

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

GILBERTO MURCIA RAMOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
LA PLATA HUILA
2021

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

GILBERTO MURCIA RAMOS

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE SISTEMAS

TUTOR:
Msc. RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
LA PLATA HUILA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

La Plata Huila, 1 de diciembre de 2021

AGRADECIMIENTOS

Agradecimientos en primera mediada a Dios por brindarme diariamente la posibilidad de contar con una excelente salud lo que permite trazar metas y darles el cumplimiento adecuado.

Agradecimientos a todos los tutores que me han acompañado en el transcurso de esta carrera brindando siempre lo mejor de ellos para garantizar nuestro aprendizaje.

Agradecimientos muy especiales a mi madre Cecilia Ramos Ricardo y a mi padre Gilberto Murcia Rojas, por brindarme siempre ese apoyo incondicional en todos los proyectos que me he propuesto.

Agradecimientos muy especiales y con mucho amor a mi esposa Marly Lizeth Solano Oteca, por ese apoyo brindado y por ser siempre ese eslabón que me impulsa a seguir adelante en cada uno de los proyectos propuestos.

CONTENIDO

| | |
|------------------------|----|
| AGRADECIMIENTOS..... | 5 |
| CONTENIDO | 6 |
| LISTA DE TABLAS | 7 |
| LISTA DE FIGURAS | 9 |
| GLOSARIO | 10 |
| RESUMEN..... | 11 |
| ABSTRACT | 12 |
| INTRODUCCIÓN | 13 |
| DESARROLLO | 14 |
| Escenario 1 | 14 |
| Escenario 2 | 23 |
| CONCLUSIONES | 59 |
| BIBLIOGRAFÍA..... | 60 |

LISTA DE TABLAS

| | |
|---|----|
| Tabla 1 Direccionamiento | 15 |
| Tabla 2 Tareas de configuración para R1 | 16 |
| Tabla 3 Tareas de configuración de S1 | 19 |
| Tabla 4 Configuración del equipo PC-A | 21 |
| Tabla 5. Configuración del equipo PC-B | 22 |
| Tabla 6 Inicializar y volver a cargar los routers y los switches..... | 24 |
| Tabla 7 Configurar la computadora de Internet..... | 26 |
| Tabla 8 Configurar R1 | 28 |
| Tabla 9 Configurar R2 | 30 |
| Tabla 10 Configurar R3..... | 33 |
| Tabla 11 Configurar S1 | 35 |
| Tabla 12 Configurar S3 | 36 |
| Tabla 13 Verificar la conectividad de la red | 37 |
| Tabla 14 Configurar S1 | 39 |
| Tabla 15 Configurar S3 | 41 |
| Tabla 16 Configurar R1..... | 42 |
| Tabla 17 Verificar la conectividad de la red | 43 |
| Tabla 18 Configurar OSPF en el R1..... | 45 |
| Tabla 19 Configurar OSPF en el R2..... | 46 |
| Tabla 20 Configurar OSPFv3 en el R2 | 47 |
| Tabla 21 Verificar la información de OSPF..... | 48 |

| | |
|--|----|
| Tabla 22 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23..... | 50 |
| Tabla 23 Configurar la NAT estática y dinámica en el R2..... | 51 |
| Tabla 24 Verificar el protocolo DHCP y la NAT estática..... | 53 |
| Tabla 25 Configurar NTP | 55 |
| Tabla 26 Restringir el acceso a las líneas VTY en el R2..... | 56 |
| Tabla 27 Comandos CLI..... | 57 |

LISTA DE FIGURAS

| | |
|---|----|
| Figura 1 Topología de red..... | 14 |
| Figura 2 Topología de red..... | 15 |
| Figura 3 Comando ipconfig /all PC-A..... | 21 |
| Figura 4 Comando ipconfig /all PC-B..... | 22 |
| Figura 5 Topología de red..... | 23 |
| Figura 6 Topología de red..... | 24 |
| Figura 7 Show flash en S1 | 26 |
| Figura 8 Show flash en S2..... | 26 |
| Figura 9 Configurar la computadora de Internet..... | 27 |
| Figura 10 Ping desde R1 a R2, s0/2/0 | 38 |
| Figura 11 Ping desde R2 a R3, s0/2/1 | 38 |
| Figura 12 Ping PC internet a Gateway predeterminado | 39 |
| Figura 13 S1 a R1, dirección VLAN 99..... | 44 |
| Figura 14 S3 a R1, dirección VLAN 99..... | 44 |
| Figura 15 S1 a R1, dirección VLAN 21 | 44 |
| Figura 16 S3 a R1, dirección VLAN 23..... | 45 |
| Figura 17 Comando show ip protocols..... | 49 |
| Figura 18 Comando show ip route ospf..... | 49 |
| Figura 19 Comando show running-config..... | 49 |
| Figura 20 Protocolo DHCP PC-A..... | 53 |
| Figura 21 Protocolo DHCP PC-C..... | 54 |
| Figura 22 Pin PC-A a PC-C... .. | 54 |
| Figura 23 Petición al servidor web..... | 55 |
| Figura 24 Show ntp status... .. | 56 |
| Figura 25 Show access-list en R2... .. | 57 |
| Figura 26 Show ip interface | 58 |
| Figura 27 Show ip interface | 59 |

GLOSARIO

Topología: Tipo y estructura de una red incluyendo la topología física (nodos y cables) y lógica (Flujo de datos).

Local Área Network (LAN): Red que permite la conexión de ordenadores en áreas pequeñas como una oficina, una habitación, etc.

Switch: Dispositivo que permite la conexión de ordenadores y periféricos que permiten la conexión dentro de una misma red.

IPv6: Protocolo de comunicación que enruta tráfico mediante el internet, el cual proporciona sistema de ubicación e identificación en las computadoras que se encuentran dentro de la red.

OSPF: Protocolo de enrutamiento de estado de enlace desarrollado para direcciones IP basado en el algoritmo Shortest Path First (SPF), en una red OSPF los sistemas dentro de la misma área mantienen una base de datos idéntica la que describe la topología.

NAT: Proceso que consiste en cambiar direcciones IP, puertos de origen y destino y permite ocultar los rangos de direcciones privadas, proceso que se realiza mediante enrutadores o firewalls.

RESUMEN

En presente documento cuenta con la solución de 2 escenarios que hacen parte del Diplomado de Profundización CISCO, contempla el desarrollo de dos topologías de redes que consisten en la configuración de dispositivos de una red pequeña, permitiendo el establecimiento de enrutamiento para cada uno de los elementos conectados en donde se realiza mediante conexiones IPV4 y IPv6. Las Ipv4 se caracterizan por utilizar un formato de 32 bits y es un método de direccionamiento numérico mientras que la versión IPv6 un método de direccionamiento alfanumérico, de igual forma ambas permiten la conmutación permitiendo el flujo de información desde el origen hasta el destino requerido.

El desarrollo de los escenarios permite obtener habilidades prácticas en el diagnóstico y soluciones en problemas específicos de redes permitiendo al usuario el conocimiento necesario para una certificación de CCNA (Cisco Certified Networking Associate). Que está diseñada a todo tipo de profesional cercano a los Sistemas, la Electrónica y las Telecomunicaciones.

Palabras clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes.

ABSTRACT

In this document, it has the solution of 2 scenarios that are part of the CISCO Deepening Diploma, it contemplates the development of two network topologies that consist of the device configuration of a small network, allowing the establishment of routing for each of the elements connected where it is done through IPV4 and IPV6 connections. The IPV4 are characterized by using a 32-bit format and it is a numerical addressing method while the IPV6 version an alphanumeric addressing method, in the same way both allow switching allowing the flow of information from the source to the required destination.

The development of the scenarios allows obtaining practical skills in the diagnosis and solutions of specific network problems, allowing the user the necessary knowledge for a CCNA (Cisco Certified Networking Associate) certification. Which is designed for all types of professionals close to Systems, Electronics and Telecommunications.

Keywords: CISCO, CCNA, Switching, Routing, Networks.

INTRODUCCIÓN

El Diplomado de Profundización CISCO, nos prepara para llevar a cabo las diversas configuraciones de dispositivos, mediante la utilización de una herramienta llamada Packet Tracer y laboratorios en Smartlab a la vez con la ayuda de guías que presenta paso a paso las líneas de código para llevarlas a cabo y que funcionen, para esto dispone de una serie de ejercicios prácticos y/o de laboratorio, lo cual permite identificar las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes.

En el presente trabajo se llevara a cabo el desarrollo de 2 ejercicios que buscan lograr que apliquemos lo aprendido durante el diplomado, estos ejercicios están representados como ESCENARIO 1 Y 2, como primera entrega se pretende realizar la configuración de dispositivos de una red pequeña. En donde se configurara un router, un switch y equipos, e igual forma se diseñara un esquema de direccionamiento IPv4 para las LAN propuestas.

