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

CESAR EMIRO MONTES GUEVARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERIA DE SISTEMAS
COROZAL
2022

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

CESAR EMIRO MONTES GUEVARA

Diplomado como opción de grado para optar el título de Ingeniero de Sistemas

PAOLITA FLOR SALAZAR

Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
COROZAL
2022

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Corozal, 22 de noviembre de 2022

AGRADECIMIENTOS

A Dios que me brinda la oportunidad de perseverar en los objetivos planteados en mi vida, a mi familia que me han apoyado incondicionalmente en este proceso y a mi compañera de vida que me ha dado aliento para no desfallecer ante las dificultades y salir adelante en todo este proceso.

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Subnetting: Definido de la forma más simple, el término subnetting hace referencia a la subdivisión de una red en varias subredes. El Subneteo permite a los

administradores de red, por ejemplo, dividir una red empresarial en varias subredessin hacerlo público en Internet[1]

IPV4: Un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET. Definida en el RFC 791, el IPv4 usa direcciones de 32 bits.[2]

IPv6: Es una actualización al protocolo IPv4, diseñado para resolver el problema deagotamiento de direcciones[3]

PACKET TRACERT: 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[4].

---

[1] Edwards, B. (1997). Cómo dividir en subredes ProxyARP. *Proyecto de documentación de Linux* .

[2] Wu, Peng y col. "Transición de IPv4 a IPv6: una encuesta de vanguardia". *Encuestas y tutoriales de comunicaciones IEEE* 15.3 (2012): 1407-1424.

[3] Loshin, P. (2004). IPv6: teoría, protocolo y práctica.

[4] Barragán Rojas, Diana Jessenia, and Sthepanie Sofía Jurado Solís. "Aplicación del Simulador Packet Tracer para la realización de Prácticas en la Asignatura Telemática I de la Carrera de Ingeniería en Telecomunicaciones." (2012).

ROUTER: Dispositivo de hardware que permite la interconexión de ordenadores enred. Este dispositivo es el encargado de distribuir la conexión a Internet a distintos computadores vinculados a una misma red local actuando como un puente entre nuestros dispositivos y la interne[5]

[5] Leguizamón, G. P., Ortega, B., Capmany, J., & Fajardo, C. S. (2010). Arquitectura y prestaciones de un router de conmutación de paquetes ópticos para las futuras redes de Internet. *Revista Facultad de Ingeniería Universidad de Antioquia*, (55), 144-152.

RESUMEN

En el presente trabajo se muestra el desarrollo de la prueba final de habilidades prácticas de CCNA del diplomado de profundización CISCO como requisito para optar al grado de Ingeniería de Sistemas de la Universidad Nacional Abierta y a Distancia – UNAD. Al desarrollar esta prueba cuyo tema principal era el diseño e implementación de soluciones integradas en redes LAN y WAN, se experimentó el papel que cumple un administrador de red en tareas de configuración e implementación de los diferentes elementos que conformanuna red empresarial y de los recursos a utilizar. Palabras Clave: CISCO, CCNA, Conmutación,Enrutamiento, Redes, sistemas.

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

ABSTRACT

This paper shows the development of the final CCNA practical skills test of the CISCO in depth diploma as a requirement to qualify for the degree in Systems Engineering at the National Open and Distance University - UNAD. When developing this test whose main topic was the design and implementation of integrated solutions in LAN and WAN networks, the role of a network administrator in configuration and implementation tasks of the different elements thatmake up a business network and the resources was experienced to use.

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

INTRODUCCIÓN

En el presente trabajo tiene como objetivo identificar el desarrollo de las herramientas utilizadas están los aplicativos GNS3 o Packet Tracer en los comandos escenarios planteados, a su vez demostraciones en los informes presentados.

En el primer escenario establecerá el desarrollo de las configuraciones de los elementos de una red como lo son equipos, router y switchcon conexiones IPv4 e IPv6 mediante la configuración de enrutamientos DHCP, VLAN y conexos.

En el segundo escenario mediante el uso de conexiones IPv4 e IPv6 con los elementos anteriormente mencionados, se logra la configuración de estos mediante comandos para el uso deprotocolos, seguridad, direcciones dinámicas entre otros.

DESARROLLO DE ESENARIO 1

1.1. Topología

Figura 1 Topología Escenario 1

Fuente: Prueba de habilidades diplomado CCNA

Fuente: AUTOR

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2 Parte 3:Configurar los aspectos básicos de los dispositivos de

la Red propuesta. Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figuray configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en lafigura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo conlos requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 172.XY.3.0 donde XY corresponde a los últimosdos dígitos de su cédula.

Tabla de direccionamiento:

Ítem	Requerimiento
Dirección de Red	172.11.3.0
Requerimiento de host Subred LAN1	60 172.11.3.0/26
Requerimiento de host Subred LAN2	20 172.11.3.64/27
R1 G0/0/1	Última dirección de host de la subred LAN1 172.11.0.62/26
R1 G0/0/0	Última dirección de host de la subred LAN2 172.11.3.158/27

S1 SVI	Segunda dirección de host de la subred LAN1 172.11.3.2/26
PC-A	Décima dirección de host de la subred LAN1 172.11.3.10/26

Parte 3: Configure aspectos básicos.

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos.

