

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

PEDRO LUIS DUQUE SALAZAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA-ECBTI
INGENIERIA DE SISTEMAS
POPAYAN
2022

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

PEDRO LUIS DUQUE SALAZAR

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

PAULITA SALAZAR

Directora de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA-ECBTI
INGENIERIA DE SISTEMAS

POPAYAN

2022

2

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

POPAYAN, 7 de diciembre de 2022

DEDICATORIA

Esta dedicatoria tan especial primero Que todo darle la gloria a DIOS, Quien sabe con tanto esfuerzo he podido realizar la carrera, a mi familia padres y mi esposa, pero principalmente a mi hija María Antonia Duque, que gracias a ella soy lo que soy y es mi motor para que día a día sea una mejor persona y pueda darle una vida digna.

AGRADECIMIENTOS

Inicialmente darle las gracias a Dios por permitirnos realizar lo que deseamos día tras día, a nuestra querida tutora paulita Salazar por cada una de las recomendaciones y sugerencias y correcciones de cada uno de los puntos y actividades planteadas durante el transcurso del diplomado, a mi familia que siempre han estado en los momentos duros de mi vida y a mi esposa Diana Lucia, y a mi hija amada María Antonia por ser los motores y las fuerzas que me dan para salir adelante y construir un mejor país.

A los compañeros de curso y los directores de centro que siempre han brindado todas las herramientas necesarias para poder concluir y finalizar la carrera y convertir profesionales de verdad.

CONTENIDO

| | |
|---|----|
| Resumen..... | 11 |
| Introducción | 15 |
| Desarrollo De Escenarios | 16 |
| Las Tareas De Configuración De S1 Incluyen Lo Siguiete..... | 21 |
| Configurar Los Equipos..... | 23 |
| Probar Y Verificar La Conectividad De Extremo A Extremo | 25 |
| Desarrollo Escenario 2 | 28 |
| Inicializar Y Recargar Y Configurar Aspectos Básicos De Los Dispositivos..... | 31 |
| Configure S1 Y S2 | 37 |
| Configuración De Infraestructura De Red (Vlan,Trunking, Etherchannel) | 42 |
| Configure El S2 | 45 |
| Configurar Soporte De Host | 48 |
| Configure R1 | 48 |
| Configurar Los Servidores..... | 50 |
| Conclusiones | 63 |
| Bibliografía..... | 63 |

Anexos 65

TABLA DE TABLAS

| | |
|---|----|
| Tabla 1. Direccionamiento Escenario 1 | 15 |
| Tabla 2. Configuración router R1 | 17 |
| Tabla 3. Configuración switch S1 | 19 |
| Tabla 4. Configuración ipv4 PC-A | 22 |
| Tabla 5. Configuración ipv4 PC-B | 22 |
| Tabla 6. Verificación de conectividad dispositivos de red | 23 |
| Tabla.7 nombre de las VLAN | 27 |
| Tabla 8. Tabla de asignación de direcciones | 28 |
| Tabla 9. Configuración router R1 | 29 |
| Tabla 10. Configuración Switch S1 y S2 | 34 |
| Tabla 11. Configuración S1 | 38 |
| Tabla 12. Configuración S2 | 41 |
| Tabla 13. Configuración router R1 | 43 |
| Tabla 14. Configuración de red de PC-A | 46 |
| Tabla 15. Configuración de PC-B | 46 |
| Tabla 16. Probar y verificar la conectividad de extremo a extremo | 47 |

LISTA DE FIGURAS

| | |
|---|----|
| Figura 1 Topología de escenario 1 | 15 |
| Figura 2 Realización de Autor Escenario n1 | 17 |
| Figura 3. Configuración del PC-1 | 24 |
| Figura 4. Configuración del PC-2..... | 24 |
| Figura 5. Ping R1 G0/0/0 172.46.3.1 | 25 |
| Figura 6. Ping R1 G0/0/1 172.46.3.75..... | 25 |
| Figura .7. Ping S1 VLAN 1 172.46.3.2..... | 26 |
| Figura 8. Ping Desde el pc1 al pc2 172.46.3.75..... | 26 |
| Figura 9. Ping R1 G0/0/0172.46.3.1 | 26 |
| Figura 10 Ping R1 G0/0/1 172.46.3.75..... | 26 |
| Figura 11. Ping S1 VLAN1172.46.3.2 | 27 |
| Figura 12. Ping PC 1 A PC2 172.46.3.10..... | 28 |
| Figura 13. Topología Escenario 2..... | 29 |
| Figura 14. Simulador Packet Tracer Escenario 2 | 29 |
| Figura 15. Ping R1, G0/0/1.20 10.46.8.1 | 56 |
| Figura 16.Ping ipv6 E80::200:CFF:FE3A:1E39.Ping..... | 56 |
| Figura 17. Ping R1, G0/0/1.3010.46.8.65..... -- | 56 |
| Figura 18. Ping ipv6 2001:DB8:ACAD:B::1/64 | 57 |
| Figura 19. Ping R1, G0/0/1.40 10.46.8.97 | 57 |
| Figura 20.Ping Ipv6 2001:DB8:ACAD:C::1 | 57 |
| Figura 21. Ping SV1 VLAN 40 10.46.8.98 | 58 |
| Figura 22. Ping ipv6 2001:DB8:ACAD:209::1 | 58 |
| Figura 23. Ping 10.46.8.99 | 58 |
| Figura 24. Ping ipv6 2001:DB8:ACAD:C::1 | 59 |
| Figura 25. Ping 10.46.8.65..... | 59 |
| Figura 26. Ping 2001:db8:acad:b: :1 | 59 |
| Figura 27. Ping ipv6 209.165.201.1..... | 60 |
| Figura 28 Ping ipv6 2001:db8:acad:209: :1 | 60 |

| | |
|--|----|
| Figura 29. Ping bucle.209.165.201.1..... | 60 |
| Figura 30. Ping ipv6 2001:db8:acad:209: :1 | 61 |
| Figura 31. Ping R1. G0/0/1.20 10.46.8.1 | 61 |
| Figura 32. Ping 2001:db8:acad:a::1 | 61 |
| Figura 33. Ping R1G0/0/1.30 10.46.8.65..... | 62 |
| Figura 34. Ping 2001:db8:acad:b::1 | 63 |
| Figura 35. Ping R1G0/0/1.40 10.46.8.97..... | 63 |
| Figura 36. Ping ipv6 2001:db8:acad:c::1 | 63 |
| Figura 37. Ping R1G0/0/1.40 10.46.8.98..... | 64 |
| Figura 38. Ping ipv6 2001:db8:acad:c::98 | 64 |
| Figura 39 Ping SV2 VLAN 40. 10.46.8.98..... | 65 |

RESUMEN

En el primer escenario vamos a identificar y a desarrollar una conectividad básica en una red local, mediante la distribución inicial de conectores y terminales. Con su referente control de seguridad para el acceso al router y los switches, el tipo de cableado que se utilizara, su configuración de direccionamiento IPv4 y configuración de redes LAN, a través de la simulación de escenarios gracias a la herramienta Packet Tracer, nos va a ejecutar la simulación para poder tener un conocimiento más profundo de una conectividad local.

El segundo realizaremos una configuración de dispositivos de una red mediana, donde se tendremos la configuración de un router el cual nos permite crear unas rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, se configuraran dos switches y dos equipos que admitan tanto la conectividad IPv4 también donde se crea un grupo DHCP para VLAN, como IPv6 para los hosts soportados. El router y los switches también deben dirigir de forma segura. Construirá el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Palabras claves: Enrutamiento, VLAN, DHCP, Etherchannel y port-security, LAN, configuración.

ABSTRACT

At present we can understand the importance of telecommunications systems, computer networks as a basis to be a good systems engineer in the future, are the fundamental bases to obtain good practices in performance within a company or organization. When we get to know Packet Tracer, we go into depth about how each of the terminologies seen throughout the academic period of the open and distance university works, and the accompaniment is essential by the course director, the resolution of connectivity problems and the real tests that is generated in the simulator leads us to have an awareness of how most companies work at a general level.

In this report, the knowledge acquired during the CISCO CCNA Deepening Diploma course will be demonstrated in a practical way, applying the skills and competencies acquired throughout it. The devices will be configured in each of the scenarios and at the end it will be verified if the implemented configurations were properly applied and that the networks work correctly.