Para el SCENARIO 2 encontraremos como se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

DESARROLLO

1. ESCENARIO 1

Topología

Figura 1 Topología de red



Fuente: Guía de actividades

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

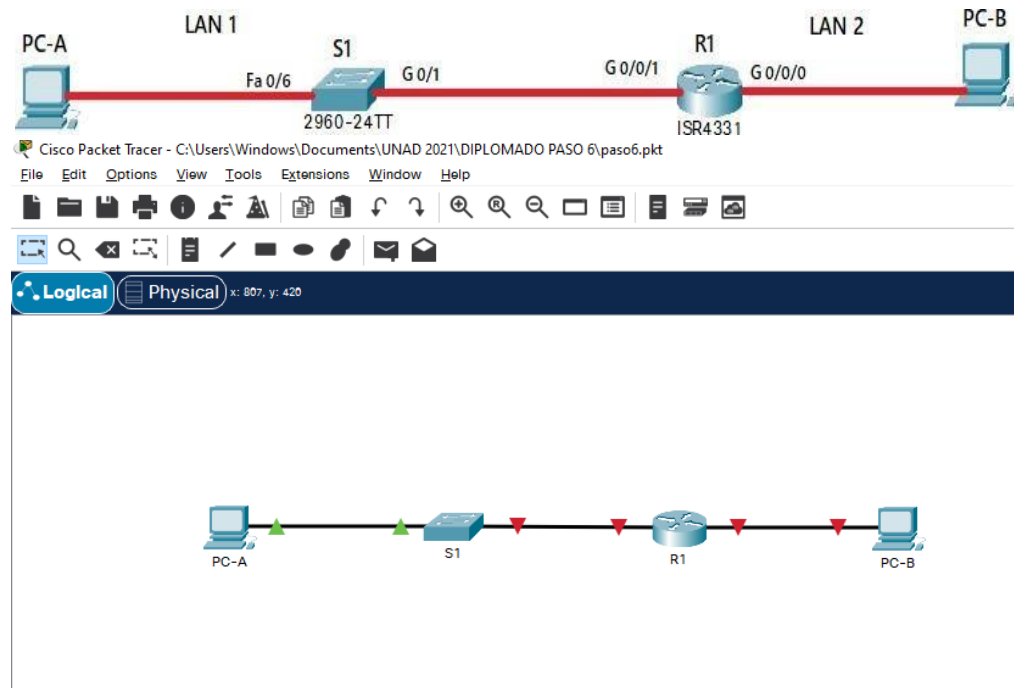
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

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

Creamos la topología en la herramienta de Packet Tracer como se evidencia en la siguiente imagen:

Figura 2 Topología de red



Fuente: Autoría Propia

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 con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1 Direccionamiento

| Item | Requerimiento |
|------------------|--|
| Dirección de Red | 192.168.17.0 /24 Teniendo en cuenta que mi cedula termina en 17 (C.C. 12284217). |

| | |
|-----------------------------------|---|
| Requerimiento de host Subred LAN1 | 100 |
| Requerimiento de host Subred LAN2 | 50 |
| R1 G0/0/1 | Primera dirección de host de la subred LAN1 192.168.17.1 Mascara 255.255.255.128 |
| R1 G0/0/0 | Primera dirección de host de la subred LAN2 192.168.17.129 Mascara 255.255.255.192 |
| S1 SVI | Segunda dirección de host de la subred LAN1 192.168.17.127 |
| PC-A | Última dirección de host de la subred LAN1 192.168.17.126 |
| PC-B | Última dirección de host de la subred LAN2 192.168.17.190 |

Fuente: Guía de actividades

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Tabla 2 Tareas de configuración para R1:

| Tarea | Especificación |
|----------------------------|--|
| Desactivar la búsqueda DNS | Damos clic en R1 seguidamente clic en CLI y damos enter y ingresamos enable para habilitar: Router>enable |

| | |
|--|--|
| | <p>Continuamos con el comando config term para entrar al modo de configuración global: Router#config term</p> <p>Y inhabilitamos la búsqueda DNS utilizamos el comando: Router(config)#no ip domain-lookup</p> |
| Nombre del router | <p>Para asignar nombre a R1 lo hacemos ingresando el siguiente comando: Router(config)#hostname R1</p> <p>Al presionar enter podemos observar que el sistema pasa de Router(config)# a R1(config)#</p> |
| Nombre de dominio | <p>ccna-lab.com</p> <p>Para agregar el nombre de dominio en R1 ingresamos el siguiente comando seguido del nombre: R1(config)#ip domain-name ccna-lab.com</p> |
| Contraseña cifrada para el modo EXEC privilegiado | <p>ciscoenpass</p> <p>Para asignar la contraseña cifrada en modo EXEC privilegiado introducimos el comando: R1(config)#enable secret ciscoenpass</p> |
| Contraseña de acceso a la consola | <p>ciscoconpass</p> <p>para anexar la contraseña de consola ingresamos los siguientes comandos: R1(config)#line console 0 R1(config-line)#password ciscoconpass</p> <p>Y habilitamos el inicio de sesión: R1(config-line)#login</p> |
| Establecer la longitud mínima para las contraseñas | <p>10 caracteres</p> <p>Para establecer el mínimo de longitud en las contraseñas empleamos el comando: R1(config)# security password min-length 10</p> |
| Crear un usuario administrativo en la base de datos local | <p>Nombre de usuario: admin</p> <p>Password: admin1pass</p> <p>Para crear un usuario administrativo en la base de datos local asignamos el siguiente comando: R1(config)# username admin secret admin1pass</p> |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | <p>Ingresamos el comando : R1(config)# line vty 0 15</p> |
| Configurar VTY solo aceptando SSH | <p>Para que VTY solo acepte SSH ingresamos los siguientes comandos: R1(config-line)# privilege level 15 R1(config-line)# login local R1(config-line)# transport input ssh</p> |

| | |
|--|---|
| Cifrar las contraseñas de texto no cifrado | Para cifrar la contraseñas de texto no cifrado introducimos el siguiente comando: R1(config)# service password-encryption |
| Configure un MOTD Banner | Para realizar este proceso requerimos del comando: R1(config)#banner motd #ingeniero el acceso no autorizado está prohibido# |
| Configurar interfaz G0/0/0 | Establecemos la descripción mediante el comando: R1(config)#int g0/0/0 Establecemos la dirección IPv4 introduciendo el siguiente comando: R1(config-if)# ip address 192.167.17.129 255.255.255.192 Activamos la interfaz mediante el comando: R1(config-if)#no shutdown |
| Configurar interfaz G0/0/1 | Establecemos la descripción mediante el comando: R1(config)#int g0/0/1 Establecemos la dirección IPv4 introduciendo el siguiente comando: R1(config-if)#ip address 192.168.17.1 255.255.255.128 Activamos la interfaz mediante el comando: R1(config-if)#no shutdown |
| Generar una clave de cifrado RSA | Módulo de 1024 bits Para generar una clave cifrada en RSA introducimos el siguiente comando: R1(config)#crypto key generate rsa El sistema nos presenta la siguiente descripción: The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. Seguidamente agregamos los 1024 bits: How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] Y finalizamos con un enter: R1(config)# *Mar 1 1:52:46.570: %SSH-5-ENABLED: SSH 1.99 has been enabled |

Fuente: Guía de actividades

Tabla 3 Tareas de configuración de S1

| Tarea | Especificación |
|--|--|
| Desactivar la búsqueda DNS. | Damos clic en S1 seguidamente clic en CLI y damos enter y inhabilitamos la búsqueda DNS utilizamos el comando: Switch(config)#no ip domain-lookup |
| Nombre del switch | S1 Para asignar nombre a S1 lo hacemos ingresando el siguiente comando: Switch(config)#hostname S1 Al presionar enter podemos observar que el sistema pasa de Switch(config)# a S1(config)# |
| Nombre de dominio | ccna-lab.com Para agregar el nombre de dominio en R1 ingresamos el siguiente comando seguido del nombre: S1(config)#ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass Para asignar la contraseña cifrada en modo EXEC privilegiado introducimos el comando: S1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass para anexar la contraseña de consola ingresamos los siguientes comandos: S1(config)#line console 0 S1(configline)#password ciscoconpass |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Password: admin1pass Para crear un usuario administrativo en la base de datos local asignamos el siguiente comando: S1(config)# username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | Ingresamos el comando : S1(config)# line vty 0 15 |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | Para que VTY solo acepte SSH ingresamos los siguientes comandos: S1(config-line)# privilege level 15 S1(config-line)# login local S1(config-line)# transport input ssh |
| Cifrar las contraseñas de texto no cifrado | Para cifrar las contraseñas de texto no cifrado introducimos el siguiente comando: S1(config)# service password-encryption |

| | |
|--|---|
| Configurar un MOTD Banner | Para realizar este proceso requerimos del comando: S1(config)#banner motd #ingeniero el acceso no autorizado está prohibido# |
| Generar una clave de cifrado RSA | Módulo de 1024 bits Para generar una clave cifrada en RSA introducimos el siguiente comando: S1(config)#crypto key generate rsa El sistema nos presenta la siguiente descripción: The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. Seguidamente agregamos los 1024 bits: How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] Y finalizamos con un enter: S1(config)# *Mar 1 1:52:46.570: %SSH-5-ENABLED: SSH 1.99 has been enabled |
| Configurar la interfaz de administración (SVI) | En la configuración de la interface de S1 introducimos los siguientes comandos, creando la vlan conforme a la ip y la máscara: S1(config)#int vlan 1 S1(config-if)#ip address 192.168.17.127 255.255.255.0 S1(config-if)#no shut |
| Configuración del gateway predeterminado | Para configurarla puerta de enlace ingresamos el siguiente comando con relación a la tabla de direccionamiento: S1(config)#ip default-gateway 192.168.17.1 Guardamos la configuración mediante el siguiente comando: S1#copy running-config startup-config |

