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

VIVIANA CAROLINA RODRÍGUEZ MARTÍNEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS ECBTI
INGENIERÍA DE SISTEMAS
TUNJA -BOYACÁ
2020

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

VIVIANA CAROLINA RODRÍGUEZ MARTÍNEZ

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 TECNOLOGÍAS E INGENIERÍAS ECBTI
INGENIERÍA DE SISTEMAS
TUNJA -BOYACÁ
2020

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL JURADO

_____

FIRMA DEL ASESOR

TUNJA,20 OCTUBRE 2020

AGRADECIMIENTOS

A Dios por permitirme el logro de una nueva meta, tal vez la más anhelada hasta ahora; pero la más provechosa a pesar de las dificultades y tropiezos que he tenido.

A mis padres y mis hermanas por el apoyo incondicional.

A mi esposo e hija por el tiempo, dedicación y sacrificio a la familia, mi esposo el cual me corregía los trabajos y me sacaba lágrimas, mi hija la cual me daba ánimo y fortaleza para continuar a pesar de las adversidades.

A mis tutore de la universidad los cuales me brindaron el apoyo y acompañamiento en cada uno de los pasos para cumplir ésta meta.

A mi abuelita por sus oraciones diarias.

A mi abuelito que ésta en el cielo.

Y a todo aquel que de una y otra forma intervino en la ejecución de este logro.

CONTENIDO

página

AGRADECIMIENTOS....4
CONTENIDOS....5
LISTA DE TABLAS....6
LISTA DE FIGURAS....8
GLOSARIO....10
RESUMEN....11
ABSTRACT....12
INTRODUCCIÓN....13
ESCENARIO 1....14
DESARROLLO....14
ESCENARIO 2....38
DESARROLLO….....39
CONCLUSIONES....60
REFERENCIA BIBLIOGRÁFICA....61
ANEXO….....63

LISTA DE TABLAS

Tabla 1. Vlans 14
Tabla 2. Asignación de direcciones 15
Tabla 3. Configuración inicial deR1 16
Tabla 4. Configuración inicial S1 y S2 20
Tabla 4.1. Creación Vlans y configuración S1 23
Tabla 4.2. Creación Vlans y configuración S2 26
Tabla 5. Configuración Routing y DCHP Ipv4 para Vlan 2 y Vlan 3 29
Tabla 6. Configuración Network de PC-A 30
Tabla 6.1. Configuración Red de PC-A 31
Tabla 7. Verificación de conectividad 32
Tabla 8 inicialización R2 39
Tabla 9 direccionamiento servidor internet 40
Tabla 10. Configuración inicial R1 40
Tabla 11 configuración inicial R2 41
Tabla 12. Configuración R3 43
Tabla 13 configuración S1 44
Tabla 14 configuración S3 45
Tabla 15 tabla verificación de conectividad 46
Tabla 16 creación y asignación de Vlan S1 47
Tabla 17 creación y asignación de Vlan S3 49
Tabla 18 configuración subinterfaz 802.1Q en R1 50
Tabla 19 conectividad entre S1 a R1.S3 a R1 50
Tabla 20 Configurar OSPF en el R1 52

Tabla 21 Configurar OSPF en el R2 52
Tabla 22 Configurar OSPFv3 en el R2 53
Tabla 23 verificación OSPF 54
Tabla 24 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 54
Tabla 25 Configurar la NAT estática y dinámica en el R2 55
Tabla 26 Verificar el protocolo DHCP y la NAT estática 56
Tabla 27 Configurar NTP 58
Tabla 28 Restringir el acceso a las líneas VTY en el R2 58
Tabla 29 respuesta 59

LISTA DE FIGURAS

Figura 1. Escenario 1 14
Figura 2. PC-A 32
Figura 3. PC-A 32
Figura 4. PC-A 32
Figura 5. PC-A 32
Figura 6. PC-A 33
Figura 7. PC-A 33
Figura 8. PC-A 33
Figura 9. PC-A 33
Figura 10. PC-A 33
Figura 11. PC-A 34
Figura 12. PC-A 34
Figura 13. PC-A 34
Figura 14. PC-A 34
Figura 15. PC-A 34
Figura 16. PC-B 35
Figura 17. PC-B 35
Figura 18. PC-B 35
Figura 19. PC-B 35
Figura 20. PC-B 35
Figura 21. PC-B 36
Figura 22. PC-B 36
Figura 23. PC-B 36
Figura 24. PC-B 36
Figura 25. PC-B 36
Figura 26. PC-B 36
Figura 27. PC-B 37

Figura 28. ESENARIO 2 32
Figura 29. R1 a R2.....46
Figura 30. R2 a R3..... 46
Figura 31. Internet… 47
Figura 32. S1 a R1 Vlan99 y Vlan 21..... 51
Figura 33.S3 a R1 Vlan99 y Vlan 23..... 51
Figura 34. PC-A DHCP 56
Figura 35. PC-C DHCP… 57
Figura 36. Ping PC-A -PC-C 57
Figura 37. ACL… 59

GLOSARIO

ACL: es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

ACADEMIA CISCO: es un programa educativo sin ánimo de lucro cuyo objetivo es contribuir a la preparación de estudiantes en el diseño, configuración y mantenimiento de redes, a través de uno de los modelos online más avanzados.

Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA.

Routers: se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios.

Switches: se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos.

RESUMEN

Se presenta dos escenarios, donde se realiza la configuración del Router, el Switch y los hosts con el direccionamiento ipv4 e ipv6 y con ayuda del packet tracer; sabiendo que ésta es una herramienta la cual sirve para simular una red con múltiples representaciones visuales y pruebas de conectividad a través del comando ping antes de llevarlo a un funcionamiento real.

Entre las configuraciones podemos encontrar el DHCP el cual permite desde el router realizar la configuración a los hosts, otra y no menos importante en la de seguridad ya que con las contraseñas se protege los dispositivos de cualquier persona ajena al sistema el cual nos arroja un mensaje indicando acceso restringido; para identificar los dispositivos se deben colocar un nombre los cuáles podamos identificar, además de esto se crean la Vlnas con sus respectivos nombres y configuración para que se le agine un direccionamiento ipv4 e ipv6.

Para la realización de cada topología se debe primero verificar a que interfaz va conectada y una vez configurada hay que activarla, las otras que no se necesitan se desactivan para no generar tanto tráfico y evitar que entren en conflicto entre ellas; esto con los comandos shutdown y no shutdown, se crean troncales las cuales pasan el tráfico de red por la configuración predeterminada.

Hay que tener en cuenta que algunos comandos no los toma el packet tracer, en un simulador, pero al aplicarlos en la vida real si,

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, y tecnología de la comunicación.

ABSTRACT

Two scenarios are presented, where the configuration of Router, Switch and hosts is done with ipv4 and ipv6 addressing and with the help of the packet tracer; knowing that this is a tool which serves to simulate a network with multiple visual representations and connectivity tests through the ping command before taking it to a real operation.

Among the configurations we can find the DHCP which allows from the router to make the configuration to the hosts, another one and not less important the security one since with the passwords the devices of any person outside the system are protected which throws a message to us indicating restricted access; to identify the devices a name must be placed which we can identify, in addition to this the Vlnas with its respective names and configuration are created so that an ipv4 and ipv6 direction is agin.

In order to carry out each topology, it is first necessary to verify to which interface it is connected and once it is configured, it must be activated, the others that are not needed are deactivated so as not to generate so much traffic and avoid conflict between them; this, with the shutdown and no shutdown commands, trunks are created which pass the network traffic through the predetermined configuration.

It should be noted that some commands are not taken by the packet tracer, in a simulator, but when applied in real life they are,

Keywords: CISCO, CCNA, Switching, Routing, Networks, and communication technology.

INTRODUCCIÓN

Gracias a las redes informáticas se puede comunicar a grandes distancias y a través de diferentes dispositivos alámbricos e inalámbricos enviando paquetes entre sí, además de esto con la seguridad de la información se puede proteger los datos más importantes de ataques de los hackers.

Como ingenieros de sistemas estamos en la capacidad de realizar configuraciones para que cualquier persona no puede ingresar a los dispositivos ni conectarse, ya que estos están protegidos mediante contraseñas y mensajes los cuales impiden el ingreso a personas ajenas a una red específica. Ésta protección se logra a través de la configuración de Routes, switchs, host y direccionamiento Ivp4 e Ipv6, igualmente se evita el robo de información por parte de los ciberdelincuentes.