Las tareas de configuración para R1 incluyen las siguientes

Tabla 1Direccionamiento Escenario 1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure t Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)# Router(config)#no ip domain-l
	Router(config)#no ip domain-lookup Router(config)#exit Router#
Nombre del router	Router#CONFIGURE Terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)# Router(config)#HOSTNAME R1 R1(config)#exit

Nombre de dominio	ccna-sa.com ccna-sa.com R1#configure t R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)# R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modoEXEC privilegiado	Ciscoenpass ciscoenpass R1#configure t R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#configure t R1(config)#configure ter R1(config)#enable s R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line)#pass 1(config-line)#password ciscoconpass R1(config-line)#exit
Establecer la longitud mínima paralas contraseñas	10 caracteres

Fuente: AUTOR Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** R1(config)#username admin secret admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vtyR1(config)#line R1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1(config)#line vty 0 15 R1(config- line)#login local
	R1(config-line)#transport input sshR1(config-line)#exit
Cifrar las contraseñas de texto nocifrado	R1(config)#service password-encryption
Configurar un banner MOTD	R1(config)#banner motd $R1 CESAR MONTES INGENIERO DE SISTEMAS$ R1(config)#EXIT
Configuración de interfaz G0/0/0	R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 172.11.3.94 255.255.255.224 R1(config-if)#no shutdown

Configuración de interfaz G0/0/1	R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 172.11.3.62 255.255.255.192 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Int erface GigabitEthernet0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed stateto up

Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-key modulus 1024 The name for the keys will be: R1.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 0:22:40.659: %SSH-5-ENABLED: SSH 1.99 has been enabled

Fuente: Autor

- Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 2 Tareas de Configuración de S1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup Switch(config)#exit Switch# %SYS-5-CONFIG_I: Configured from console by console
Nombre del switch	S1 Switch#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname S1 S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console

Nombre de dominio	ccna-sa.com S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass S1(config-line)#password ciscoconpass S1(config-line)#login
Apagar todos los puertos sin usar	F0/1-4, F0/7-24, G0/1-2 S1(config)#int range F0/1-4, F0/7-24, G0/1-2 S1(config-if-range)#sh
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** S1(config)#username admin password admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption

Configurar un banner MOTD	S1(config)#banner motd $S1 CESAR MONTES INGENIERO DE SISTEMAS
Generar una clave de cifrado RSA	Módulo de 1024 bits Módulo de 1024 bits S1(config)#crypto key generate rsa general-keys modulus 1024
	The name for the keys will be: S1.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 0:53:51.226: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config)#
Configure la interfaz de administración (SVI) en VLAN1	S1(config)# interface vlan 1 S1(config-if)#ip address 172.11.3.2 255.255.255.192

Fuente: Autor

Paso 2. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 3 Configuración de Red PC-A

Configuración de red de PC-A	
Descripción	Utilizamos el comando **ipconfig /all** para validar la información.
Dirección física	0001.6332.16DB
Dirección IPv4	172.11.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.11.3.1

Fuente: Autor

Tabla 4 Configuración de Red de PC-B

Configuración de red de PC-B	
Descripción	utilizamos el comando **ipconfig /all** para validar la información
Dirección física	0006.2A34.A34C
Dirección IPv4	172.11.3.74
Máscara de subred	Máscara de subred 255.255.255.224
Puerta de enlace IPv4 predeterminada	172.11.3.129

Fuente: Autor

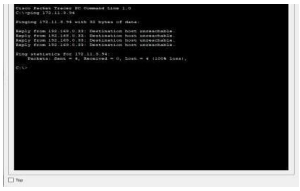
Parte 4: Probar y verificar la conectividad de extremo a extremo

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

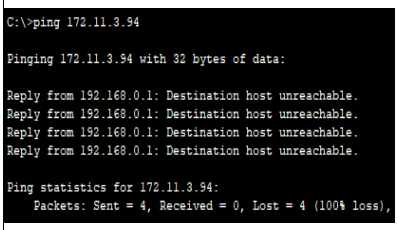
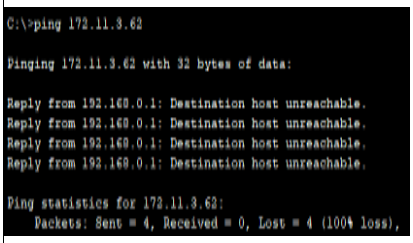
Nota: Si los pings a los servidores fallan, deshabilite temporalmente el firewall del equipo yvuelvaa realizar la verificación.

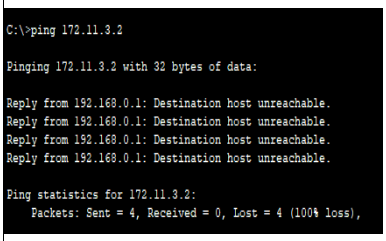
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 5 Probar y verificar conectividad

Desde	**A**	**DirecciónIP**	**Resultados de ping**	
PC-A	R1 G0/0/0	172.11.3.94	*figura 2-7 Prueba de ping PC-A a R1 G0/0/0*  Fuente: Autor	
	R1 G0/0/1		172.11.3.62	*figura 3- 8 Prueba de ping PC-A a R1 G0/0/1*