Fuente: Guía de actividades

Paso 2. Configurar los equipos

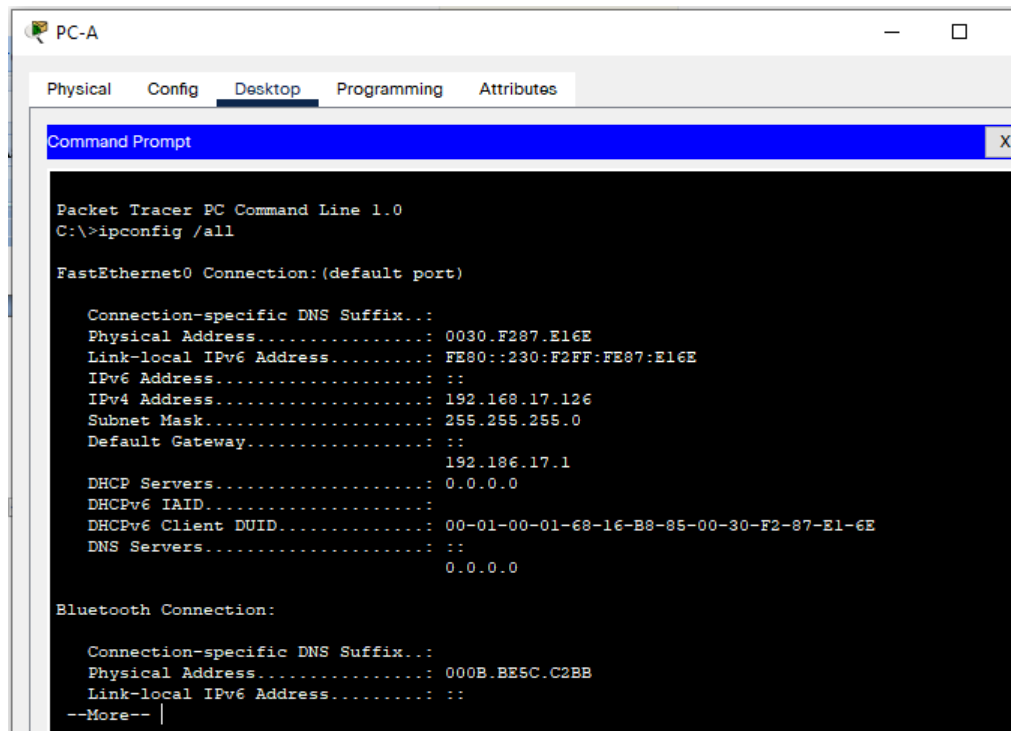
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 4 Configuración del equipo PC-A

| PC-A Network Configuration | |
|----------------------------|---|
| Descripción | Damos clic en el PC-A y vamos la ventana Desktop y damos clic en Command Prompt e ingresamos el comando ipconfig /all el cual nos permite visualizar la dirección física, dirección IP, máscara y el Gateway. |
| Dirección física | Physical Address..... 0030.F287.E16E |
| Dirección IP | IPv4 Address.....: 192.168.17.126 |
| Máscara de subred | Subnet Mask: 255.255.255.0 |
| Gateway predeterminado | Default Gateway:.....:192.168.17.1 |

Fuente: Guía de actividades

Figura 3 comando ipconfig /all PC-A



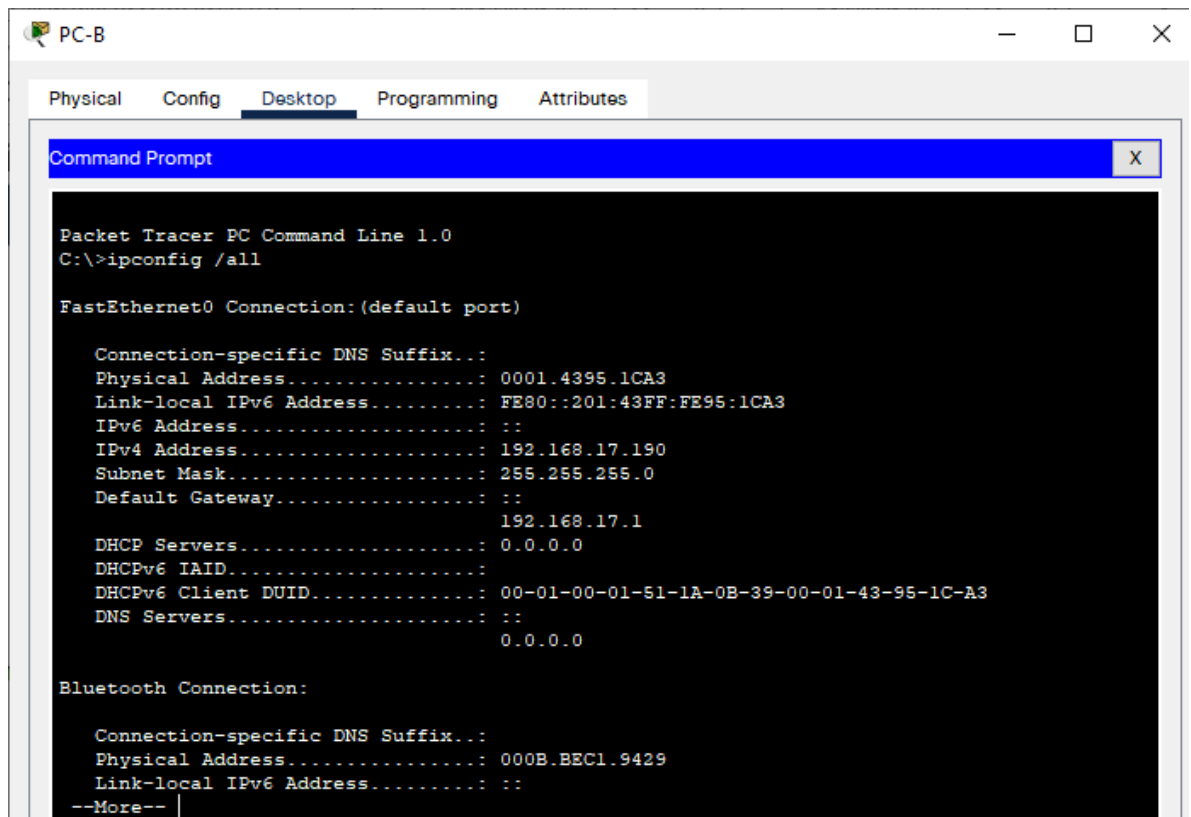
Fuente: Autoría Propia

Tabla 5 Configuración del equipo PC-B:

| PC-B Network Configuration | |
|----------------------------|---|
| Descripción | Damos clic en el PC-B y vamos la ventana Desktop y damos clic en Command Prompt e ingresamos el comando ipconfig /all el cual nos permite visualizar la dirección física, dirección IP, máscara y el Gateway. |
| Dirección física | Physical Address..... 0030.F287.E16E |
| Dirección IP | IPv4 Address.....: 192.168.17.126 |
| Máscara de subred | Subnet Mask: 255.255.255.0 |
| Gateway predeterminado | Default Gateway:.....:192.168.17.1 |