The simulator applied for the development of the two scenarios is the CISCO proprietary application called Packet Tracer that allows the basic configurations of switches and routers. In addition, the configuration of interoperability of IPv4 and IPv6 protocols, routing protocols, security, application of virtual networks VLANs, dynamic addressing, establishment of access control lists and translation of NAT network addresses. In this way, the consolidation of this work allows us to organize the acquisition of knowledge, skills and abilities in the design and implementation of computer networks that allow the processing, interoperability, secure access, command and control and information management.

Keywords: command, IPV6, NAT, Cisco, Network, applied, information.

GLOSARIO

Dirección IP: son un conjunto de números con los cuales se identifica de manera lógica y jerárquica los equipos que están conectados en una red de datos.

Router: en ingles router que traducido seria encaminador, es un dispositivo de red sirve para interconectar computadoras que funcionan en una red, estableciendo la ruta para conectarse con otra de y poder enviar paquetes de datos.

Switch: que traducido al español es interruptor, conmutador es un dispositivo que permite interconectar equipos en una red de datos, trabaja en la capa de enlace de datos y permite interconectar dos o más equipos de una red permitiendo pasar datos de un segmento a otro.

VLAN1: es una interfaz que se usa en el switch, la cual es nativa del switch, y a la que se le asigna una dirección ip para poder administrar el dispositivo remotamente IPv4: (Protocolo de Internet versión 4), el cual está formado de 32 bits separados en cuatro octetos que son cada uno compuestos de 8 bits, y que se usa en una notación decimal separados por puntos. IPv6: es una actualización del protocolo IPv4, este tiene un tamaño de 128 bits el cual se separa en ocho campos de 16 bits, separado por dos puntos.

SDM: Viene de las siglas (Switching Database Manager), son plantillas de Cisco, con las cuales se puede configurar los switches para poder sacarles el mayor rendimiento, en función de lo que vayan a trabajar OSPF: De la sigla en inglés Open Shortest Path First que traducen abrir el camino más corto primero, es un protocolo de red para realizar encaminamiento jerárquico de pasarela interior o Interior Gateway.

NAT: el cual significa traducción de direcciones de red y se conoce como enmascaramiento de ip, se usa en los routers para conservar direcciones IP, logrando que se conecten a Internet las redes de con ip privada.

NTP: de las siglas en ingles Network Time Protocol, es un protocolo de Internet que se usa para sincronizar los relojes o horas de los dispositivos que componen la red por medio del enrutamiento de paquetes en redes con latencia variable

DHCP: de las siglas en ingles Dynamic Host Configuration Protocol, es un protocolo que sirve para poder asignar ip a los equipos automáticamente. 10 ACL: de las siglas en ingles access control list, el cual consiste en controlar el flujo del tráfico en equipos de redes filtrando el tráfico para permitir o denegar el tráfico de red de acuerdo a alguna condición o listas creadas.

HTTP: que traduce protocolo de transferencia de hipertexto, el cual es un protocolo de comunicaciones que permite las transferencias de información en la World Wide Web o internet. Router-on-a-Stick: Consiste en crear interfaces virtuales sobre un puerto físico del router para que atreves de cada interfaz se pueda se pueda transmitir información de una vlan, cuando no se usa Router-on-a-Stick es necesario que por cada vlan se use un puerto físico, esto es un inconveniente pues los router no tiene muchas interfaces. Enlace troncal o trunk: es la configuración que se le realiza a una interfaz ya sea de un switches o un router para que por este se pueda enviar y recibir el tráfico de las distintas VLANs que se han configurado,

Dot1q: es un protocolo esencial que le da vida a los enlaces que se han configurado como troncal o trunk y pertenece al estándar IEEE 802.1Q. Vlan

Nativa: es una Vlan que se configura para transportar tráfico sin etiquetar o tráfico que no se encapsula 802.1Q, el número de la vlan nativa deber ser igual en ambos extremos de la conexión de los switches o router. EtherChannel: es una tecnología con estándares 802.3 que permite full-dúplex Fast Ethernet, y con el cual se puede agrupar lógicamente varias interfaces físicas que son tratadas como un único enlace sumando la velocidad nominal de cada puerto físico y enlace troncal de alta velocidad, también sirve como una conexión de respaldo.

Ref

(<https://ccnadesdecero.es/glosario/>, 2015)

INTRODUCCIÓN

En la actualidad podemos entender la importancia de los sistemas de telecomunicaciones, las redes informáticas como base para ser un buen ingeniero de sistemas en el futuro, son las bases fundamentales para obtener unas buenas prácticas en el desempeño dentro de una compañía u organización. Cuando conocemos Packet Tracer entramos en profundidad como funciona cada uno de las terminologías vistas durante todo el periodo académico de la universidad abierta y a distancia, y el acompañamiento es fundamental por parte del director de curso, la resolución de problemas de conectividad y las pruebas reales que se generan en el simulador nos llevan a tener una conciencia de cómo funcionan la mayoría de las empresas a nivel general.

En el presente informe se demostrará de forma práctica los conocimientos adquiridos durante el curso Diplomado de Profundización CCNA de CISCO aplicando las habilidades y competencias adquiridas a lo largo de este. Se configurarán los dispositivos en cada uno de los escenarios y al final se verificarán si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente.

El simulador aplicado para el desarrollo de los dos escenarios es la aplicación propietaria de CISCO denominado Packet Tracer que permite las configuraciones básicas de switches y router. Además, la configuración de interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, seguridad, aplicación de redes virtuales VLAN, direccionamiento dinámico, establecimiento de listas de control de acceso y traducción de direcciones de red NAT. De esta manera, la consolidación de este trabajo nos permite organizar la adquisición de conocimientos, habilidades y destrezas en el diseño e implementación de redes informáticas que permiten el procesamiento, interoperabilidad, acceso seguro, comando y control y gestión de la información.

DESARROLLO DE ESCENARIOS

ESCENARIO N°1

Figura 1

Topología



Fuente: Guía Prueba de habilidades prácticas CCNA.

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.

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (60 host) y la LAN2 (20 hosts).

DESARROLLO ESQUEMA DE DIRECCIONAMIENTO IP

El espacio de red disponible es 172.46.3.0. Desde allí se parte el subnetting con los resultados mostrados en la tabla 1.

Descripción: para esta red local asignamos direcciones ipv4 a las interfaces G0/0/1 y G0/0/0 del router R1, los cuales también estarán configurados con las redes LAN 1, LAN 2, se asignaron direcciones a los respectivos PC1, PC2 donde vamos a desarrollar nuestro esquema.

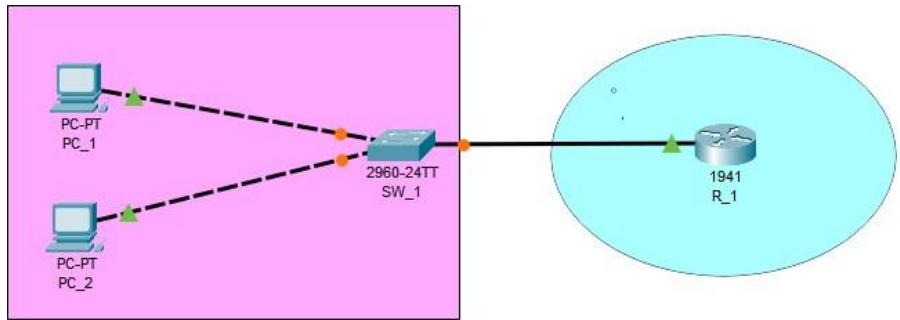
Tabla 1. Direccionamiento Escenario 1

| |
|-----------------------------|
| Dirección de Red 172.46.3.0 |
| Red LAN_1 |
| Máximo de host 62 |
| 172.46.3.0 |
| 255.255.255.192 |
| Red LAN_2 |
| Máximo de host 30 |
| 172.46.3.128 |
| 255.255.255.224 |

| ÍTEM | REQUERIMIENTO |
|-----------|---|
| R1 G0/0/1 | <p>Última dirección de host de la subred LAN1</p> <pre>R1(config)#interface G0/0/1 R1(config-if)#ip address 172.46.3.1 255.255.192 R1(config-if)#no shutdown</pre> |
| R1 G0/0/0 | <p>Última dirección de host de la subred LAN2</p> <pre>R1(config)#interface G0/0/0 R1(config-if)#ip address 172.46.3.75 255.255.255.224 R1(config-if)#no shutdown</pre> |
| S1 SVI | <p>Segunda dirección de host de lasubred LAN1</p> <pre>S1(config)#interface vlan 1 S1(config-if)#ip address 172.46.3.2 255.255.255.192 S1(config-if)#no shutdown</pre> |
| PC-A | <p>Décima dirección de host de lasubred LAN1</p> <p>Red IPv4 172.46.3.10</p> |
| PC-B | <p>Décima dirección de host de lasubred LAN2</p> <p>Red IPv4 172.46.3.75</p> |

Fuente Autor

Figura 2 Realización de Autor Escenario n1



Fuente Autor

CONFIGURE ASPECTOS BÁSICOS

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

Descripción: una vez realizado el direccionamiento, venimos a realizar la configuración básica de los dispositivos intermediarios, para el router 1 se tuvo en cuenta lo siguiente:

Designamos al router, también al dominio, se crean claves de acceso modo EXEC privilegiado facilitando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, generamos clave de cifrado.