En el siglo XXI todo se está manejando con tecnología es por eso que como ingenieros de sistemas deben estar a la vanguardia y actualidad de la red para así dar soluciones a la problemática presentada en la vida cotidiana como la conexión por fibra óptica en los lugares más apartados y difíciles de llegar, de esta manera se puede brindar asesoría para la conectividad de red y seguridad de la información.

Incluso la nueva tecnología de las redes ha permitido la conexión para que las entidades educativas no paren en estos tiempos de pandemia (covid-19) para la cual no estaba preparada, sino que por el contrario continúen con su labor a través de redes telemáticas; y a su vez el desarrollo de la telemedicina para que así desde casa se puede tener una cita especializada y sin tener que desplazarse a otros lugares.

Escenario 1

Topología

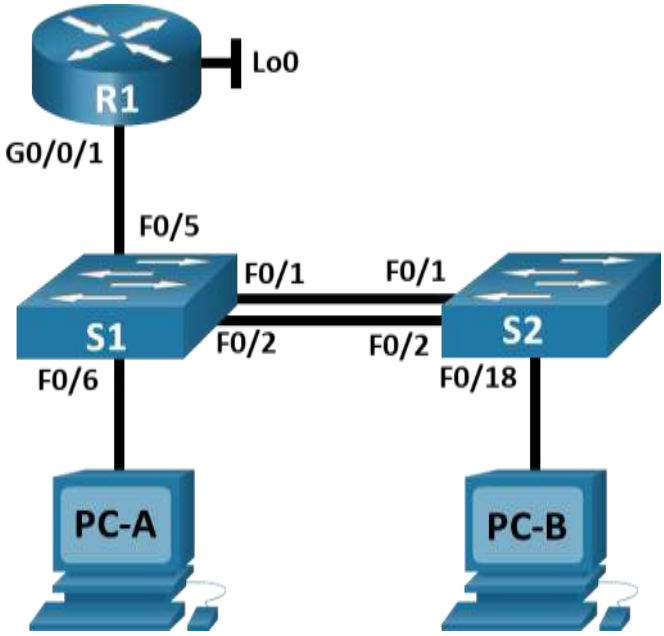


FIGURA 1.

Con este ejercicio se configurarán dispositivos de una pequeña red, los dispositivos a configurar son router4331 y switch multicapa 3560 con conectividad ipv4 al igual que ipv6 esta red debe administrase de forma segura Configurará y se configurara el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN 1

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
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para Ipv4	DHCP para puerta de enlace predeterminada Ipv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección Ipv4	DHCP para puerta de enlace predeterminada Ipv4
	2001:db8:acad:b: :50 /64	fe80::1

Desarrollo escenario1

Parte 1: Inicializar y Recargar y Configurar aspectos 16ccess16 de los dispositivos

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

Antes de realizar la configuración de los dispositivos router y switch se inicializan y se vuelven a cargar esto con el fin de que no tenga ninguna configuración predeterminada.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se configura el router inicial con sus respectivas contraseñas así se da protección al Router, se da un nombre al router el cual será R1, con la configuración entre líneas con su respectivo direccionamiento ipv4 e ipv6 activándolas y su respectivo mensaje de si e ingreso mal la contraseña ya que solo se permite a personal autorizado, se da un nombre al dominio, se asigna direccionamiento ipv4 e ipv6 con su respectiva troncal, por último se genera una clave criptográfica con rsa de 1024 bits.

Tabla 3. Configuración inicial R2

Tarea	Especificación
Desactivar la búsqueda DNS	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
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password ciscoconpass

	R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config-line)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15
Configurar VTY solo aceptando SSH	R1(config-line)#login local 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 #Unauthorized access is strictly prohibited. #
Habilitar el routing Ipv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config-if)#interface GigabitEthernet0/0/1.2 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)#no shutdown R1(config-subif)#interface GigabitEthernet0/0/1.3

	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)#no shutdown R1(config-subif)#interface GigabitEthernet0/0/1.4 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)#no shutdown R1(config-subif)#interface GigabitEthernet0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description native

Configure el Loopback0 interface	R1(config-subif)#interface Loopback0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)#no shutdown R1(config-if)#
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024

Paso 3: Configure S1 y S2.

Se realiza las configuraciones básicas del switch para proteger las líneas de comando y los puertos de consola a través de contraseñas, se utiliza el comando no ip domain-looukpel cual sirve para desactivar la traducción de nombres a dirección del dispositivo R1 o S1,S2, se asigna nombres a los switch S1 y S2; se asigna el direccionamiento ipv4 e ipv6 con sus respectivos troncales y vlans, con esta configuración protegemos y damos nombres a los dispositivos, para que de esta manera solo pueda ingresar al dispositivo la persona encargada y no personal ajeno y de esta manera damos seguridad a la red.

Tabla 4. Configuración S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Unauthorized access is strictly prohibited. #
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	S1(config-if)#interface vlan4 s1(config-subif)#description Management S1(config-if)#ip address 10.19.8.98 255.255.255.248

	S1(config-if)#no shut S1(config-if)#ip default-gateway 10.19.8.97 S1(config)#exit S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#no shutdown S1(config-if)#end **S2** Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#hostname S2 S2(config)#ip domain name ccna-lab.com S2(config)#enable secret ciscoenpass S2(config)#line vty 0 15 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#service password-encryption S2(config)#banner motd #Unauthorized access is strictly prohibited. # S2(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S2.ccna-lab.com % The key modulus size is 1024 bits

	% Generating 1024 bit RSA keys, keys will be non-exportable…[OK] *Mar 1 0:36:2.307: %SSH-5-ENABLED: SSH 1.99 has been enabled S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface vlan4 S2(config-if)#description Management S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#no shutdown S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#no shutdown S2(config-if)#
Configuración del 22ccess22 predeterminado	S1(config-if)#ip default-gateway 10.19.8.97 S2(config-if)#ip default-gateway 10.19.8.97

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

Paso 4: Configurar S1

Se crean las Vlans con sus respectivos nombres para S1, Crear troncos 802.1Q que utilicen la VLAN 6 nativa Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se Configura el puerto de acceso de host para VLAN 2, se da seguridad los puertos de acceso y se protege las interfaces que no se utilizan. Esto con el fin de facilitar la intercomunicación entre distintas vlans

Se configura las vlans con sus respectivos nombre e interfaces se crean sus respectivas troncales, se crean grupos de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se Configurar el puerto de acceso de host para VLAN 2 y se da seguridad a los puertos de acceso. Esto con el fin de dar conexión entre diferentes switch y Router.

Tabla 4.1. creación Vlans y configuración S1

Tarea	**Especificación**
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Brikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface range f0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#

	S1(config)#interface range f0/5 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación S1(config)#interface range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport mode trunk Command rejected: An interface whose trunk encapsulation is “Auto” can not be configured to “trunk” mode.. S1(config-if)#switchport trunk native vlan 6 S1(config-if)#
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 S1(config)#Interface F0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down S1(config-if)#switchport port-security S1(config-if)#

Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar Acceso vlan 5 descripcion interface 3 y 4 A7 la 24 g 0/1-2 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 interface no use S1(config-if-range)# no 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 interface no use S1(config-if-range)#no 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 interface no use S1(config-if-range)#no shutdown

Paso 5: Configure el S2.

Se configura las vlans con sus respectivos nombre e interfaces se crean sus respectivas troncales, se crean grupos de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se Configurar el puerto de acceso de host para VLAN 2 y se da seguridad a los puertos de acceso de tal manera que ninguna persona ajena pueda ingresar al S2 esto con el fin de proteger la red. S2 se configura de tal manera que pueda conectarse entre S1, S2 y R1

Tabla 4.2 creación Vlans configuración S2

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	Interfaces F0/1 y F0/2 S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#interface range f0/1-2

	S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación S2(config)#interface range f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#Creating a port-channel interface Port-channel 1 S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 S2(config)#Interface F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security S2(config-if)#
Configure port-security en los 27ccess ports	permite 3 MAC addresses S2(config-if)#switchport port-security maximum 3

Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2(config)#Interface F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#exit 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 interface no use S2(config-if-range)#no shutdown S2(config-if-range)# S2(config-if-range)#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 interface no use S2(config-if-range)#no shutdown S2(config-if-range)# S2(config-if-range)#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 interface no use S2(config-if-range)#no shutdown S2(config-if-range)#

Parte 1: <u>Configurar soporte de host</u>

Paso 1: Configure R1

Primero se crean rutas predeterminadas para Ipv4 e Ipv6 que dirijan el tráfico a la interfaz Loopback 0, luego se Configura Default Routing; para configurar Ipv4 DHCP para VLAN 2 se toma la última dirección ip de la Vlan 2: 1 a 53 se excluye 54 a 63 se utilizan y para la configuración Ipv4 DHCP para VLAN 3 65 a la 86 se excluyen 86 a 95 se utilizan.