Fuente: Guía de actividades

Figura 4 Comando ipconfig /all PC-B



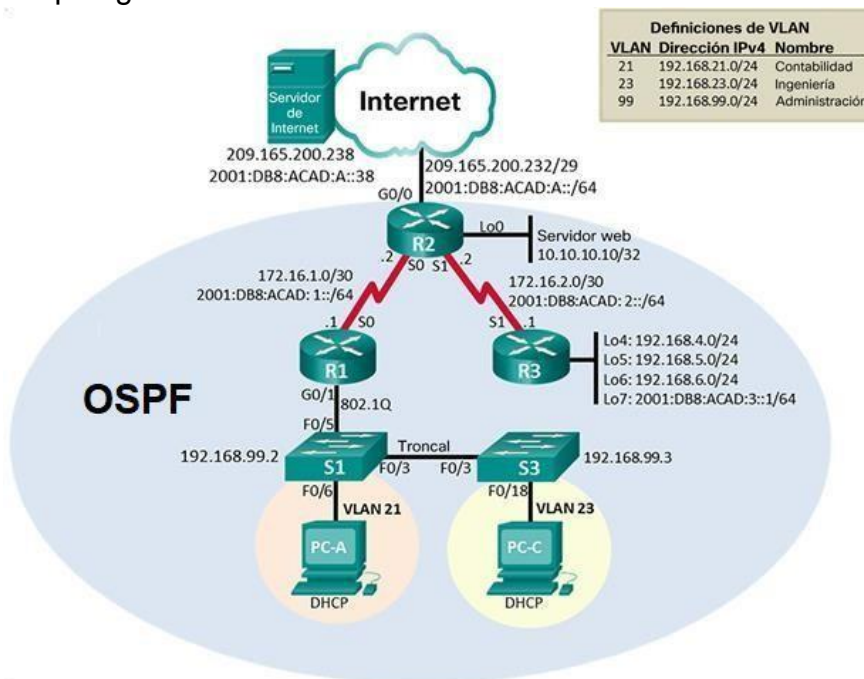
Fuente: Autoría Propia

2. ESCENARIO 2

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

Topología

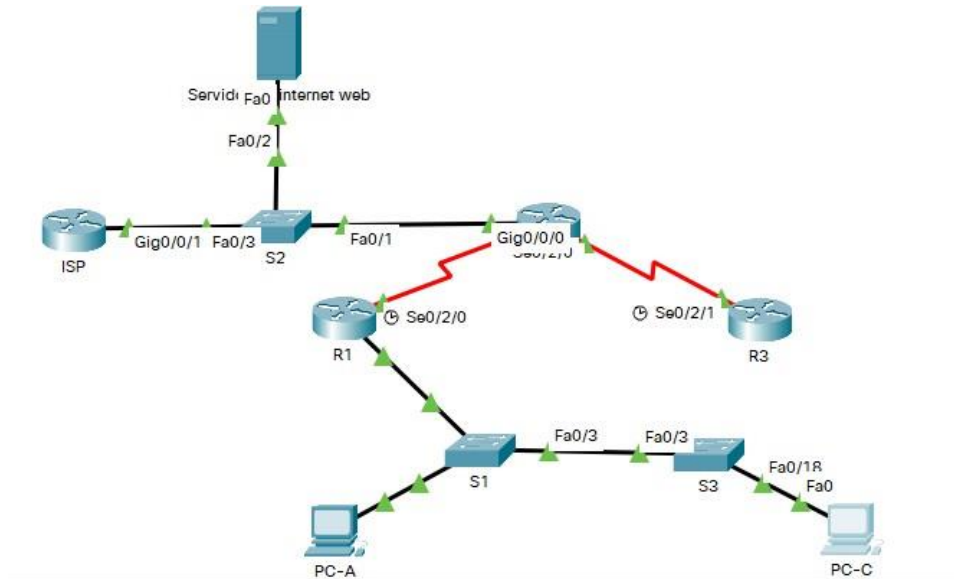
Figura 5 Topología de red



Fuente: Guía de actividades

Como primera medida realizamos la topología en la herramienta Packet Tracer, como se evidencia en la siguiente imagen:

Figura 6 Topología de red



Fuente: Autoría Propia

Parte 1: Inicializar dispositivos.

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6 Inicializar y volver a cargar los routers y los switches

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | <p>Para este proceso es necesario dar clic en el routers a intervenir (R1, R2, R3), posteriormente ingresamos a la ventana de CLI, presionamos enter y continuamos con el ingreso de los comandos:</p> <pre>Router>enable Router#erase startup-config</pre> <p>Al insertar el comando el sistema pide confirmación para borrar el archivo de configuración de inicio, para esto presionamos la tecla enter.</p> <pre>Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete</pre> |

| | |
|---|---|
| | %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram |
| Volver a cargar todos los routers | Para volver a cargar los routers (R1, R2, R3) lo hacemos mediante el comando reload: Router#reload Al insertar el comando reload nos pide que confirmemos, lo cual lo hacemos mediante un enter. Proceed with reload? [confirm] Seguidamente el sistema inicia la carga. |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Para este proceso es necesario dar clic en el switches a intervenir (S1,S3), posteriormente ingresamos a la ventana de CLI, presionamos enter y continuamos con el ingreso de los comandos: Switch>enable Switch#erase startup-config Al insertar el comando el sistema pide confirmación para borrar el archivo de configuración de inicio, para esto presionamos la tecla enter. 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 Continuamos a eliminar la base de datos de VLAN mediante el comando delete velan.dat: Switch#delete velan.dat Nos indica que confirmemos, lo cual lo hacemos mediante enter: Delete filename [velan.dat]? Delete flash:/velan.dat? [confirm] %Error deleting flash:/velan.dat (No such file or directory) |
| Volver a cargar ambos switches | Para volver a cargar los switches (S1, S3) lo hacemos mediante el comando reload: Switch#reload Al insertar el comando reload nos pide que confirmemos, lo cual lo hacemos mediante un enter. Proceed with reload? [confirm] Seguidamente el sistema inicia la carga. |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | Para verificar este proceso usamos el comando show flash: Switch#show flash Directory of flash:/' |

| | |
|--|--|
| | <pre>1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) En donde podemos observar el archivo no está.</pre> |
|--|--|

Fuente: Guía de actividades

S1

Figura 7 Show flash en S1

```
Switch>
Switch>show flash
Directory of flash:/

 1 -rw-      4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch>
```