Tabla 2. Configuración router R1

| TAREA | ESPECIFICACIÓN |
|---|---|
| Desactivar la búsqueda DNS: | R1(config)#no ip domain-lookup R1(config)# |
| Nombre del router : | Router(config)#hostname R1 |
| Nombre de dominio : | ccna-sa.com R1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado: | ciscoenpass R1(config)#enable password ciscoenpass |
| Contraseña de acceso a la consola: | Ciscoconpass R1(config)#line console 0 R1(config-line)#passwordciscoconpass R1(config-line)#login |
| Establecer la longitud mínima para las contraseñas | 10 caracteres |
| crear un usuario administrativo en la base de datos local : | Nombre de usuario: admin Contraseña: admin1pass R1(config)#username admin password admin1pass R1(config)#login local |

| | |
|--|--|
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local: | R1(config)#line vty 04 R1(config-line)#login local |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH : | R1(config)#ip ssh version 2 R1(config)#line vty 0 15 R1(config-line)#transport input ssh |
| Cifrar las contraseñas de texto nocifrado: | R1(config)#service password-encryption |
| Configurar un banner MOTD: ejecutamos el comando banner motdy entre comillas escribimos “ Cisco Pack Trace, Pedro Luis Duque Salazar Vela,Ingenieria de Sistemas” y damos enter. | Debe contener el nombre del dispositivo, el nombre completo de estudiante y el programa académico al que pertenece. R1(config)#banner motd “ Para mayor información contáctese con: Pedro Luis Duque Salazar Código 08 Ingeniería de Sistemas |
| Configuración de interface G0/0/0: | Establecer la descripción establecer dirección Ipv4 activar interfaz. R1(config)#interface gigabitEthernet0/0/0 R1(config-if)#ip address 172.46.3.1 255.255.255.224 R1(config-if)#no shutdown |
| Configuración de interface G0/0/1 | Establecer la descripción establecer dirección Ipv4 activar interfaz. R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 172.46.3.65 255.255.255.192 R1(config-if)#no shutdown |
| Generar una clave de cifrado RSA : | R1(config)#crypto key generate rsa How many bits in the modulus [512]:1024 |

LAS TAREAS DE CONFIGURACIÓN DE S1 INCLUYEN LO SIGUIENTE:

En el switch le determinamos nombre también de dominio, se crean claves de acceso modo EXEC privilegiado facilitando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, generamos clave de cifrado.

Tabla 3. Configuración switch S1

| TAREA ESPECIFICACIÓN | TAREA ESPECIFICACIÓN |
|---|---|
| Desactivar la búsqueda DNS: | S1(config)#no ip domain-lookup |
| Nombre del switch: | switch1(config)#hostname S1 |
| Nombre de dominio : | ccna-sa.com S1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modoEXEC privilegiado: | ciscoenpass S1(config)#enable password ciscoenpass |
| Contraseña de acceso a la consola: | ciscoconpass S1(config)#line 0 S1(config-line)#password ciscoconpass S1(config-line)#login |

| | |
|------------------------------------|--|
| | F0/1-4, F0/7-24, G0/1-2 |
| Apagar todos los puertos sin usar: | S1(config)#interface range fastEthernet0/1-4 |

| | |
|---|--|
| | <pre>S1(config-if-range)#shutdown S1(config)#interface range fastEthernet 0/7-24 S1(config-if-range)#shutdown S1(config)#interface range GigabitEthernet 0/1-2 S1(config-if-range)#shutdown</pre> |
| Crear un usuario administrativo en labase de datos local: | <pre>Nombre de usuario: admin Contraseña: admin1pass S1(config)#username admin password admin1pass</pre> |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local: | <pre>S1(config)#line vty 0 4 S1(config-line)#login local</pre> |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH: | <pre>S1(config)#ip ssh version 2 S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local</pre> |
| Cifrar las contraseñas de texto no cifrado: ejecutamos el comando luego ingrsamos el comando service password-encryption. | <pre>S1(config)#service password-encryption</pre> |

Tabla 5

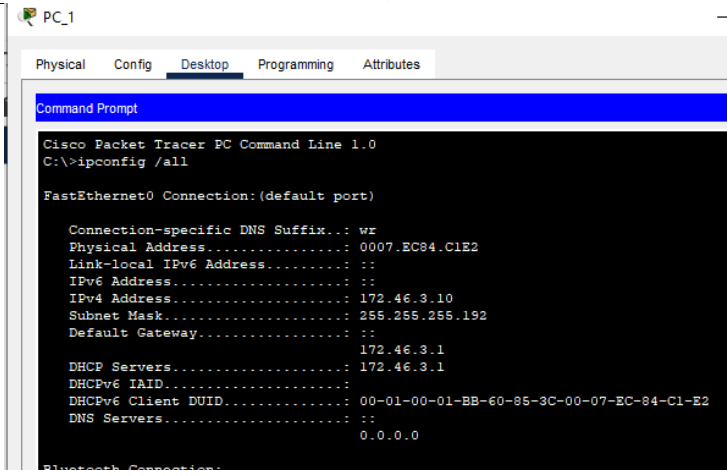
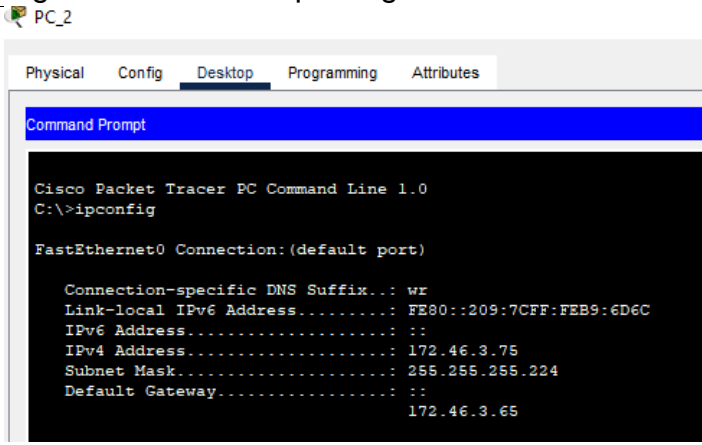
| | |
|---|--|
| <p>Configurar un banner MOTD: banner motd y entre comillas escribimos " Cisco Pack Tracer PEDRO LUIS DUQUE SALAZAR ,Ingeniería de Sistemas" y damos enter.</p> | <p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <p>S1(config)#banner motd " Pedro Luis Duque Salazar Código 08 Ingeniería de Sistemas"</p> |
| <p>Generar una clave de cifrado RSA: Ejecutamos el comando crypto key generate rsa y al final donde dice How many bits in the modulus [512]: agregamos 1024 bits y damos enter.</p> | <p>Módulo de 1024 bits</p> <p>S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com How many bits in the modulus [512]: 1024</p> |

Fuente Autor

CONFIGURAR LOS EQUIPOS

En este caso se ejecutó el comando ipconfig /all a los equipos PC-A y B, nos muestra un informe de su dirección física, dirección Ipv4, mascara de subred y puerta de enlace Ipv4 predeterminado.

