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

ANGELA PATRICIA SALAMANCA MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
DUITAMA
2021

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

ANGELA PATRICIA SALAMANCA MARTINEZ

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

DIRECTOR: NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
DUITAMA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Duitama, 30 Noviembre de 2021

AGRADECIMIENTOS

Mi gratitud, primeramente con Dios a quién le debo la vida y todo lo que ha venido con ella, desde lo más sencillo hasta lo más grande, tanto lo visible como lo intangible. El camino ha sido diverso, lleno de retos, sacrificios y también de experiencias satisfactorias. Durante el proceso resalto la motivación recibida de mi familia, mi esposo y amigos, personas únicas e incondicionales con las que sigo contando y con quienes mi gratitud permanece viva. En este transcurrir he conocido grandes maestros; generosos en conocimiento y grandeza de espíritu, amantes del saber, a quienes agradezco su profesionalismo, esfuerzo y dedicación; ejemplo de ello Ing. Raúl Bareño para quién su compromiso no tiene fecha, día, ni hora.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Gateway o puerta de enlace: es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.

LAN: Infraestructura de la Red que proporciona acceso a los usuario o terminales en una red geográfica pequeña.

Listas de control de Acceso: Filtran el acceso y el reenvío de tráfico. Las listas de control de acceso se pueden usar para filtrar paquetes entrantes o salientes en una interfaz para controlar el tráfico

Puerto físico: Conector o conexión en un dispositivo de Red donde se conectan los medios a un terminal u otro dispositivo de red.

Telnet (Teletype Network1) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente.

RESUMEN

Aplicando tecnología Cisco se desarrollaran dos escenarios propuestos, comenzando desde la configuración básica de Switches y Routers, hasta el aprovechamiento de diferentes protocolos como DHCP Y OSPF, así también aplicando prácticas de seguridad en las redes con el uso de contraseñas encriptadas, validación de inicio de sesión y listas de acceso, esto con el fin de evitar posibles accesos de personas no autorizadas que quieran ingresar a la red.

En el desarrollo del escenario 1 se busca evidenciar el conocimiento adquirido en configuración por consola de aspectos básicos de los dispositivos de la Red propuesta, se desarrollara el esquema de direccionamiento ip para las LAN 1 Y LAN 2 verificación de la configuración de los equipos.

Para el Escenario 2 Se debe configurar una red que admita conectividad ipv4 e ipv6, seguridad de Switches, Routing entre las Vlans, la utilización de listas de control de acceso y donde se aplique Protocolo DHCP, traducción de direcciones (NAT) y el protocolo de tiempo de red servidor/cliente, es decir en el escenario 2 se desarrollara una configuración más amplia y completa que permitirá mayor seguridad y rendimiento en la red.

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

ABSTRACT

Applying Cisco technology, two proposed scenarios will be developed, starting from the basic configuration of Switches and Routers, to the use of different protocols such as DHCP and OSPF, as well as applying security practices in networks with the use of encrypted passwords, validation of login and access lists, this in order to avoid possible access by unauthorized people who want to enter the network.

In the development of scenario 1, it is sought to demonstrate the knowledge acquired in the configuration of the console of basic aspects of the devices of the proposed network, the ip addressing scheme for LAN 1 and LAN 2 will be developed, verification of the configuration equipment.

For Scenario 2, a network must be configured that supports ipv4 and ipv6 connectivity, switch security, routing between Vlans, the use of access control lists and the DHCP protocol, address translation (NAT), and server / client protocol. Network time, that is, in scenario 2 a more comprehensive and complete configuration will be developed that allows greater security and performance on the network.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking.

INTRODUCCION

El internet y las herramientas que se despliegan de él han tomado bastante fuerza en los últimos años. El uso de las herramientas digitales ha crecido notoriamente y algunas empresas que no estaban muy vinculadas con ello, ahora disfrutan de sus beneficios; sin embargo hay ciertos riesgos cuando no se cuenta con parámetros de privacidad y bloqueos a las redes, bien sean pequeñas o grandes empresas.

Para entender un poco más lo anteriormente mencionado se desarrollaran dos escenarios en donde se aplicaran algunos aspectos con los que debería contar una empresa. Por lo tanto y teniendo como base los conocimientos adquiridos en el Diplomado de Profundización de Cisco, se realiza El desarrollo del escenario 1 que tiene como fin afianzar los conocimiento en el desarrollo del esquema de direccionamiento ip. Aplicando estos en un escenario especifico que cuenta con dos LAN, en donde se deben configurar aspectos básicos de seguridad en todos los dispositivos que hacen parte del escenario, estos son Router, switch y 2 Host.

Del mismo modo en el desarrollo del Escenario 2, se tendrán en cuenta parámetro básicos, así como el adecuado desarrollo y/o configuración de cada uno de los dispositivos que conforman la red y que brindará a la Red, seguridad, efectividad y confianza en su ejecución, teniendo en cuenta la aplicación de diferentes protocolos como dhcp, ospf, listas de control de acceso, entre otros, que disminuirán los riesgos de intrusión de personas no autorizadas.

ESCENARIO 1

Figura 1. Topología Escenario 1

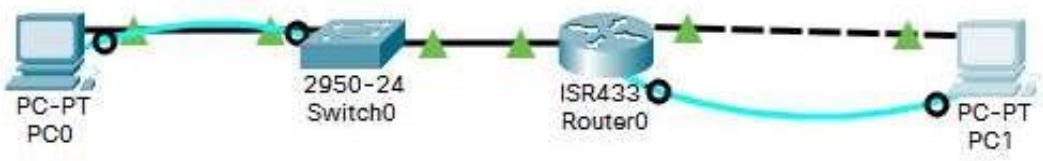
Fuente: Autor

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

Parte 1: Construir la Red

Construcción de red de acuerdo con la topología lógica que se plantea en la figura 1, cable conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2. Simulación Topología Red



Fuente: Propia

Parte 2: Desarrollo 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.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Direccionamiento

Ítem	Requerimiento
Dirección de Red	192.168.24.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.24.1/25
R1 G0/0/0	192.168.24.129/26
S1 SVI	192.168.24.2/25
PC-A	192.168.24.126/25
PC-B	192.168.24.190/26

Fuente: Propia

Parte 3: Configure aspectos básicos

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

Paso 1: Configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Tareas de Configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del Router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXECprivilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass**

Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Propia

Para iniciar la configuración requerida iniciamos cambiando el modo a configuración.
Router>enable
Router#conf t

- **Desactivar la búsqueda DNS**

Desactivamos la búsqueda DNS mediante el Comando no ip domain-lookup.
Router(config)#no ip domain-lookup
Router(config)#

Nombre del Router

Mediante el Comando hostname asignamos el Nombre al Router en este caso R1. Escribimos Hostname seguido del nombre deseado.

Router(config)#Hostname R1

- **Nombre de dominio**

Para asignar el nombre del dominio usamos “ip domain–name” seguido del nombre. El que Usaremos para este ejercicio es: cccna_lab.com, lo asignamos con el siguiente comando:

R1(config)#ip domain-name ccna_lab.com

- **Contraseña cifrada para el modo EXEC privilegiado**

Escribimos enable secret seguido de la contraseña deseada.

R1(config)#enable secret ciscoenpass

- **Contraseña de acceso a la consola**

En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

R1(config)#line console 0 // Ingresa al modo de configuración de línea de consola
R1(config-line)#password ciscoconpass // asignamos contraseña en este caso "ciscoconpass"
R1(config-line)#login //configuración para que requiera autenticación al iniciar sesión
R1(config-line)#exit // Salimos de la configuración de línea de consola

- **Establecer la longitud mínima para las contraseñas.**

Indicamos que la contraseña debe ser de 10 caracteres como mínimo.

R1(config)#security password min-length 10

- **Crear un usuario administrativo en la base de datos local.**

Con username asignamos usuario **admin** y con password la contraseña **admin1pass.**

R1(config)#username admin password admin1pass

- **Configurar el inicio de sesión en las líneas VTY para que use la base de datos local**

R1(config)#line vty 0 4 //líneas configuradas
R1(config-line)#password ciscocisco //asignación de contraseña
R1(config-line)#login local //credenciales configuradas localmente
R1(config-line)#transport input ssh //configuración para permitir solo SSH
R1(config-line)#exit //salir

- **Cifrar las contraseñas de texto no cifrado**

R1(config)#service password-encryption // Accede al servicio de cifrado de contraseñas.

- **Configure un MOTD Banner**

Se configura mensaje de alerta

R1(config)#banner motd # Este es router de la UNAD cualquier intrusión tendrá efectos judiciales#
R1(config)#

- **Configurar interfaz G0/0/0**

R1(config)#int g0/0/0 //ingresamos a la interfaz g0/0/0
R1(config-if)#ip address 192.168.24.129 255.255.255.192 // asignamos ip y mascara de red
R1(config-if)#description esta es la interfaz de la lan2 // asignamos una descripción de la interfaz
R1(config-if)#no shutdown ***//*** activamos la interfaz con configuración asignada
R1(config-if)#exit // salimos de la interfaz g0/0/0

- **Configurar interfaz G0/0/1**

R1(config)#int g0/0/1 //ingresamos a la interfaz g0/0/1
R1(config-if)#description esta es la interfaz de la lan1 // asignamos una descripción de la interfaz
R1(config-if)#ip address 192.168.24.1 255.255.255.128 // asignamos ip y mascara de red
R1(config-if)#no shutdown

- **Generar una clave de cifrado RSA**

R1(config)#ip domain name ccna-lab.com //asignamos nombre dominio
R1(config)#crypto key generate rsa //generamos clave de cifrado RSA
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.
How many bits in the modulus [512]: 1024 //Asignamos *Módulo* de 1024 bits

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Tareas de Configuración S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	*Switch(config)#no ip domain-lookup*
Nombre del switch	**S1**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	
Configurar las líneas VTY para que acepten únicamentelas conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla dedireccionamiento.