Ctrl+F6 to exit CLI focus Copy

Fuente: Autoría Propia

S2

Figura 8 Show flash en S2

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

Switch>
Switch>show flash
Directory of flash:/

 1 -rw-      4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch>
```

Ctrl+F6 to exit CLI focus Copy Paste

Fuente: Autoría Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

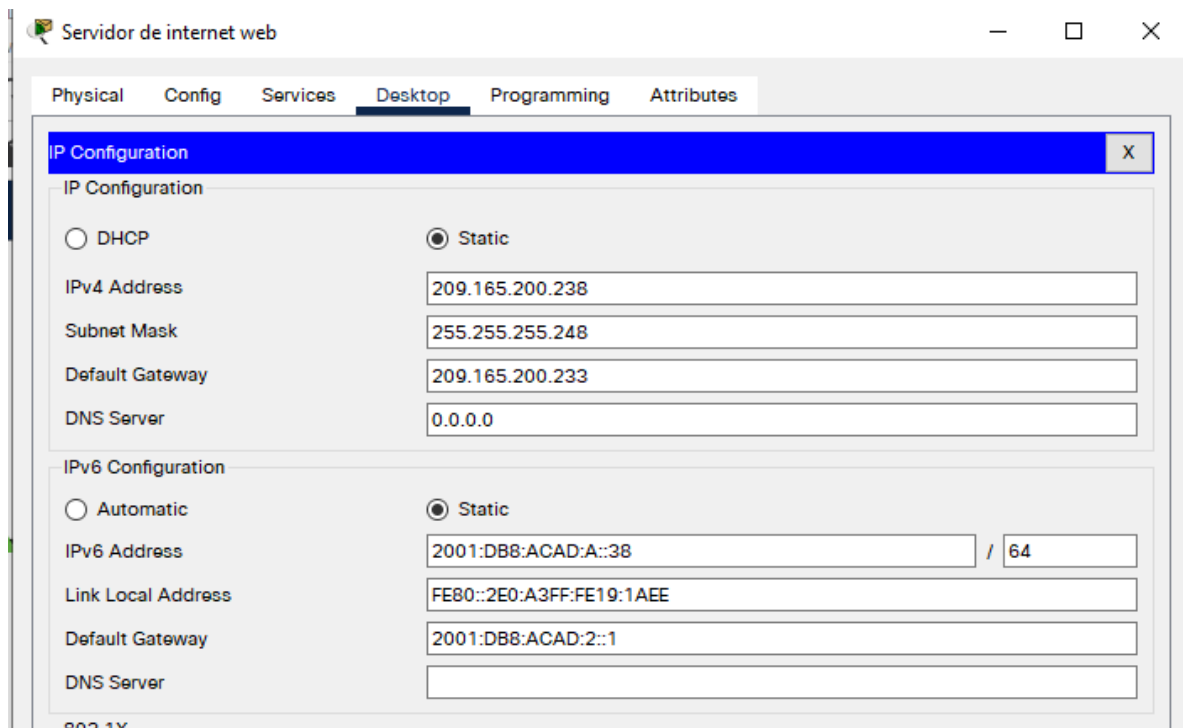
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 7 Configurar la computadora de Internet

| Elemento o tarea de configuración | Especificación |
|-----------------------------------|---|
| Dirección IPv4 | 209.165.200.238 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.225 Este dato lo cambiamos debido a la dirección de ip de la topología y solicitud que se realiza más adelante en la configuración del router R2. 209.165.200.233 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:2::1 |

Fuente: Guía de actividades

Figura 9 Configurar la computadora de Internet



Fuente: Autoría Propia

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8 Configurar R1

| Elemento o tarea de configuración | Especificación |
|--|--|
| Desactivar la búsqueda DNS | Utilizamos el comando #no ip domain-lookup. Damos clic en R1 y vamos a la ventana de CLI, damos enter e ingresamos el comando: Router>enable Router#config term Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup |
| Nombre del router | R1 Para el nombre del router usamos el comando #hostname R1: Router(config)#hostname R1 Si observamos el sistema cambia inmediatamente de Router(config)# a: R1(config)# |
| Contraseña de ejecución privilegiado cifrada | class Ingresamos el comando #enable secret class con la contraseña: R1(config)#enable secret class |
| Contraseña de acceso a la consola | cisco Ingresamos los comandos: #line console 0, #password más la contraseña: R1(config)#line console 0 R1(config-line)#password cisco Agregamos el comando #login para requerir autenticación al iniciar sesión: R1(config-line)#login R1(config-line)#exit R1(config)#exit |
| Contraseña de acceso Telnet | cisco Ingresamos los comandos: #line vty 04, #password más la contraseña: |

| | |
|--|--|
| | <p>R1(config)#line vty 04 R1(config-line)#password cisco Agregamos el comando #login para requerir autenticación al iniciar sesión: R1(config-line)#login R1(config-line)#exit</p> |
| Cifrar las contraseñas de texto no cifrado | <p>Ingresamos el comando: #service password-encryption: R1(config)#service password-encryption</p> |
| Mensaje MOTD | <p>Se prohíbe el acceso no autorizado. Para este proceso utilizamos el comando #banner motd, más el mensaje: R1(config)#banner motd # Se prohíbe el acceso no autorizado.#</p> |
| Interfaz S0/0/0 | <p>En esta instancia al momento de realizar el proceso de la conexión del puerto serial quedo establecido s0/2/0, teniendo en cuenta esto comenzamos la configuración mediante los comandos: R1(config)#interface s0/2/0 Realizamos la descripción mediante el comando: R1(config-if)#description connect to R2 Establecemos la dirección IPv4 con relación al diagrama de topología mediante el comando: R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecemos la dirección IPv6 según la topología mediante el comando: R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 Para establecer la frecuencia del reloj en 128000 usamos el comando: R1(config-if)#clock rate 128000 Activamos la interface mediante el comando R1(config-if)#no shutdown</p> |
| Rutas predeterminadas | <p>Configuración de rutas IPv4 y IPv6 predeterminadas de S0/2/0, mediante los comandos: R1(config)#ip route 0.0.0.0.0.0.0.0 s0/2/0 R1(config)#ipv6 route ::1/64 s0/2/0</p> |

Fuente: Guía de actividades

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9 Configurar R2

| Elemento o tarea de configuración | Especificación |
|---|--|
| Desactivar la búsqueda DNS | Utilizamos el comando #no ip domain-lookup. Damos clic en R2 y vamos a la ventana de CLI, damos enter e ingresamos el comando: Router>enable Router#config term Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup |
| Nombre del router | R2 Para el nombre del router usamos el comando #hostname R2: Router(config)#hostname R2 Si observamos el sistema cambia inmediatamente de Router(config)# a: R2(config)# |
| Contraseña de exec privilegiado cifrada | class Ingresamos el comando #enable secret class con la contraseña: R2(config)#enable secret class |
| Contraseña de acceso a la consola | cisco Ingresamos los comandos: #line console 0, #password más la contraseña: R2(config)#line console 0 R2(config-line)#password cisco Agregamos el comando #login para requerir autenticación al iniciar sesión: R2(config-line)#login R2(config-line)#exit R2(config)#exit |
| Contraseña de acceso Telnet | cisco Ingresamos los comandos: #line vty 04, #password |

| | |
|--|--|
| | <p>más la contraseña: R2(config)#line vty 04 R2(config-line)#password cisco Agregamos el comando #login para requerir autenticación al iniciar sesión: R2(config-line)#login R2(config-line)#exit</p> |
| Cifrar las contraseñas de texto no cifrado | <p>Ingresamos el comando: #service password-encryption: R2(config)#service password-encryption</p> |
| Habilitar el servidor HTTP | <p>Proceso que se realiza mediante el comando ip http-server, pero Packet tracer no soporta la habilitación de un router como servidor HTTP. R2(config)# ip http-server</p> |
| Mensaje MOTD | <p>Se prohíbe el acceso no autorizado. Para este proceso utilizamos el comando #banner motd, mas el mensaje: R2(config)#banner motd # Se prohíbe el acceso no autorizado.#</p> |
| Interfaz S0/0/0 | <p>En esta instancia al momento de realizar el proceso de la conexión del puerto serial quedo establecido s0/2/0, teniendo en cuenta esto comenzamos la configuración mediante los comandos: R2(config)#interface s0/2/0 Realizamos la descripción mediante el comando: R2(config-if)#description connect to R1 Establecemos la dirección IPv4 con relación al diagrama de topología mediante el comando: R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establecemos la dirección IPv6 según la topología mediante el comando: R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 Activamos la interface mediante el comando: R2(config-if)#no shutdown</p> |
| Interfaz S0/0/1 | <p>En esta instancia al momento de realizar el proceso de la conexión del puerto serial quedo establecido s0/2/1, teniendo en cuenta esto comenzamos la configuración mediante los comandos: R2(config)#interface s0/2/1</p> |

| | |
|--|---|
| | <p>Realizamos la descripción mediante el comando: R2(config-if)#description connect to R3 Establecemos la dirección IPv4 con relación al diagrama de topología mediante el comando: R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establecemos la dirección IPv6 según la topología mediante el comando: R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 Para establecer la frecuencia del reloj en 128000 usamos el comando: R2(config-if)#clock rate 128000 Activamos la interface mediante el comando: R2(config-if)#no shutdown</p> |
| <p>Interfaz G0/0 (simulación de Internet)</p> | <p>Realizamos la descripción mediante el comando: R2(config)#interface g0/0/0 R2(config-if)# description connect to Internet Establecemos la dirección IPv4 con relación al diagrama de topología mediante el comando: R2(config-if)# ip address 209.165.200.233 255.255.255.248 Establecemos la dirección IPv6 según la topología mediante el comando: R2(config-if)# ipv6 address 2001:db8:acad:a:: 233/64 Esta es la nueva R2(config-if)#ipv6 address 2001:DB8:ACAD:A::38/64 Activamos la interface mediante el comando: R2(config-if)# no shutdown</p> |
| <p>Interfaz loopback 0 (servidor web simulado)</p> | <p>Establecer la descripción. Establezca la dirección IPv4. R2(config)#interface loopback 0 R2(config-if)#description loopback 0 Servidor Web R2(config-if)#ip address 10.10.10.10 255.255.255.255</p> |

| | |
|---------------------|---|
| Ruta predeterminada | Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0.0.0.0.0 g0/0/0 R2(config)#ipv6 route ::1/64 g0/0/0 |
|---------------------|---|

Fuente: Guía de actividades

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10 Configurar R3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Utilizamos el comando #no ip domain-lookup. Damos clic en R3 y vamos a la ventana de CLI, damos enter e ingresamos el comando: Router>enable Router#config term Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup |
| Nombre del router | R3 Para el nombre del router usamos el comando #hostname R3: Router(config)#hostname R3 Si observamos el sistema cambia inmediatamente de Router(config)# a: R3(config)# |
| Contraseña de exec privilegiado cifrada | class Ingresamos el comando #enable secret class con la contraseña: R3(config)#enable secret class |
| Contraseña de acceso a la consola | cisco Ingresamos los comandos: #line console 0, #password mas la contraseña: R3(config)#line console 0 R3(config-line)#password cisco Agregamos el comando #login para requerir |

| | |
|--|--|
| | <p>autenticación al iniciar sesión:</p> <pre>R3(config-line)#login R3(config-line)#exit R3(config)#exit</pre> |
| Contraseña de acceso Telnet | <p>cisco</p> <p>Ingresamos los comandos: #line vty 04, #password mas la contraseña:</p> <pre>R3(config)#line vty 04 R3(config-line)#password cisco</pre> <p>Agregamos el comando #login para requerir autenticación al iniciar sesión:</p> <pre>R3(config-line)#login R3(config-line)#exit</pre> |
| Cifrar las contraseñas de texto no cifrado | <p>Ingresamos el comando: #service password-encryption:</p> <pre>R3(config)#service password-encryption</pre> |
| Mensaje MOTD | <p>Se prohíbe el acceso no autorizado. Se prohíbe el acceso no autorizado.</p> <p>Para este proceso utilizamos el comando #banner motd, más el mensaje:</p> <pre>R3(config)#banner motd # Se prohíbe el acceso no autorizado.#</pre> |
| Interfaz S0/0/1 | <p>En esta instancia al momento de realizar el proceso de la conexión del puerto serial quedo establecido s0/2/1, teniendo en cuenta esto comenzamos la configuración mediante los comandos:</p> <pre>R3(config)#interface s0/2/1</pre> <p>Realizamos la descripción mediante el comando:</p> <pre>R3(config-if)#description connect to R2</pre> <p>Establecemos la dirección IPv4 con relación al diagrama de topología mediante el comando:</p> <pre>R3(config-if)#ip address 172.16.2.1 255.255.255.252</pre> <p>Establecemos la dirección IPv6 según la topología mediante el comando:</p> <pre>R3(config-if)#ipv6 address 2001:db8:acad:2::1/64</pre> |

| | |
|---------------------|---|
| | Activamos la interface mediante el comando: R3(config-if)#no shutdown |
| Interfaz loopback 4 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 |
| Interfaz loopback 5 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface loopback 5 R3(config-if)# R3(config-if)#ip address 192.168.5.1 255.255.255.0 |
| Interfaz loopback 6 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface loopback 6 R3(config-if)# R3(config-if)#ip address 192.168.6.1 255.255.255.0 |
| Interfaz loopback 7 | Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config)#ip route 0.0.0.0.0.0.0.0 s0/2/1 R3(config)#ipv6 route ::1/64 s0/2/1 |

Fuente: Guía de actividades

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11 Configurar S1

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

| | |
|--|---|
| | Switch(config)#hostname S1 |
| Contraseña de exec privilegiado cifrada | class S1(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 |
| Contraseña de acceso Telnet | cisco S1(config)#line vty 04 S1(config-line)#password cisco S1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | S1(config)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. S1(config)#banner motd #Se prohíbe el acceso no autorizado.# |

Fuente: Guía de actividades

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12 Configurar S3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch>enable Switch#config term Switch(config)#no ip domain-lookup |
| Nombre del switch | S3 Switch(config)#hostname S3 |
| Contraseña de exec privilegiado cifrada | class S3(config)#enable secret class |
| Contraseña de acceso a la consola | cisco S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit |
| Contraseña de acceso Telnet | cisco S3(config)#line vty 04 |

| | |
|--|---|
| | S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S3(config)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. S3(config)#banner motd #Se prohíbe el acceso no autorizado.# |

Fuente: Guía de actividades

Paso 7: Verificar la conectividad de la red

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

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

Tabla 13 Verificar la conectividad de la red.

| Desde | A | Dirección IP | Resultados de ping |
|----------------|------------------------|--------------------------|--|
| R1 | R2, S0/2/0 | R1#ping 172.16.1.2 | Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms |
| R2 | R3, S0/2/1 | R2#ping 172.16.2.1 | Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/21 ms |
| PC de Internet | Gateway predeterminado | C:\>ping 209.165.200.233 | Reply from 209.165.200.233: bytes=32 time=1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 |

| | | | |
|--|--|--|---|
| | | | Reply from 209.165.200.233: bytes=32 time=20ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 20ms, Average = 5ms |
|--|--|--|---|

Fuente: Guía de actividades

R1 a R2, S0/0/0

Figura 10 ping desde R1 a R2, s0/2/0