Tabla 5. Configuración R1 con dhcp ipv4 y routing.

Tarea	**Especificación**
Configure Default Routing	Crear rutas predeterminadas para Ipv4 e Ipv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#Interface Loopback 0 R1(config-if)#Ip route 0.0.0.0 0.0.0.0 Loopback 0 R1(config)#Ipv6 route ::/0 Loopback 0 R1(config)#
Configurar Ipv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada 1 a 53 se excluye 54 a 63 se utilizan R1(config)#Ip dhcp pool vlan2-Bikes R1(dhcp-config)#Network 10.19.8.0 255.255.255.192 R1(dhcp-config)#Domain-name ccna-a.net R1(dhcp-config)#domain-name ccna-a.ne

	R1(dhcp-config)#ip dhcp excluded-address 10.19.8.2 10.19.8.51
Configurar DHCP Ipv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada 65 a la 86 se excluyen 86 a 95 se utilizan R1(config)#Ip dhcp pool vlan3-Trikes R1(dhcp-config)#Network 10.19.8.64 255.255.255.224 R1(dhcp-config)#Domain-name ccna-a.net R1(dhcp-config)#Default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#ip dhcp excluded-address 10.19.8.66 10.19.8.83

Paso 2: Configurar los servidores

Se realiza la Configuración de los equipos host PC-A y PC-B para que utilicen DHCP para Ipv4 y asigne estáticamente las direcciones Ipv6 GUA y Link Local.

Tabla 6 configuración Network de PC-A

PC-A Network Configuration	
Descripción	*0060.5CB5.DD73*
Dirección física	*00D0.D3B7.B10E*
Dirección IP	*10.19.8.87*

Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado Ipv6	*FE80::1*

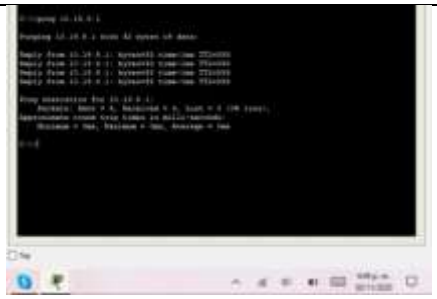
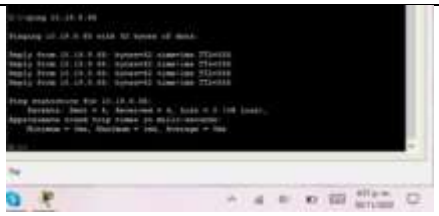
Tabla 6.1 configuración de red PC-A

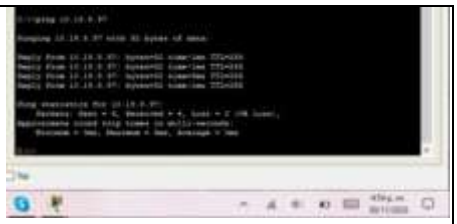
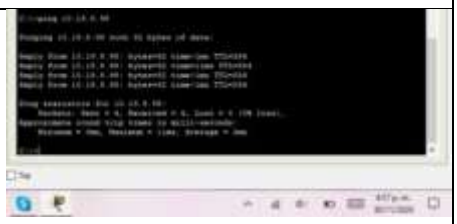
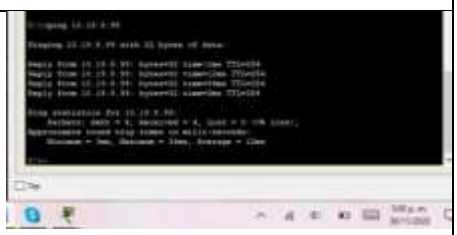
Configuración de red de PC-A	
Descripción	*0000.0CE4.D30C*
Dirección física	*0060.5CB5.DD73*
Dirección IP	*10.19.8.87*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado Ipv6	*FE80::1*

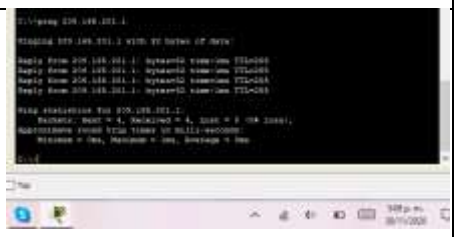
Parte 2: Probar y verificar la conectividad de extremo a extremo

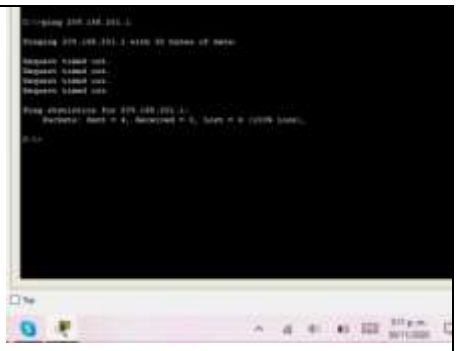
Use el comando ping para probar la conectividad Ipv4 e Ipv6 entre todos los dispositivos de red.

Tabal.7 de verificación de conectividad.

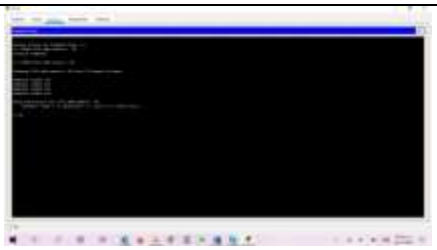
Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	 Figura 2. PC-A
PC-A	*R1, G0/0/1.2*	Ipv6	2001:db8:acad:a::1	 Figura 3. PC-A
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	 Figura 4. PC-A
PC-A	*R1, G0/0/1.3*	Ipv6	2001:db8:acad:b::1	 Figura 5. PC-A

PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	 Figura 6. PC-A
PC-A	*R1, G0/0/1.4*	Ipv6	2001:db8:acad:c::1	 Figura 7. PC-A
PC-A	S1, VLAN 4	Dirección	10.19.8.98	 Figura 8. PC-A
PC-A	*S1, VLAN 4*	Ipv6	2001:db8:acad:c::98	 Figura 9. PC-A
PC-A	S2, VLAN 4	Dirección	10.19.8.99	 Figura 10. PC-A

PC-A	*S2, VLAN 4*	Ipv6	2001:db8:acad:c::99	 Figura 11. PC-A
PC-A	PC-B	Dirección	10.19.8.52	 Figura 12. PC-A
PC-A	*PC-B*	Ipv6	2001:db8:acad:b::50	 Figura 13. PC-A
PC-A	R1 Bucle 0	Dirección	209.165.201.1	 Figura 14. PC-A
PC-A	*R1 Bucle 0*	Ipv6	2001:db8:acad:209: :1	 Figura 15. PC-A

PC-B	R1 Bucle 0	Dirección	209.165.201.1	 Figura 16. PC-B
PC-B	*R1 Bucle 0*	Ipv6	2001:db8:acad:209: :1	 Figura 17. PC-B
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	 Figura 18. PC-B
PC-B	*R1, G0/0/1.2*	Ipv6	2001:db8:acad:a::1	 Figura 19. PC-B
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	 Figura 20. PC-B

PC-B	*R1, G0/0/1.3*	Ipv6	2001:db8:acad:b::1	 Figura 21. PC-B
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	 Figura 22. PC-B
PC-B	*R1, G0/0/1.4*	Ipv6	2001:db8:acad:c::1	 Figura 23. PC-B
PC-B	S1, VLAN 4	Dirección	10.19.8.98	 Figura 24. PC-B
PC-B	*S1, VLAN 4*	Ipv6	2001:db8:acad:c::98	 Figura 25. PC-B
PC-B	S2, VLAN 4	Dirección	10.19.8.99	 Figura 26. PC-B

PC-B	S2, VLAN 4	IPv6	2001:db8:acad:c::99	 Figura 27. PC-B

Observación:

Teniendo en cuanta la configuración del DHCP en el R1 se configura de tal manera que funciones las conexiones con el comando ping, pero al verificar la conexión solo da conexión con PC-A ipv4 y error con PC-A ipv6 de igual manera error en PC-B ipv4 e ipv6.

