfaces de Loopback en R1.....	18
Figura 9. Interfaces de Loopback en R2.....	19
Figura 10. Interfaces de Loopback en R2.....	20
Figura 11. Configuración de IPs.....	21
Figura 12. Rutas EIGRP en OSPF.....	22
Figura 13. Comando show ip route.....	23
Figura 14. Comando show ip route.....	23
Figura 15. Escenario 2.....	24
Figura 16. Simulación del escenario 2.....	24
Figura 17. Se aplica código R1.....	25
Figura 18. Configuración código R2.....	26
Figura 19. Configuración código R3.....	27
Figura 20. Configuración código R4.....	28
Figura 21. Correcta configuración de R1 y R2.....	29
Figura 22. Correcta configuración de R1 y R2.....	30
Figura 23. Correcta configuración de R3.....	31
Figura 24. Aplicando código R4.....	32
Figura 25. Aplicando código R1.....	32
Figura 26. Aplicando código R2.....	33
Figura 27. Aplicando código R3.....	33
Figura 28. Aplicando código R4.....	34

GLOSARIO

LAN: local area network, Es una red que conecta ordenadores en un área pequeña y predeterminada ejemplo: un edificio.

VLAN: (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

NAT: (Network Address Translation ó Traducción de Dirección de Red) es un mecanismo utilizado por routers y equipos para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

ACL: es un concepto de seguridad informática usado para fomentar la separación de privilegios, esto permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches.

Enrutamiento: es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

RESUMEN

El propósito fundamental de este artículo es la articulación de acciones, tendientes a profundizar el desarrollo y aprendizaje del CISCO, para lo cual se tiene presente la configuración de diversos dispositivos que estructuran una red, con aspectos tan importantes como el tema seguridad determinado por la validación mediante el cumplimiento de un requisito preestablecido, ya sea contraseña o algo similar, como nombrar las vlan, red local y de tipo virtual , aprovechando la misma para la configuración de redes lógicas independientes, las cuales hacen parte constitutiva de la misma red física. Además, se plantea la manera de configuración con el empleo de comandos y proceso de encapsulamiento para otorgar alta seguridad a la información y equipos, procurando al máximo el robo de información o daño en los dispositivos y en la red en general. Además de lo descrito se presenta la implementación y manera de configurar el protocolo DHCP y el NAT, que facilitan el manejo de direcciones IP dentro de rangos de direcciones previamente establecidas.

Palabras claves: vlan, encapsulamiento, seguridad, DHCP, NAT, CISCO, configuración, rede

ABSTRACT

fundamental purpose of this article is the articulation of actions, tending to deepen the development and learning of the CISCO, for which the configuration of various devices that structure a network is taken into account, with aspects as important as the security issue determined by the validation by fulfilling a pre-established requirement, be it a password or something similar, such as naming the vlan, local network and virtual type, taking advantage of it for the configuration of independent logical networks, which are a constitutive part of the same physical network. In addition, the way of configuration is proposed with the use of commands and the encapsulation process to provide high security to the information and equipment, ensuring to the maximum the theft of information or damage to the devices and the network in general. In addition to what has been described, the implementation and way of configuring the DHCP protocol and NAT are present which facilitate the management of IP addresses within previously established address ranges.

Keywords: vlan, encapsulation, security, DHCP, NAT, CISCO, configuration, networks.

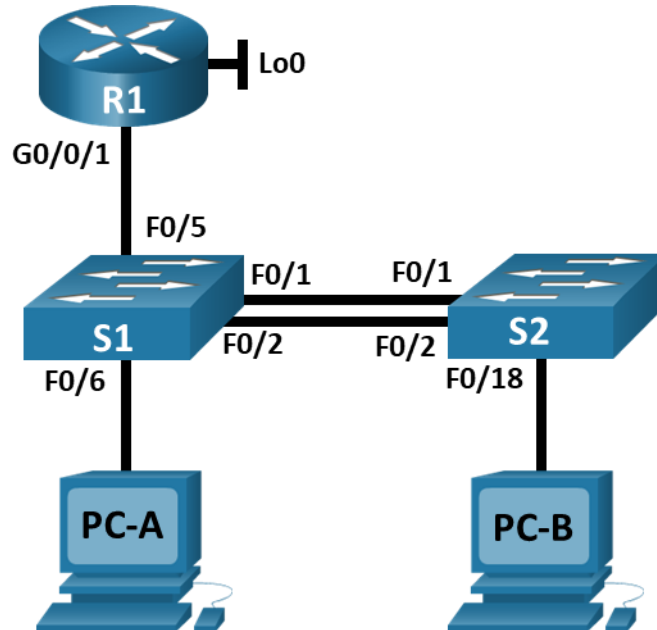
INTRODUCCIÓN

Se plantea el desarrollo de lo presente con el propósito de recibir la capacitación referente a la solución de temas, problemas y conflictos atinentes al tema de conectividad y otros aspectos del asunto en cuestión. Mi universidad la UNAD, me brinda la oportunidad a través de este diplomado de adquirir y profundizar conocimientos en diversos aspectos de las redes informáticas estructuradas en CISCO, con el método ABE o sea el sistema de aprendizaje basado en escenarios, y se tienen dos de estos. Mi sustentación está dirigida al escenario dos, en la cual se establecen conocimientos de configuración de Swichs y Router, teniendo presente el manejo de la seguridad de la información y equipos en base a el cumplimiento de protocolos de ingreso.

Además de lo anterior teniendo presente los hosts, se efectúa la respectiva configuración DHCP y también NAT, para la dinamización y efectividad en el manejo y operatividad de direcciones IP que están incluidas en un grupo de las mismas previamente asignadas. Se emplean los respectivos comandos y elementos para designar datos de fecha y hora. Se tienen en cuenta las vlan que han sido enlazadas con las interfaces y subinterfaces, con el fin de aprovechar al máximo la red.

Escenario 1

Topología



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. Configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1. VLAN

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 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

DESARROLLO ESCENARIO 1

Se Borra las configuraciones de inicio y las VLAN del router y del switch y vuelve a cargar los dispositivos, 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.

Configurar R1

configuración para R1 incluyen las siguientes:

se desactiva el DNS para que no llame a otro dominio, se da un nombre al Router, se establece contraseñas para proteger al mismo de posibles configuraciones erróneas por último se crea un mensaje el cual indica que solo es personal autorizado.

Tabla 3 configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	Hostname R1
Nombre de dominio	ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Enable secret ciscoenpass
Contraseña de acceso a la consola	Line console 0 Password ciscoconpass Login Exit
Establecer la longitud mínima para las contraseñas	Username admin privilege 10 password admins1pass
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	ip ssh version 2 line vty 0 15 transport input ssh login local exit

Configurar VTY solo aceptando SSH	Crypto key generate rsa : 1024
Cifrar las contraseñas de texto no cifrado	Service Password-encryption
Configure un MOTD Banner	Banner motd #!!!!!!!!!!!!!!!!!!!!!!ACCESO NO AUTORIZADO!!!!!!!!!!!!!!!!!!#
Habilitar el routing IPv6	Interface GigabitEthernet0/0/1 ipv6 enable
Configurar interfaz G0/0/1 y subinterfaces	Interface GigabitEthernet0/0/1.2 Ip address 10.19.8.1 255.255.255.192 GigabitEthernet0/0/1.2 ipv6 address 2001:db8:acad:a: :1 /64 Interface GigabitEthernet0/0/1.3 Ip address 10.19.8.65 255.255.255.192 Interface GigabitEthernet0/0/1.3 ipv6 address 2001:db8:acad:b: :1 /64 Interface GigabitEthernet0/0/1.4 Ip address 10.19.8.97 255.255.255.248 Interface GigabitEthernet0/0/1.4 ipv6 address 2001:db8:acad:c: :1 /64 Interface GigabitEthernet0/0/1 ipv6 address 2001:db8:acad:fe80: :1 /64
Configure el Loopback0 interface	Interface Loopback 0 Ip address 209.165.201.1255.255.255.224 Interface Loopback 0 ipv6 address 2001:db8:acad:209: :1 /64 Interface Loopback 0 ipv6 address 2001:db8:acad:fe80: :1 /64
Generar una clave de cifrado RSA	Crypto key generate rsa :1024

Configuración S1 Las tareas de configuración incluyen lo siguiente:

Desactivar la búsqueda DNS:

Nombre del switch, Nombre de dominio, Contraseña cifrada para el modo EXEC privilegiado, Contraseña de acceso a la consola se Crea un usuario administrativo en la base de datos local se Configurar el inicio de sesión en las líneas VTY para que use la base de datos local se Configura las líneas VTY para que acepten únicamente las conexiones SSH:

Tabla 4. Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	no ip domain-lookup
Nombre del switch	hostname S1
Nombre de dominio	ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Enable secret ciscoenpass
Contraseña de acceso a la consola	Line console 0 Password ciscoconpass Login Exit
Crear un usuario administrativo en la base de datos local	Username admin privilege 10 password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Ip ssh version 2 Line vty 0 15 Transport input ssh Login local exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Line vty 0 4 Password admin1pass Login End exit
Cifrar las contraseñas de texto no cifrado	Service Password-encryption
Configurar un MOTD Banner	Banner motd #!!!!ACCESO NO AUTORIZADO!!!!!!!!!!!!#

Generar una clave de cifrado RSA	Crypto key generate rsa :1024
Configurar la interfaz de administración (SVI)	S1(config)#sdm prefer dual- ipv4- and-ipv6 VLAN Interface Vlan 4 Ip address10.19.8.98 /29 Interface Vlan 4 Ipv6 address 2001:db8:acad:c: :98 /64 fe80: :98
Configuración del gateway predeterminado	Ip default – Gateway 10.19.8.97

Configure S2:

Las tareas de configuración incluyen lo siguiente:

Se desactiva la búsqueda DNS se asigna un nombre, se realiza la configuración básica de switch con contraseñas para la seguridad del dispositivo, además se da su respectivo direccionamiento.

Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3.

Tabla 5 configuración S2

Tarea	Especificación
Desactivar la búsqueda DNS.	no ip domain-lookup
Nombre del switch	hostname S2
Nombre de dominio	ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Enable secret ciscoenpass
Contraseña de acceso a la consola	Line console 0 Password ciscoconpass Login Exit

Tarea	Especificación
Crear un usuario administrativo en la base de datos local	Username admin privilege 10 password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Ip ssh version 2 Line vty 0 15 Transport input ssh Login local Exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Line vty 0 4 Password admin1pass Login End exit
Cifrar las contraseñas de texto no cifrado	Service Password-encryption
Configurar un MOTD Banner	Banner motd #!!!!ACCESO NO AUTORIZADO!!!!!!!!!!#
Generar una clave de cifrado RSA	Crypto key generate rsa : 1024
Configurar la interfaz de administración (SVI)	S1(config)#sdm prefer dual- ipv4- and-ipv6 VLAN Interface Vlan 4 Ip address10.19.8.99 255.255.255.248 Interface Vlan 4 Ipv6 address 2001:db8:acad:c: :99 /64 fe80: :9
Configuración del gateway predeterminado	Ip default – Gateway 10.19.8.97

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

Configurar S1

La configuración del S1 incluye las siguientes tareas: se crean vlans con sus respectivos nombres y direccionamientos, creando troncos 802.1Q que utilicen la VLAN 6 nativa

Tabla 6 configuración S1 Vlan

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

Tarea	Especificación
<p>Crear troncos 802.1Q que utilicen la VLAN 6 nativa</p>	<pre> S1(config)#interface fastEthernet 0/1 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 6 S1(config- if)#switchport mode TRUNK S1(config)#interface fastEthernet 0/2 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 6 S1(config- if)#switchport mode TRUNK S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 6 S1(config- if)#switchport mode TRUNK </pre>

<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<pre> S1(config)#interface range fastEthernet 0/1-2 S1(config-if- range)#channel-protocol lacp S1(config-if-range) #channel-group 1 mode active S1(config-if-range) #exit </pre>
<p>Configurar el puerto de acceso de host para VLAN 2</p>	<pre> S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 2 </pre>

Tarea	Especificación
<p>Configurar la seguridad del puerto en los puertos de acceso</p>	<pre> S1(config)#interface range fastEthernet 0/1- 2 S1(config-if-range) #switchport mode access S1(config-if-range)# switchport port- security S1(config-if-range)# switchport port- security maximum 3 S1(config-if-range)# switchport port- security violation shutdown S1(config-if-range)# switchport port- security violation mac-address sticky </pre>

Tarea	Especificación
<p>Proteja todas las interfaces no utilizadas</p>	<pre> S1(config)#interface fastEthernet 0/3- 4 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 5 S1(config-if)#shut down S1(config-if)#description apagar puertos S1(config-if)#exit S1(config)#interface fastEthernet 0/3- 7-17 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 5 S1(config-if)#shut down S1(config-if)#description apagar puertos S1(config-if)#exit S1(config)#interface fastEthernet 0/3- 19-24 S1(config-if)#switchport mode access S1(config- if)#switchport access VLAN 5 S1(config-if)#shut down S1(config-if)#description apagar puertos S1(config-if)#exit </pre>

Configure el S2.

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

Se crean vlans, con sus respectivas interfaces, Crear troncos 802.1Q que utilicen la VLAN 6 nativa; se Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2.

Tabla 7 creación Vlan S2

Tarea	Especificación
Crear VLAN	<pre> S2(config)#VLAN 2 S2(config-vlan) #name Bikes S2(config)#VLAN 3 S2(config-vlan) #name Trikes S2(config)#VLAN 4 S2(config-vlan) #name Management S2(config)#VLAN 5 S2(config-vlan) #name Parking S2(config)#VLAN 6 S2(config-vlan) #name Native </pre>
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	<pre> S2(config)#interface fastEthernet 0/1 S2(config- if)#switchport mode access S2(config-if)#switchport access VLAN 6 S2(config- if)#switchport mode TRUNK S2(config)#interface fastEthernet 0/2 S2(config- if)#switchport mode access S2(config-if)#switchport access VLAN 6 </pre>

	S2(config-if)#switchport mode TRUNK
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 1 mode passive S2(config-if-range)#exit

Tarea	Especificación
<p>Configurar el puerto de acceso del host para la VLAN 3</p>	<pre> S2(config)#interface fastEthernet 0/18 S2(config- if)#switchport mode access S2(config-if)#switchport access VLAN 3 S2(config- if)#exit </pre>
<p>Configure port-security en los access ports</p>	<pre> S2(config)#interface range fastEthernet 0/1- 2 S2(config-if-range)#switchport mode access S2(config-if-range)# switchport port- security S2(config-if-range) # switchport port- security maximum 3 S2(config-if-range)# switchport port- security violation shutdown S2(config-if-range)# switchport port- security violation mac-address sticky permite 3 MAC address </pre>

<p>Asegure todas las interfaces no utilizadas.</p>	<pre> S2(config)#interface fastEthernet 0/3- 17 S2(config-if)#switchport mode access S2(config- if)#switchport access VLAN 5 S2(config-if)#shut down S2(config-if)#description apagar puertos S2(config-if)#exit S2(config)#interface fastEthernet 0/19-24 S2(config-if)#switchport mode access S2(config- if)#switchport access VLAN 5 S2(config-if)#shut down S2(config-if)#description apagar puertos S2(config-if)#exit </pre>
--	--

Configurar soporte de host

Configure R1

tareas de configuración para R1 incluyen las siguientes:

se configura el router R1 con el DHCP para que al dar conexión con los hosts estos tomen directamente sin configurar manualmente los dispositivos, sino que directamente toman conexión.

Tabla 8. configuración R1 con DHCP

Tarea	Especificación
Configure Default Routing	<pre> R1(config)#ip route 209.165.201.1 255.255.255.192 10.19.8.1 R1(config)#ip route 209.165.201.1 255.255.255.224 10.19.8.65 R1(config)#ip route 209.165.201.1 255.255.255.248 10.19.8.97 R1(config)#ip route 209.165.201.1 255.255.255.192 2001:db8:acad:a :1 /64 R1(config)#ip route 209.165.201.1 255.255.255.224 2001:db8:acad:b :1 /64 R1(config)#ip route 209.165.201.1 255.255.255.248 2001:db8: acad:c: :1 /64 </pre>
Configurar IPv4 DHCP para VLAN 2	<pre> R1(config)#ip dhcp pool Vlan2 R1(dhcp-config) network 10.19.8.99 255.255.255.248 R1(dhcp-config) default-router 10.19.8.1 R1(config)# ip dhcp excluded-address 10.19.8.246 10.19.8.254 R1(config)# ip domain-name <ccna-a.net> </pre>
Configurar DHCP IPv4 para VLAN 3	<pre> R1(config)#ip dhcp pool Vlan3 R1(dhcp-config) #netwo R1(dhcp-config)#network 10.19.8.99 255.255.255.248 R1(dhcp-config)#defau R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#ip dhcp excluded-address 10.19.8.246 10.19.8.254 </pre>

	R1(config)#
--	--------------------

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 9. Direccionamiento Pc-A

PC-A Network Configuration	
Descripción	PC-A
Dirección física	000A.F3A1.51E2
Dirección IP	169.254.81.226
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0
Gateway predeterminado IPv6	FE80::20A:F3FF:FEA1:51E2