```

Password:
R1#
R1#
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/19 ms

```

Fuente: Autoría Propia

R2 a R3, S0/0/1

Figura 11 ping desde R2 a R3, s0/2/1

```

R2#
R2#
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
R2#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Autoría Propia

PC de Internet a Gateway predeterminado

Figura 12 ping PC internet a Gateway predeterminado

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time=1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time=20ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 5ms

C:\>
```

Fuente: Autoría Propia

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14 Configurar S1

| Elemento o tarea de configuración | Especificación |
|-----------------------------------|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administración S1(config-vlan)#exit |

| | |
|---|--|
| Asignar la dirección IP de administración. | <p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología</p> <p>Se coloca 99.2 ya que la 1 la usaremos en el routers</p> <pre>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0</pre> |
| Asignar el gateway predeterminado | <p>Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.</p> <p>La primera es 99.1</p> <pre>S1(config)#ip default-gateway 192.168.99.1</pre> |
| Forzar el enlace troncal en la interfazF0/3 | <pre>S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk</pre> <p>Utilizar la red VLAN 1 como VLAN nativa</p> <pre>S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre> |
| Forzar el enlace troncal en la interfazF0/5 | <pre>S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk</pre> <p>Utilizar la red VLAN 1 como VLAN nativa</p> <pre>S1(config-if)#switchport trunk native vlan 1</pre> |
| Configurar el resto de los puertos como puertos de acceso | <p>Utilizar el comando interface range</p> <pre>S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)# switchport mode access S1(config-if-range)#exit</pre> |
| Asignar F0/6 a la VLAN 21 | <pre>S1(config)#interface f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#exit</pre> |
| Apagar todos los puertos sin usar | <pre>S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#sh</pre> |

Fuente: Guía de actividades

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15 Configurar S3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | <p>Creamos cada una de las VLAN indicadas en la topología mediante los comandos:</p> <pre>S3#config term S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion</pre> |
| Asignar la dirección IP de administración | <p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología. Asignamos la IP 192.168.99.3 porque la 99.2 la tiene el S1 y la .1 será para los routers.</p> <pre>S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0</pre> |
| Asignar el gateway predeterminado. | <p>Asignar la primera dirección IP en la subred como gateway predeterminado.</p> <pre>S3(config)#ip default-gateway 192.168.99.1</pre> |
| Forzar el enlace troncal en la interfaz F0/3 | <pre>S3(config)#interface f0/3 S3(config-if)#switchport mode trunk</pre> <p>Utilizar la red VLAN 1 como VLAN nativa</p> <pre>S3(config-if)#switchport trunk native vlan 1</pre> |
| Configurar el resto de los puertos como puertos de acceso | <p>Utilizar el comando interface range</p> <pre>S3(config)#interface range f0/1-2, f0/4-24, g0/1 -2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit</pre> |
| Asignar F0/18 a la VLAN 21 | <pre>S3(config)#interface f0/18 S3(config-if)#switchport access vlan 21</pre> |
| Apagar todos los puertos sin usar | <pre>S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#sh</pre> |

Fuente: Guía de actividades

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 Configurar R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 enG0/1 | <p>Descripción: LAN de Contabilidad Asignar la VLAN 21</p> <p>Asignar la primera dirección disponible a esta interfaz</p> <pre>R1(config)#interface g0/0/1.21 R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit</pre> |
| Configurar la subinterfaz 802.1Q .23 enG0/1 | <p>Descripción: LAN de Ingeniería Asignar la VLAN 23</p> <p>Asignar la primera dirección disponible a esta interfaz</p> <pre>R1(config)#interface g0/0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit</pre> |
| Configurar la subinterfaz 802.1Q .99 enG0/1 | <p>Descripción: LAN de Administración Asignar la VLAN 99</p> <p>Asignar la primera dirección disponible a esta interfaz</p> <pre>R1(config)#interface g0/0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit</pre> |
| Activar la interfaz G0/1 | <pre>R1(config)#interface g0/0/1 R1(config-if)#no sh</pre> |

| | |
|--|--|
| | Podemos observar que la conexión aparece encendida |
|--|--|

Fuente: Guía de actividades

Paso 4: Verificar la conectividad de la red

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

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

Tabla 17 Verificar la conectividad de la red

| Desde | A | Dirección IP | Resultados de ping |
|-------|-----------------------|--------------|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.0, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms |
| S3 | R1, dirección VLAN 23 | 192.168.23.1 | Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms |

Fuente: Guía de actividades

S1 a R1, dirección VLAN 99

Figura 13 S1 a R1, dirección VLAN 99

```
S1#
S1#ping 192.168.99.1

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

S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#
```

Ctrl+F6 to exit CLI focus Copy Pas

Fuente: Autoría Propia

S3 a R1, dirección VLAN 99

Figura 14 S3 a R1, dirección VLAN 99

```
S3#
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

S3#
```

Ctrl+F6 to exit CLI focus Copy

Fuente: Autoría Propia

S1 a R1, dirección VLAN 21

Figura 15 S1 a R1 dirección VLAN 21

```
S1#
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#
```

Ctrl+F6 to exit CLI focus Copy Paste

Fuente: Autoría Propia

S3 a R1, dirección VLAN 23

Figura 16 S3 a R1, dirección VLAN 23