Fuente: Propia

Para iniciar la configuración requerida iniciamos cambiando el modo a configuración.
Switch>enable
Switch#conf t

- **Desactivar la búsqueda DNS**

Desactivamos la búsqueda DNS mediante el Comando no ip domain-lookup.

Switch(config)#no ip domain-lookup

- **Nombre del Switch**

Mediante el Comando hostname asignamos el Nombre al Switch en este caso S1. Escribimos Hostname seguido del nombre deseado.
Switch(config)#hostname S1

- **Nombre de dominio**

Para asignar el nombre del dominio usamos “ip domain –name” seguido del nombre. El que Usaremos para este ejercicio es: cccna_lab.com, lo asignamos con el siguiente comando:

S1(config)#ip domain-name ccna-lab.com

- **Contraseña cifrada para el modo EXEC privilegiado**

Escribimos enable secret seguido de la contraseña deseada.

S1(config)#enable secret ciscoenpass

- **Contraseña de acceso a la consola**

En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

S1(config)#line console 0 // Ingresa al modo de configuración de línea de consola
S1(config-line)#password ciscoconpass // asignamos contraseña en este caso “ciscoconpass”

S1(config-line)#login //configuración para que requiera autenticación al iniciar sesión
S1(config-line)#exit // Salimos de la configuración de línea de consola

- **Crear un usuario administrativo en la base de datos local.**

Con username asignamos usuario **admin** y con password la contraseña **admin1pass.**
S1(config)#username admin password admin1pass

- **Configurar el inicio de sesión en las líneas VTY para que use la base de datos local**

S1(config)#line vty 0 15 //líneas configuradas
S1(config-line)#password ciscocisco //asignación de contraseña
S1(config-line)#login local //credenciales configuradas localmente

- **Configurar las líneas VTY para que acepten únicamente las conexiones SSH**

S1(config-line)#transport input ssh //configuración para permitir solo SSH
S1(config-line)#exit //salir

- **Cifrar las contraseñas de texto no cifrado**

S1(config)#service password-encryption // Accede al servicio de cifrado de contraseñas.

- **Configure un MOTD Banner**

S1(config)#banner motd # Este es Switch de la UNAD por favor no acceder#
S1(config)#

- **Generar una clave de cifrado RSA**

S1(config)#ip domain-name ccna-lab.com // Asignamos nombre dominio
S1(config)#crypto key generate rsa //generamos clave de cifrado RSA

The name for the keys will be: S1.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.

How many bits in the modulus [512]: 1024 //Asignamos *Módulo* de 1024 bits

- **Configurar la interfaz de administración (SVI)**

S1(config)#int vlan1 //Ingresa a la interfaz a configurar
S1(config-if)#ip address 192.168.24.2 255.255.255.128 //Asignamos dirección y mascara
S1(config-if)#no shutdown //Activamos los cambios

- **Configuración del gateway predeterminado**

S1(config-if)#exit // salimos de la interfaz anterior
S1(config)#ip default-gateway 192.168.24.1 //Asignamos puerta de enlace
S1(config)#exit // Salir

Paso 2. Configurar los equipos

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

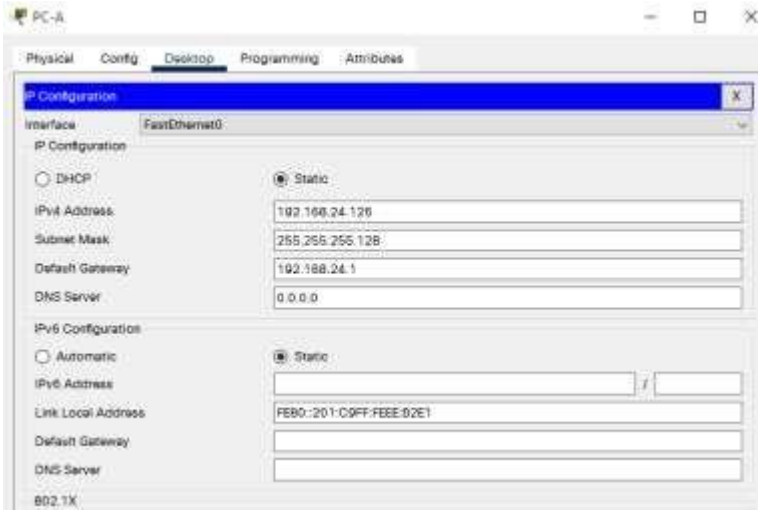
Tabla 4. Tabla configuración de equipos PC-A

PC-A Network Configuration	
Descripción	Configuración PC-A
Dirección física	0001.C9EE.B2E1
Dirección IP	192.168.24.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.24.1

Fuente: Propia

Asignamos dirección, mascara y puerta de enlace al PC-A

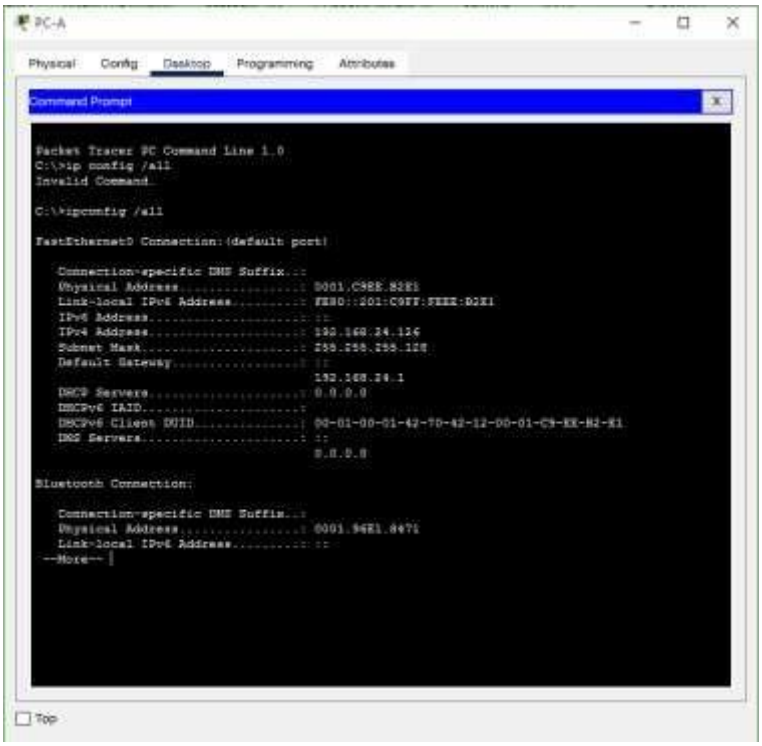
Figura 3. Configuración PC-A



Fuente: Propia

- Consulta mediante el comando **ipconfig /all**.

Figura 4. Consulta ipconfig/all PC-A



Fuente: Propia

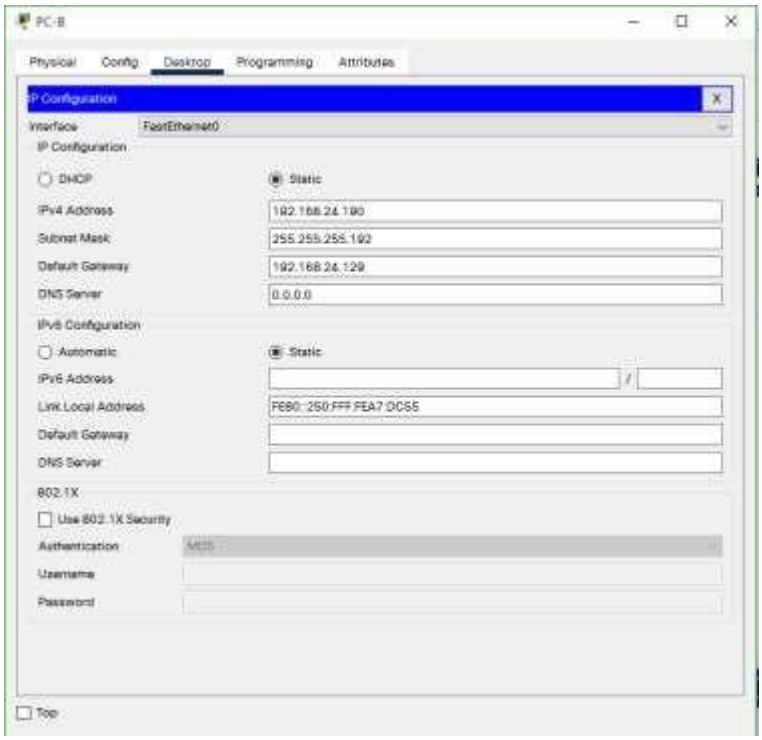
Tabla 5. Configuración de equipos PC-B

PC-B Network Configuration	
Descripción	Configuración PC-B
Dirección física	0050.0FA7.DC55
Dirección IP	192.168.24.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.24.129