Tabla 9.1 direccionamiento Pc--B

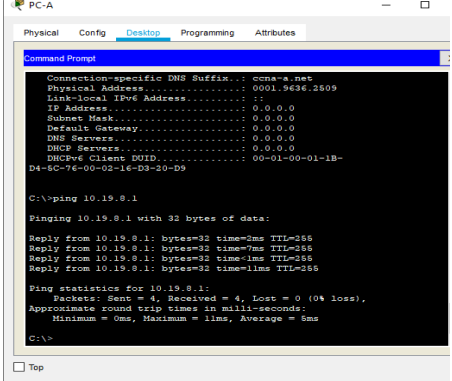
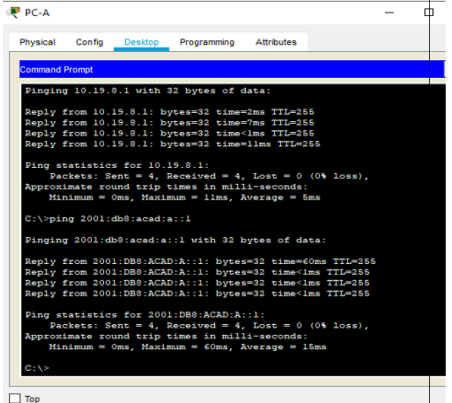
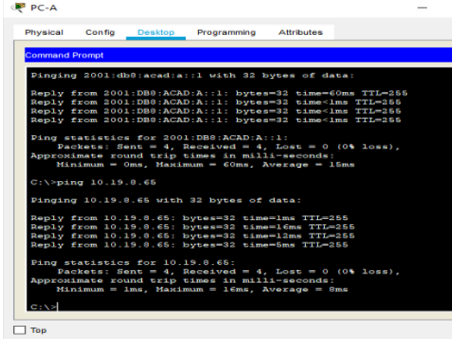
Configuración de red de PC-A	
Descripción	PC -A
Dirección física	000A.F3A1.51E2
Dirección IP	169.254.81.226
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0
Gateway predeterminado IPv6	FE80::20A:FF:FEA1:51E2

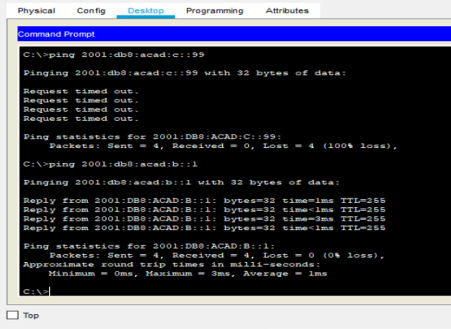
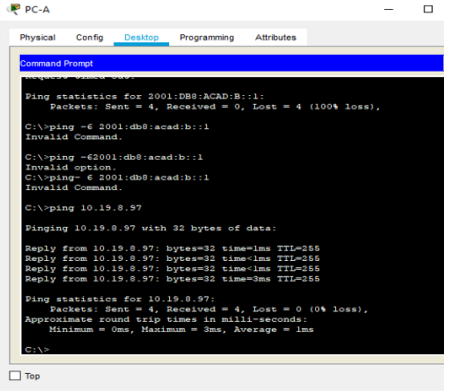
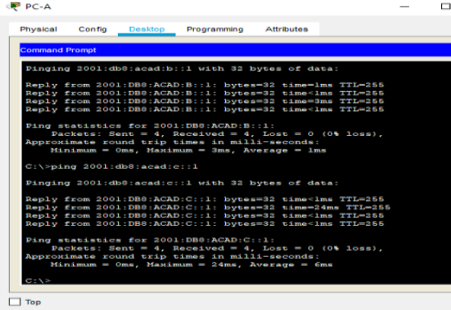
Probar y verificar la conectividad de extremo a extremo

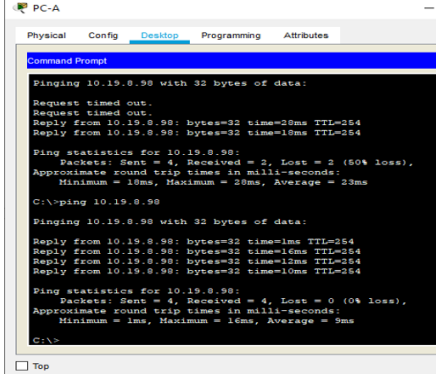
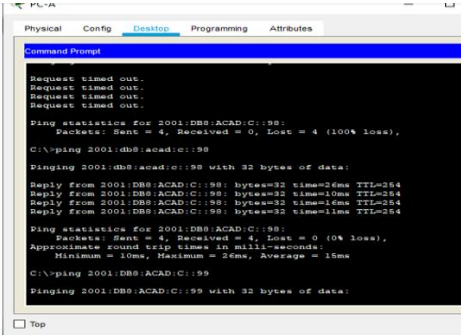
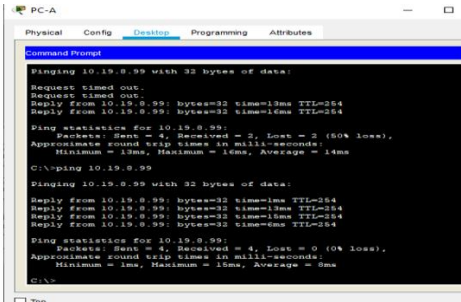
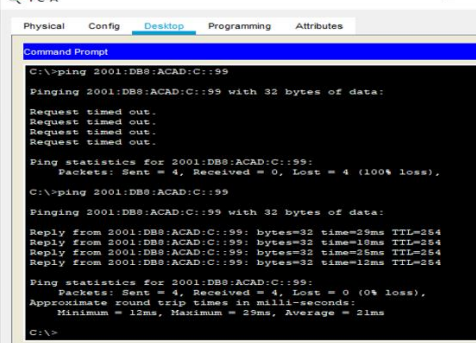
se usa el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

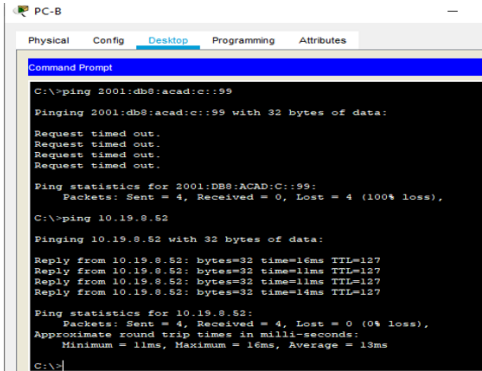
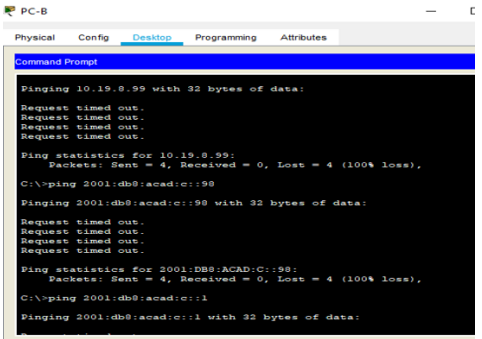
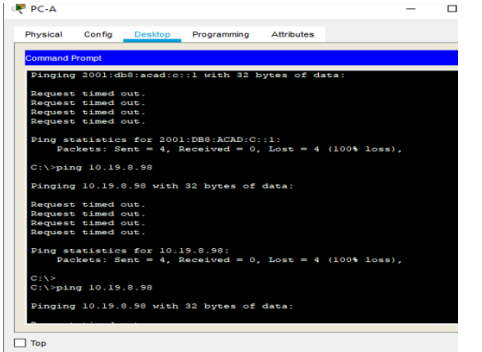
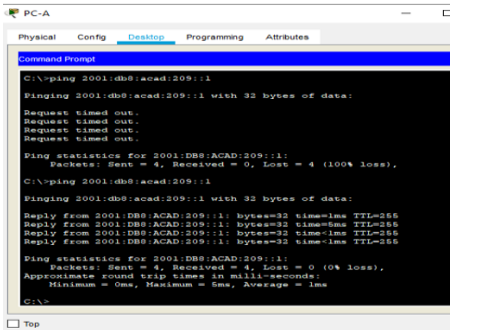
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla

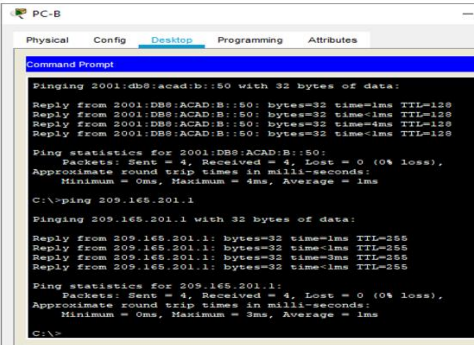
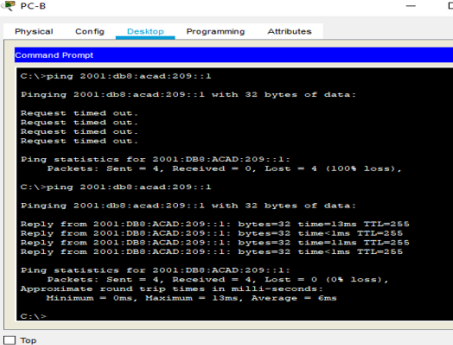
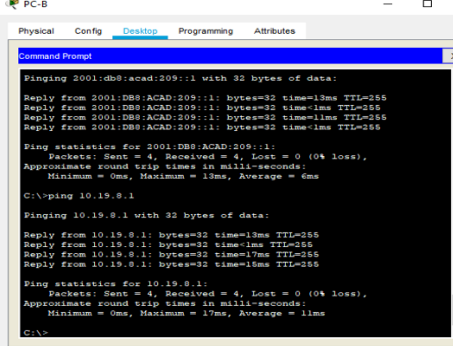
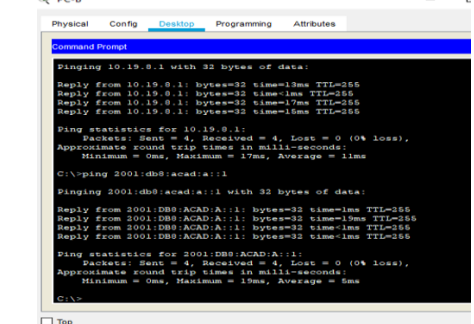
Tabla10. conectividad

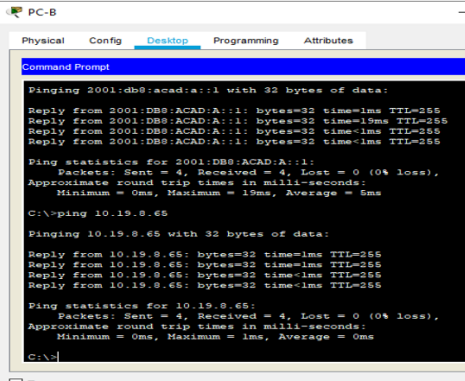
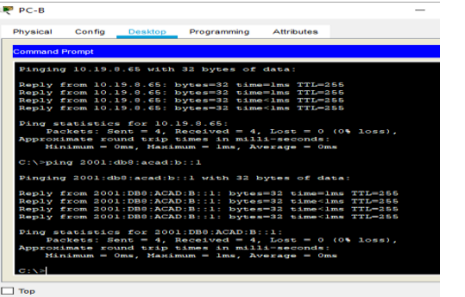
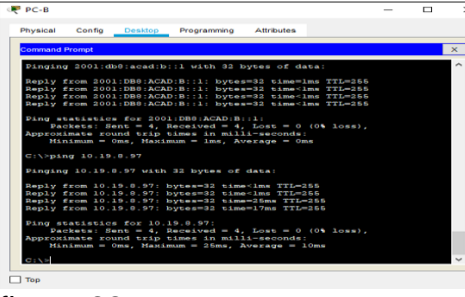
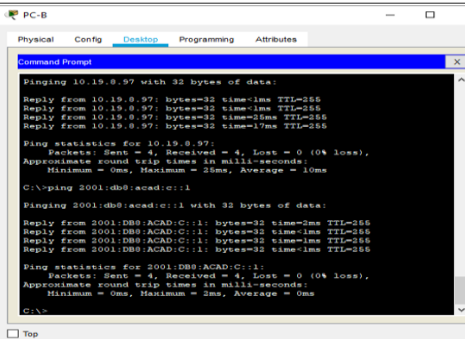
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	 <p>Figura 2</p>
		IPv6	2001:db8:acad:a:1	 <p>Figura 3</p>
	R1, G0/0/1.3	Dirección	10.19.8.65	

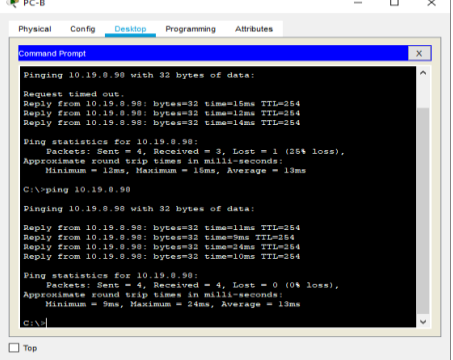
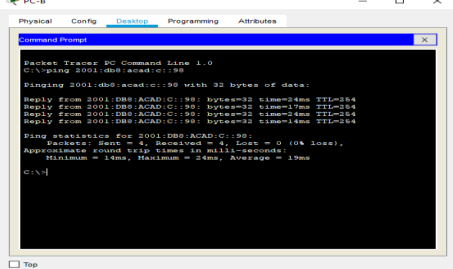
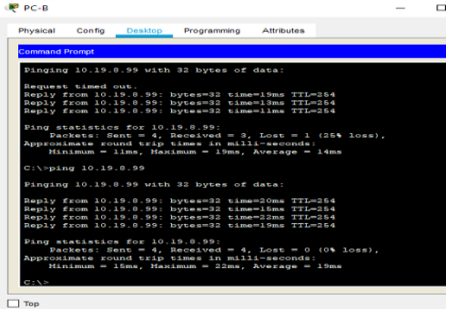
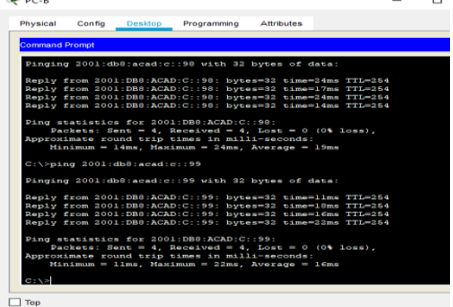
				<p>Figura 4</p>  <p>Figura 5</p>
	R1, G0/0/1. 4	Direcció n	10.19.8.97	 <p>figura 6</p>
		IPv6	2001:db8:acad:c: :1	 <p>Figura 7</p>

	S1, VLAN 4	Direcció n	10.19.8.98	 <p>Figura 8</p>
		IPv6	2001:db8:acad:c: :98	 <p>figura 9</p>
	S2, VLAN 4	Direcció n	10.19.8.99.	 <p>figura 10</p>
		IPv6	2001:db8:acad:c: :99	 <p>figura 11</p>

	PC-B	Direcció n	IP address will vary.	 <p>PC-B</p> <pre> Physical Config Desktop Programming Attributes Command Prompt C:\>ping 2001:db8:acad:c::99 Pinging 2001:db8:acad:c::99 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 10.19.0.52 Pinging 10.19.0.52 with 32 bytes of data: Reply from 10.19.0.52: bytes=32 time=16ms TTL=127 Reply from 10.19.0.52: bytes=32 time=11ms TTL=127 Reply from 10.19.0.52: bytes=32 time=14ms TTL=127 Reply from 10.19.0.52: bytes=32 time=14ms TTL=127 Ping statistics for 10.19.0.52: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 11ms, Maximum = 16ms, Average = 13ms C:\> </pre> <p>figura 12</p>
		IPv6	2001:db8:acad:b: :50	 <p>PC-B</p> <pre> Physical Config Desktop Programming Attributes Command Prompt Pinging 10.19.0.99 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 10.19.0.99: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 2001:db8:acad:c::90 Pinging 2001:db8:acad:c::90 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:C::90: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 2001:db8:acad:c::1 Pinging 2001:db8:acad:c::1 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 10.19.0.99 Pinging 10.19.0.99 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 10.19.0.99: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> </pre> <p>figura 13</p>
	R1 Bucle 0	Direcció n	209.165.201.1	 <p>PC-A</p> <pre> Physical Config Desktop Programming Attributes Command Prompt Pinging 2001:db8:acad:c::1 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 10.19.0.99 Pinging 10.19.0.99 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 10.19.0.99: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 10.19.0.98 Pinging 10.19.0.98 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 10.19.0.98: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> </pre> <p>figura 14</p>
		IPv6	2001:db8:acad:2 09::1	 <p>PC-A</p> <pre> Physical Config Desktop Programming Attributes Command Prompt C:\>ping 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time=5ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=5ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=5ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=5ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 5ms, Maximum = 5ms, Average = 5ms C:\> </pre> <p>figura 15</p>