Tabla 5. Configuración ipv4 PC-1

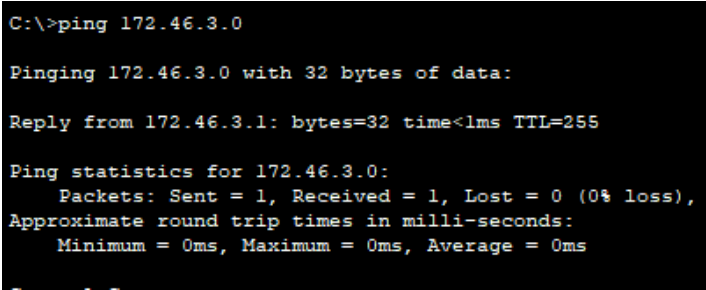
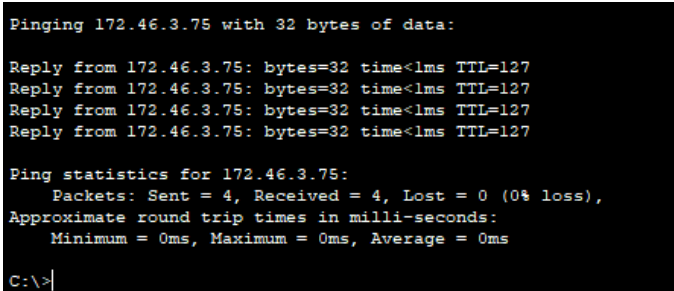
| CONFIGURACIÓN DE RED DE PC-1 | |
|------------------------------|---|
| Descripción CAPTURA | <p>Figura 3. Comando ipconfig /all PC-1</p>  <pre> Cisco Packet Tracer PC Command Line 1.0 C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix. : wr Physical Address. : 0007.EC84.C1E2 Link-local IPv6 Address. : :: IPv6 Address. : :: IPv4 Address. : 172.46.3.10 Subnet Mask. : 255.255.255.192 Default Gateway. : :: 172.46.3.1 DHCP Servers. : 172.46.3.1 DHCPv6 IAID. : DHCPv6 Client DUID. : 00-01-00-01-BB-60-85-3C-00-07-EC-84-C1-E2 DNS Servers. : :: 0.0.0.0 </pre> |
| Dirección IPv4 | 172.46.3.10 |
| Máscara de subred | 255.255.255.192 |
| Configuración de red de PC-2 | |
| Descripción IMAGEN | <p>Figura 4. Comando ipconfig /all PC2</p>  <pre> Cisco Packet Tracer PC Command Line 1.0 C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix. : wr Link-local IPv6 Address. : FE80::209:7CFF:FEB9:6D6C IPv6 Address. : :: IPv4 Address. : 172.46.3.75 Subnet Mask. : 255.255.255.224 Default Gateway. : :: 172.46.3.65 </pre> |
| Dirección IPv4 | 172.46.3.75 |
| Máscara de subred | 255.255.255.224 |

Fuente Autor

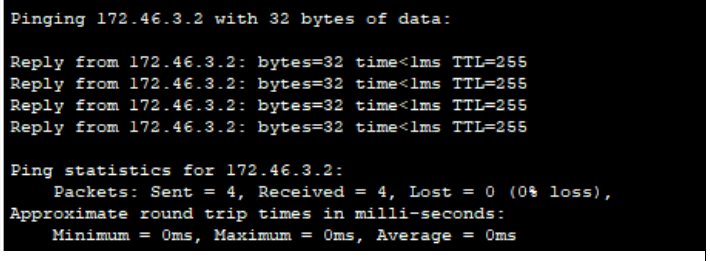
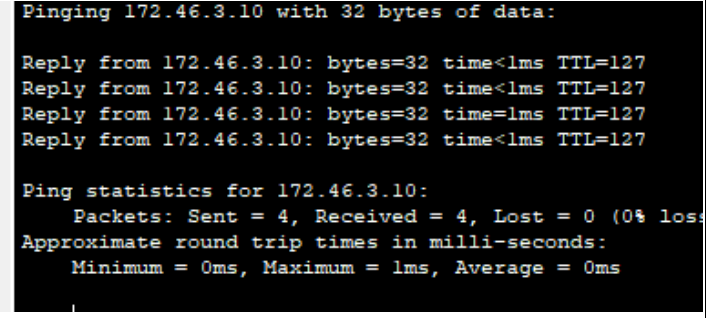
PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Para poder verificar la correctamente el ejercicio del escenario 1, vamos a realizar pruebas de ping a todos.

Tabla 6. Verificación de conectividad dispositivos de red

| DESDE | 1 | DIRECCIÓN IP | RESULTADOS DE PING |
|-------|--------------|--------------|--|
| PC1 | R1 G0/0/0 | 172.46.3.1 | <p>Figura 5</p>  |
| PC2 | R1 G0/0/1 | 172.46.3.75 | <p>Figura 6</p>  |

| | | | |
|-----|--------------|-------------|---|
| PC1 | S1 VLAN1 | 172.46.3.2 | <p>Figura 7</p> <pre>Pinging 172.46.3.2 with 32 bytes of data: Reply from 172.46.3.2: bytes=32 time<lms TTL=255 Reply from 172.46.3.2: bytes=32 time<lms TTL=255 Reply from 172.46.3.2: bytes=32 time<lms TTL=255 Reply from 172.46.3.2: bytes=32 time<lms TTL=255 Ping statistics for 172.46.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC1 | PC 2 | 172.46.3.75 | <p>Figura 8</p> <pre>Pinging 172.46.3.75 with 32 bytes of data: Reply from 172.46.3.75: bytes=32 time<lms TTL=127 Reply from 172.46.3.75: bytes=32 time<lms TTL=127 Reply from 172.46.3.75: bytes=32 time<lms TTL=127 Reply from 172.46.3.75: bytes=32 time<lms TTL=127 Ping statistics for 172.46.3.75: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC2 | R1 G0/0/0 | 172.46.3.1 | <p>Figura 9</p> <pre>Pinging 172.46.3.1 with 32 bytes of data: Reply from 172.46.3.1: bytes=32 time<lms TTL=255 Reply from 172.46.3.1: bytes=32 time<lms TTL=255 Reply from 172.46.3.1: bytes=32 time<lms TTL=255 Reply from 172.46.3.1: bytes=32 time<lms TTL=255 Ping statistics for 172.46.3.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC2 | R1 G0/0/1 | 172.46.3.75 | <p>Figura 10</p> <pre>Pinging 172.46.3.75 with 32 bytes of data: Reply from 172.46.3.75: bytes=32 time<lms TTL=128 Reply from 172.46.3.75: bytes=32 time=3ms TTL=128 Reply from 172.46.3.75: bytes=32 time=6ms TTL=128 Reply from 172.46.3.75: bytes=32 time=26ms TTL=128 Ping statistics for 172.46.3.75: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 26ms, Average = 8ms</pre> |

| | | | |
|-----|-------------|-------------|---|
| PC2 | S1 VLAN1 | 172.46.3.2 | <p>Figura 11</p>  <pre> Pinging 172.46.3.2 with 32 bytes of data: Reply from 172.46.3.2: bytes=32 time<1ms TTL=255 Reply from 172.46.3.2: bytes=32 time<1ms TTL=255 Reply from 172.46.3.2: bytes=32 time<1ms TTL=255 Reply from 172.46.3.2: bytes=32 time<1ms TTL=255 Ping statistics for 172.46.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre> |
| PC2 | PC 1 | 172.46.3.10 | <p>Figura 12</p>  <pre> Pinging 172.46.3.10 with 32 bytes of data: Reply from 172.46.3.10: bytes=32 time<1ms TTL=127 Reply from 172.46.3.10: bytes=32 time<1ms TTL=127 Reply from 172.46.3.10: bytes=32 time=1ms TTL=127 Reply from 172.46.3.10: bytes=32 time<1ms TTL=127 Ping statistics for 172.46.3.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms </pre> |

Fuente Autor

Reporte de ping genera

FIGURA 4 se puede evidenciar que el ping del PC –1 es exitoso porque la dirección corresponde a la puerta de enlace que está en la última dirección de host de la subred LAN2.

FIGURA 5 se puede evidenciar que el ping del PC –1 es exitoso porque la dirección corresponde a la puerta de enlace que está en la última dirección de host de la subred LAN1.

FIGURA 6 se puede evidenciar que el ping del PC –1 es exitoso porque la dirección corresponde al switch S1 de la VLAN.

FIGURA 7 se puede evidenciar que el ping del PC –1 es exitoso porque la dirección corresponde a la IP del PC-B.

FIGURA 8 se puede evidenciar que el ping del PC –2 es exitoso porque la dirección corresponde a la última dirección de host de la subred LAN2.

FIGURA 9 se puede evidenciar que el ping del PC -2 es exitoso porque la dirección corresponde a la última dirección de host de la subred LAN1.