Fuente: Propia

- Asignamos dirección, mascara y puerta de enlace al PC-B

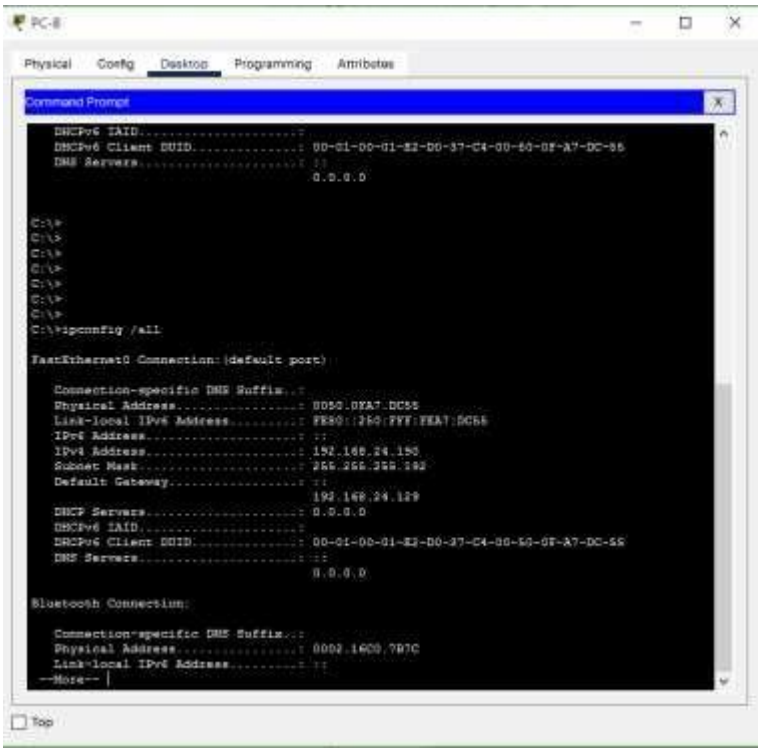
Figura 5. Configuración PC-B



Fuente: Propia

- Consulta mediante el comando **ipconfig /all**.

Figura 6. Consulta ipconfig/all PC-B

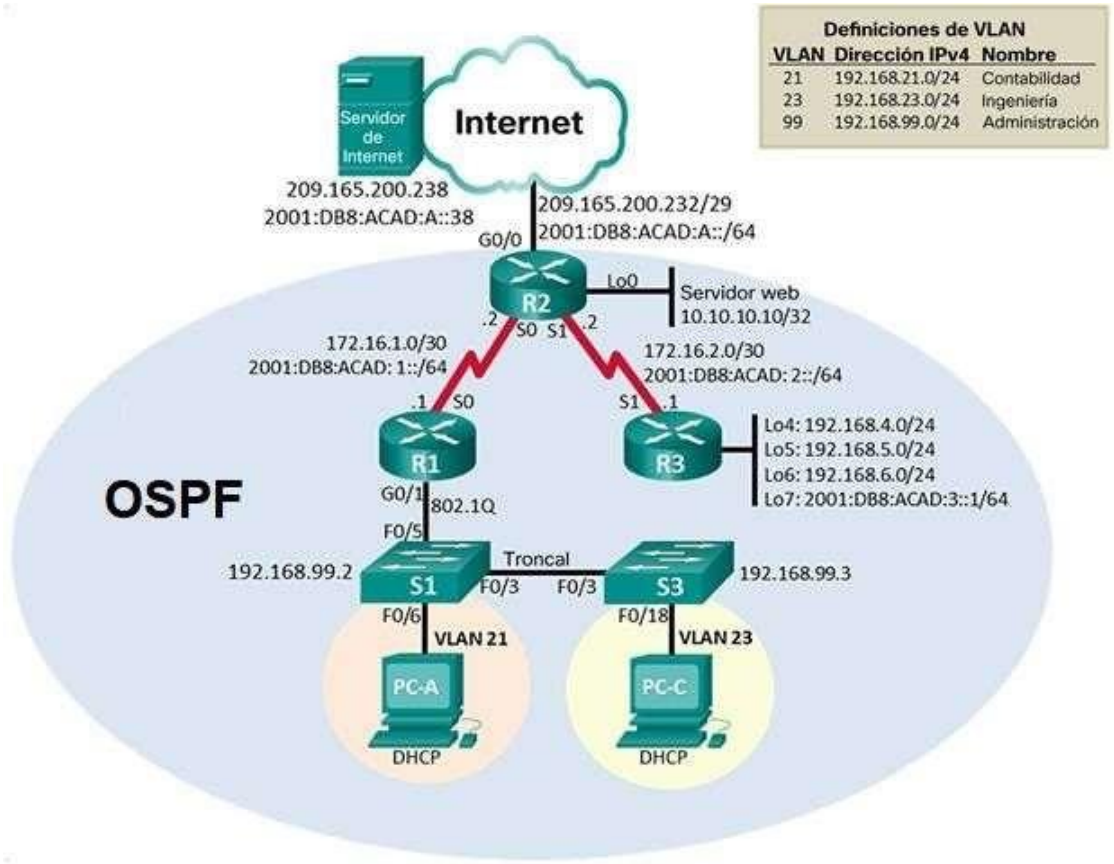


Fuente: Propia

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



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 Dispositivos

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

Fuente: Propia

Se elimina el archivo de startup-config de todos los routers y se vuelven a cargar.
Se elimina el archivo de startup-config de todos los Swtich y se vuelven a cargar.

Figura 7. Show vlan de S1

Fuente: Propia

Se Verifica que la base de datos de VLAN no está en la memoria flash del Switch

Figura 8. Show vlan de S2

Fuente: Propia
Se Verifica que la base de datos de VLAN no está en la memoria flash del Switch

Figura 9. Show vlan de S3

Fuente: Propia

Se Verifica que la base de datos de VLAN no está en la memoria flash del Switch

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 informaciónde las direcciones IP, consulte la topología):

Tabla 7. Configuración 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	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Propia

Figura 10. Configuración computadora de Internet

Fuente: Propia

Se ingresan los datos de configuración de la computadora de Internet.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	*no ip domain-lookup*
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	*R1(config)#service password-encryption*
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/2/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama detopología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/2/0Configurar una ruta IPv6 predeterminada de S0/2/0

Fuente: Propia

Nota: Todavía no configure G0/1.

- **Desactivar la búsqueda DNS**

Desactivamos la búsqueda DNS mediante el Comando no ip domain-lookup.

Router(config)#no ip domain-lookup
Router(config)#

- **Nombre del Router**

Mediante el Comando hostname asignamos el Nombre al Router en este caso R1. Escribimos Hostname seguido del nombre deseado.

Router(config)#Hostname R1 //Asignar nombre a Router

- **Contraseña cifrada para el modo EXEC privilegiado**

Escribimos enable secret seguido de la contraseña *class*.

R1 (config)#enable secret class //Establece contraseña Class

- **Contraseña de acceso a la consola**

En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

R1(config)#line console 0 // Ingresa al modo de configuración de línea de consola
R1(config-line)#password cisco // asignamos contraseña en este caso “cisco”
R1(config-line)#login //configuración para que requiera autenticación al iniciar sesión
R1(config-line)#exit // Salimos de la configuración de línea de consola

- **Contraseña de acceso a Telnet**

R1(config)#line vty 0 4 //líneas configuradas
R1(config-line)#password cisco //asignación de contraseña
R1(config-line)#login local //credenciales configuradas localmente

- **Cifrar las contraseñas de texto no cifrado**

Accede al servicio de cifrado de contraseñas.
R1(config)#service password-encryption *//Activa servicio de encriptación*

- **Configure un MOTD Banner**

R1(config)#banner motd # Se prohíbe el acceso no autorizado # //Configura mensaje *de alerta*
R1(config)#

- **Configuración Interfaz S0/2/0**

R1(Config)# interface serial 0/2/0 *// Entra a configuración de la interfaz*
R1(Config-if)# description lan1 *// Agrega descripción de la LAN*
R1(Config-if)#ip address 172.16.1.1 255.255.255.252 //Asignación dirección
R1(Config-if)#ipv6 address 2001:DB8:ACAD: 1::1/64 *//Asignación ipv6*
R1(Config-if) #clock rate 128000
R1(Config-if)# no shutdown

- **Rutas predeterminadas**

R1(Config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 *//Configura rutas predeterminadas*

R1(Config)# ipv6 route ::/0 2001:DB8:ACAD:1::2 *//Configura rutas predeterminadas ipv6*

Paso 3: Configurar R2

- La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	*Router(config)#no ip domain-lookup*
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	*R2(config)#service password-encryption*
Habilitar el servidor HTTP	*R2(config)#Ip http server*
Mensaje MOTD	*R2(config)#*Se prohíbe el acceso no autorizado#
Interfaz S0/2/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.Activar la interfaz
Interfaz S0/2/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primeradirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primeradirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente: Propia

- **Desactivar la búsqueda DNS**

Desactivamos la búsqueda DNS mediante el Comando no ip domain-lookup.