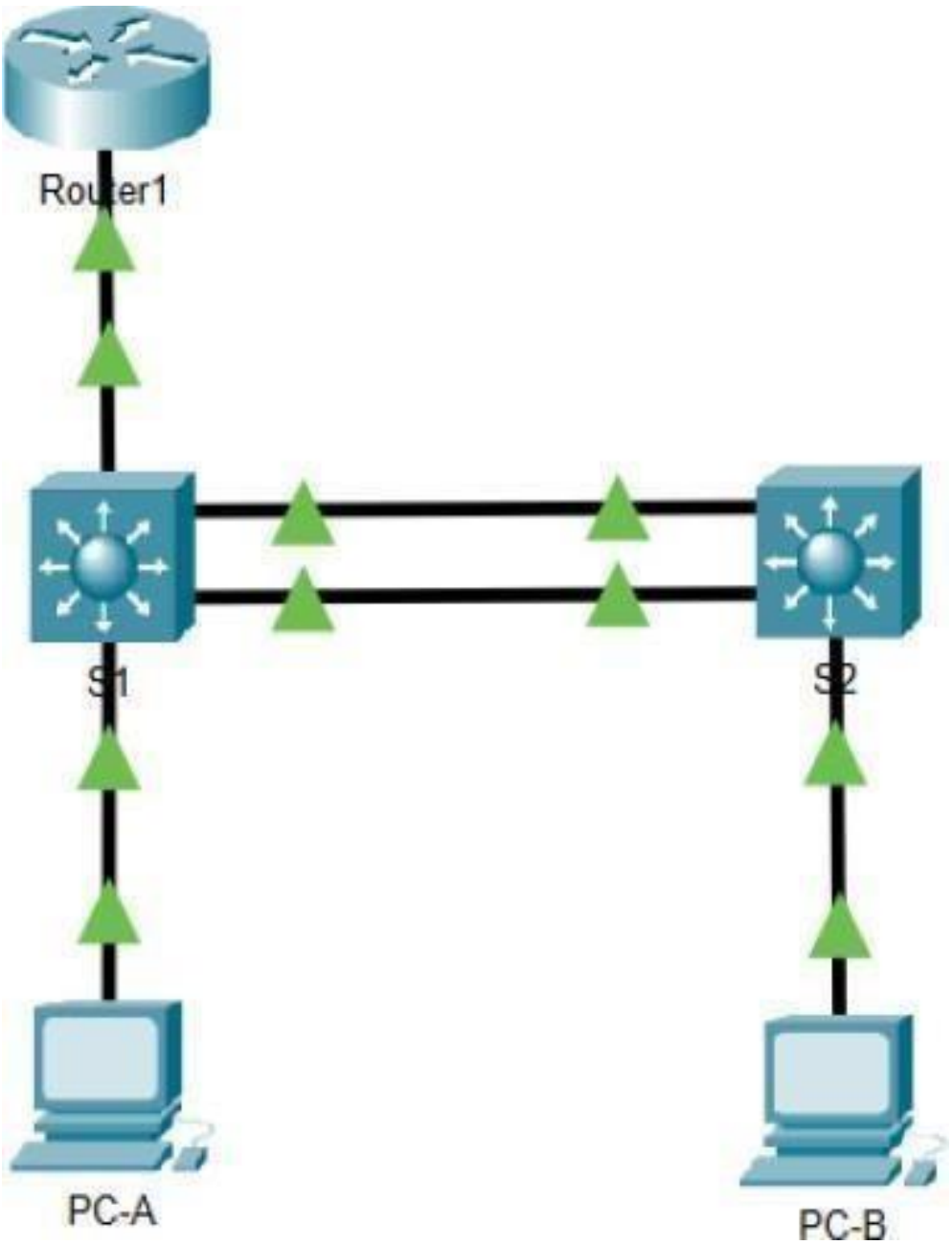
			C:\>ping 172.11.3.2 Pinging 172.11.3.2 with 32 bytes of data: Reply from 192.168.0.33: Destination host unreachable. Reply from 192.168.0.33: Destination host unreachable. Reply from 192.168.0.33: Destination host unreachable. Reply from 192.168.0.33: Destination host unreachable. Ping statistics for 172.11.3.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), Fuente: Autor
	S1 VLAN 1	172.11.3.2	*figura 4-9 Prueba de ping PC-A a S1 VLAN 1* C:\>ping 172.11.3.62 Pinging 172.11.3.62 with 32 bytes of data: Reply from 192.168.0.33: Destination host unreachable. Reply from 192.168.0.33: Destination host unreachable. Reply from 192.168.0.33: Destination host unreachable. Reply from 192.168.0.33: Destination host unreachable. Ping statistics for 172.11.3.62: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> Fuente: Autor
	PC-B	172.11.3.74	*figura 5-10 Prueba de ping PC-A a PC-B* Cisco Packet Tracer PC Command Line 1.0 C:\>ping 172.11.3.74 Pinging 172.11.3.74 with 32 bytes of data: Reply from 192.168.0.1: Destination host unreachable. Reply from 192.168.0.1: Destination host unreachable. Reply from 192.168.0.1: Destination host unreachable. Reply from 192.168.0.1: Destination host unreachable. Ping statistics for 172.11.3.74: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss Fuente: Autor

PC-B	R1 G0/0/0	172.11.3.94	*figura 6-11 Prueba de ping PC-B a R1 G0/0/0*  Fuente: Autor
	R1 G0/0/1	172.11.3.62	*figura 7-12 Prueba de ping de PC-B a R1 G0/0/1*  Fuente: Autor

	S1 VLAN1	172.11.3.2	*figura 8- 13 Prueba de ping de PC-B a S1 VLAN 1*  Fuente: Autor

Fuente: Autor

figura 9 Escenario 2 Ejecutado



Fuente: Autor

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

Tabla 6 VLAN

VLAN	**Nombre de la VLAN**
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

Fuente: Autor

Tabla de asignación de direcciones

NOTA: Tenga en cuenta que para el direccionamiento donde aparezca XY deberáreemplazarlos por los últimos dos dígitos de su número de

identificación.

Tabla 7 Asignación de direcciones

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.11.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.11.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.11.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 40	10.11.8.98 /29	10.11.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde

S2 VLAN 40	10.11.8.99 /29	10.11.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminadaIPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminadaIPv4

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
	2001:db8:acad:b: :50 /64	fe80::1

Fuente. Autor

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos Paso 1:Inicializar y volver a cargar el router y el switch

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargarlosdispositivos.