PC-B	R1 Bucle 0	Direcció n	209.165.201.1	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>Pinging 2001:db8:acad:b::50 with 32 bytes of data: Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128 Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128 Reply from 2001:DB8:ACAD:B::50: bytes=32 time=4ms TTL=128 Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=128 Ping statistics for 2001:DB8:ACAD:B::50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 4ms, Average = 1ms 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=3ms 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 = 3ms, Average = 1ms C:\></pre> <p>Top</p> <p>figura 16</p>
		IPv6	2001:db8:acad:209::1	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>C:\>ping 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>ping 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time=13ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 13ms, Average = 6ms C:\></pre> <p>Top</p> <p>figura 17</p>
R1, G0/0/1. 2	Direcció n	10.19.8.1		 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time=13ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 13ms, Average = 6ms 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=13ms TTL=255 Reply from 10.19.8.1: bytes=32 time=1ms TTL=255 Reply from 10.19.8.1: bytes=32 time=17ms TTL=255 Reply from 10.19.8.1: bytes=32 time=16ms 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 = 17ms, Average = 11ms C:\></pre> <p>Top</p> <p>figura 18</p>
	IPv6	2001:db8:acad:a::1		 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>Pinging 10.19.8.1 with 32 bytes of data: Reply from 10.19.8.1: bytes=32 time=13ms TTL=255 Reply from 10.19.8.1: bytes=32 time=1ms TTL=255 Reply from 10.19.8.1: bytes=32 time=17ms TTL=255 Reply from 10.19.8.1: bytes=32 time=16ms 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 = 17ms, Average = 11ms C:\>ping 2001:db8:acad:a::1 Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 19ms, Average = 5ms C:\></pre> <p>Top</p> <p>figura 19</p>

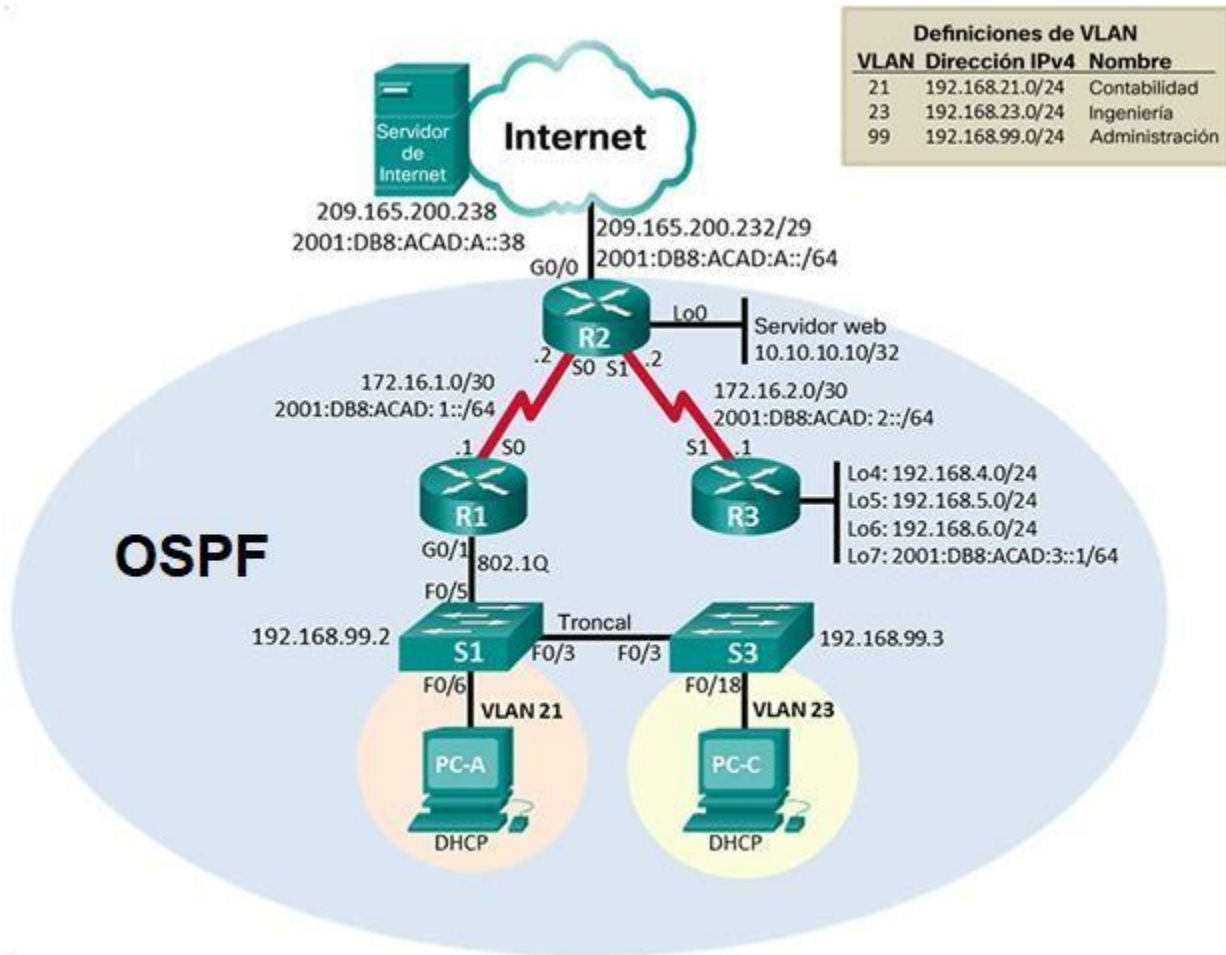
	R1, G0/0/1. 3	Direcció n	10.19.8.65	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>Pinging 2001:db8:acad:a::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=19ms TTL=255 Reply 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 = 19ms, Average = 5ms 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=1ms 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 = 1ms, Average = 0ms C:\></pre> <p>figura 20</p>
		IPv6	2001:db8:acad:b: :1	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>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=1ms 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 = 1ms, Average = 0ms 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=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 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 = 1ms, Average = 0ms C:\></pre> <p>figura 21</p>
	R1, G0/0/1. 4	Direcció n	10.19.8.97	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>Pinging 2001:db8:acad:b::1 with 32 bytes of data: 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 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 = 1ms, Average = 0ms C:\>ping 10.19.8.97 Pinging 10.19.8.97 with 32 bytes of data: Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 Ping statistics for 10.19.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 1ms C:\></pre> <p>figura 22</p>
		IPv6	2001:db8:acad:c: :1	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre>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=2ms 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 = 2ms, Average = 1ms C:\>ping 2001:db8:acad:c::1 Pinging 2001:db8:acad:c::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::1: bytes=32 time=2ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 0ms C:\></pre> <p>figura 23</p>

	S1, VLAN 4	Direcció n	10.19.8.98	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre> Pinging 10.19.8.98 with 32 bytes of data: Request timed out. Reply from 10.19.8.98: bytes=32 time=15ms TTL=254 Reply from 10.19.8.98: bytes=32 time=13ms TTL=254 Reply from 10.19.8.98: bytes=32 time=14ms TTL=254 Ping statistics for 10.19.8.98: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 13ms, Maximum = 15ms, Average = 13ms 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=11ms TTL=254 Reply from 10.19.8.98: bytes=32 time=9ms TTL=254 Reply from 10.19.8.98: bytes=32 time=10ms TTL=254 Reply from 10.19.8.98: bytes=32 time=10ms 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 = 9ms, Maximum = 24ms, Average = 13ms C:\> </pre> <p>Top</p> <p>Figura 24</p>
		IPv6	2001:db8:acad:c: :98	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre> Packet Tracer PC Command Line 1.0 C:\>ping 2001:db8:acad:c::98 Pinging 2001:db8:acad:c::98 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::98: bytes=32 time=20ms TTL=254 Reply from 2001:DB8:ACAD:C::98: bytes=32 time=19ms TTL=254 Reply from 2001:DB8:ACAD:C::98: bytes=32 time=20ms TTL=254 Reply from 2001:DB8:ACAD:C::98: bytes=32 time=18ms TTL=254 Ping statistics for 2001:DB8:ACAD:C::98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 18ms, Maximum = 20ms, Average = 19ms C:\> </pre> <p>Top</p> <p>Figura 25</p>
	S2, VLAN 4	Direcció n	10.19.8.99.	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre> Pinging 10.19.8.99 with 32 bytes of data: Request timed out. Reply from 10.19.8.99: bytes=32 time=19ms TTL=254 Reply from 10.19.8.99: bytes=32 time=13ms TTL=254 Reply from 10.19.8.99: bytes=32 time=12ms TTL=254 Reply from 10.19.8.99: bytes=32 time=19ms TTL=254 Ping statistics for 10.19.8.99: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 11ms, Maximum = 19ms, Average = 14ms 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=20ms TTL=254 Reply from 10.19.8.99: bytes=32 time=19ms TTL=254 Reply from 10.19.8.99: bytes=32 time=22ms TTL=254 Reply from 10.19.8.99: bytes=32 time=19ms 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 = 18ms, Maximum = 22ms, Average = 19ms C:\> </pre> <p>Top</p> <p>Figura 26</p>
		IPv6	2001:db8:acad:c: :99	 <p>PC-B</p> <p>Physical Config Desktop Programming Attributes</p> <p>Command Prompt</p> <pre> Pinging 2001:db8:acad:c::99 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::99: bytes=32 time=24ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=17ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=24ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=18ms TTL=254 Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 14ms, Maximum = 24ms, Average = 19ms C:\>ping 2001:db8:acad:c::99 Pinging 2001:db8:acad:c::99 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::99: bytes=32 time=11ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=19ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=15ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=23ms TTL=254 Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 11ms, Maximum = 23ms, Average = 16ms C:\> </pre> <p>Top</p> <p>Figura 27</p>