Router(config)#no ip domain-lookup
Router(config)#

- **Nombre del Router**

Mediante el Comando hostname asignamos el Nombre al Router en este caso R1. Escribimos Hostname seguido del nombre deseado.

Router(config)#Hostname R2

- **Contraseña cifrada para el modo EXEC privilegiado**

Escribimos enable secret seguido de la contraseña *class*.

R2(config)#enable secret class

- **Contraseña de acceso a la consola**

En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

R2(config) #line console 0 // Ingresa al modo de configuración de línea de consola
R2(config-line)#password cisco // asignamos contraseña en este caso “cisco”
R2(config-line)#login //configuración para que requiera autenticación al iniciar sesión
R2(config-line)#exit // Salimos de la configuración de línea de consola

- **Contraseña de acceso a Telnet**

R2(config)#line vty 0 4 //líneas configuradas
R2(config-line)#password cisco //asignación de contraseña
R2(config-line)#login local //credenciales configuradas localmente

- **Cifrar las contraseñas de texto no cifrado**

Accede al servicio de cifrado de contraseñas.
R2(config)#service password-encryption // Activamos servicio de encriptación de contraseñas

- **Habilitar el servidor HTTP**

R2(config)# ip http server // al ingresar el comando, packet tracer lo toma como invalido.

- **Configure un MOTD Banner**

R2(config)#banner motd # Se prohíbe el acceso no autorizado # // Crea mensaje de alerta
R2(config)#

- **Configuración Interfaz S0/2/0**

R2(Config)# interface serial 0/2/0 //Ingresa a la interface serial 0/2/0
R2(Config-if)# description lan 2 //Asigna el descripción de la LAN2
R2(Config-if)#ip address 172.16.1.2 255.255.255.252 //Asigna dirección ip4
R2(Config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 //Asigna dirección ipv6
R2(Config-if) #clock rate 128000 //Activa la sincronización y fija la velocidad
R2(Config-if)# no shutdown *// Activa la interfaz*

- **Configuración Interfaz S0/2/1**

R2(Config)# interface serial 0/2/1 //Ingresa la interface serial 0/2/1
R2(Config-if)# description lan 2 //Asina el descripción de la LAN2
R2(Config-if)#ip address 172.16.2.2 255.255.255.252 //Asigna dirección ip4
R2(Config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 //Asigna dirección ipv6
R2(Config-if)#clock rate 128000 //Activa la sincronización y fija la velocidad
R2(Config-if)# no shutdown

- **Interfaz G0/0/0 (simulación de Internet)**

R2(Config)#int g0/0/0 //Ingresa la interface g 0/2/0
*R2(Config-if)# ip address 209.165.200.233 255.255.255.*248 //Asigna dirección ipv4
R2(Config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 //Asigna dirección ipv6
R2(Config-if)#description conexión servidor //descripción
R2(Config-if)#no shutdown //Activa interfaz

- **Interfaz loopback 0 (servidor web simulado)**

R2(Config)#interface loopback 0 //Ingresa a interfaz virtual loopback *0*
R2(Config-if)#ip address 10.10.10.10 255.255.255.255 // configura la dirección ip
R2(Config-if)#description conexión servidor web //Añade descripción

- **Ruta predeterminada**

R2(Config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1 //Configura ruta predeterminada
R2(Config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1 //Configura ruta predeterminada
R2(Config)#ipv6 route ::/0 2001:DB8:ACAD:1::1 //Configura ruta pred IPV6
R2(Config)#ipv6 route::/0 2001:DB8:ACAD:2::1 //Configura ruta predeterminada IPV6

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:
Tabla 10. Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R3

Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	*R3(config)#service password-encryption*
Mensaje MOTD	*R3(config)#banner motd # Se prohíbe el acceso no autorizado #*
Interfaz S0/2/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente direcciónd isponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera direcciónd isponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera direcciónd isponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera direcciónd isponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas Predeterminadas	*R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2* *R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2*

Fuente: Propia

- **Desactivar la búsqueda DNS**

Desactivamos la búsqueda DNS mediante el Comando no ip domain-lookup.

Router(config)#no ip domain-lookup
Router(config)#

- **Nombre del Router**

Mediante el Comando hostname asignamos el Nombre al Router en este caso R1. Escribimos Hostname seguido del nombre deseado.

Router(config)#Hostname R3

- **Contraseña cifrada para el modo EXEC privilegiado**

Escribimos enable secret seguido de la contraseña *class*.

R3(config)#enable secret class

- **Contraseña de acceso a la consola**

En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

R3(config)#line console 0 // Ingresa al modo de configuración de línea de consola
R3(config-line)#password cisco // asignamos contraseña en este caso “cisco”
R3(config-line)#login //configuración para que requiera autenticación al iniciar sesión
R3(config-line)#exit // Salimos de la configuración de línea de consola

- **Contraseña de acceso a Telnet**

R3(config)#line vty 0 4 //líneas a configurar
R3(config-line)#password cisco //asignación de contraseña
R3(config-line)#login local //credenciales configuradas localmente

- **Cifrar las contraseñas de texto no cifrado**

Accede al servicio de cifrado de contraseñas.
R3(config)#service password-encryption //Activa servicio encriptar contraseñas

- **Configure un MOTD Banner**

Configura mensaje de alerta

R3(config)#banner motd # Se prohíbe el acceso no autorizado
R3(config)#

- **Configuración Interfaz S0/2/1**

R3(Config)# interface serial 0/2/1 //Ingreso a la Interface serial
R3(Config-if)# description lan 2 // descripción
R3(Config-if)#ip address 172.16.2.1 255.255.255.252 //asignación dirección ip y mascara
R3(Config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 //Asignación ipv6
R3(Config-if)# no shutdown //Activa interface serial

- **Interfaz loopback 4**

R3(Config-if)#interface loopback4
R3(Config-if)#ip address 192.168.4.1 255.255.255.0 //Establece dirección ipv4

- **Interfaz loopback 5**

R3(Config-if)#interface loopback5
R3(Config-if)#ip address 192.168.5.1 255.255.255.0 //Establece dirección ipv4

- **Interfaz loopback 6**

R3(Config-if)#interface loopback6
R3(Config-if)#ip address 192.168.6.1 255.255.255.0 //Establece dirección ipv4

- **Interfaz loopback 7**

R3(Config-if)#interface loopback7 //Establece dirección ipv6
R3(Config-if)#ipv6 address

- **Ruta predeterminada**

R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 //Ruta predeterminada para ipv4
R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2//Ruta predeterminada para ipv6

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración S1

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

Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Propia

Paso 6: Configurar el S3

Tabla 12. Configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#Hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Propia

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:

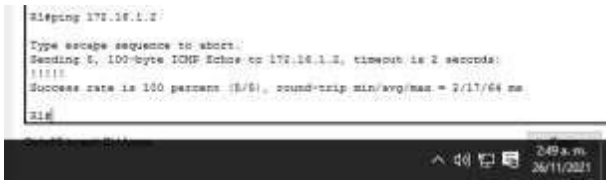
Tabla 13. Conectividad de la Red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio

Fuente: Propia

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

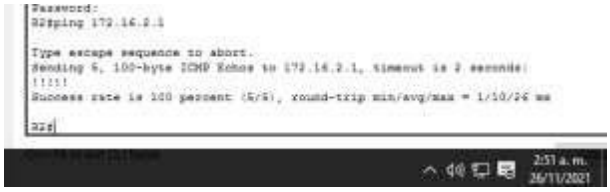
Figura 11. Verificar Conectividad 172.16.1.2



Fuente: Propia

Se evidencia ping satisfactorio

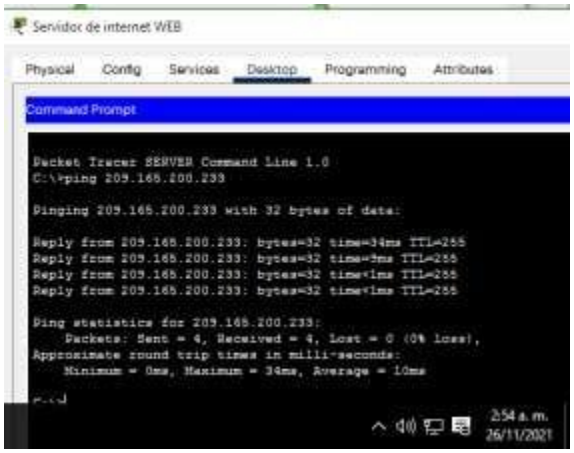
Figura 12. Verificar conectividad 172.16.2.1



Fuente: Propia

Se evidencia ping satisfactorio

Figura 13. Verificar conectividad con servidor



Fuente: Propia

Se evidencia ping satisfactorio

Parte 3: Configurar seg. del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración Seguridad 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
Asignar la dirección IP deadministración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como elgateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz	

F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	*S1(config)#int f0/6* *S1(config-if)#switchport access vlan 21*
Apagar todos los puertos sin usar	*S1(config-if)#in range f0/1-2, f0/4, f0/7-24* *S1(config-if-range)#shutdown*

Fuente: Propia

- Crear la base de datos de VLAN

S1(config)#vlan 21 // Configuración vlan 21
S1(config-vlan)#name Contabilidad //Asignación nombre vlan 21
S1(config-vlan)#exit //Salir

S1(config)#vlan 23 // Configuración vlan 23
S1(config-vlan)#name ingeniería //Asignación nombre vlan 23
S1(config-vlan)#exit //Salir

S1(config)#vlan 99 // Configuración vlan 99
S1(config-vlan)#name Administración //Asignación nombre vlan 99
S1(config-vlan)#exit //Salir

- Asignar la dirección IP deadministración.