Escenario 2

Topología

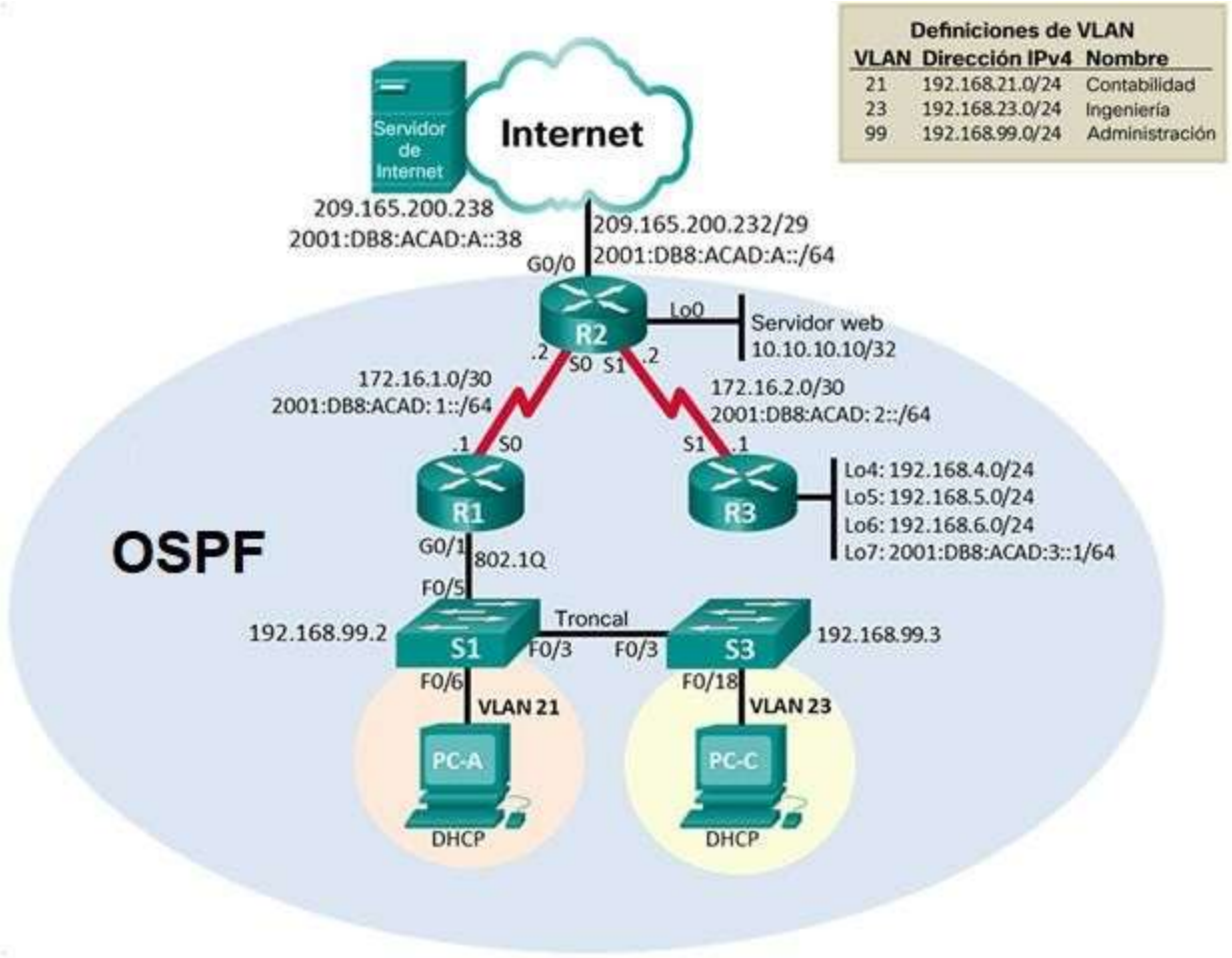


Figura 28.

Desarrollo escenario 2

Parte 1: Inicializar dispositivos

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

Para el desarrollo de este escenario se realiza la topología en el packet tracer el cual seleccionamos 3 Routers 2911,2 Switches 2960 con un servidor de internet y 2 PC; En este paso se realizar el proceso de eliminar la configuración establecida por el Router con el comando **startup-config** y se vuelve a cargar con el comando **reload**, esto para no apagar y volver a encender el Router se realiza con estos

comandos, para verificar la base de datos de la vlan se utiliza el siguiente comando show **flash;** esto se hace con los Router y los Switches

Tabla 8 inicialización R2

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Router# Router>enable Router#erase startup-config Router# Router>enable Router#erase startup-config Router#
Volver a cargar todos los routers	Router#reload Router#reload Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete vlan.dat Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show flash Switch# show flash

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Es este paso se da la configuración del servidor de internet el cual se ingresa la ip v4 209.165.200.238 nos arroja la máscara de subred e ingresamos el Gateway predeterminado de igual manera con el direccionamiento ipv6.

Tabla 9 direccionamiento servidor internet.

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

Paso 2: Configurar R1

Continuamos con la configuración del R1 en el cual se utilizan una serie de comandos para ingresar contraseñas las cuales ninguna persona ajena pueda ingresar al router esto con el fin de proteger nuestro router, en caso tal de que un usuario acceda y no sepa la contraseña el sistema arrojara un mensaje de acceso prohibido.

se configura la interfaz S0/0/0, S0/0/1,G0/0 con direccionamiento ipv4 e ipv6,interfaz Loopback 0 esto con el fin de dar conectividad con el resto de los enrutadores.

Tabla 10. Configuración inicial R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#

Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Unauthorized access is strictly prohibited. #
Interfaz S0/0/0	R1(config)#interface Serial0/0/0 R1(config-if)#description conection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#no shutdown R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#no shutdown R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 S0/0/0

Paso 3: Configurar R2

Se realiza la configuración del R2 en el cual por medio de comandos se agina un nombre al Router, se crean contraseñas para que ninguna persona ajena pueda ingresar a desconfigurar o alterar la información esto con el fin de seguridad de la información y los equipos.

Se realiza la configuración de la interfaz S0/0/0,S0/0/1,g0/1 y servidor web loopback 0 configurando por último la ruta predeterminada.

Tabla 11 configuración inicial R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class

Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http secure-server no lo soporta packet tracer
Mensaje MOTD	R2(config)#banner motd #Unauthorized access is strictly prohibited. #
Interfaz S0/0/0	R2(config)#interface Serial0/0/0 R2(config-if)#description conection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#interface Serial0/0/1 R2(config-if)#description conection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#no shutdown R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#interface GigabitEthernet0/0 R2(config-if)#description conection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shutdown 2001:bd8:acad:a::1/64 R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)	R2(config-if)#interface lo0 R2(config-if)#description simulated Web server R2(config-if)#ip address 10.10.10.10 255.255.255.255
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

En esta configuración se configura las contraseñas de acceso, se desactiva la búsqueda NDS para desactivar la traducción de nombres de dirección, con el uso de contraseñas podemos evitar que personal ajeno pueda acceder al router y realizar algún tipo de configuración fraudulenta; para esto el sistema arroja un mensaje de alerta, se configura la interfaz S0/2/1, loopback de la 4 a la 6 con direccionamiento ipv4 loopback 7 con direccionamiento ipv6 esto con el fin de asignar a un puerto y no se conecte a otro dispositivo y para probar y administrar un dispositivo.

Tabla 12. Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Unauthorized access is strictly prohibited. #

Interfaz S0/2/1	R3(config)#interface Serial0/2/1 R3(config-if)#description conection 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)#interface lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#
Interfaz loopback 5	R3(config-if)#interface lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#
Interfaz loopback 6	R3(config-if)#interface lo6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#
Interfaz loopback 7	R3(config-if)#interface lo7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1 R3(config)#ipv6 route ::/0 s0/2/1 R3(config)#

Paso 5: Configurar S1

Para esta configuración se asigna un nombre al switch y una contraseña de inicio esto con el fin de proteger el S1 se crea un banner el cual indica mensaje de alerta si no se sabe la contraseña, esto es la configuración inicial de S1

Tabla 13 configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1

Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Unauthorized access is strictly prohibited. #

Paso 6: Configurar el S3

En esta configuración de inicio se da un nombre a switch el cual es muy importante para identificar el dispositivo se ingresan contraseñas y mensaje de alerta por si algún usuario desconocido quisiera acceder, pero no le permite ya que las contraseñas son incorrectas.