```
S3#
S3#
S3#ping 192.168.23.1

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

S3#
```

Ctrl+F6 to exit CLI focus Copy

Fuente: Autoría Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 Configurar OSPF en el R1

| Elemento o tarea de configuración | Especificación |
|--|--|
| Configurar OSPF área 0 | R1(config)#router ospf 17 |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente. R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)# network 172.16.1.0 0.0.0.3 area 0 |
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface g0/0/1 R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99 |

| | |
|--------------------------------------|--|
| | R1(config-router)#exit |
| Desactive la sumarización automática | No se puede realizar, OSPF no sumariza |

Fuente: Guía de actividades

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19 Configurar OSPF en el R2

| Elemento o tarea de configuración | Especificación |
|---|--|
| Configurar OSPF área 0 | R2#config term R2(config)#router ospf 17 |
| Anunciar las redes conectadas directamente | Nota: Omitir la red G0/0 R2(config)#router ospf 17 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config-router)#passive-interface loopback 0 R2(config-router)#exit R2(config-router)#passive-interface loopback 0 R2(config-router)#ipv6 router ospf 18 R2(config-rtr)#router-id 1.1.1.1 R2(config-rtr)#exit |
| Desactive la sumarización automática. | La sumarización automática no se puede realizar en este sistema de enrutamiento solo se hace en RIP y en EIGRP |

Fuente: Guía de actividades

Paso 3: Configurar OSPFv3 en el R2

OSPFv3 es el protocolo de enrutamiento Open Shortest Path First para IPv6 no para redes ipv4 además de acuerdo a las indicaciones dadas en la web conferencia existe error en la guía, por tal razón la configuración de las interfaces se deben hacer de la siguiente manera:

```
R2(config)#
R2(config)#interface s0/2/0
R2(config-if)#ipv6 ospf 18 area 0
R2(config-if)#exit
```

```
R2(config)#interface s0/2/1
R2(config-if)#ipv6 ospf 18 area 0
R2(config-if)#exit
```

```
R2(config)#interface g0/0/0
R2(config-if)#ipv6 ospf 18 area 0
R2(config-if)# exit
```

La configuración del R3 incluye las siguientes tareas:

Tabla 20 Configurar OSPFv3 en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2#config term R2(config)#router ospf 17 |
| Anunciar redes IPv4 conectadas directamente | R2(config)#router ospf 17 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 48 R3(config-rtr)#router-id 2.2.2.2 R3(config-rtr)#exit R3(config)#interface s0/2/1 R3(config-if)#ipv6 ospf 48 area 0 R3(config-if)#exit R3(config)# 01:01:59: %OSPFv3-5-ADJCHG: |

| | |
|---|---|
| | <pre> Process 48, Nbr 1.1.1.1 on Serial0/2/1 from LOADING to FULL, Loading Done R3(config)#ipv6 router ospf 48 R3(config-rtr)#passive-interface loopback 4 R3(config-rtr)#passive-interface loopback 5 R3(config-rtr)#passive-interface loopback 6 R3(config-rtr)#exit </pre> |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | Loopback no cuenta con direcciones sobre IPv6. |
| Desactive la sumarización automática. | Este protocolo se realiza mediante la wildcard y en IPv6 no se hace. |

Fuente: Guía de actividades

Paso 4: Verificar la información de OSPF

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

Tabla 21 Verificar la información de OSPF

| Pregunta | Respuesta |
|---|---|
| ¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router? | Este proceso se realiza mediante el comando <code>show ip protocols</code> |
| ¿Qué comando muestra solo las rutas OSPF? | El comando <code>show ip route ospf</code> nos permite mirar las rutas OSPF |
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución? | El comando <code>show running-config</code> |

Fuente: Guía de actividades

Comando show ip protocols

Figura 17 Comando show ip protocols

```
R2#
R2#show ip protocols
Routing Protocol is "ospf 17"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
  10.10.10.10       110           00:21:03
  192.168.99.1      110           00:21:03
  Distance: (default is 110)
```

Fuente: Autoría Propia

Comando show ip route ospf

Figura 18 Comando show ip route ospf

```
-----
R2#
R2#
R2#
R2#show ip route ospf
O   192.168.21.0 [110/65] via 172.16.1.1, 00:19:41, Serial0/2/0
O   192.168.23.0 [110/65] via 172.16.1.1, 00:19:41, Serial0/2/0
O   192.168.99.0 [110/65] via 172.16.1.1, 00:19:41, Serial0/2/0

R2#
R2#
R2#
```

Fuente: Autoría Propia

Comando show running-config

Figura 19 Comando show running-config

```
interface Vlan1
  no ip address
  shutdown
!
router ospf 17
  log-adjacency-changes
  passive-interface Loopback0
  network 10.10.10.10 0.0.0.0 area 0
  network 172.16.1.0 0.0.0.3 area 0
  network 172.16.2.0 0.0.0.3 area 0
!
ipv6 router ospf 48
  router-id 1.1.1.1
  log-adjacency-changes
  passive-interface Loopback0
!
ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.233
ip nat inside source static 10.10.10.10 209.165.200.234
ip classless
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0/0
ipv6 route ::/64 GigabitEthernet0/0/0
!
ip access-list standard ADMIN-MGT
  permit host 172.16.1.1
  deny any
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
access-list 1 permit 192.168.4.0 0.0.3.255
```

Fuente: Autoría Propia

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

| Elemento o tarea de configuración | Especificación |
|--|--|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | R1#config term R1(config)#service dhcp R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 |
| Crear un pool de DHCP para la VLAN 21. | Nombre: ACCT R1(config)#ip dhcp pool ACCT R1(dhcp-config)# network 192.168.21.1 255.255.255.0 R1(config)#ip dhcp pool ACCT R1(dhcp-config)# network 192.168.21.0 255.255.255.0 Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com R1(dhcp-config)#dns-server 10.10.10.10 Este proceso no se puede realizar en packet tracer sin embargo comparto el comando como se debería realizar. R1(dhcp-config)# domain-name ccna-sa.com Establecer el gateway predeterminado R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#exit R1(dhcp-config)#default-router 192.168.21.0 R1(dhcp-config)#exit |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGR R1(config)#ip dhcp pool ENGR R1(dhcp-config)# network 192.168.23.1 255.255.255.0 R1(dhcp-config)# NETWORK 192.168.23.0 255.255.255.0 |

| | |
|--|--|
| | <p>Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com</p> <pre>R1(dhcp-config)#dns-server 10.10.10.10</pre> <p>Este proceso no se puede realizar en packet tracer sin embargo comparto el comando como se debería realizar.</p> <pre>R1(dhcp-config)# domain-name ccna-sa.com</pre> <p>Establecer el gateway predeterminado</p> <pre>R1(dhcp-config)#default-router 192.168.23.1</pre> <pre>R1(dhcp-config)#exit</pre> |
|--|--|

Fuente: Guía de actividades

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23 Configurar la NAT estática y dinámica en el R2

| Elemento o tarea de configuración | Especificación |
|---|--|
| <p>Crear una base de datos local con unacuenta de usuario</p> | <p>Para poder crear la NAT se requiere la creación de un nuevo router y switch ya que la topología inicial no contaba con esta parte.</p> <p>Switch lo registramos como S2 ya que contábamos con el 1 y el 3, procedemos a realizar una configuración:</p> <pre>Switch#configure term</pre> <p>Enter configuration commands, one per line. End with CNTL/Z.</p> <pre>Switch(config)#hostname S2</pre> <pre>S2(config)#exit</pre> <p>Configuramos el Router:</p> <pre>ISP</pre> <pre>Router>enable</pre> <pre>Router#config term</pre> <p>Enter configuration commands, one per line. End with CNTL/Z.</p> <pre>Router(config)#hostname ISP</pre> <pre>ISP(config)#interface g0/0/1</pre> <pre>ISP(config-if)#ip address 209.165.200.237 255.255.255.248</pre> |

| | |
|--|--|
| | <pre>ISP(config-if)#no sh ISP(config-if)#exit Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2#config term R2(config)#username webuser privilege 15 password cisco12345</pre> |
| Habilitar el servicio del servidor HTTP | <pre>Para este proceso usamos el comando ip http server, pero este no funciona en packet tracer R2(config)#ip http server</pre> |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | <pre>Packet tracer no permite este proceso de igual manera les comparto como seria la aplicación del comando: R2(config)#ip http authentication local</pre> |
| Crear una NAT estática al servidor web. | <pre>Dirección global interna: 209.165.200.229 Dirección global externa: 209.165.200. 237 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237</pre> |
| Asignar la interfaz interna y externa para la NAT estática | <pre>R2(config)#interface g0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#interface g0/0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/2/0 R2(config-if)#ip nat inside R2(config-if)#int s0/2/1 R2(config-if)#ip nat inside</pre> |
| Configurar la NAT dinámica dentro de una ACL privada | <pre>Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN(loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255</pre> |

| | |
|---|---|
| | R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 |
| Defina el pool de direcciones IP públicasutilizables. | Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

Fuente: Guía de actividades

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 24 Verificar el protocolo DHCP y la NAT estática

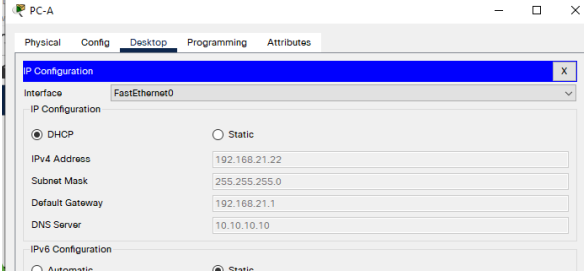
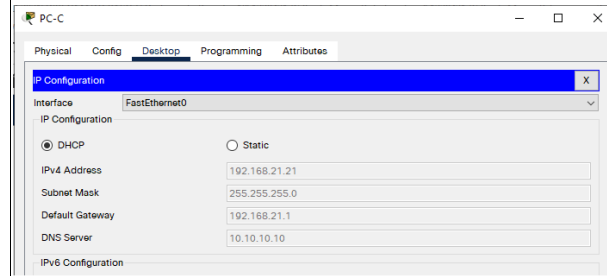
| Prueba | Resultados |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | <p>Ipv4 Address 192.168.21.22 Subnet Mask 255.255.255.0</p> <p>Figura 20 Protocolo DHCP PC-A</p>  |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | <p>Ipv4 Address 192.168.21.21 Subnet Mask 255.255.255.0</p> |

Figura 21 Protocolo DHCP PC-C



Fuente: Autoría Propia

Verificar que la PC-A pueda hacer ping ala PC-C

Nota: Quizá sea necesario deshabilitar elfirewall de la PC.