Router>enable

Router#delete vlan.data

Delete filename [vlan.data]?

Delete flash:/vlan.data? [confirm]

%Error deleting flash:/vlan.data (No such file or directory)

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

Initializing Hardware ...

Switch>enable

Switch#delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload

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: 00E0.A346.5AC5

Xmodem file system is availabl

Después de recargar el switch, configure la plantilla SDM para que admita IPv6según sea necesario y vuelva a cargar el switch

PROCEDIMIENTO

Switch(config)#sdm prefer ?

default Default bias

dual-ipv4-and-ipv6 Support both IPv4 and IPv6

lanbase-routing Lanbase routing

qos Qos bias

Switch(config)#sdm prefer dual-ipv4-and-ipv6 ?

default Default bias

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

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

Switch#reload

Switch>enable

Switch#sh sdm prefer

The current template is "dual-ipv4-and-ipv6 default" template.

The selected template optimizes the resources in

the switch to support this level of features for

0 routed interfaces and 1024 VLAN

Switch>

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8 Configuración R1

Tarea	**Especificación**
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class
Contraseña de acceso a la consola	cisco
Establecer la longitud mínima para las contraseñas	5 caracteres
Crear un usuario administrativo en labase de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneasVTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	

Fuente: Autor

Tabla 9 Cifrar las Contraseña

Tarea	**Especificación**
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.
Habilitar el routing IPv6	
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interfaz	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Autor

AJUSTES BASICOS DEL R 1

Router>enable

Router(config)#no ip domain-lookup

Router (config)#hostname R1

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

R1(config)#enable secret class

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#security password min-length 5

R1(config)#username admin privilege 15 secret admin1pass

R1(config)#line vty 0 4

R1(config-line)#login local

R1(config-line)#transport input ssh

R1(config-line)#exit

R1(config)#service password-encryption

R1#banner motd "R1 – CESAR MONTES - ING DE SISTEMAS"

R1(config-line)#exit

R1(config)#exit

SE AJUSTA LA INTERFAZ Y LA SUBINTERFACES

R1: CESAR MONTES. - ING. DE SISTEMAS

User Access Verification

Password:

```
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0/1
R1(config)#int g0/0/1.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.11.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#int g0/0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.11.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 10.11.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

```
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.56
R1(config-subif)#encapsulation dot1Q 56
R1(config-subif)#exit

R1(config)#int g0/0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#int g0/0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.30, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.40, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.60, changed state to up

SE AJUSTA EL LOOPBACK 0

R1(config)#interface loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#interface loopback 0
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)#exit

PROCEDEMOS AGENERAR UNA CLAVE DE CIFRADO RSA CISCO

R1(config)#crypto key generate rsa general-key modulus 1024

The name for the keys will be: R1.ccna-sa.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 4:16:36.27: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1(config)#

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 10 Tareas de configuración S1 y S2

Tarea	**Especificación**
Desactivar la búsqueda DNS.	
Nombre del switch	S1 o S2, según proceda
Nombre de dominio	ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class

Contraseña de acceso a la consola	cisco
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass**

Fuente: Autor

Tabla 11 S1 Y S2

Tarea	**Especificación**
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	
Configurar las líneas VTY para que acepten únicamentelas conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académicoal que pertenece.
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1y FE80: :99 para S2** Establecer la dirección IPv6 de capa3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.11.8.97 para IPv4

Fuente. Autor

- **SE PROCEDE A LOS AJUSTES BÁSICOS DEL S1**

- Switch>en
- Switch#conf t
- Enter configuration commands, one per line. End with CNTL/Z.
- Switch(config)#no ip domain-lookup
- Switch(config)#hostname S1
- S1(config)#ip domain-name ccna-sa.com
- S1(config)#enable secret class
- S1(config)#line console 0
- S1(config-line)#password cisco
- S1(config-line)#login
- S1(config-line)#exit
- S1(config)#username admin privilege 15 secret admin1pass
- S1(config)#line vty 0 4
- S1(config-line)#login local
- S1(config-line)#transport input ssh
- S1(config-line)#exit
- S1(config)#service password-encryption
- S1(config)#banner motd "S1: CESAR MONTES. - ING DE SISTEMAS"
- S1(config)#crypto key generate rsa general-key modulus 1024
- The name for the keys will be: S1.ccna-sa.com
- % The key modulus size is 1024 bits
- % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
- *Mar 1 3:26:51.957: %SSH-5-ENABLED: SSH 1.99 has been enabled

- S1(config)#

- **SE PROCEDE A LOS AJUSTES BÁSICOS DEL 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-sa.com

S2(config)#enable secret class

S2(config)#line console 0

S2(config-line)#password cisco

S2(config-line)#login

S2(config-line)#exit

S2(config)#username admin privilege 15 secret admin1pass

S2(config)#line vty 0 4

S2(config-line)#login local

S2(config-line)#transport input ssh

S2(config-line)#exit

S2(config)#service password-encryption

S2(config)#banner motd "S2: CESAR MONTES. - ING DE SISTEMAS"

S2(config)#crypto key generate rsa general-key modulus 1024

The name for the keys will be: S2.ccna-sa.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 3:16:5.411: %SSH-5-ENABLED: SSH 1.99 has been enabled

S2(config)#

- **SE PROCEDE A LOS AJUSTES DE VLAN 40 EN S1**
- S1: CESAR MONTES. - ING DE SISTEMAS
- User Access Verification
- Password:
- S1>enable
- Password:
- S1#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- S1(config)#interface vlan 40
- S1(config-if)#ip address 10.11.8.98 255.255.255.248
- S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
- S1(config-if)#ipv6 address fe80::98 link-local
- S1(config-if)#exit
- S1(config)#ip default-gateway 10.11.8.97
- S1(config)# no shutdown
- **SE PROCEDE A LOS AJUSTES DE VLAN 40 EN S2**