Tabla 14 configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#login local
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption

Mensaje MOTD	S3(config)#banner motd #Unauthorized access is strictly prohibited. #

Paso 7: Verificar la conectividad de la red

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

En esta conectividad se realiza pruebas entre los dispositivos R1 a R2,R2 a r3,por ultimo de servidor de internet al Gateway predeterminado.

Tabla 15 tabla verificación de conectividad.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	perfecta
R2	R3, S0/0/1	172.16.2.2	perfecta
PC de Internet	Gateway predeterminado	209.165.200.233	perfecta

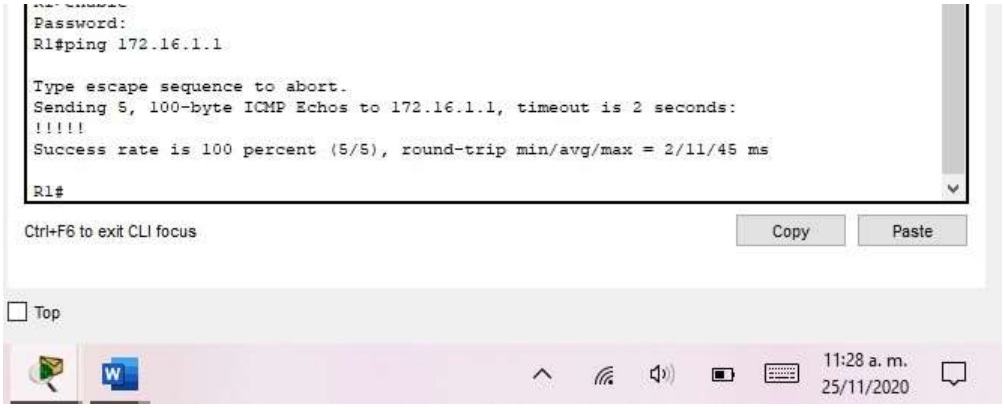


Figura 29.R1 a R2

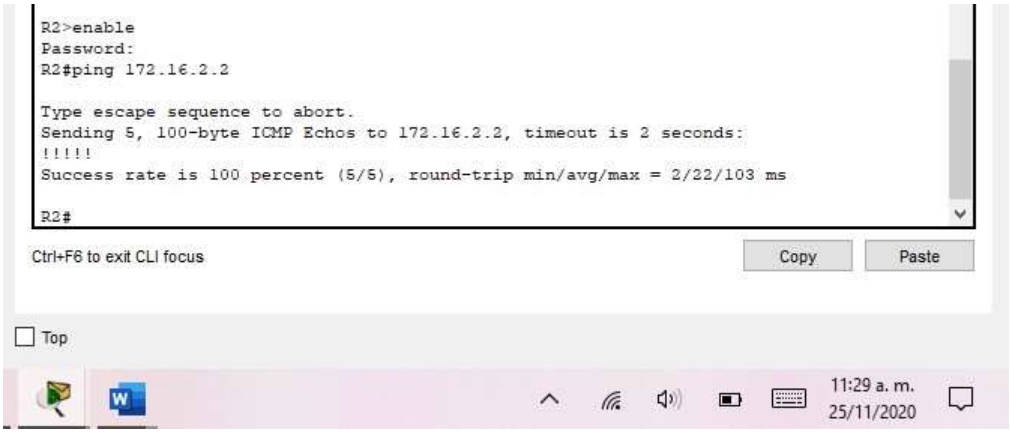


Figura 30. R2 a R3

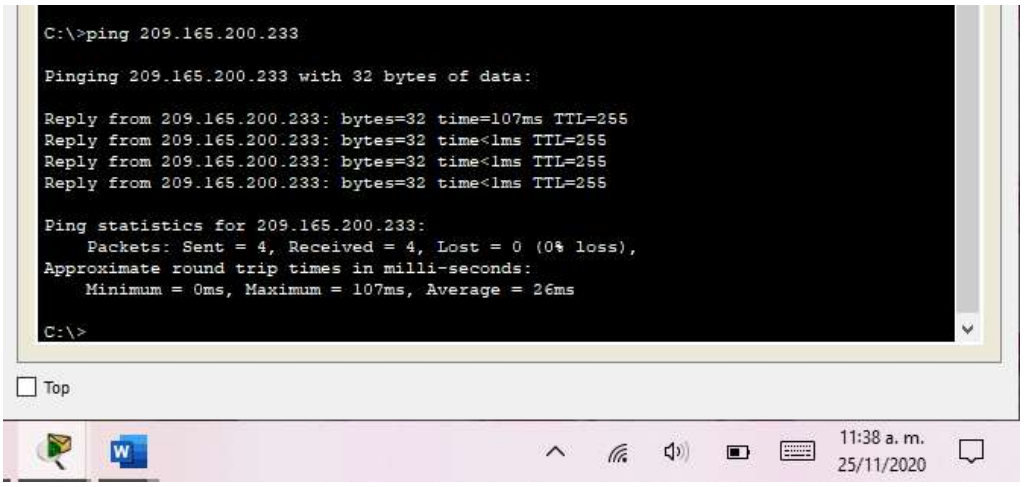


Figura 31. Internet

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

Paso 1: Configurar S1

Se crean Vlan con sus respectivos nombres, se asigna a cada vlan su direccionamiento ip, en las interfaz f0/3,f0/5 se utiliza la Vlan como nativa, se configuran los puertos de acceso con el comando range f0/1-2, f0/4, f0/6-24,g0/1-2, se pagan los comandos que no se utilicen f0/1-2,f0/4,f0/7-24,g0/1-2 con shutdown.

Tabla 16 creación y asignación de Vlan S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. 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-vlan)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown

Asignar el gateway predeterminado	S1(config-if)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface FastEthernet0/3 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)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#interface range f0/1-2, f0/4, f0/6-24,g0/1-2 S1(config-if-range)#switchport mode access
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface 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)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#interface range f0/1-2, f0/4, f0/7-24,g0/1-2
Apagar todos los puertos sin usar	S1(config-if-range)#interface range f0/1-2,f0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

En esta configuración se crea y asigna el nombre a cada Vlan con su respectivo direccionamiento ip, configurar el resto de puertos con de acceso con el

comando S3(config-if-range)#interface range f0/1-2, f0/4-24, g0/1-2, por último se apagan los puertos que no se utilizan con el comando range y shutdown

Tabla 17 creación y asignación de Vlan S3

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-vlan)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config-if)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface FastEthernet0/3 S3(config-if)#switch mode trunk S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#interface range f0/1-2,f0/4-24,g0/1-2
Configurar el resto de los puertos como puertos de acceso	S3(config-if-range)#interface range f0/1-2, f0/4-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config-if-range)#switchport mode access S3(config)#interface FastEthernet0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#interface range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

En este paso se configuran la subinterfaz 802.1Qen la G0/1 y se activa esto con el fin de dar conectividad entre dispositivos.

Tabla 18 configuración subinterfaz 802.1Q en R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface 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)#interface 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)#interface 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)#interface g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

Con el comando **ping** se proba la conectividad entre los switches y el R1.

Tabla 19 conectividad entre S1 a R1.S3 a R1.