FIGURA 10 se puede evidenciar que el ping del PC -A es exitoso porque la dirección corresponde a la última dirección de la switch S1 VLAN 1.

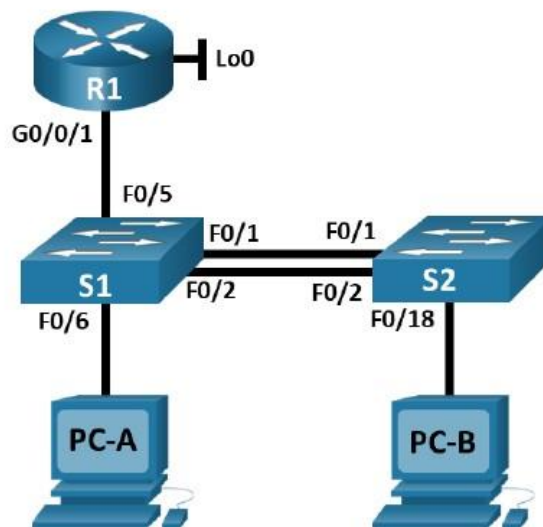
FIGURA 11 se puede evidenciar que el ping del PC -2 es exitoso porque la dirección corresponde al switch S1 de la IP del PC-A.

DESARROLLO ESCENARIO 2

Figura 13. Topología Escenario 2

Escenario 2

Topología



Fuente: prueba de habilidades diplomado CCNA.

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

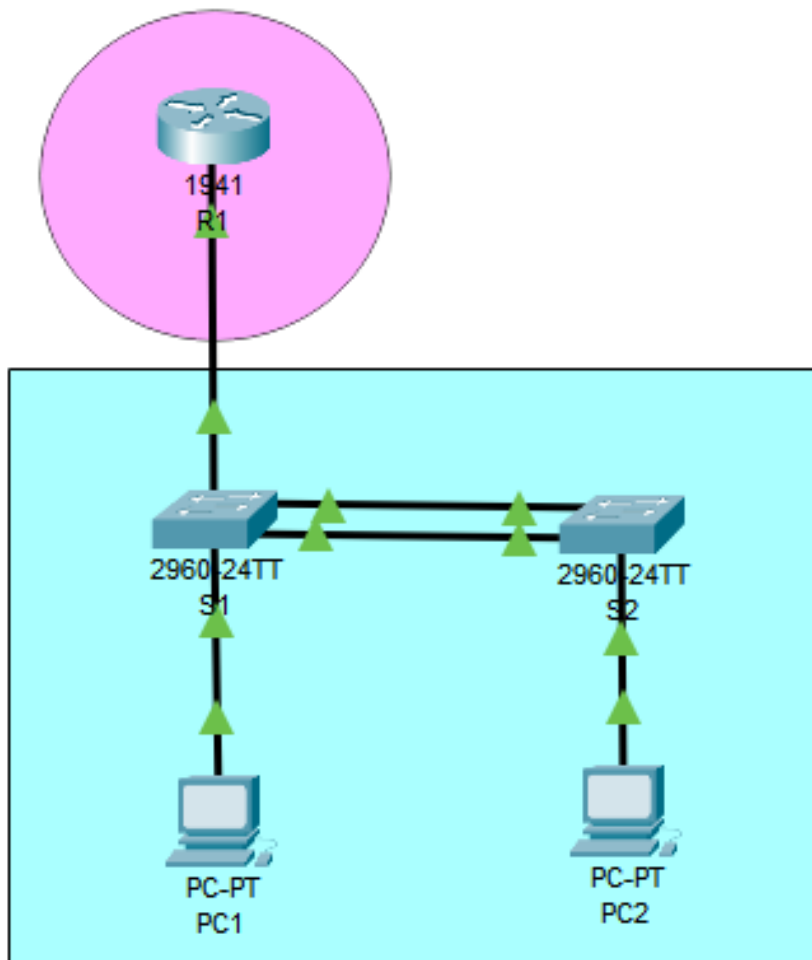
Tabla 7 Nombres de las VLAN

| Tabla de VLAN | Nombre de la VLAN |
|---------------|-------------------|
| 20 | Docentes |
| 30 | Estudiantes |
| 40 | Invitados |
| 50 | Usuarios |
| 56 | Native |

Fuente Autor

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

Figura 14 Simulador Packet Tracer



Fuente Autor

Tabla 8. Tabla de asignación de direcciones

| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
|------------------------|---------------------------|--|
| R1 G0/0/1.20 | 10.XY.8.1 /26 | No corresponde |
| <i>R1 G0/0/1.2</i> | 2001:db8:acad:a :1 /64 | No corresponde |
| R1 G0/0/1.30 | 10.XY.8.65 /27 | No corresponde |
| <i>R1 G0/0/1.3</i> | 2001:db8:acad:b :1 /64 | No corresponde |
| R1 G0/0/1.40 | 10.XY.8.97 /29 | No corresponde |
| <i>R1 G0/0/1.4</i> | 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 |
| <i>R1 Loopback0</i> | 2001:db8:acad:209: :1 /64 | No corresponde |
| S1 VLAN 4 | 10.XY.8.98 /29 | 10.19.8.97 |
| <i>VLAN S1 4</i> | 2001:db8:acad:c :98 /64 | No corresponde |
| <i>S1 VLAN 4</i> | fe80: :98 | No corresponde |
| S2 VLAN 4 | 10.XY.8.99 /29 | 10.19.8.97 |
| <i>S2 VLAN 4</i> | 2001:db8:acad:c :99 /64 | No corresponde |
| <i>S2 VLAN 4</i> | fe80: :99 | No corresponde |
| PC-A NIC | Dirección DHCP para IPv4 | DHCP para puerta de enlace predeterminada IPv4 |
| <i>PC-A NIC</i> | 2001:db8:acad:a :50 /64 | fe80::1 |
| PC-B NIC | DHCP para dirección IPv4 | DHCP para puerta de enlace predeterminada IPv4 |

fuente: Guía Prueba de habilidades prácticas CCNA.

INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

Inicializar y volver a cargar el router y el switch

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Se hace de la siguiente manera: erase startup-config reload

CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Al router le asignamos nombre, también de dominio, se crean claves de acceso modo EXEC privilegiado proporcionando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se configura un banner MOTD, se realiza configuración de interfaces, GigabitEthernet0/0/1.20, GigabitEthernet0/0/1.30, GigabitEthernet0/0/1.40, GigabitEthernet0/0/1.50, GigabitEthernet0/0/1.56, el Loopback0 generamos clave de cifrado, se habilita el routing IPv6, establecemos dirección IPv4 y la dirección local de enlace.

Tabla 9. Configuración router R1

| TAREA | ESPECIFICACIÓN |
|--|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain lookup |
| Nombre del router | R1 Router(config)#hostname R1 |
| Nombre de dominio | ccna-sa.com R1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | class R1(config)#enable password class |
| Contraseña de acceso a la consola | cisco R1(config)#enable secret cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login |
| Establecer la longitud mínima para las contraseñas | 5 caracteres R1(config)#security passwords min-length 5 |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Password: admin1pass R1(config)#username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | R1(config)#line vty 0 14 R1(config-line)#login local |
| Configurar VTY solo aceptando SSH | R1(config-line)#transport input ssh |

| | |
|--|--|
| Cifrar las contraseñas de texto no Cifrado | R1(config)#service password-Encryption |
| Configure un MOTD Banner | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece: |

| | |
|--|--|
| | R1(config)#banner motd "PEDRO LUIS DUQUE SALAZAR INGENIERIA DE SISTEMAS UNAD" |
| Habilitar el routing IPv6 | R1(config)#ipv6 unicast-routing |
| Configurar interfaz G0/0/1 y subinterfaces | <p>Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80::1 Establece la dirección IPv6. Activar la interfaz.</p> <pre> R1(config)#interface GigabitEthernet0/0/1.20 R1(config-subif)#encapsulation dot1q20 R1(config-subif)#description Docentes R1(config-subif)#ip address 10.46.8.1 255.255.255.192 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)# interface GigabitEthernet0/0/1.30 </pre> |

| | |
|---|---|
| <p>Configurar interfaz G0/0/1 y subinterfaces</p> | <pre> R1(config-subif)#encapsulation dot1q30 R1(config-subif)#description Estudiantes R1(config-subif)#ip address 10.46.8.65 255.255.255.224 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-subif)# interface GigabitEthernet0/0/1.40 R1(config-subif)#encapsulation dot1q40 R1(config-subif)#description Invitados R1(config-subif)#ip address 10.92.8.97 255.255.255.248 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-subif)#)# interface GigabitEthernet0/0/1.50 R1(config-subif)#encapsulation dot1q 50 </pre> |
|---|---|

| | |
|--|--|
| Configurar interfaz G0/0/1 y subinterfaces | <pre> R1(config-subif)#description UsuariosR1(config-subif)#exit R1(config-subif)# interface GigabitEthernet0/0/1.56 R1(config-subif)#encapsulation dot1q56 R1(config-subif)#description Native R1(config-subif)#exit R1(config-subif)# interface GigabitEthernet0/0/1 R1(config-if)#no shutdown </pre> |
| Configure el Loopback0 interface | <pre> Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1 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)#exit </pre> |
| Generar una clave de cifrado RSA | <pre> Módulo de 1024 bits R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 </pre> |

Fuente: Autor

CONFIGURE S1 Y S2.