- S2: CESAR MONTES. - ING DE SISTEMA
- User Access Verificatio
- Password:
- S2>enable
- Password:
- S2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- S2(config)#ipv6 unicast-routing
- S2(config)#interface vlan 40
- S2(config-if)#ip address 10.11.8.99 255.255.255.248
- S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
- S2(config-if)#ipv6 address fe80::99 link-local
- S2(config-if)#exit
- S2(config)#ip default-gateway 10.11.8.97
- S2(config)#no shutdown
-

  Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)Paso 4: Configurar S1

  La configuración del S1 incluye las siguientes tareas:

Tabla 12 Configuración de la Infraestructura de Red VLAN

Tarea	**Especificación**
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native

Tarea	**Especificación**
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interfaz F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo deacceso, agregar una descripción y apagar

Fuente.: Autor

- **SE PROCEDE A DAR NOMBRE DE LAS VLAN S1**
- S1: CESAR MONTES. - ING DE SISTEMAS
-
- User Access Verification
-
- Password:
-
- S1>enable
- Password:
- Password:
- S1#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.

- S1(config)#vlan 20
- S1(config-vlan)#name Docentes
- S1(config-vlan)#exit
- S1(config)#vlan 30
- S1(config-vlan)#name Estudiantes
- S1(config-vlan)#exit
- S1(config)#vlan 40
- S1(config-vlan)#name Invitados
- S1(config-vlan)#exit
- S1(config)#vlan 50
- S1(config-vlan)#name Usuarios
- S1(config-vlan)#exit
- S1(config)#vlan 56
- S1(config-vlan)#name Native
- S1(config-vlan)#exit
- S1(config)#exit
-

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
20   Docentes                          active
30   Estudiantes                       active
40   Invitados                         active
50   Usuarios                          active
56   Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

- **PROCEDEMOS A LA CONFIGURACION “TRUNK” 802.1Q QUE UTILICE LA VLAN 56NATIVE**
- S1#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- S1(config)#int f0/1
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk native vlan 56
- S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
-
- S1(config)#int f0/2
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk native vlan 56
- S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56

-
- S1(config)#int f0/5
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk native vlan 56
- S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56

- **SE COMPRUEBA LA CONFIGURACION Y USO DE VLAN 6 “NATIVE”**

S1#show interface f0/1 switchport

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 56 (Native)

Voice VLAN: none

S1#show interface f0/2 switchport

Name: Fa0/2

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 56 (Native)

Voice VLAN: none

S1#show interface f0/5 switchport

Name: Fa0/5

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 56 (Native)

Voice VLAN: none

- **SE PROCEDE A CREAR UN GRUPO DE PUERTOS ETHERCHANNEL DE LA CAPA 2 QUEUSE INTERFACES F0/1 Y F0/2**

- S1(config)#int range f0/1-2
- S1(config-if-range)#channel-group 1 mode active
- S1(config-if-range)#
- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
-
- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
-
- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
-
- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
-
- S1(config-if-range)#exit
- S1(config)#int port-channel 1
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
- S1(config-if)#exit

CONFIGURAR EL PUERTO DE ACCESO DE HOST PARA VLAN 2

S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56

S1(config-if)#exit

S1(config)#int f0/6

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#exit

S1(config)#exit

S1#

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
20   Docentes                         active    Fa0/6
30   Estudiantes                      active
40   Invitados                        active
50   Usuarios                         active
56   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

CONFIGURAR LA SEGURIDAD DEL PUERTO EN LOS PUERTOS DE ACCESO

S1(config)#int f0/6

S1(config-if)#switchport mode access

S1(config-if)#switchport port-security maximum 4

S1(config-if)#switchport port-security violation shutdown

S1(config-if)#switchport port-security mac-address sticky

S1(config-if)#exit

S1(config)#exit

PROTEJA TODAS LAS INTERFACES NO UTILIZADAS

```
S1(config)#interface range g0/1-2, f0/3-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#shutdown
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#exi
```

- **Paso 5: Configure el S2.**

Tabla 13 Configuraciones S2

Entre las tareas de configuración de S2 se incluyen las siguientes: Tarea	**Especificación**
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18

Tarea	**Especificación**
Configure port-security en los access ports	permite 4 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar

Fuente: Autor

- **SE HACE UNA CREACION DE LOS NOMBRES DE LAS VLAN S2**

  S1: CESAR MONTES. - ING DE SISTEMAS

  User Access Verification

  Password:

  S2>enable
  Password:
  S2#configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.

```
S2(config)#vlan 20
S2(config-vlan)#name Docentes
S2(config-vlan)#exit
S2(config)#vlan 30
S2(config-vlan)#name Estudiantes
S2(config-vlan)#exit
S2(config)#vlan 40
S2(config-vlan)#name Invitados
S2(config-vlan)#exit
S2(config)#vlan 50
S2(config-vlan)#name Usuarios
S2(config-vlan)#exit
S2(config)#vlan 56
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#exit
```