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

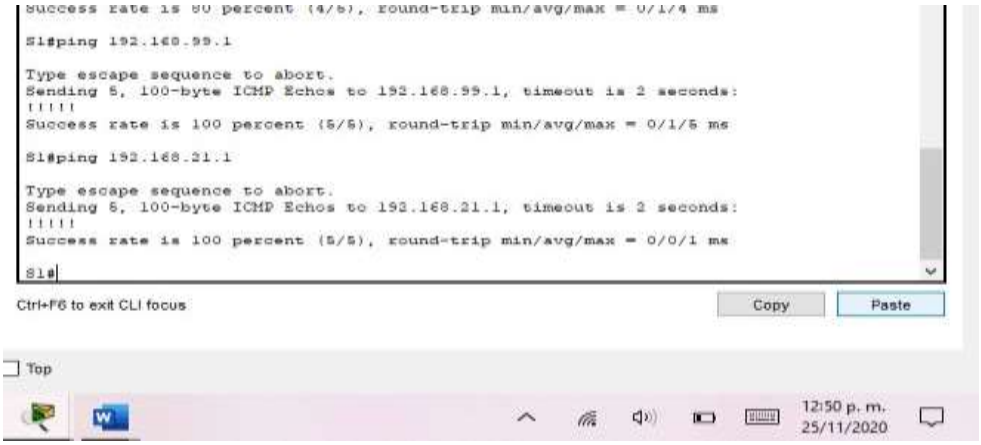


Figura 32. S1 a R1 Vlan 99 y vlan 21

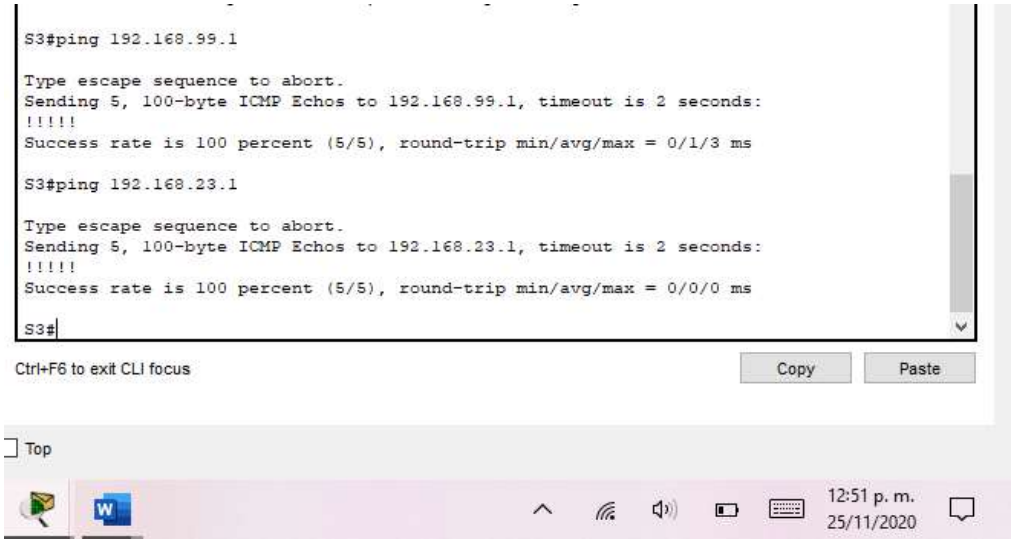


Figura 33. S3 a R1 Vlan 99 y Vlan 23

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Esta configuración se realiza con el fin de que el OSPF esté activo en el router con las direcciones de red y la información de área específica con mascara wildcard y no con mascara de subred, esta mascara wildcard representa las direcciones de enlaces o host que estén presentes.

Tabla 20 Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Anunciar las redes conectadas directamente	R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.3 area 0 R1(config-router)#network 192.168.23.0 0.0.0.3 area 0 R1(config-router)#network 192.168.99.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar OSPF en el R2

Esta configuración se realiza con el fin de que el OSPF esté activo en el router con las direcciones de red y la información de área específica con mascara wildcard y no con mascara de subred, esta mascara wildcard representa las direcciones de enlaces o host que estén presentes.

Tabla 21 Configurar OSPF en el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)# network 10.10.10.10 0.0.0.7 area 0

Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)# network 10.10.10.10 0.0.0.7 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar OSPFv3 en el R2

Esta configuración se realiza con el fin de que el OSPF esté activo en el router con las direcciones de red y la información de área específica con mascara wildcard y no con mascara de subred, esta mascara wildcard representa las direcciones de enlaces o host que estén presentes.

Tabla 22 Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R1(config-router)# network 172.16.2.0 0.0.0.255 area 0
Anunciar redes IPv4 conectadas directamente	R2(config-router)# network 172.16.2.0 0.0.0.255 area 0 R2(config-router)#network 192.168.4.0 0.0.0.255 area 0 R2(config-router)#network 192.168.5.0 0.0.0.255 area 0 R2(config-router)#network 192.168.6.0 0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config-router)#passive-interface loopback 4 R2(config-router)#passive-interface loopback 5 R2(config-router)#passive-interface loopback 6

Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 4: Verificar la información de OSPF

Para la verificación de OSPF esté funcionando como se espera, se utilizan los comandos **show ip protocols**, **Show ip route ospf**, **Shuw run**.esto con el fin de rar respuesta a cada pregunta.

Tabla 23 verificación OSPF

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

Parte 5: Implementar DHCP y NAT para IPv4

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

En este paso se Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas, de igual manera con la Vlan 23, se Crea un pool de DHCP para la VLAN 21 y VLAN 23.

Tabla 24 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

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

Crear un pool de DHCP para la VLAN 21.	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 ccnasa.com
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccnasa.com

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

Crear una base de datos local con una cuenta de usuario, pero el packet tracer no soporta el comando para HTTP

Tabla 25 Configurar la NAT estática y dinámica en el R2

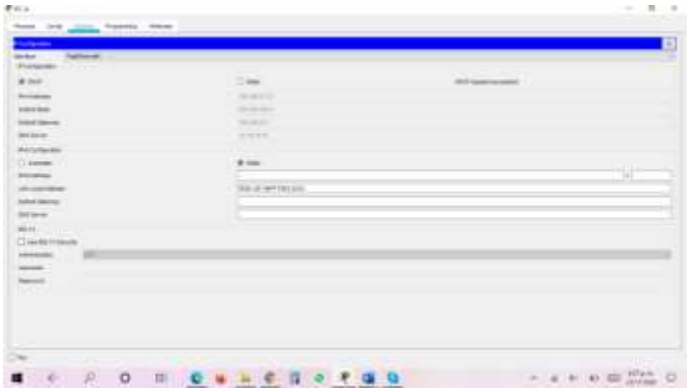
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet tracer no soporta los comandos de habilitación del servidor HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Packet tracer no soporta los comandos de habilitación del servidor HTTP
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	

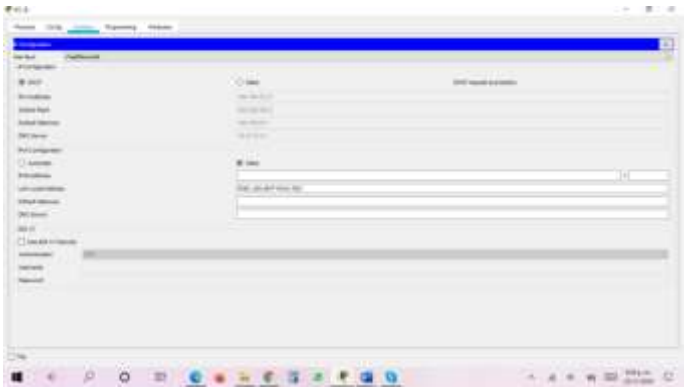
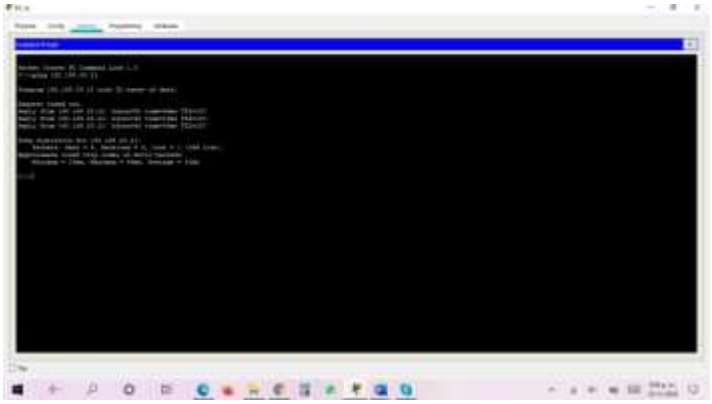
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 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.

Tabla 26 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 Figura 34 PC-A- DHCP

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Figura 35. PC-C DHCP
Verificar que la PC-A pueda hacer ping a la PC-C	 Figura 36. Ping PC-A-PC-C
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	No se puede acceder ya no se pudo configurar el servidor http.

Parte 6: Configurar NTP

Se ajusta la fecha y hora en R2; hay comandos que packet gtracer no acepta.

Tabla 27 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 ? R2#clock set 09:00:00 5 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2** Packet tracer no soporta el comando
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Packet tracer no soporta el comando
Verifique la configuración de NTP en R1.	Packet tracer no soporta el comando

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

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

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, Aplicar la ACL con nombre a las líneas VTY y Permitir acceso por Telnet a las líneas de VTY.

Tabla 28 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 R2(config-std-nacl)#

Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#
Permitir acceso por Telnet a las líneas de VTY	Packet tracer no soporta el comando
Verificar que la ACL funcione como se espera	 Figura 37 ACL

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

Con los siguientes comandos se ejecutan los dispositivos y de ahí se da respuesta a las preguntas planteadas.