S1(config)#interface vlan 99 //Ingreso interface vlan 99
S1(config-vlan)#ip address 192.168.99.2 255.255.255.0 // Asignación ip y mascara
S1(config-vlan)#exit //Salir

- Asignar el gateway predeterminado

S1(config)#ip default-gateway 192.168.99.1 //Asignación Gateway predeterminado

- Forzar el enlace troncal en la interfazF0/3

S1(config)# interface fa0/3 //Entra a la interface a configurar
S1(config-if)# switchport mode trunk //Configura el Puerto como troncal
S1(config-if)# switchport trunk native vlan 1 // Asigna la Vlan 1 como nativa al Puerto troncal
S1(config-if)# switchport nonegotiate //Desactiva la negociación automática
S1(config-if)# no shutdown //Activa la interfaz

- Forzar el enlace troncal en la interfazF0/5

S1(config)# interface fa0/5 //Entra a la interface a configurar
S1(config-if)# switchport mode trunk //Configura el Puerto como troncal
S1(config-if)# switchport trunk native vlan 1 // Asigna la Vlan 1 como nativa al Puerto troncal
S1(config-if)# switchport nonegotiate //Desactiva la negociación automática
S1(config-if)# no shutdown

- Configurar el resto de los puertos comopuertos de acceso

S1(config-if)# interface range f0/1-2, f0/4, f0/6-24, g0/-2 // ingreso interface de los puertos a configurar
S1(config-if)# switchport mode access //Configurar como puertos de acceso

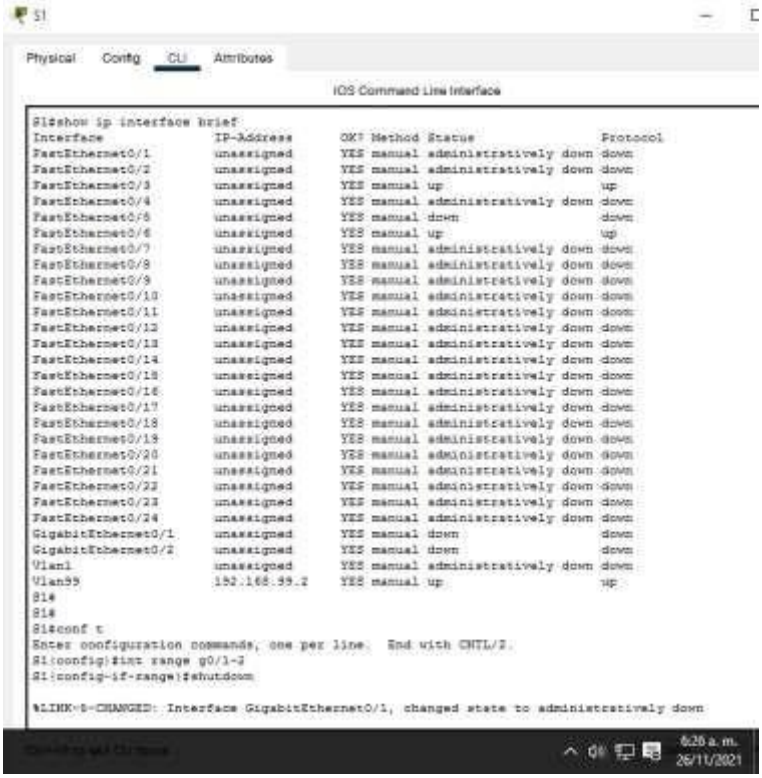
- Asignar F0/6 a la VLAN 21

S1(config)#int f0/6 //ingresa a la interfaz
S1(config)#switchport access vlan 21 *//Asigna el f/06 a vlan 21*

- Apagar todos los puertos sin usar

S1(config)#int range f0/1-2,f0/4, f0/7-24, g0/1-2 *//Establece el rango interfaces a config.*
S1(config)#shutdown *//Apaga las interfaces*

Figura 14. Configuración S1



Fuente: Propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuración S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombrea cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama detopología

Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gatewaypredeterminado.
Forzar el enlace troncal en la interfazF0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos comopuertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config)#switchport access vlan 21
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2,f0/4-17,f0/19-24, g0/1-2 S3(config)#shutdown

Fuente: Propia

- Crear la base de datos de VLAN

S3(config)#vlan 21 // Configuración vlan 21
S3(config-vlan)#name Contabilidad //Asignación nombre vlan 21
S3(config-vlan)#exit //Salir

S3(config)#vlan 23 // Configuración vlan 23
S3(config-vlan)#name Ingeniería //Asignación nombre vlan 23
S3(config-vlan)#exit //Salir

S3(config)#vlan 99 // Configuración vlan 23
S3(config-vlan)#name administración //Asignación nombre vlan 23
S3(config-vlan)#exit //Salir

- Asignar la dirección IP deadministración.

S3(config)#interface vlan 99 //Ingreso interface vlan 99
S3(config-vlan)#ip address 192.168.99.3 255.255.255.0 //Asigna ip y mascara
S3(config-vlan)#exit *//Salir*

- Asignar el gateway predeterminado

S3(config)#ip default-gateway 192.168.99.1 *//Asigna Gateway predeterminado*

- Forzar el enlace troncal en la interfazF0/3

S3(config)# interface fa0/3 //Entra a la interface a configurar
S3(config-if)# switchport mode trunk //Configura el Puerto como troncal
S3(config-if)# switchport trunk native vlan 1 // Asigna la Vlan 1 como nativa al Puerto troncal
S3(config-if)# switchport nonegotiate //Desactiva la negociación automática
S3(config-if)# no shutdown //Activa la interfaz

- Configurar el resto de los puertos comopuertos de acceso

S3(config-if)# interface range f0/1-2, f0/4, f0/6-24, g0/1-2 //puertos a configurar
S3(config-if-range)# switchport mode access //Configura puertos como puertos de acceso

- Asignar F0/18 a la VLAN 21

S3(config)#int f0/18 *// Ingresa a la interface a configurar*
S3(config)#switchport access vlan 21 *//Asigna f0/18 a vlan 21*

- Apagar todos los puertos sin usar

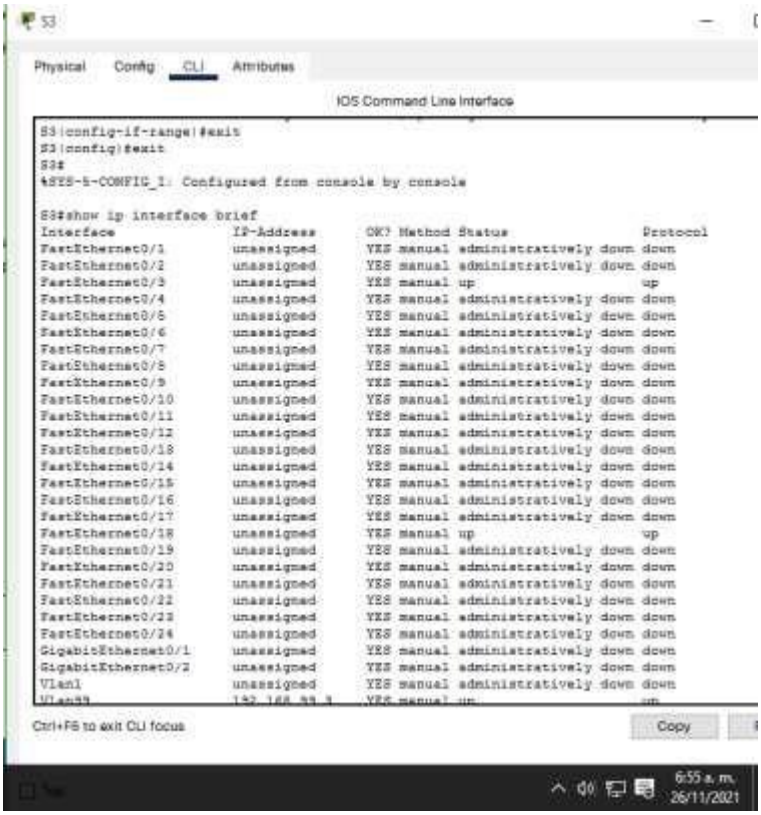
S3(config)#int range f0/1-2,f0/4-17, f0/19-24, g0/1-2 //Ingresa a las interfaces a configurar
S3(config)#shutdown *//Apaga las interfaces*

A continuación se valida que la configuración se haya realizado correctamente utilizando el siguiente comando:

S3 #Show ip interfaces brief

El cual arroja el siguiente resultado:

Figura 15. Validación Configuración S3



Fuente: Propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 enG0/0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 enG0/0/1	Descripción: LAN de IngenieríaAsignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99	Descripción: LAN de Administración Asignar la VLAN 99

enG0/0/1	Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/0/1	*R1#conf t* *R1(config)#interface g0/0/1* *R1(config-if)#no shutdown*

Fuente: Propia

- Configurar la subinterfaz 802.1Q .21 enG0/0/1

R1 (Config)# interface g0/0/1.21 //Ingresa a la Sub interfaz
R1 (Config-subif)#encapsulation do1Q 21 //se habilita y asocia a vlan
R1 (Config-subif)#ip address 192.168.21.1 255.255.255.0 //dirección de sub interfaz
R1 (Config-subif)#description vlan 21 //Descripción
R1 (Config-subif)#no shutdown //Activa interfaz

- Configurar la subinterfaz 802.1Q .23 enG0/0/1

R1 (Config)# interface g0/0/1.23 //Ingresa a la Sub interfaz
R1 (Config-subif)#encapsulation do1Q 23 //se habilita y asocia a vlan
R1 (Config-subif)#ip address 192.168.23.1 255.255.255.0 //dirección de sub interfaz y mascara
R1 (Config-subif)#description vlan 23 //Descripción
R1 (Config-subif)#no shutdown //Activa interfaz

- Configurar la subinterfaz 802.1Q .99 enG0/0/1

R1 (Config)# interface g0/0/1.99 //Ingresa a la Sub interfaz
R1 (Config-subif)#encapsulation do1Q 299 //se habilita y asocia a vlan
R1 (Config-subif)#ip address 192.168.99.1 255.255.255.0 //dirección de sub interfaz y mascara
R1 (Config-subif)#description vlan 99 //Descripción
R1 (Config-subif)#no shutdown //Activa interfaz

- Activar la interfaz G0/0/1

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:

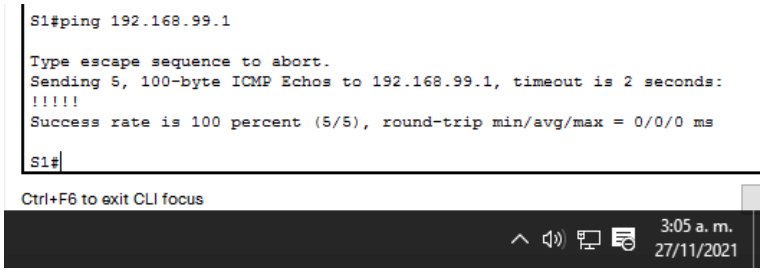
Tabla 15. Verificar conectividad

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

Fuente: Propia

- **PING S1 A R1 VLAN 99 IP 192.168.99.1**

Figura 16. PING S1 A R1 VLAN 99 IP 192.168.99.1

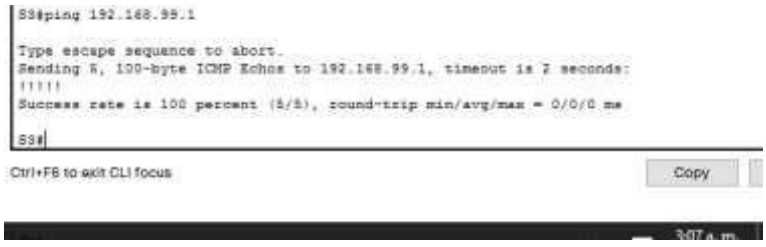


Fuente: Propia

Se evidencia conexión exitosa

- **PING S3 A R1 VLAN 99 IP 192.168.99.1**

Figura 17. PING S3 A R1 VLAN 99 IP 192.168.99.1



Fuente: Propia

Se evidencia conexión exitosa

- **PING S1 A R1 VLAN 21 IP 192.168.21.1**

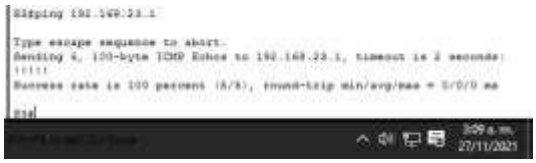
Figura 18. PING S1 A R1 VLAN 21 IP 192.168.21.1

Fuente: Propia

Evidenciamos conexión exitosa

- **PING S3 A R1 VLAN 23 IP 192.168.23.1**

Figura 19. PING S3 A R1 VLAN 23 IP 192.168.23.1



Fuente: Propia

Se evidencia conexión exitosa

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 16. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#conf t R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1

Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 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
Establecer todas las interfaces LAN como pasivas	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
Desactive la sumarización automática	OSPF no realiza un resumen automático, por lo que no es un comando necesario.

Fuente: Propia

Paso 2: Configurar OSPF en el R2

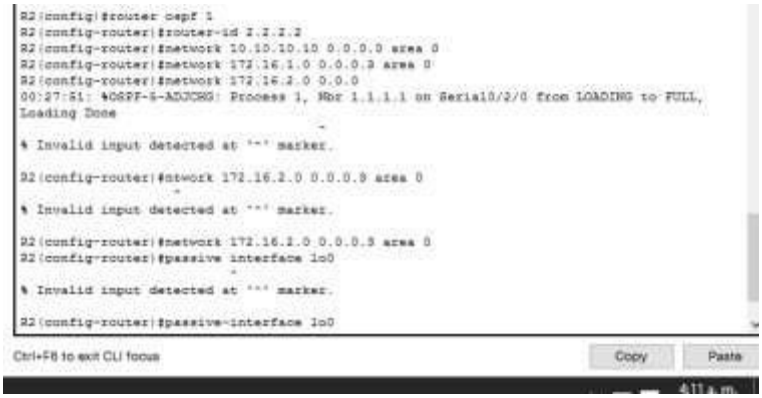
La configuración del R2 incluye las siguientes tareas:
R1(config)#router ospf 1
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 //Configura red a área 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 //Configura red a área 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 //Configura red a área 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 //Configura red a área 0
R1(config-router)#passive-interface g0/0/1 //Se establece interfaz como pasiva
R1(config-router)#passive-interface g0/0/1.21 //Se establece interfaz como pasiva
R1(config-router)#passive-interface g0/0/1.23 //Se establece interfaz como pasiva
R1(config-router)#passive-interface g0/0/1.99 //Se establece interfaz como pasiva

Tabla 17. Configuración OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2#conf t R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2 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 0.0.0.0 area 0 0.0.1.0
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	No aplica

Fuente: Propia

Figura 20. Configuración OSPF en el R2



Fuente: Propia

3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 18. Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config-rtr)#int g0/0/0 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#ipv6 ospf 1 area 0
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)# R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 R3(config-router)#exit
Establecer todas las interfaces de LAN IPv4 (Loopback)como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#exit
Desactive la sumarización automática.	No Aplica

Fuente: Propia

Figura 21. Configuración OSPF en el R3

Fuente Propia

Paso 4: Verificar la información de OSPF

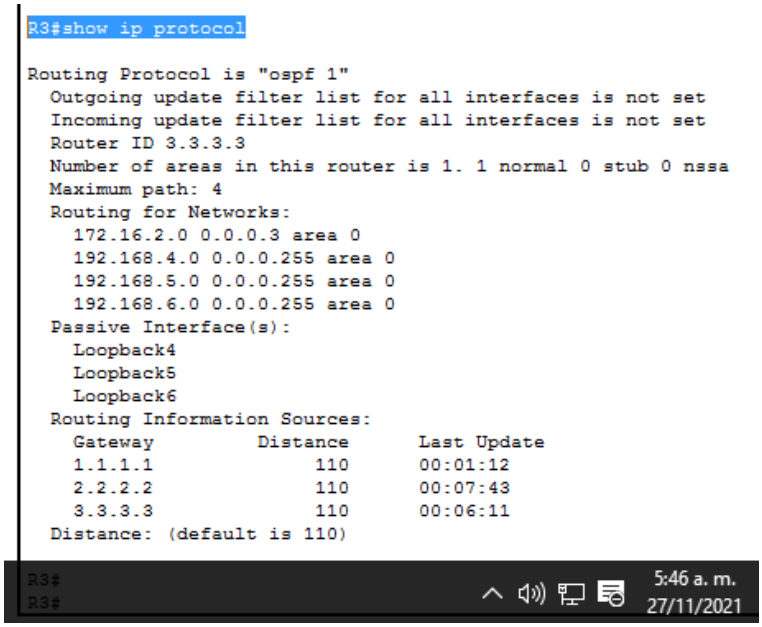
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado paraobtener la siguiente información:

Tabla 19. Verificación 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?	R3#show ip protocol
¿Qué comando muestra solo las rutas OSPF?	R3#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuraciónen ejecución?	R3#show ip ospf