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
20   Docentes                          active
30   Estudiantes                       active
40   Invitados                         active
50   Usuarios                          active
56   Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#
```

- **SE CONFIGURA TRUNK 802.1Q QUE SE UTILICE VLAN 56 NATIVE**

  S2(config)#int f0/1

  S2(config-if)#switchport mode trunk

  S2(config-if)#switchport trunk native vlan 56

  S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56

  S2(config-if)#exit

  S2(config)#int f0/2

  S2(config-if)#switchport mode trunk

  S2(config-if)#switchport trunk native vlan 56

  S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56

  S2(config-if)#exit

- **PROCEDEMOS A COMPROBAR LA CONFIGURACION Y EL USO DE VLAN 56 NATIVE**

S2#show interface f0/1 switchport

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 56 (Native)

Voice VLAN: none

S2#show interface f0/2 switchport

Name: Fa0/2

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 56 (Native)

Voice VLAN: none

- **PROCEDEMOS A CREAR UN GRUPO DE PUERTOS ETHERCHANNEL DE LA CAPA 2 QUESE USE 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)#channel-group 1 mode active

S2(config-if-range)#

Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

S2(config-if-range)#exit
S2(config)#interface port-channel 1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S2(config-if)#exit
S2(config)#exit

- **PROCEDEMOS A CONFIGURAR EL PUERTO DE ACCESO DE HOST PARA VLAN 30**

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#exit
S2(config)#exit

```
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
20   Docentes                          active
30   Estudiantes                       active    Fa0/18
40   Invitados                         active
50   Usuarios                          active
56   Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- **VAMOS A CONFIGURAR LA SEGURIDAD DEL PUERTO EN LOS PUERTOS DE ACCESO**

  S2#conf t

  Enter configuration commands, one per line. End with CNTL/Z.

  S2(config)#int f0/18

  S2(config-if)#switchport mode access

  S2(config-if)#switchport port-security

  S2(config-if)#switchport port-security maximum 4

  S2(config-if)#switchport port-security violation shutdown

  S2(config-if)#switchport port-security mac-address sticky

  S2(config-if)#exit

  S2(config)

- **PROCEDEMOS A PROTEGER TODAS LAS INTERFASES NO UTILIZADAS**

S2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)#interface range g0/1-2, f0/3-17, f0/19-24

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

S2(config-if-range)#switchport access vlan 50

S2(config-if-range)#shutdown

S2(config-if-range)#switchport port-security

S2(config-if-range)#switchport port-security violation shutdown

S2(config-if-range)#exit

S2(config)#exit

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14 Configuración Soporte de HOST

Tarea	**Especificación**
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 quedirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y

VLAN 2	especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por lasúltimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del routerpara la subred involucrada

Fuente: Autor

- **PROCEDEMOS ALA CONFIGURACION IPV4 DHCP PARA VLAN 20**

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp pool vlan20

R1(dhcp-config)#network 10.11.8.0 255.255.255.192

R1(dhcp-config)#default-router 10.11.8.1

R1(dhcp-config)#domain-name ccna-sa.net

R1(dhcp-config)#ip dhcp excluded-address 10.11.8.2 10.11.8.51

R1(config)#

- **SE PROCEDE A CONFIGURAR IPV4 DHCP PARA VLAN 30**

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp pool vlan30

R1(dhcp-config)#network 10.11.8.64 255.255.255.224

R1(dhcp-config)#default-router 10.11.8.65

R1(dhcp-config)#domain-name ccna-sb.net

R1(dhcp-config)#ip dhcp excluded-address 10.11.8.66 10.11.8.83

R1(config)#exit

Paso 2: Configurar los servidores

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

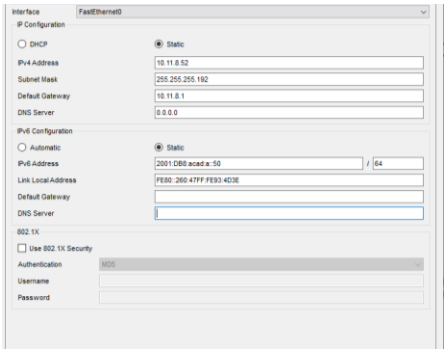
Tabla 15 Configuraciones de Servidores

Configuración de red de PC-A	
Descripción	
Dirección física	

Configuración de red de PC-A	
Dirección IP	
Máscara de subred	
Gateway predeterminado	
Gateway predeterminado IPv6	

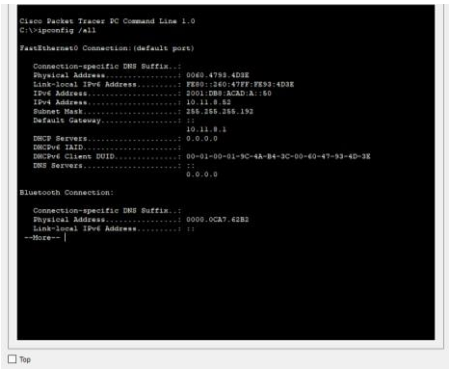
Fuente: Autor

figura 10 configuración en PC-A



Fuente: Autor

figura 11 Comando PING en PC-A



Fuente: Autor

Tabla 16 Configuraciones de Red PC-B

Configuración de red de PC-B	
Descripción	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway predeterminado	
Gateway predeterminado IPv6	

Fuente: Autor

figura 12 configuración de Red PC-B

Fuente: autor

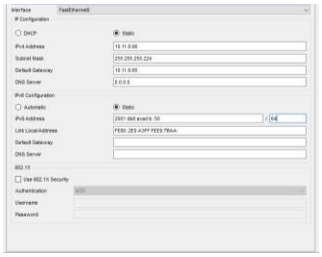
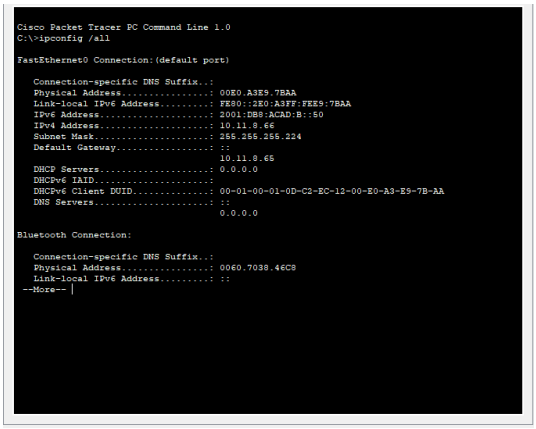