Tabla 29 respuesta

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show ip access-list
Restablecer los contadores de una lista de acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translations

CONCLUCIONES

Se realiza la configuración inicial de los Switchs S1 y S2 y R1 donde se crean contraseñas de seguridad para impedir el acceso a personal ajeno a la red, se crean las vlans y se da sus respectivos nombres, se presenta dificultad en el Subneteo ya que si indica que se toman 10 direcciones para la configuración de la vlan 4.

Se logra la comprensión e importancia del direccionamiento y denominación esquemas en varias capas de redes de datos en entornos IPv4 e IPv6
con sus respectivos troncales.

Gracias al convenio entre la Universidad Nacional Abierta y a Distancia (UNAD) y CISCO se puede medir el conocimiento adquirido a través de cada guía y practica realizada en el packet tracer, a través de los comandos para cada configuración de los protocolos DHCP, NAT, VLAN, NTP, OSPF.

A través de las pruebas de conectividad se puede verificar que los escenarios realizados con los comandos para cada configuración quedaron funcionando, ya que se muestra que sí hay la conectividad requerida.

REFERENCIAS BIBLIOGRÁFICAS

1992-2012 Cisco Systems, Inc. Todos los derechos reservados, recuperado de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-

assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

Educación Programas educativos Cisco Networking Academy, recuperado de, https://www.pue.es/pue-academy/cisco-networking-academy#:~:text=Cisco%20Networking%20Academy%20(CNA)%20es,los%20modelos%20online%20m%C3%A1s%20avanzados Publicado el 30 septiembre, 2014 por erickosvaldovg, recuperado de, https://erickosvaldovg.wordpress.com/2014/09/30/que-es-packet-tracer/

ANEXOS

ANEXO1

Enlace de descarga de archivos de simulación

https://drive.google.com/file/d/1Yabd3kCKp-F8bTX5Fs2WXe-nKRlfESow/view?usp=sharing

ANEXO 2

Artículo Científico IEEE

Packet Traser En La Solución De Un Escenario

Viviana Carolina Rodríguez Martínez
Universidad Nacional Abierta y a Distancia (UNAD), vcrodriguezm@unadvirtual.edu.co

Resumen

En este articulo Se presenta dos escenarios, donde se realiza la configuración del Router, el Switch y los hosts con el direccionamiento ipv4 e ipv6 y con ayuda del packet tracer; sabiendo que ésta es una herramienta la cual sirve para simular una red con múltiples representaciones visuales y pruebas de conectividad a través del comando ping antes de llevarlo a un funcionamiento real.
Entre las configuraciones podemos encontrar el DHCP el cual permite desde el router realizar la configuración a los hosts, otra y no menos importante en la seguridad ya que con las contraseñas se protege los dispositivos de cualquier persona ajena al sistema el cual nos arroja un mensaje indicando acceso restringido; para identificar los dispositivos se deben colocar un nombre los cuáles podamos identificar, además de esto se crean la Vlnas con sus respectivos nombres y configuración para que se le agine un direccionamiento ipv4 e ipv6.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, y tecnología de la comunicación.

Abstract:

Two scenarios are presented, where the configuration of Router, Switch and hosts is done with ipv4 and ipv6 addressing and with the help of the packet tracer; knowing that this is a tool which serves to simulate a network with multiple visual representations and connectivity tests through the ping command before taking it to a real operation.
Among the configurations we can find the DHCP which allows from the router to make the configuration to the hosts, another one and not less important the security one since with the passwords the devices of any person outside the system are protected which throws a message to us indicating restricted access; to identify the devices a name must be placed which we can identify, in addition to this the Vlnas with its respective names and configuration are created so that an ipv4 and ipv6 direction is agin.

Keywords: CISCO, CCNA, Switching, Routing, Networks, and communication technology.

INTRODUCCIÓN

Gracias a las redes informáticas se puede comunicar a grandes distancias y a través de diferentes dispositivos alámbricos e inalámbricos enviando paquetes entre sí, además de ésto con la seguridad de la información se puede proteger los datos más importantes de ataques de los hackers. Como ingenieros de sistemas estamos en la capacidad de realizar configuraciones para que cualquier persona no puede ingresar a los dispositivos ni conectarse, ya que estos están protegidos mediante contraseñas y mensajes los cuales impiden el ingreso a personas ajenas a una red específica. Ésta protección se logra a través de la configuración de Routes, switchs, host y direccionamiento Ivp4 e Ipv6, igualmente se evita el robo de información por parte de los ciberdelincuentes.

En el siglo XXI todo se está manejando con tecnología es por eso que como ingenieros de sistemas deben estar a la vanguardia y actualidad de la red para así dar soluciones a la problemática presentada en la vida cotidiana como la conexión por fibra óptica en los lugares más apartados y difíciles de llegar, de esta manera se puede brindar asesoría para la conectividad de red y seguridad de la información.

Metodología

se realiza la topología en el packet tracer el cual se requiere de 3 Routers 2911, 2 Switches 2960 con un servidor de internet y 2 PC; En este paso se realizar el proceso de eliminar la configuración establecida por el Router con el comando startup-config y se vuelve a cargar con el comando reload, esto para no apagar y volver a encender el Router se realiza con estos comandos, para verificar la base de datos de la vlan se utiliza el siguiente comando show flash; esto se hace con los Router y los Switches.
Se conectan los dispositivos a cada interfaz correspondiente, esto con el fin de dar conectividad antes de realizar la configuración de los dispositivos.

Implementación:

se tiene un escenario en el cual se quiere configurar la red de seguridad, antes de ello se realiza la configuración de cada dispositivo de red utilizando el packet traser el cul es un simulador de redes donde permite visualizar en tiempo real una configuración según la topología. En este escenario tenemos 3 router,2 Switch, 1 servidor web y 2 Pc. En este escenario se configura los dispositivos dando primero un nombre a cada uno y luego una serie de contraseñas las cuales nos permiten tener seguridad a los dispositivos, en los R se deben desactivar el DNS para desactivar la traducción

de nombres de direcciones, se configura las interfaces según su direccionamiento Ip ipv4 e ipv6, se implementa el protocolo DHCP el cual perite asignar direccionamiento a los hosts y el protocolo NAT el cual permite asignar cualquier dirección ip definiendo un rango para mostrar como origen.
Se configuran los switch dándoles un nombre el cual los identifica también configurando todas las interfaces que tengan, creando y direccionando las Vlan según la ip asignada.
Se direcciona el servidor de internet para que este proporcione red a los dispositivos conectados.

Una vez los dispositivos estén conectados y configurados se realiza pruebas de conectividad con el comando pin el cual sirve para realizar dicha prueba.

Tabla 1 conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	perfecta
R2	R3, S0/0/1	172.16.2.2	perfecta
PC de Internet	Gateway predeterminado	209.165.200.233	perfecta

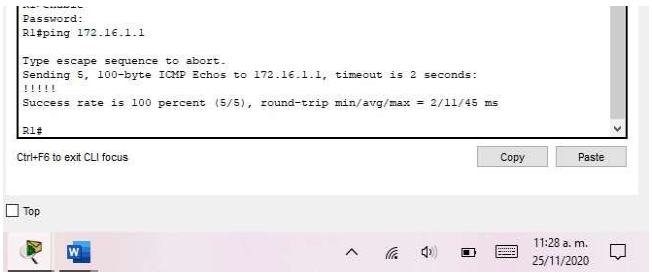


Figura 1 R1 a R2

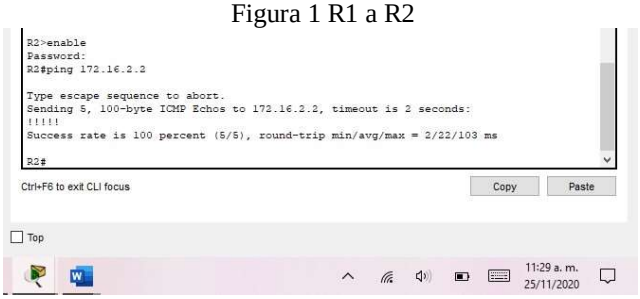


Figura 2 R2 a R3

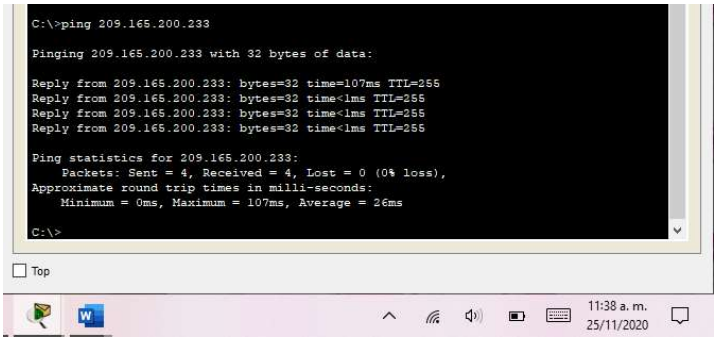


Figura 3 servidor de internet

Se crean Vlan con sus respectivos nombres, se asigna a cada vlan su direccionamiento ip, en las interfaz f0/3,f0/5 se utiliza la Vlan como nativa, se configuran los puertos de acceso con el comando range f0/1-2, f0/4, f0/6-24,g0/1-2, se pagan los comandos que no se utilicen f0/1-2,f0/4,f0/7-24,g0/1-2 con shutdown.