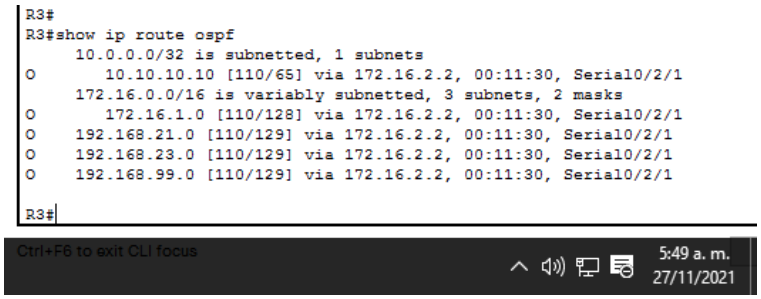
Fuente: Propia

Figura 22. Show ip protocol



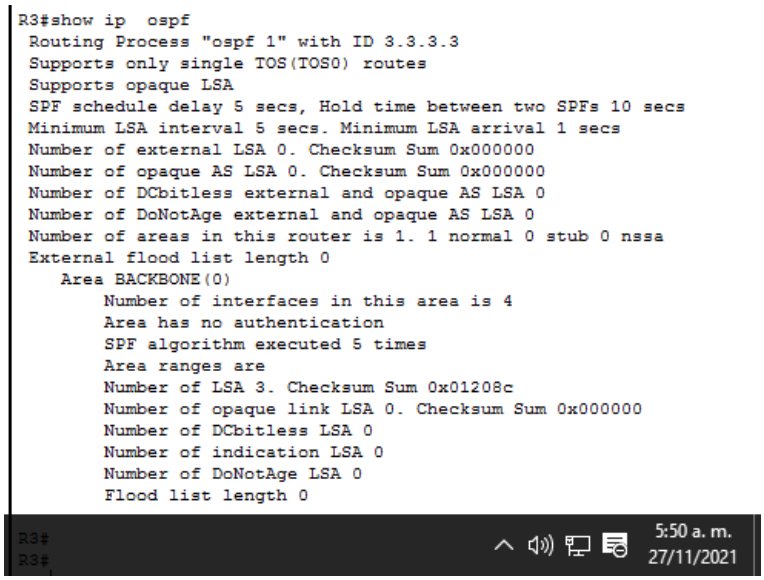
Fuente: Propia

Figura 23. Show ip route ospf



Fuente: Propia

Figura 24. Show ip ospf



Fuente: 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 20. Configurar el R1 como servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Fuente: Propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 21. Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con unacuenta de usuario	Nombre de usuario:**webuser**Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#user webuser privilege 15

	secret 12345
Habilitar el servicio del servidor HTTP	R2(config)# ip http server Este el comando que se utiliza pero packet tracer no lo soporta.
Configurar el servidor HTTP para utilizar labase de datos local para la autenticación	R2# Conf t R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para laNAT estática	R2#conf t R2(config)#interface g0/0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#interface Lo0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de unaACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y deIngeniería en el R1 Permitir la traducción de un resumen de las redes LAN(loopback) en el R3
Defina el pool de direcciones IP públicasutilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Propia

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 //Lista de acceso vlan Contabilidad

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 //Lista de acceso vlan Ingenieria

R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255 //Lista de acceso para redes Lan(loopback)R3

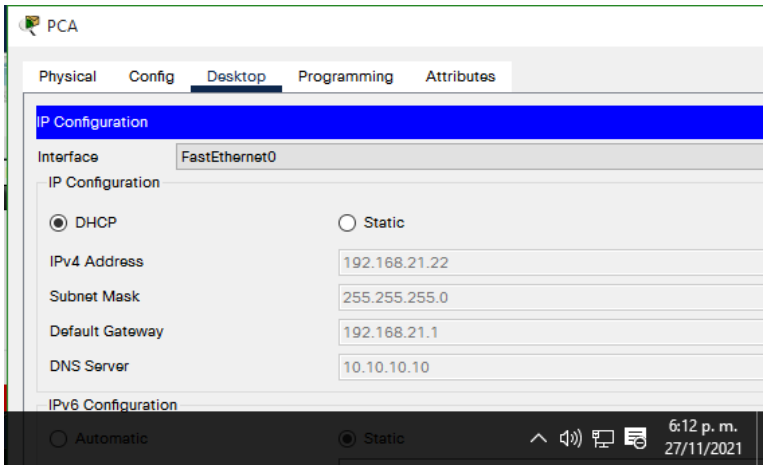
Paso 3: Verificar el protocolo DHCP y la NAT estática

Tabla 22. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Conexión PC-A DHCP
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Conexión PC-C DHCP
Verificar que la PC-A pueda hacer ping ala PC-C **Nota:** Quizá sea necesario deshabilitar elfirewall de la PC.	Ping PC-A a PC-C
Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Ping PC-A a PC-C

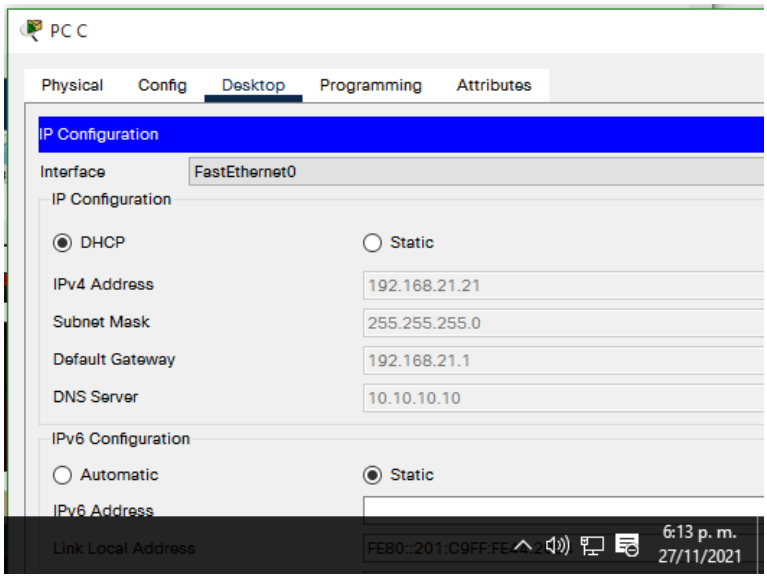
Fuente: Propia

Figura 25. Conexión PC-A DHCP



Se evidencia obtención de ip por DHCP para la PC-A

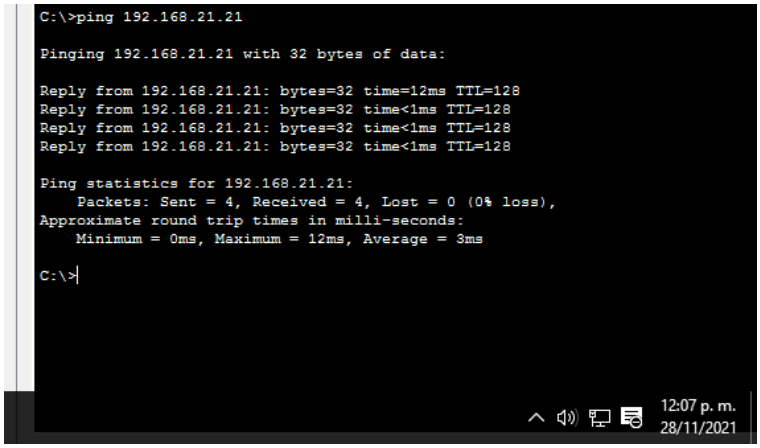
Figura 26. Conexión PC-C DHCP



Fuente Propia

Se evidencia obtención de ip por DHCP para la PC-C

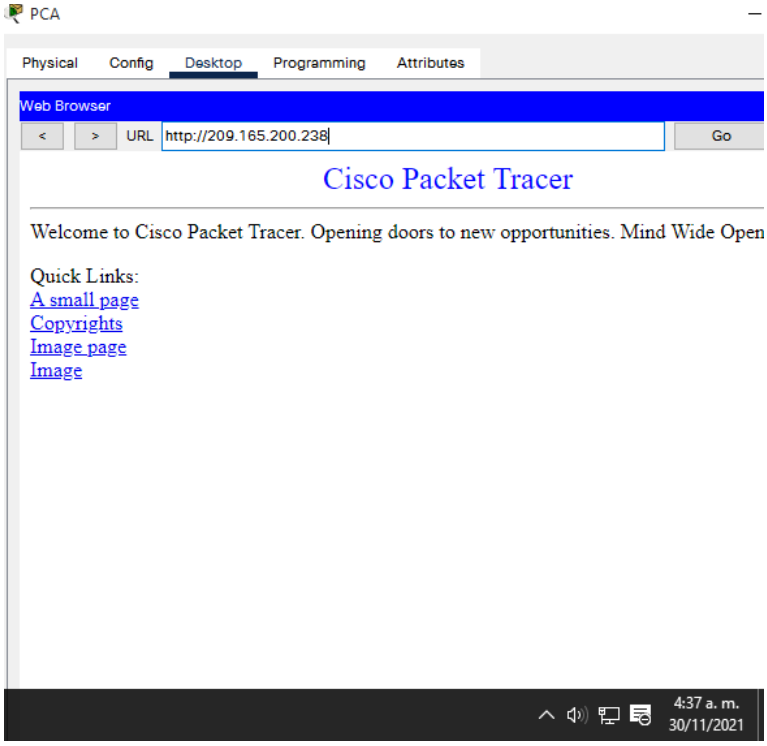
Figura 27. Ping PC-A a PC-C



Fuente: Propia

Se evidencia conexión exitosa

Figura 28. Conexión servidor



Fuente: Propia

Se evidencia conexión con el servidor web

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 pingsse realicen correctamente.