```
C:\>ping 192.168.21.22
```

```
C:\>ping 192.168.21.22
```

```
Pinging 192.168.21.22 with 32 bytes of data:
```

```
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.21.22: bytes=32 time=11ms TTL=128
```

```
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.21.22: bytes=32 time=1ms TTL=128
```

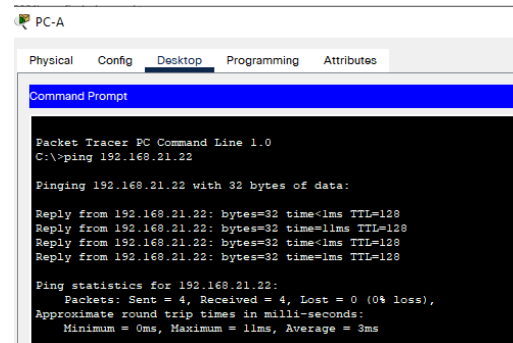
```
Ping statistics for 192.168.21.22:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```


```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Figura 22 Pin PC-A a PC-C



Fuente: Autoría Propia

| | |
|--|---|
| <p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p> | <p>Recordemos que Packet Tracer no soporta un servidor http por eso en el paso anterior se anunció como se haría mas no se pudo aplicar.</p> <p>Para verificación usamos la ip 209.165.200.338</p> <p>Figura 23 Petición al servidor</p>  <p>Fuente: Autoría Propia</p> |
|--|---|

Fuente: Guía de actividades

Parte 6: Configurar NTP

Tabla 25 Configurar NTP.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | 5 de marzo de 2016, 9 a. m. R2#clock set 09:00 05 march 2016 |
| Configure R2 como un maestro NTP. | Nivel de estrato:5 R2#config term R2(config)#ntp master 5 |
| Configurar R1 como un cliente NTP. | Servidor: R2 R1#confi term R1(config)#ntp server 172.16.1.2 |
| Configure R1 para actualizaciones de calendario periódicas con horaNTP. | R1(config)#ntp update-calendar R1(config)#exit Packet Tracer no permite realizar este proceso en caso de un servidor real deberías esperar un tiempo para poder ver el resultado. |

Verifique la configuración de NTP en R1.

Para este proceso aplicaremos el comando show ntp status.
R1#show ntp status
R1#show ntp status
Clock is synchronized, stratum 5, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is DA622B7B.00000027 (20:45:47.039 UTC Sun Mar 6 2016)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 15 sec ago.

Figura 24 Show ntp status

```

password:
R1>enable
Password:
R1#
R1#show ntp status
Clock is synchronized, stratum 5, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
reference time is DA622B7B.00000027 (20:45:47.039 UTC Sun Mar 6 2016)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.12 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000
poll interval is 4, last update was 15 sec ago.
R1#
R1#

```

Fuente: Autoría Propia

Fuente: Guía de actividades

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

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

Tabla 26 Restringir el acceso a las líneas VTY en el R2

| Elemento o tarea de configuración | Especificación |
|---|--|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host |

| | |
|--|--|
| | 172.16.1.1 R2(config-std-nacl)#deny any R2(config-std-nacl)#exit |
| Aplicar la ACL con nombre a las líneas VTY | R2(config)# R2(config)#line vty 0 4 R2(config-line)#ip access-class ADMIN-MGT in |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-line)#transport input telnet |
| Verificar que la ACL funcione como se espera | Probamos en R1 con el comando telnet Y recibimos R1#telnet 172.16.1.2 [Connection to 172.16.1.2 closed by foreign host] Debido a que no hemos configurado un usuario y contraseña para este proceso. Probamos desde otros puntos como es R3: R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection timed out; remote host not responding |

Fuente: Guía de actividades

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

Tabla 27 Comandos CLI

| Descripción del comando | Entrada del estudiante (comando) |
|--|--|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | Show access-list Figura 25 Show access-list en R2 |

| | |
|--|--|
| | <pre> R2# R2# R2#show access -lists R2#Show access-list Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 20 deny any Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 40 permit 192.168.4.0 0.0.0.255 R2# R2# R2# </pre> <p>Fuente: Autoría Propia</p> |
| <p>Restablecer los contadores de una listade acceso</p> | <p>clear Access-lists counters</p> |
| <p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la direcciónen que se aplica?</p> | <p>show ip interface En caso que se busque una en especifica se adjuntaría la solicitada al comando. Show ip interface GigabitEthernet 0/0</p> <p>Figura 26 Show ip interface</p> <pre> --More-- R2# R2# R2# R2#show ip interface GigabitEthernet0/0/0 is up, line protocol is up (connected) Internet address is 209.165.200.233/29 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachable are always sent ICMP mask replies are never sent IP fast switching is disabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled Router Discovery is disabled --More-- </pre> <p>Fuente: Autoría Propia</p> |

| | |
|---|--|
| <p>¿Con qué comando se muestran las traducciones NAT?</p> | <p>show ip nat translations</p> <p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p> <p>Figura 27 Show ip interface...</p> <pre> R2# R2# R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.233 10.10.10.10 --- --- --- 209.165.200.234 10.10.10.10 --- --- R2# </pre> |
| <p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p> | <p>clear ip nat translation *</p> |

Fuente: Guía de actividades

CONCLUSIONES

El desarrollo del primer escenario nos permitió afianzar aún más el conocimiento sobre la configuración del Switch y Routers en donde se logró el desarrollo mediante la herramienta Packet Tracer y se logra evidenciar el tráfico de información entre los PC.

Es importante conocer los diferentes programas de simulación de redes, ya que estas nos permiten determinar y corregir errores que se presenten al momento de ejecutarlos lo que nos permite conocer si el proceso es el adecuado.

El desarrollo del escenario 2 permitió validar el aprendizaje adquirido el Diplomado de Profundización CISCO, por medio de una red pequeña con conectividad IPv4 e IPv6, uso de switches, routing, VLAN, protocolo de routing dinámico OSPF y el protocolo de configuración de hosts dinámicos (DHCP) y la traducción de direcciones de red dinámicas y estáticas (NAT), con listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

La aplicación de comandos en ambientes simulados permite que el aprendizaje sea de forma teórico práctico y que nos preparemos para afrontar casos de la vida real.

BIBLIOGRAFÍA

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.

BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Núñez, W., Sarmiento-Osorio, H., & Forero-Páez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, 16(1), 75-84.

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.

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. In 2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI) (pp. 1-5). IEEE.

Cisco, «The OSPF Not-So-Stubby Área (NSSA) Option,» 12 October 2005. [En línea]. Available: <https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcpser.html>. [Último acceso: November 2020].

Cisco, «Información sobre los modos de loopback en routers de Cisco,» 21 November 2007. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-mode-atm/permanent-virtual-circuitspvc-switched-virtual-circuits-svc/6337-atmloopback.html. [Último acceso: November 20]

DIRECCIONES NAT, ACLY DHCP.,» 2018. [En línea]. Available: <https://repository.unad.edu.co/bitstream/handle/10596/18989/1088972655.pdf?sequence=1&isAllowed=y>. [Último acceso: November 2020].

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, 12(1), 86-93.

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.

J. A. B. Bravo, «CONECTIVIDAD Y CONFIGURACIÓN DINÁMICA DE G. B. C. J. L. V. S. Y. P. S. V. Mauricio Olaya Tellez, «Principios de enrutamiento y conmutación,» 14 December 2017. [En línea]. Available: <https://repository.unad.edu.co/handle/10596/14997>. [Último acceso: November 2020].

Linux Foundation, «Securing Network Time,» 27 September 2017. [En línea]. Available: <https://web.archive.org/web/20171028123642/https://www.coreinfrastructure.org/news/blogs/2017/09/securing-network-time>. [Último acceso: 2020 November].

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in 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). IEEE.