Escenario 2

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

Topología



Inicializar 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 11. Inicialización R1

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	<pre>R1#ERase SStartup-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 R2#ERASE SStartup-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 R3#ERASE SStartup-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</pre>

Volver a cargar todos los routers	R1#reload System configuration has been modified. Save? [yes/no]:y Building configuration... [OK] R2#reload System configuration has been modified. Save? [yes/no]:y Building configuration... [OK] R3#reload System configuration has been modified. Save? [yes/no]:y Building configuration... [OK]
-----------------------------------	--

<p>Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior</p>	<pre> S1#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 S2#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 S1#vlan database % Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode. S2#vlan database % Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode. </pre>
<p>Volver a cargar ambos switches</p>	<pre> S1#reload System configuration has been modified. Save? [yes/no]:no Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960- 24TT starting... </pre>

	Base ethernet MAC Address: 0001.4341.19BC Xmodem file system is available.
--	---

	<pre> Initializing Flash... S2#reload System configuration has been modified. Save? [yes/no]: % Please answer 'yes' or 'no'. System configuration has been modified. Save? [yes/no]:no Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960- 24TT starting... Base ethernet MAC Address: 0000.0CA2.ED31 Xmodem file system is available. Initializing Flash... </pre>
<p>Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches</p>	<pre> Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory) Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory) </pre>

Configurar los parámetros básicos de los 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):

Tabla12. direccionamiento servidor

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se configura el R1 dando el nombre y las contraseñas específicas para que nadie pueda acceder a él, también se da el direccionamiento ipv4 e ipv6.

Tabla 13 configuración inicial R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	R1(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#pas R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#
Contraseña de acceso Telnet	R1(config)#line v R1(config)#line vty 0 15 R1(config-line)#pas R1(config-line)#password cisco R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#

Mensaje MOTD	R1(config)#banner motd #!!!!!!!!!!!!!!!!!!!!!!!!!!!!SE PROHIBE EL ACCESO NO AUTORIZADO!!!!!!!!!!!!!!!!!!!!# R1(config)#
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#ip ad R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#exit R1(config)#interface serial 0/0/0 R1(config-if)#ipv R1(config-if)#ipv6 ad R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#CLO R1(config-if)#CLOck RA R1(config-if)#CLOck RAte 128000 R1(config-if)#NO SH R1(config-if)#NO SHUTDOWN R1(config- if)#EXIT R1(config)#
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Configurar R2

La configuración del R2 incluye las siguientes tareas:

Se realiza la configuración inicial del R2 donde se da un nombre y direccionamiento ipv4 e ipv6 también se configura las contraseñas de acceso al R2.

Tabla 14 configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	R2(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#pas R2(config-line)#password cisco R2(config-line)#login local R2(config-line)#exit

Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config- line)#tra R2(config- line)#transport in R2(config-line)#transport input telnet R2(config-line)#transport input telnet ssh R2(config)#line vty 0 4 R2(config- line)#pas R2(config- line)#password cisco R2(config-line)#login R2(config-line)#exi
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #!!!!!!!!!!!!!!Se prohibe el acceso no autorizado!!!!!!!!!!!!!!#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config- if)#ip ad R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shu R2(config-if)#no shutdown R2(config-if)#no shutdown R2(config-if)#in

	<pre> R2(config-if)#exit R2(config)#INterface SERial 0/0/0 R2(config- if)#ipv R2(config-if)#ipv6 ad R2(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R2(config-if)#EXIT </pre>
--	--

Interfaz S0/0/1	<pre> R2(config)#INterface serial 0/0/1 R2(config-if)#ip ad R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#no sh R2(config-if)#no shutdown R2(config)#interface serial 0/0/1 R2(config-if)#ipv R2(config-if)#ipv6 ad R2(config-if)#ipv6 address 2001:DB8:ACAD:2::/64 R2(config-if)#NO SHU R2(config-if)#NO SHUtdown R2(config-if)#EXI R2(config)#INTERface SERIAL 0/0/1 R2(config-if)#CL R2(config-if)#CLock RA R2(config-if)#CLock RAte 128000 R2(config-if)#EXIT </pre>
Interfaz G0/0 (simulación de Internet)	<pre> R2(config)#interface gigabitEthernet 0/0 R2(config-if)#ip ad R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#exit R2(config)#interface gigabitEthernet 0/0 R2(config-if)#ip av R2(config-if)#ipv R2(config- if)#ipv6 ad R2(config-if)#ipv6 address 2001:DB8:ACAD:A::/64 R2(config-if)#NO SH R2(config-if)#NO SHUTDOWN </pre>

<p>Interfaz loopback 0 (servidor web simulado)</p>	<pre>R2(config)#INterface LO R2(config)#INterface LOopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#IP AD R2(config-if)#IP ADdress 10.10.10.10 255.255.255.255 R2(config-if)#EXIT</pre>
<p>Ruta predeterminada</p>	<pre>R2(config)#ip route 209.165.200.238 255.255.255.248 209.165.200.232 R2(config)#ipv6 route 2001:DB8:ACAD:A::/64 2001:DB8:ACAD:A::38</pre>

Configurar R3

La configuración del R3 incluye las siguientes tareas: se realiza la configuración inicial de R3 donde van la contraseña de protección del mismo, el nombre para identificarlo de los otros dispositivos, se realiza direccionamiento ipv4 e ipv6.

Tabla 15. configuración inicial R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3 R3(config)#
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#pas R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#tra R3(config-line)#transport in R3(config-line)#transport input telnet R3(config-line)#exit R3(config)#line vty 0 4 R3(config-line)#pas R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #!!!!!!!!!!!!!!Se prohíbe el acceso no autorizado!!!!!!!!!!!!!!# R3(config)#

<p>Interfaz S0/0/1</p>	<pre>R3(config)#interface serial 0/0/1 R3(config- if)#ip ad R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#exit R3(config)#interface serial 0/0/1 R3(config- if)#ipv R3(config-if)#ipv6 ad R3(config-if)#ipv6 address 2001:DB8:ACAD:2::/64 R3(config-if)#NO SH R3(config-if)#NO SHUTDOWN R3(config-if)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up R3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up</pre>
<p>Interfaz loopback 4</p>	<pre>R3(config)#INterface LOopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit.</pre>
<p>Interfaz loopback 5</p>	<pre>R3(config)#interface loopback 5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config-if)#ip ad R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no sh R3(config-if)#no shutdown</pre>

Interfaz loopback 6	<pre> R3(config)#interface loopback 6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no sh R3(config-if)#exit R3(config)# </pre>
---------------------	---

Interfaz loopback 7	<pre> R3(config)#interface loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up R3(config- if)#ipv R3(config- if)#ipv6 ad R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#NO SHU R3(config-if)#EXIT R3(config)# </pre>
---------------------	--

Configurar S1

La configuración del S1 incluye las siguientes tareas: se configura el S1 donde se da contraseñas para proteger el dispositivo, se da el nombre para diferenciar de los demás dispositivos.

Tabla 16. configuración inicial del S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
Nombre del switch	S1(config)#hostname S1 S1(config)#
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#pas S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#pas S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S1(config)#line vty 0 4 S1(config-line)#tra S1(config-line)#transport in S1(config-line)#transport input telnet S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Mensaje MOTD	S1(config)#banner motd #!!!!!!!!!!!!!!!!!!!!!!Se prohíbe el acceso no autorizado!!!!!!!!!!!!!!!!!!!!!!# S1(config)#

Configurar el S3

La configuración del S3 incluye las siguientes tareas: de igual manera que con los otros dispositivos se realiza la configuración inicial y la protección del S3

Tabla 17 configuración inicial S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(config)#no ip domain-lookup
Nombre del switch	S3(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#pas S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#pas S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#lin S3(config)#line v S3(config)#line vty 0 4 S3(config-line)#tra S3(config-line)#transport in S3(config-line)#transport input telnet S3(config-line)#login local S3(config-line)#exit S3(config)#
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption S3(config)#
Mensaje MOTD	S3(config)#banner motd #!!!!!!!!!!!!!!!!!!!!Se prohíbe el acceso no autorizado!!!!!!!!!!!!!!!!!!!!# S3(config)# 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 18 conectividad

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 = 1/11/51 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 = 1/2/6 ms R2#

PC de Internet	Gateway predeterminado	209.165.200.232	<pre>C:\>ping 209.165.200.232 Pinging 209.165.200.232 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 209.165.200.232:</pre>
			<pre>Packets: Sent = 4, Received = 4, Lost = 4 (100% loss), C:\></pre>