Las tareas de configuración incluyen lo siguiente:

Los switches S1 y S2 le asignamos nombre, también de dominio, se crean claves de acceso modo EXEC privilegiado proporcionando seguridad acceso completo al dispositivo y su configuración a la consola y con longitud mínima para poder mitigar los riesgos de acceso de algún usuario no autorizado, se crea un usuario administrativo en la base de datos local configurando el inicio de sesión en las líneas VTY que acepten únicamente las conexiones SSH, cifrando sus contraseñas, se Configurar un banner MOTD, se realiza configuración de sus interfaces, generamos clave de cifrado, configuramos la interfaz de administración (SVI) Establecemos dirección IPv4 de capa 3 con la puerta de enlace predeterminada y dirección local de enlace.

Tabla 10. Configuración Switch S1 y S2

| TAREA | ESPECIFICACIÓN |
|----------------------------|--|
| | Nota: estos mismos comandos y procesos los utilizaremos para configurar el Switch S1 y S2 en el orden que desee configurarlos. |
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |

| | |
|--|---|
| Nombre del switch | S1 y S2, de acuerdo a su configuración. Switch(config)#hostname S1 Switch(config)#hostname S2 |
| Nombre de dominio | ccna-sa.com S1(config)#ip domain-name ccna-sa.com S2(config)# ip domain-name ccna-sa.com |
| Contraseña cifrada para el modoEXEC privilegiado | Class S1(config)#enable secret class S2(config)#enable secret class |
| Contraseña de acceso a la consola | Cisco S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit |
| Establecer la longitud mínima para las contraseñas | 5 caracteres |

| | |
|--|---|
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Password: admin1pass S1(config)# username admin secret admin1pass S2(config)# username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | S1(config)#line vty 0 15 S1(config-line)#login local S2(config)#line vty 0 15 S2(config-line)#login local |
| Configurar VTY solo aceptando SSH | S1(config-line)#transport input ssh S1(config-line)#exit |
| | S2(config-line)#transport input ssh S2(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S1(config)#service password-encryption S2(config)#service password-encryption |
| Configure un MOTD Banner | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece S1(config)# banner motd "PEDRO LUIS DUQUE SALAZAR INGENIERIA DE SISTEMAS UNAD" |

| | |
|---|--|
| <p>Generar una clave de cifrado RSA</p> | <p>Módulo de 1024 bits</p> <p>S1(config)# crypto key generate rsa How many bits in the modulus [512]: 1024</p> <p>S2(config)# crypto key generate rsa How many bits in the modulus [512]: 1024</p> |
| <p>Configurar la interfaz de administración (SVI)</p> | <p>Establecer la dirección IPv4 de capa 3</p> <p>Establezca la dirección local de enlace</p> |

| | |
|---|--|
| <p>Configurar la interfaz de administración (SVI)</p> | <p>IPv6 como FE80: :98 para S1 y FE80: :99 para S2</p> <p>Establecer la dirección IPv6 de capa 3</p> <pre>S1(config)#int vlan40 S1(config-if)#ip address 10.46.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)# ipv6 address fe80::98 link- local S1(config-if)#description Invitados Interface S1(config-if)#no shutdown S1(config-if)#exit</pre> |
| <p>Configuración del gateway predeterminado</p> | <p>Configure la puerta de enlace predeterminada como 10.46.8.97 para IPv4</p> <pre>S1(config)#ip default-gateway 10.46.8.97</pre> |

Fuente Autor

CONFIGURACIÓN DE INFRAESTRUCTURA DE RED (VLAN,TRUNKING, ETHERCHANNEL)

CONFIGURAR S1

La configuración del S1 y S2 incluye las siguientes tareas:

Se realiza creación de las Vlan 20,30,40,50 y Se establece comunicación entre los Switch de modo troncal con el fin de manejar el tráfico entre las Vlans, se crearan un grupo de puertos de Capa 2 que use interfaces en un único canal lógico, se configura la seguridad de su puertos de acceso máximo 4 direcciones y se aseguraran todas sus interfaces no utilizadas.

Tabla 11. Configuración S1

| TAREA | ESPECIFICACIÓN |
|---|---|
| <p>Crear VLAN</p> <p>VLAN 20, nombre Docentes</p> <p>VLAN 30, nombre Estudiantes</p> <p>VLAN 40, nombre Invitados</p> <p>VLAN 50, nombre Usuarios</p> <p>VLAN 56, nombre Native</p> | <pre>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</pre> |

| | |
|--|--|
| <p>Crear troncos 802.1Q que utilicen la VLAN 56 native</p> | <p>Interfaces F0/1, F0/2 y F0/5</p> <pre>S1(config)#int range F0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56</pre> |
| <p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> | <p>Usar el protocolo LACP para la negociación</p> <pre>S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switch trunk native vlan 56</pre> |
| <p>Configurar el puerto de acceso de host para VLAN 20</p> | <p>Interface F0/6</p> <pre>S1(config)#interface F0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20</pre> |

| | |
|--|---|
| <p>Configurar la seguridad del puerto en los puertos de acceso</p> | <p>Permitir 4 direcciones MAC</p> <pre>S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 4</pre> |
| <p>Proteja todas las interfaces no utilizadas</p> | <p>Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar</p> <pre>S1(config)#interface range F0/3-4 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta en Uso S1(config-if-range)#shutdown S1(config)#interface range F0/7-24 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta en Uso S1(config-if-range)#shutdown</pre> |

Fuente Autor

CONFIGURE EL S2.

Tabla 12. Configuración S2

| TAREA | ESPECIFICACIÓN |
|--|---|
| <p>Crear VLAN</p> <p>VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native</p> | <pre>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</pre> |

| | |
|--|--|
| <p>Crear troncos 802.1Q que utilicen la VLAN 56 native</p> | <p>Interfaces F0/1 y F0/2</p> <pre>S2(config)#int range F0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56</pre> |
| <p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> | <p>Usar el protocolo LACP para la negociación</p> <pre>S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switch trunk native vlan 56</pre> |
| <p>Configurar el puerto de acceso del host para la VLAN 30</p> | <p>Interfaz F0/18</p> <pre>S2(config-if)#int F0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30</pre> |

| | |
|--|--|
| <p>Configure port-security en los access ports</p> | <p>permite 4 MAC addresses</p> <pre>S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 4</pre> |
| <p>Configure todas las interfaces no utilizadas.</p> | <p>Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar</p> <pre>S2(config-if)#int range F0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta en Uso S2(config-if-range)#shutdown</pre> <p>S2(config-if-range)#int range F0/19-24</p> <pre>S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta en Uso S2(config-if-range)#shutdown</pre> |

Fuente Autor

CONFIGURAR SOPORTE DE HOST

CONFIGURE R1

Las labores de configuración para R1 incluyen las siguientes:

En este caso se crearán unas rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, se organizarán un grupo DHCP para VLAN 20 y otro grupo DHCP para VLAN 30 donde cada uno de ellos este compuesto por las últimas 10 direcciones de la subred solamente y que se les asigne un nombre de dominio especificando de enlace predeterminada como dirección de interfaz del router.