figura 13 Comando PING en PC-B



Fuente: Autor

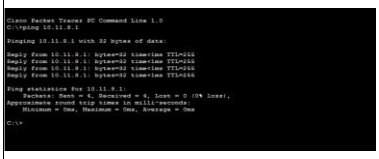
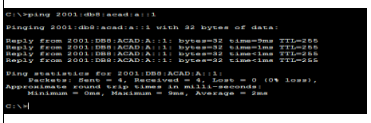
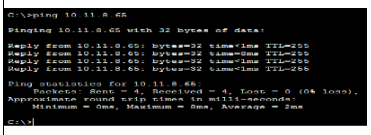
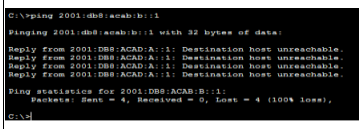
PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

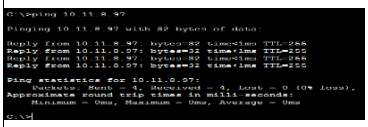
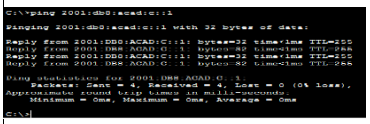
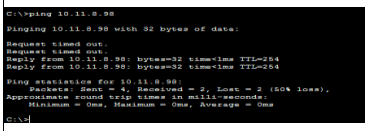
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos losdispositivos de red.

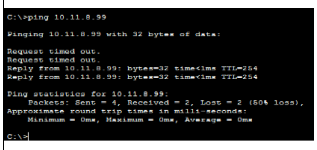
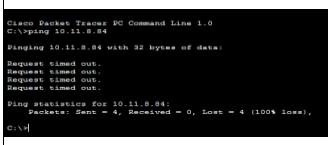
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

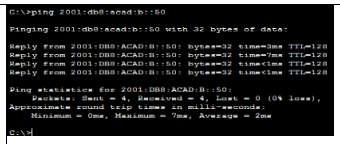
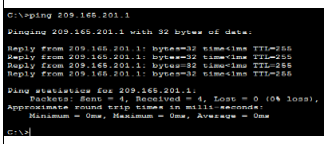
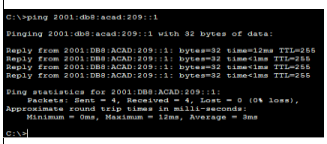
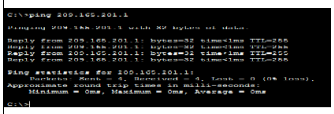
Tabla 17 Probar y Verificar la Conectividad de Extremo a Extremo

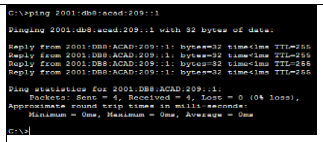
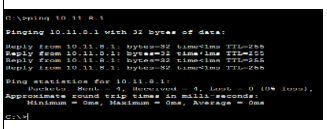
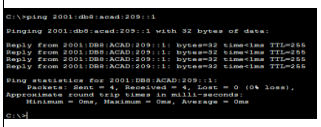
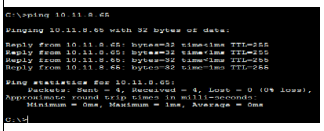
Desde	**A**		**Dirección IP**	**Resultados de ping**

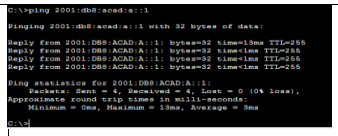
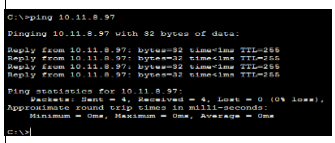
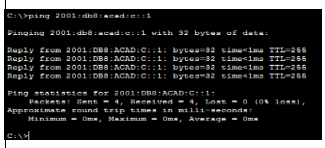
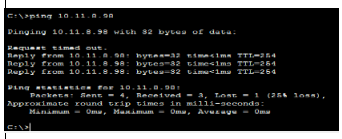
PC-A	R1, G0/0/1.2	IPv4	10.11.8.1	*figura 14 ping R1 G0/0/1.2 PC-A 10.11.8.1*  Fuente: Autor
		IPv6	2001:db8:acad:a::1	*figura 15 ping R1 G0/0/1.2 PC-A IPV 6 2001*  Fuente: Autor
	R1, G0/0/1.3	IPv4	10.11.8.65	*figura 16 ping R1 G0/0/1.3 IPV4 PC-A 10.11.8.65*  Fuente: Autor
		IPv6	2001:db8:acad:b::1	*figura 17ping R1 GO/0/1.3 IPV6 PC-A 2001*  Fuente: Autor

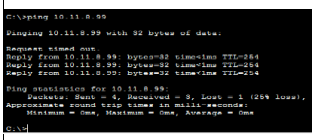
R1, G0/0/1.4	IPv4	10.11.8.97	*figura 18 ping R1 G0/0/1.4 IPV4 PC-A 10.11.8.97*  Fuente: Autor
	IPv6	2001:db8:acad:c::1	*figura 19 ping R1 G0/0/1.4 IPV6 PC-A 2001*  Fuente: Autor
S1, VLAN 4	IPv4	10.11.8.98	*figura 20 ping S1 VLAN4 IPV4 PC-A 10.11.8.98*  Fuente: Autor
	IPv6	2001:db8:acad:c::98	*figura 21 ping S1 VLAN6 IPV6 PC-A 2001*  Fuente: Autor