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

Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 19 configuración vlan en S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1(config)#Vlan 21 S1(config-vlan)#name Contabilidad S1(config- vlan)#Vlan 23 S1(config-vlan)#name Ingenieria S1(config- vlan)#Vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit</pre>

<p>Asignar la dirección IP de administración.</p>	<pre>S1(config)#interface vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S1(config-if)#ip ad S1(config-if)#ip address 192.168.99.0 255.255.255.0 Bad mask /24 for address 192.168.99.0 S1(config-if)#ip address 192.168.99.1 255.255.255.0 S1(config-if)#exit S1(config)#</pre>
<p>Asignar el gateway predeterminado</p>	<pre>S1(config)#ip default-gateway 192.168.99.1.</pre>

<p>Forzar el enlace troncal en la interfaz F0/3</p>	<pre>S1(config)#interface fastEthernet 0/3 S1(config-if)#sw S1(config-if)#switchport mo S1(config-if)#switchport mode ac S1(config-if)#switchport mode access S1(config-if)#sw S1(config-if)#switchport ac S1(config-if)#switchport access Vlan 1 S1(config-if)#exit S1(config)#int S1(config)#interface f S1(config)#interface fastEthernet 0/3 S1(config-if)#sw S1(config-if)#switchport mo S1(config-if)#switchport mode ac S1(config-if)#switchport mode access S1(config-if)#sw S1(config-if)#switchport ac S1(config-if)#switchport access tr S1(config-if)#switchport mo S1(config-if)#switchport mode tr S1(config-if)#switchport mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down</pre>
---	---

	<pre>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up S1(config-if)#exit</pre>
--	---

<p>Forzar el enlace troncal en la interfaz F0/5</p>	<pre>S1(config)#interface fastEthernet 0/5 S1(config-if)#sw S1(config-if)#switchport mo S1(config-if)#switchport mode ac S1(config-if)#switchport mode access S1(config-if)#sw S1(config-if)#switchport ac S1(config-if)#switchport access Vlan 1 S1(config-if)#exit S1(config)#in S1(config)#interface f S1(config)#interface fastEthernet 0/5 S1(config-if)#sw S1(config-if)#switchport mo S1(config-if)#switchport mode ac S1(config-if)#switchport mode access S1(config-if)#sw S1(config-if)#switchport mo S1(config-if)#switchport mode tr S1(config-if)#switchport mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up S1(config-if)#</pre>
---	---

<p>Configurar el resto de los puertos como puertos de acceso</p>	<pre>S1(config)#interface range FastEthernet 0/1-2 S1(config-if-range)#SW S1(config-if-range)#SWitchport MO S1(config-if-range)#SWitchport MOde AC S1(config-if-range)#SWitchport MOde ACcess S1(config-if-range)#EXIT S1(config)#IN S1(config)#INterface R S1(config)#INterface Range FA S1(config)#INterface Range FAstEthernet 0/4-24 S1(config-if-range)#SW S1(config-if-range)#SWitchport MOP S1(config-if-range)#SWitchport MO S1(config-if-range)#SWitchport MOde AC S1(config-if-range)#SWitchport MOde ACcess S1(config-if-range)#EXIT S1(config)#</pre>
--	---

<p>Asignar F0/6 a la VLAN 21</p>	<pre>S1(config)#interface fastEthernet 0/6 S1(config- if)#sw S1(config-if)#switchport mo S1(config-if)#switchport mode ac S1(config- if)#switchport mode access S1(config-if)#sw S1(config-if)#switchport ac S1(config-if)#switchport access Vlan 21 S1(config- if)#exit S1(config)#</pre>
----------------------------------	--

<p>Apagar todos los puertos sin usar</p>	<pre> S1(config)#interface range fastEthernet 0/1-2 S1(config-if- range)#sh S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down S1(config-if-range)# S1(config-if-range)#exit S1(config)#interface fastEthernet 0/4 S1(config- if)#sh S1(config-if)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down S1(config-if)#exit S1(config)#interface range fastEthernet 0/7-24 S1(config-if- range)#sh S1(config-if- range)#shutdown S1(config-if- range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface </pre>
--	--

	<p>FastEthernet0/10, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down</p>
--	---

	<p>%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down</p> <p>S1(config-if-range)#exit</p> <p>S1(config)#</p>
--	--

Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 20 configuración Vlan S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>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 S3(config-vlan)#exit S3(config)#</pre>
Asignar la dirección IP de administración	<pre>S3(config)#interface vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S3(config-if)#ip ad S3(config-if)#ip address 192.168.99.0 255.255.255.0 Bad mask /24 for address 192.168.99.0 S3(config-if)#ip address 192.168.99.2 255.255.255.0 S3(config-if)#</pre>
Asignar el gateway predeterminado.	<pre>S3(config)#ip default-gateway 192.168.99.1</pre>

<p>Forzar el enlace troncal en la interfaz F0/3</p>	<pre>S3(config)#interface fastEthernet 0/3 S3(config-if)#sw S3(config-if)#switchport mo S3(config-if)#switchport mode ac S3(config-if)#switchport mode access S3(config-if)#sw S3(config-if)#switchport ac S3(config-if)#switchport access vlan1 ^ % Invalid input detected at '^' marker. S3(config-if)#switchport access vlan 1 S3(config-if)#sw S3(config-if)#switchport mo S3(config-if)#switchport mode tr S3(config-if)#switchport mode trunk S3(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)# tilizar la red VLAN 1 como VLAN nativa</pre>
---	--

<p>Configurar el resto de los puertos como puertos de acceso</p>	<pre>S3(config)#interface range fastEthernet 0/1-2 S3(config-if- range)#sw S3(config-if-range)#switchport mo S3(config-if-range)#switchport mode ac S3(config-if- range)#switchport mode access S3(config-if-range)#exit S3(config)#interface range fastEthernet 0/4-24 S3(config-if- range)#sw S3(config-if-range)#switchport mo S3(config-if-range)#switchport mode ac S3(config-if-</pre>
--	---

	<pre> range)#switchport mode access S3(config-if-range)#exit S3(config)# </pre>
<p>Asignar F0/18 a la VLAN 21</p>	<pre> S3(config)#interface fastEthernet 0/18 S3(config- if)#sw S3(config-if)#switchport m S3(config- if)#switchport mode S3(config-if)#switchport mode ac S3(config-if)#switchport mode access S3(config- if)#sw S3(config-if)#switchport ac S3(config-if)#switchport access Vlan21 ^ % Invalid input detected at '^' marker. S3(config- if)#switchport access Vlan 21 S3(config-if)#exit S3(config)# </pre>

<p>Apagar todos los puertos sin usar</p>	<pre>S3(config)#interface range fastEthernet 0/1-2 S3(config-if- range)#shu S3(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down S3(config-if-range)#exit S3(config)#interface range fastEthernet 0/4-17 S3(config-if- range)#sh S3(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down</pre>
--	---

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

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

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

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

	<p>%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down S3(config-if-range)#exit S3(config)#</p> <p>S3(config)#interface range fastEthernet 0/19-24 S3(config-if-range)#shu S3(config-if-range)#shutdown</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down S3(config-if-range)#exit S3(config)#</p>
--	--

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 21 configuración R1 interfaz

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<pre>R1(config)#interface gigabitEthernet 0/0.1 R1(config-subif)#enca R1(config-subif)#encapsulation % Incomplete command. R1(config-subif)#encapsulation do R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip ad R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#no shu R1(config-subif)#exit R1(config)#</pre>
Configurar la subinterfaz 802.1Q .23 en G0/1	<pre>R1(config)#interface gigabitEthernet 0/0.1 R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#no shu R1(config-subif)#no shutdown R1(config- subif)#exit R1(config)#</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<pre>R1(config)#interface gigabitEthernet 0/0.1 R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#no shu R1(config-subif)#no shutdown R1(config-subif)#</pre>
Activar la interfaz G0/1	<pre>R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no sh R1(config-if)#no shutdown u R1(config-if)#no shu R1(config-if)#no shutdown R1(config-if)#exit R1(config)#</pre>

Paso 4: Verificar la conectividad de la red

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

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

Tabla 22 conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1
			<p>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 = 2/4/11 ms</p> <p>S1#</p>
S3	R1, dirección VLAN 99	192.168.99.1	<p>S3#ping 192.168.99.1</p> <p>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 = 0/2/10 ms</p> <p>S3#</p>

S1	R1, dirección VLAN 21	192.168.21.1	<p>S1#ping 192.168.21.1</p> <p>Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: Success rate is 0 percent (5/5)</p> <p>S1#</p>
S3	R1, dirección VLAN 23		<p>S3#ping 192.168.21.1</p> <p>Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to</p>

			<p>192.168.21.1, timeout is 2 seconds: Success rate is 0 percent (5/5)</p> <p>S3#</p>
--	--	--	---

CONCLUSIONES

Durante el curso podemos identificar muchos factores, los cuales nos permiten ver una mejor configuración de los dispositivos que requerimos usar, para este proyecto notamos como podemos interconectar varias redes como lo haríamos en un entorno real, se deben tener en cuenta los conceptos, las configuraciones que usamos nos permiten hacer un uso correcto y óptimo de dispositivos,

El uso de protocolos de enrutamiento dinámico nos permite el aprendizaje rápido de la topología de red por la cual estemos pasando y la cantidad de saltos posibles para alcanzar un destino. Como elemento de seguridad el uso de Vlan nos permite la segmentación adecuada de una red limitando el acceso a los recursos que sean absolutamente necesarios y logrando una división basada en departamentos, servicios o localidades.

REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

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

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: <https://static-courseassets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

ANEXOS

ANEXO A ESCENARIO DOS

https://drive.google.com/file/d/1rCkiS-2JZFjB_Tolz57x7HPwBmn1Czs/view?usp=sharing

ANEXO B ESCENARIO DOS

https://drive.google.com/file/d/1rCkiS-2JZFjB_Tolz57x7HPwBmn1Czs/view?usp=sharing

ANEXO C ARTICULO

https://drive.google.com/file/d/1q090KCBfwsbNPMXzPBmYa_Fd2BMRklnW/view?usp=sharing

Diseño de una red

*Deisy Yolima Cuevas Mendivelso Universidad Nacional Abierta y a Distancia
Dycuevasm@unadvirtual.edu.co*

Resumen

El propósito fundamental de este artículo es la articulación de acciones, tendientes a profundizar el desarrollo y aprendizaje del CISCO, para lo cual se tiene presente la configuración de diversos dispositivos que estructuran una red, con aspectos tan importantes como el tema seguridad determinado por la validación mediante el cumplimiento de un requisito preestablecido, ya sea contraseña o algo similar, como nombrar las vlan, red local y de tipo virtual, aprovechando la misma para la configuración de redes lógicas independientes, las cuales hacen parte constitutiva de la misma red física. Además, se plantea la manera de configuración con el empleo de comandos y proceso de encapsulamiento para otorgar alta seguridad a la información y equipos, procurando al máximo el robo de información o daño en los dispositivos y en la red en general. Además de lo

descrito se presenta la implementación y manera de configurar el protocolo DHCP y el NAT, que facilitan el manejo de direcciones IP dentro de rangos de direcciones previamente establecidas.

Palabras claves vlan, encapsulamiento, seguridad, DHCP, NAT, CISCO, configuración, redes.

ABSTRACT:

fundamental purpose of this article is the articulation of actions, tending to deepen the development and learning of the CISCO, for which the configuration of various devices that structure a network is taken into account, with aspects as important as the security issue determined by the validation by fulfilling a pre-established requirement, be it a password or something similar, such as naming the vlan, local network and virtual type, taking advantage of it for the configuration of independent logical networks, which are a constitutive part of the same physical network. In

addition, the way of configuration is proposed with the use of commands and the encapsulation process to provide high security to the information and equipment, ensuring to the maximum the theft of information or damage to the devices and the network in general. In addition to what has been described, the implementation and way of configuring the DHCP protocol and NAT are presented, which facilitate the management of IP addresses within previously established address ranges.

Keywords vlan, encapsulation, security, DHCP, NAT, CISCO, configuration, networks.

METODOLOGIA

Para el diseño de redes, el proceso se inicia con la configuración de una determinada red, que está estructurada con diversos elementos y dispositivos, para lo cual debe establecerse una actividad de autenticación para poder entrar a dichos elementos y dispositivos, empleo de password y designación de vlan, y se configura una relación a las respectivas interfaces y puertos. Para efectos de garantizar una adecuada y pertinente

seguridad recurrimos al encapsulamiento, pensando en la información como elemento a resguardar eficientemente.

INTRODUCCION

Se plantea el desarrollo de lo presente con el propósito de recibir la capacitación referente a la solución de temas, problemas y conflictos atinentes al tema de conectividad y otros aspectos del asunto en cuestión. Mi universidad la UNAD, me brinda la oportunidad a través de este diplomado de adquirir y profundizar conocimientos en diversos aspectos de las redes informáticas estructuradas en CISCO, con el método ABE o sea el sistema de aprendizaje basado en escenarios, y se tienen dos de estos. Mi sustentación está dirigida al escenario dos, en la cual se establecen conocimientos de configuración de Swichts y Router, teniendo presente el manejo de la seguridad de la información y equipos en base a el cumplimiento de protocolos de ingreso.

Además de lo anterior teniendo presente los hosts, se efectúa la respectiva configuración DHCP y también NAT, para la dinamización y efectividad en el manejo y operatividad de direcciones IP que están incluidas en un grupo de las mismas previamente asignadas. Se emplean los respectivos comandos y elementos para designar datos de fecha y hora. Se tienen en cuenta las vlan que han sido enlazadas con las interfaces y subinterfaces, con el fin

de aprovechar al máximo la red.

IMPLEMENTACION

El aspecto central del tema es la configuración de dispositivos que conforman una red de comunicación, para lo cual se emplea un simulador dinámico que me otorga los diferentes elementos y herramientas requeridas para efectuar dichas configuraciones, igual que, en tiempo real, para lo cual debo efectuar una conveniente selección de los elementos y dispositivos pertinentes acorde con la necesidad de la red en estudio y me da la oportunidad de plantear soluciones para los casos de conectividad.

Lo empleado es básicamente un servidor con internet, 3 routers, 2 switchs, 2 PC. Se requiere la contraseña para el ingreso, y como paso inicial se configura el servidor para su acceso a internet, además en los Routers se nombre las vlan y se procede a la asignación de puertos e interfaces requeridas, dejando a un lado las que no se necesiten. A continuación, se establece el protocolo DHCP, que me genera de manera automática una dirección IP los PCs y con el protocolo NAT se puede tomar cualquier dirección IP definiendo un determinado rango con la IP de origen, evidenciando efectuando ping la conectividad

requerida y la configuración de manera correcta. Con lo anterior se tiene el enrutamiento y direccionamiento para el manejo de información requerida.

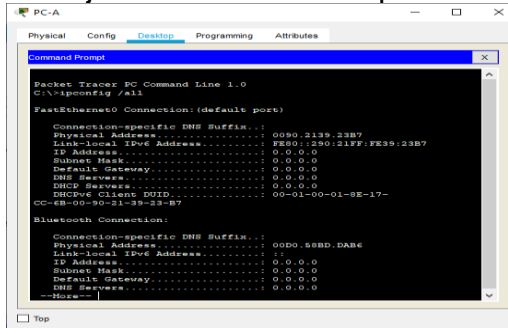


Figura 29

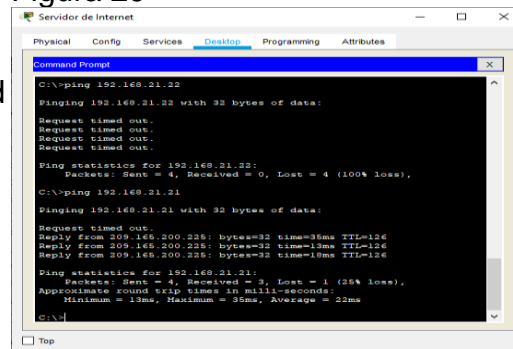


Figura 30

1.2 Escenario:

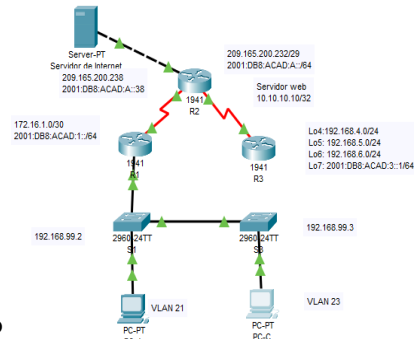


Figura 31

CONCLUSIONES

Como fruto de este proceso se logran assimilar conocimientos relativos a la parametrización de Swichts relacionados con la asignar vlan, manejar puertos e interfaces acorde con la necesidad.

Además, se adquieren otros conocimientos que son fundamentales, dados los avances tecnológicos que se tienen hoy día y que obligan a una permanente actualización de conceptos.

Es fundamental tener presente la importancia máxima de la seguridad en el manejo de la información, ya que ésta, está expuesta a diferentes peligros en las redes informáticas, para lo cual es fundamental establecer unos adecuados protocolos de ingreso.

Se trabajó con el protocolo de DHCP y NAT, y se efectuaron unas adecuadas pruebas de conectividad, para verificar el sistema funcional de los dispositivos empleados en el proceso desarrollado

REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

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

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: <https://static-courseassets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