Tabla 13. Configuración router R1

| Tarea | Especificación |
|-----------------------------------|---|
| Configure Default Routing | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#ip router 0.0.0.0 0.0.0.0 loopback 0 R1(config)# ipv6 router ::/0 loopback0 Ambas rutas estáticas para llegar a Internet |
| Configurar IPv4 DHCP para VLAN 20 | Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad- |

| | |
|-----------------------------------|---|
| | <p>ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada</p> <pre>R1(config)#ip dhcp excluded-address 10.46.8.1 10.46.8.10 R1(config)#ip dhcp pool vlan20- Docentes R1(dhcp-config)#network 10.46.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.46.8.65 R1(dhcp-config)# domain-name wr Wr lo identificamos</pre> |
| Configurar DHCP IPv4 para VLAN 30 | <p>Cree un grupo DHCP para VLAN 30, compuesto por las últimas 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 router para la subred involucrada</p> <pre>R1(config)#ip dhcp excluded-address 10.46.8.65 10.46.8.84</pre> |

| | |
|--|---|
| | <pre> R1(config)#ip dhcp pool vlan30- Estudiantes R1(dhcp-config)#network 10.46.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.46.8.65 R1(dhcp-config)# domain-name Wr Wr lo identificamos. </pre> |
|--|---|

Fuente: Autor

“En esta ocasión pusimos el domain name Wr para identificarlo diferente.”

CONFIGURAR LOS SERVIDORES

Vamos a realizar la configuración de los equipos host PC-1 y PC-2 para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registraremos las configuraciones de red del host con el comando x|.

Tabla 14. Configuración de red de PC-A

| CONFIGURACIÓN DE RED DE PC-1 | |
|------------------------------|--------------------------|
| Dirección física | FE80::200:CFF:FE3A:1E39 |
| Dirección IP | 10.46.8.11 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 10.46.8.1 |
| Gateway predeterminado IPv6 | FE80::260:70FF:FECB:6202 |

Fuente: Autor

Tabla 15. Configuración de PC-2

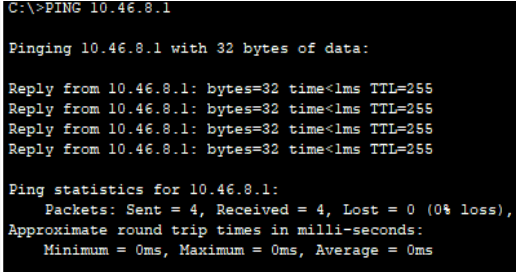
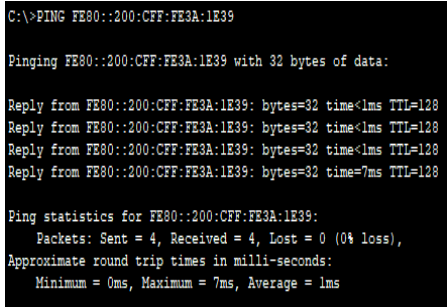
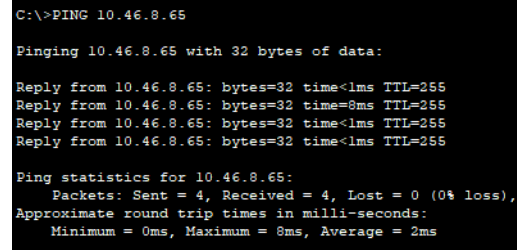
| CONFIGURACIÓN DE RED DE PC-2 | |
|------------------------------|--------------------------|
| Dirección física | 0009.7C18.11BD |
| Dirección IP | 10.46.8.75 |
| Máscara de subred | 255.255.255.224 |
| Gateway predeterminado | 10.46.8.65 |
| Gateway predeterminado IPv6 | FE80::260:70FF:FECB:6202 |

Fuente: Autor

PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Para verificar la correcta implementación del escenario 2, se realizan pruebas de ping desde los dispositivos finales PC a los demás dispositivos de la topología.

Tabla 16. Probar y verificar la conectividad de extremo a extremo

| Desde | PC | Ref | Dirección IP | Resultados de ping |
|-------|------------------|------|-----------------------------|--|
| PC-1 | R1, G0/0/1.20 | IPv4 | 10.46.8.1 | <p>Figura 15</p>  <pre>C:\>PING 10.46.8.1 Pinging 10.46.8.1 with 32 bytes of data: Reply from 10.46.8.1: bytes=32 time<1ms TTL=255 Reply from 10.46.8.1: bytes=32 time<1ms TTL=255 Reply from 10.46.8.1: bytes=32 time<1ms TTL=255 Reply from 10.46.8.1: bytes=32 time<1ms TTL=255 Ping statistics for 10.46.8.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC1 | | IPV6 | FE80::200:CFF:F E3A:1E39 | <p>Figura 16</p>  <pre>C:\>PING FE80::200:CFF:FE3A:1E39 Pinging FE80::200:CFF:FE3A:1E39 with 32 bytes of data: Reply from FE80::200:CFF:FE3A:1E39: bytes=32 time<1ms TTL=128 Reply from FE80::200:CFF:FE3A:1E39: bytes=32 time<1ms TTL=128 Reply from FE80::200:CFF:FE3A:1E39: bytes=32 time<1ms TTL=128 Reply from FE80::200:CFF:FE3A:1E39: bytes=32 time=7ms TTL=128 Ping statistics for FE80::200:CFF:FE3A:1E39: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 7ms, Average = 1ms</pre> |
| PC-1 | R1, G0/0/1.30 | IPv4 | 10.46.8.65 | <p>Figura 17</p>  <pre>C:\>PING 10.46.8.65 Pinging 10.46.8.65 with 32 bytes of data: Reply from 10.46.8.65: bytes=32 time<1ms TTL=255 Reply from 10.46.8.65: bytes=32 time=8ms TTL=255 Reply from 10.46.8.65: bytes=32 time<1ms TTL=255 Reply from 10.46.8.65: bytes=32 time<1ms TTL=255 Ping statistics for 10.46.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 8ms, Average = 2ms</pre> |

| | | | | |
|------|------------------|------|-----------------------|---|
| PC-1 | | IPv6 | 2001:DB8:ACAD:B::1/64 | <p>Figura 18</p> <pre>Pinging 2001:DB8:ACAD:B::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time=51ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 51ms, Average = 12ms</pre> |
| PC-1 | R1, G0/0/1.40 | IPv4 | 10.46.8.97 | <p>Figura 19</p> <pre>C:\>ping 10.46.8.97 Pinging 10.46.8.97 with 32 bytes of data: Reply from 10.46.8.97: bytes=32 time<1ms TTL=255 Reply from 10.46.8.97: bytes=32 time<1ms TTL=255 Reply from 10.46.8.97: bytes=32 time<1ms TTL=255 Reply from 10.46.8.97: bytes=32 time<1ms TTL=255 Ping statistics for 10.46.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-1 | R1, G0/0/1.40 | IPv6 | 2001:DB8:ACAD:C::1 | <p>Figura 20</p> <pre>C:\>ping 2001:DB8:ACAD:C::1 Pinging 2001:DB8:ACAD:C::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |

| | | | | |
|------|-----------------|------|--------------------------|--|
| PC-1 | SV1, VLAN 40 | IPv4 | 10.46.8.98 | <p>Figura 21</p> <pre>Pinging 10.46.8.98 with 32 bytes of data: Reply from 10.46.8.98: bytes=32 time<1ms TTL=254 Reply from 10.46.8.98: bytes=32 time<1ms TTL=254 Reply from 10.46.8.98: bytes=32 time<1ms TTL=254 Reply from 10.46.8.98: bytes=32 time<1ms TTL=254 Ping statistics for 10.46.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre> |
| PC-1 | SV1, VLAN 40 | IPv6 | 2001:DB8:ACAD: 209::1 | <p>Figura 22</p> <pre>Pinging 2001:DB8:ACAD:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-1 | SV2, VLAN 40 | IPv4 | 10.46.8.99 | <p>Figura 23</p> <pre>Pinging 10.46.8.99 with 32 bytes of data: Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Ping statistics for 10.46.8.99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |

| | | | | |
|------|-----------------|------|-------------------------|--|
| PC-1 | SV2, VLAN 40 | IPv6 | 2001:DB8:ACAD: C::1: | <p>Figura 24</p> <pre>Pinging 2001:db8:acad:c::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-2 | R1, VLAN 40 | IPv4 | 10.46.8.65 | <p>Figura 25</p> <pre>C:\>ping 10.46.8.65 Pinging 10.46.8.65 with 32 bytes of data: Reply from 10.46.8.65: bytes=32 time<lms TTL=255 Reply from 10.46.8.65: bytes=32 time<lms TTL=255 Reply from 10.46.8.65: bytes=32 time<lms TTL=255 Reply from 10.46.8.65: bytes=32 time<lms TTL=255 Ping statistics for 10.46.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre> |
| PC-2 | R1, VLAN 40 | IPv6 | 2001:db8:acad:b: :1 | <p>Figura 26</p> <pre>Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<lms TTL=255 Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |

| | | | | |
|------|---------------|------|----------------------|---|
| PC-2 | R1 BUCLE 0 | IPv4 | 209.165.201.1 | <p>Figura 27</p> <pre>Pinging 209.165.201.1 with 32 bytes of data: Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Ping statistics for 209.165.201.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-2 | R1 BUCLE 0 | IPv6 | 2001:db8:acad:209::1 | <p>Figura 28</p> <pre>Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\></pre> |
| PC-2 | R1 BUCLE 0 | IPv4 | 209.165.201.1 | <p>Figura 29</p> <pre>C:\>PING 209.165.201.1 Pinging 209.165.201.1 with 32 bytes of data: Reply from 209.165.201.1: bytes=32 time=lms TTL=255 Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Reply from 209.165.201.1: bytes=32 time<lms TTL=255 Ping statistics for 209.165.201.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = lms, Average = 0ms C:\></pre> |

| | | | | |
|------|------------------|------|----------------------|--|
| PC-2 | | IPv6 | 2001:db8:acad:209::1 | <p>Figura 30</p> <pre> C:\>PING 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time=19ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 19ms, Average = 4ms </pre> |
| PC-2 | R1, G0/0/1.20 | IPv4 | 10.46.8.1 | <p>Figura 31</p> <pre> Pinging 10.46.8.1 with 32 bytes of data: Reply from 10.46.8.1: bytes=32 time<lms TTL=255 Reply from 10.46.8.1: bytes=32 time<lms TTL=255 Reply from 10.46.8.1: bytes=32 time<lms TTL=255 Reply from 10.46.8.1: bytes=32 time<lms TTL=255 Ping statistics for 10.46.8.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre> |
| PC-2 | | IPv6 | 2001:db8:acad:a::1 | <p>Figura 32</p> <pre> Pinging 2001:db8:acad:a::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre> |

| | | | | |
|------|-----------------|------|--------------------|---|
| PC-2 | R1G0/0/1. 30 | IPv4 | 10.46.8.65 | <p>Figura 33</p> <pre>Pinging 10.46.8.65 with 32 bytes of data: Reply from 10.46.8.65: bytes=32 time<ms TTL=255 Reply from 10.46.8.65: bytes=32 time<ms TTL=255 Reply from 10.46.8.65: bytes=32 time<ms TTL=255 Reply from 10.46.8.65: bytes=32 time<ms TTL=255 Ping statistics for 10.46.8.65: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-2 | | IPv6 | 2001:db8:acad:b::1 | <p>Figura 34</p> <pre>C:\>PING 2001:db8:acad:b::1 Pinging 2001:db8:acad:b::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms TTL=255 Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-2 | R1G0/0/1. 40 | IPv4 | 10.46.8.97 | <p>Figura 35</p> <pre>Pinging 10.46.8.97 with 32 bytes of data: Reply from 10.46.8.97: bytes=32 time<ms TTL=255 Reply from 10.46.8.97: bytes=32 time<ms TTL=255 Reply from 10.46.8.97: bytes=32 time<ms TTL=255 Reply from 10.46.8.97: bytes=32 time<ms TTL=255 Ping statistics for 10.46.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre> |

| | | | | |
|------|-----------------|------|---------------------|--|
| PC-2 | | IPv6 | 2001:db8:acad:c::1 | <p>Figura 36</p> <pre>Pinging 2001:db8:acad:c::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</pre> |
| PC-2 | R1G0/0/1. 40 | IPv4 | 10.46.8.98 | <p>Figura 37</p> <pre>Pinging 10.46.8.98 with 32 bytes of data: Reply from 10.46.8.98: bytes=32 time<lms TTL=254 Reply from 10.46.8.98: bytes=32 time<lms TTL=254 Reply from 10.46.8.98: bytes=32 time<lms TTL=254 Reply from 10.46.8.98: bytes=32 time<lms TTL=254 Ping statistics for 10.46.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| PC-2 | | IPv6 | 2001:db8:acad:c::98 | <p>Figura 38</p> <pre>Pinging 2001:db8:acad:c::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<lms TTL=255</pre> |

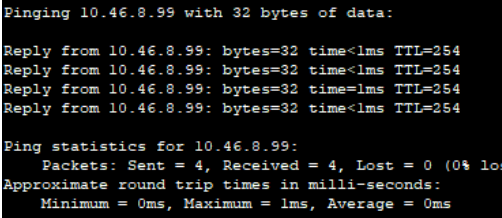
| | | | | |
|------|-----------------|------|------------|---|
| PC-2 | SV2, VLAN 40 | IPv6 | 10.46.8.98 | <p>Figura 39</p>  <pre> Pinging 10.46.8.99 with 32 bytes of data: Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Reply from 10.46.8.99: bytes=32 time<1ms TTL=254 Ping statistics for 10.46.8.99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms </pre> |
|------|-----------------|------|------------|---|

FIGURA 13 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.20.

FIGURA 14 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.20.

FIGURA 15 se puede evidenciar que el ping del PC –A es exitoso porque la dirección pv4 corresponde a la interfaz del router R1 G0/0/1.3

FIGURA 16 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.30.

FIGURA 17 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.40.

FIGURA 18 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.40.

FIGURA 19 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde al S1 en la VLAN 40.

FIGURA 20 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 que corresponde al S1 en la VLAN 40

FIGURA 21 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde al S2 en la VLAN 40.

FIGURA 22 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 que corresponde al S2 en la VLAN 40.

FIGURA 23 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 corresponde al PC-B.

FIGURA 24 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 corresponde al PC-B.

FIGURA 25 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv4 es del Bucle 0 configurado en el router R1.

FIGURA 26 se puede evidenciar que el ping del PC –A es exitoso porque la dirección ipv6 es del Bucle 0 configurado en el router R1.

FIGURA 27 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 es del Bucle 0 configurado en el router R1

FIGURA 28 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 es del Bucle 0 configurado en el router R1.

FIGURA 29 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.20.

FIGURA 30 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.20.

FIGURA 31 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.30.

FIGURA 32 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.30.

FIGURA 33 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde a la interfaz del router R1 G0/0/1.40.

FIGURA 34 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 corresponde a la interfaz del router R1 G0/0/1.40.

FIGURA 35 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde al S1 en la VLAN 40.

FIGURA 36 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 que corresponde al S1 en la VLAN 40.

FIGURA 37 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv4 corresponde al S2 en la VLAN 40.

FIGURA 38 se puede evidenciar que el ping del PC –B es exitoso porque la dirección ipv6 que corresponde al S2 en la VLAN 40.

CONCLUSIONES

Asumiendo la importancia para la realización de cada uno de los dos escenarios, se elaboraron todo lo requerido con sus respectivas simulaciones y el desarrollo de sus actividades, se utilizaron las buenas practicas con las normas y las configuraciones estudiadas que nos han de llevar a un nivel de aprendizaje más exigente y en concreto sobre las redes y sus situaciones cotidianas.

En el escenario 1, se realizó la configuración de los dispositivos de una red pequeña. Donde es importante resaltar cada uno de los comandos utilizados para la distribución de: un router, un switch y los equipos, para diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Así mismo para el escenario 2, 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. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

BIBLIOGRAFIA

CASTAÑO,R.j.j y LOPEZ, f.j. Redes locales.Macmillan Iberia S.A. Madrid.{en línea } (2013){26 de noviembre de 2022}Disponible en:
<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=215>

CASTAÑO,R.j. y LOPEZ, f.j. Redes locales.Macmillan Iberia S.A. Madrid.{en línea } (2013){26 de noviembre de 2022} Disponible en:
<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=233>

CASTAÑO, R. r. j., y López, F. J. Redes locales.Macmillan Iberia S.A. Madrid.{en línea } (2013){26 de noviembre de 2022}Disponible en:
<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=193>

PEREZ, Flor. Modelo TCP/IP [OVI].{en línea } (2021){26 de noviembre de2022}Disponible en:
<https://repository.unad.edu.co/handle/10596/43437>

ANEXOS

Anexo a: Enlace de descarga de las simulaciones de los escenarios.

<https://drive.google.com/drive/folders/1E-ZwFBDe1IfWn2Ct0aQVF1QsLGLkCeBV?usp=sharing>