Tabal 2 conectividad entre S

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

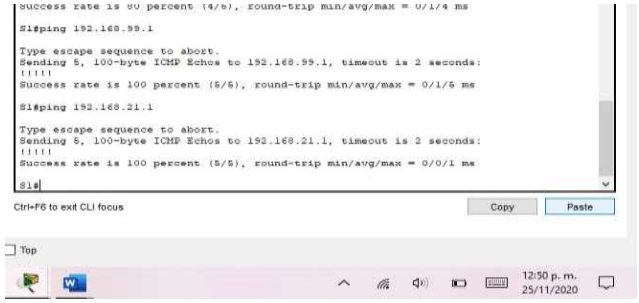


Figura 4 de S1 a R1 Vlan 99 y 21

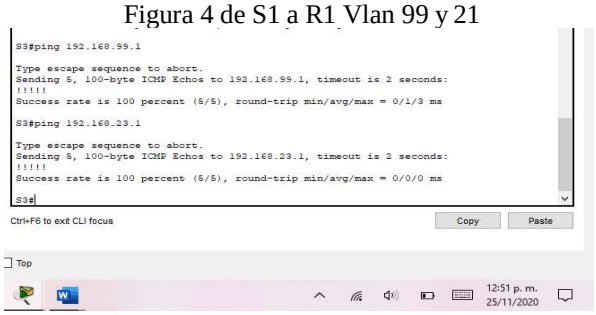


Figura 5 de S3 a R1 Vlan 99 y 23

Tabla 3 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 9 PC-A- DHCP
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 10. PC-C DHCP
Verificar que la PC-A pueda hacer ping a la PC-C	Figura 11. Ping PCA-Pc-C

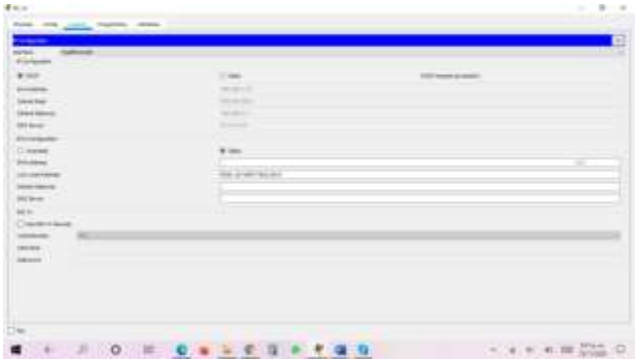


Figura 9 PC-A- DHCP

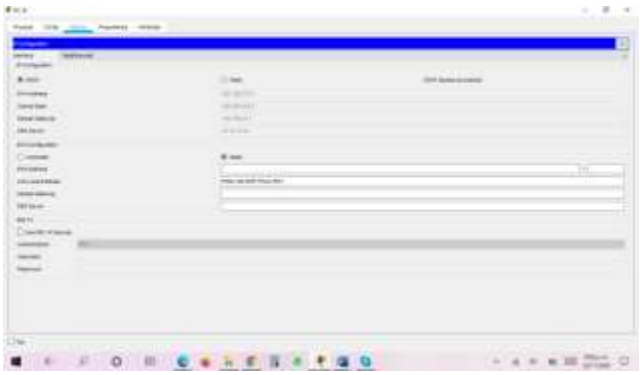


Figura 10.PC-C DHCP

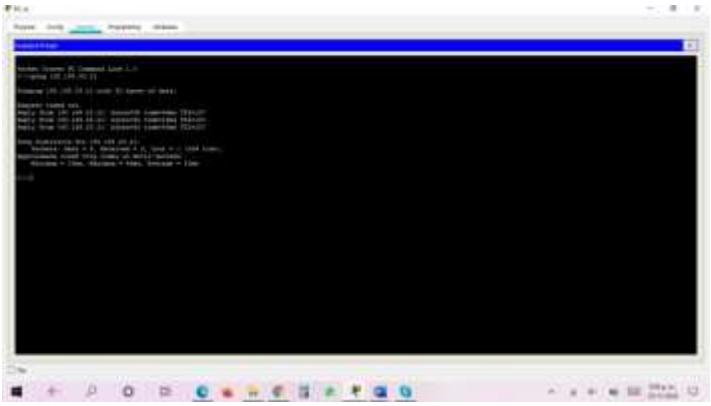


Figura 11. Ping PCA-Pc-C

Escenario

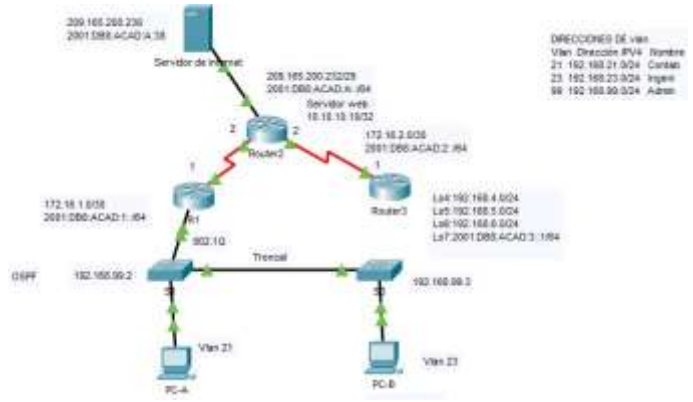


Figura 12. Topologia

RESULTADO

como resultado final del desarrollo del escenario con todos sus comandos se obtiene una buena conexión ya que se comprueba mediante el comando ping en cada uno de los dispositivos de la topología dando con resultado 100% de conectividad, como se muestra en las figuras anterior demostrando así la seguridad de cada uno de los equipos, minimizando las posibles amenazas o ataques producidos por los hackers o ciber delincuentes.

Se logra la comprensión e importancia del direccionamiento y denominación esquemas en varias capas de redes de datos en entornos IPv4 e IPv6 con sus respectivos troncales.

CONCLUCIONES

Se realiza la configuración inicial de los Switchs S1 y S2 y R1 donde se crean contraseñas de seguridad para impedir el acceso a personal ajeno a la red, se crean las vlans y se da sus respectivos nombres, se presenta dificultad en el Subneteo ya que si indica que se toman 10 direcciones para la configuración de la vlan 4.

Se logra la comprensión e importancia del direccionamiento y denominación esquemas en varias capas de redes de datos en entornos IPv4 e IPv6 con sus respectivos troncales.

Gracias al convenio entre la Universidad Nacional Abierta y a Distancia (UNAD) y CISCO se puede medir el conocimiento adquirido a través de cada guía y practica realizada en el packet tracer, a través de los comandos para cada configuración de los protocolos DHCP, NAT, VLAN, NTP, OSPF.

A través de las pruebas de conectividad se puede verificar que los escenarios realizados con los comandos para cada configuración quedaron funcionando, ya que se muestra que sí hay la conectividad requerida.

Referencias

Educación Programas educativos Cisco Networking Academy, recuperado de, https://www.pue.es/pue-academy/cisco-networking-academy#:~:text=Cisco%20Networking%20Academy%20(CNA)%20es,los%20modelos%20online%20m%C3%A1s%20avanzados

Publicado el 30 septiembre, 2014 por erickosvaldovg, recuperado de, https://erickosvaldovg.wordpress.com/2014/09/30/que-es-packet-tracer/

1992-2012 Cisco Systems, Inc. Todos los derechos reservados, recuperado de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10