Desde	**A**		**Dirección IP**	**Resultados de ping**
	S2, VLAN 4	IPv4	10.11.8.99	*figura 22 ping S2 VLAN4 IPV4 PC-A 10.11.8.99*  Fuente: Autor
		IPv6	2001:db8:acad:c::99	*figura 23 ping S2 VLAN4 IPV6 PC-A 2001*  Fuente: Autor
	PC-B	IPv4	10.11.8.84	*figura 24 ping PC-A a PCB IPV4 10.11.8.84*  Fuente: Autor
		IPv6	2001:db8:acad:b::50	*figura 25 ping PC-A a PC-B IPV6 2001*

				 Fuente: Autor
	R1 Bucle 0	IPv4	209.165.201.1	*figura 26 ping PC-A R1 Bucle 0 IPV4 209.165.201.1*  Fuente: Auto
		IPv6	2001:db8:acad:209::1	*figura 27 ping PC-A R1 Bucle 0 ipv6 2001*  Fuente: Autor
PC-B	R1 Bucle 0	IPv4	209.165.201.1	*figura 28 ping PC-BR1 Bucle 0 IPV4 209.165.201*  FUENTE: Autor
		IPv6	2001:db8:acad:209::1	*figura 29 ping PC-B R1 Bucle 0 IPV6 2001*

				 Fuente: Autor
	R1, G0/0/1.2	IPv4	10.11.8.1	*figura 30 ping PC-B R1 G0/0/1.2 IPV4 10.11.8.1*  Fuente: Autor
		IPv6	2001:db8:acad:209::1	*figura 31 ping PC-B R1 G0/0/1.2 IPV6 2001*  Fuente: Autor
	R1, G0/0/1.3	IPv4	10.11.8.65	*figura 32 ping PC-B R1 G0/0/1.3 IPV4 10.11.8.65*  Fuente: Autor
		IPv6	2001:db8:acad:a::1	*figura 33 ping PC-B R1, G0/0/1.3 IPV6 2001*

				 Fuente: Autor
	R1, G0/0/1.4	IPv4	10.11.8.97	*figura 34 ping PC-B R1, G0/0/1.4 IPV4 10.11.8.97*  Fuente: Autor
		IPv6	2001:db8:acad:c::1	*figura 35 ping PC-B R1, G0/0/1.4 IPV6 2001*  Fuente: Autor
	S1, VLAN 4	IPv4	10.11.8.98	*figura 36 ping PC-B S1 VLAN4 IPV4 10.11.8.98*  Fuente: Autor

		IPv6	2001:db8:acad:c::98	*figura 37 ping PC-B S1 VLAN6 2001*  Fuente: Autor
	S2, VLAN 4	IPv4	10.11.8.99	*figura 38 ping PC-B S2 VLAN4 IPV4 10.11.8.99*  Fuente: Autor
		IPv6	2001:db8:acad:c::99	*figura 39 ping PC-B S2 VLAN4 IPV6 2001*  Fuente: Autor

Fuente: Autor

CONCLUSION

Se logró realizar las simulaciones a través de laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN, permitiendo realizar un análisis sobreel comportamiento de diversos protocolos y métricas de enrutamiento.

La herramienta virtual Packet Tracer permitió la viabilidad del desarrollo del presente proyecto, siendo de una herramienta de gran importancia que, con su utilización puesta en marcha en toda la estructura, este programa puede funcionar y se programar este tipo de redes, facilitando tanto el diseño como enrecursos económicos, ya que no se tiene que empezar a realizar la red sin tenerdatos virtuales, permitiendo la versatilidad de la programación en eficacia y rendimiento.

Lográndose establecer la implementación conocimientos básicos de principio a fin, se puede avanzar en las diferentes configuraciones a lo largo del curso, cumpliendo con los objetivos exigidos en cada escenario presentado, no solo en la configuración de comandos y en la ejecución de estos, a su vez que cada uno de ellos se pueda integrar para el correcto funcionamiento y rendimiento de manera simbiótica en las diferentes configuraciones se vaya a emplear.

REFERENCIAS BIBLIOGRAFICAS

]AUCAPEÑA Macias, C. C. (2015). Diseño y simulación de una red que implemente enrutamiento estático para el protocolo de internet versión 4 y6. (22 de noviembre del 2022)

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco. (22 de noviembre del 2022)

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. .(22 de noviembre del 2022)

BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W.,Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónicocon características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, *16*(1), 75-84. (22 de noviembre del 2022)

.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham. (22 de noviembre del 2022)

.

GARIMELLA, P., Sung, Y. W. E., Zhang, N., & Rao, S. (2007, August). Characterizing VLAN usage in an operational network. In *Proceedings of the 2007SIGCOMM workshop on Internet network management* (pp. 305-306). (22 de noviembre del 2022)

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad. (22 de noviembre del 2022)

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, *14*(1), 127-138. (22 de noviembre del 2022)

IN *2017 Congreso Internacional de Innovacion y Tendencias en Ingeniería (CONIITI)* (pp. 1-5). IEEE.*International Journal of Computer Science Issues (IJCSI)*, *9*(3), 314.IPv6. *Inge Cuc*, *12*(1), 86-93. (22 de noviembre del 2022)

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Foundin Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-6). IEEAli, A. N. A. (2012). Comparison study between IPV4 & IPV6. (22 de noviembre del 2022)

ANEXOS

Anexo A - Enlace de descarga de las simulaciones de los escenarios:

https://drive.google.com/file/d/19fB1lhK-izziSpXAVqRK4HlnkGxTAG59/view?usp=sharing