Parte 6: Configurar NTP

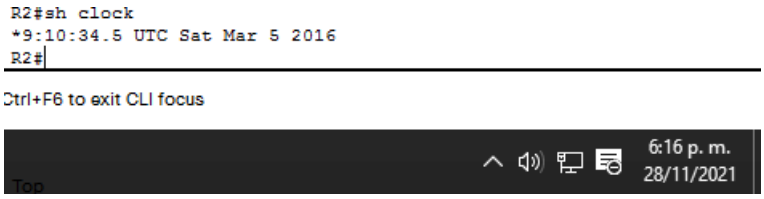
Tabla 23. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 09:00:00 05 march 2016 Para verificar que la hora quedó configurada usamos R2#sh clock

Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	R2(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R2(config)#show ntp translations

Fuente: Propia

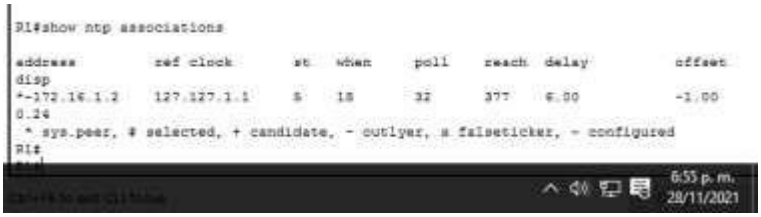
Figura 29. Verificación Configuración



Fuente: Propia

Se evidencia correcta configuración de hora y fecha

Figura 30. Verificación Configuración



Fuente Propia

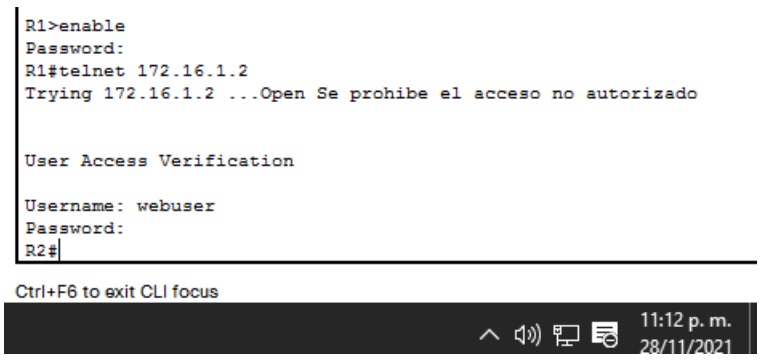
Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Tabla 24. Listas de control de acceso (ACL)

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 Utilizamos las siguientes líneas para configurar: *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)#!*
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#exit
Verificar que la ACL funcione como se espera	R2#show access-list

Fuente Propia

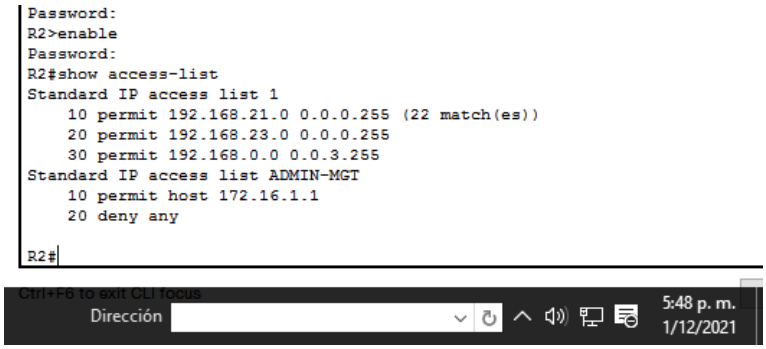
Figura 31. Configuración lista de Acceso.



Fuente: Propia

Se puede ver como El router 1 puede acceder al Router 2 en la figura 48.

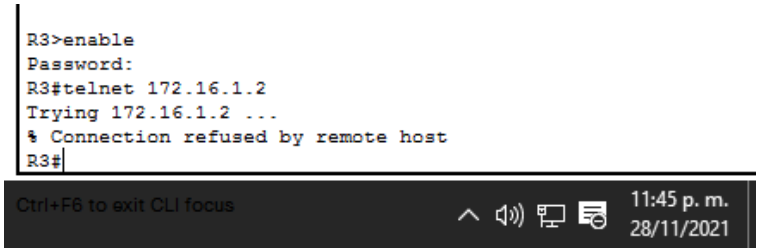
Figura 32. Verificar ACL



Fuente Propia

Se verifica el ACL y se evidencia match

Figura 33. Validación de no conexión por ip fuera de lista de acceso



Fuente: Propia

Se evidencia que al intentar desde ip fuera de lista de acceso no se permite el ingreso.

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

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

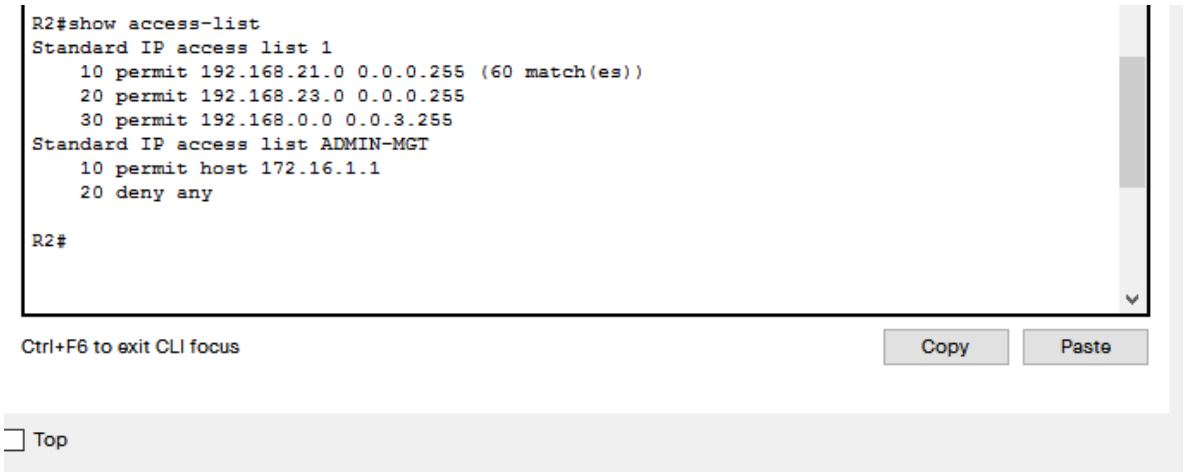
Tabla 25. Comando CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	*R2#show access-list*
Restablecer los contadores de una listade acceso	*R2#clear ip access-list counters*

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	*R2#show ip interface*
¿Con qué comando se muestran las traducciones NAT?	*R2#Show ip nat traslations* **Nota:** Las traducciones para la PC-A y la PC-C se agregarona la tabla cuando la computadora de Internet intentó hacerping 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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*R2#clear ip nat translation **|

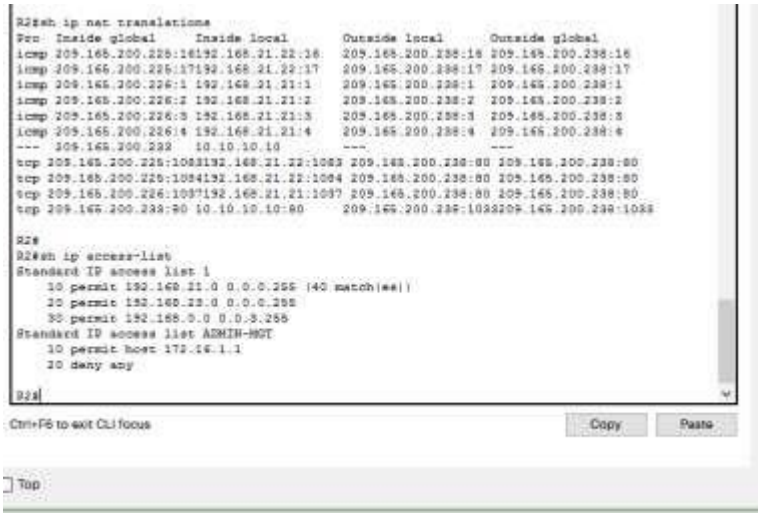
Fuente: Propia

Figura 34. Coincidencias recibidas



Fuente: Propia

Figura 35. Show ip Nat Translations



Fuente: Propia

CONCLUSIONES

Para la construcción de una Red bien sea en el simulador o en un entorno más real y/o tangible, es indispensable contar con un esquema de direccionamiento bien realizado, pues es la base en el proceso, para proceder a configurar los aspectos básicos de la Red, de esta manera se trabaja ordenadamente.

Para el correcto funcionamiento de la red es crucial configurar ajustes de seguridad en router y Switch, los cuales protegerán los dispositivos de intrusiones inesperadas, que afecten la red. El recordar que trabajar de forma inteligente al aplicar un poco más y que ese adicional en una configuración puede hacer un gran cambio para una red es de gran provecho como profesionales.

Se aplicaron Protocolos Importantes como el OSPF para direccionamiento de eficaz y DHCP para administrar, distribuir y supervisar las direcciones ip, los cuales nos demuestran que utilizar las herramientas adecuadas hacen más efectivo e incluso más rápido el trabajo. Este tipo de protocolos ayudan que el desarrollo y rendimiento de la Red sea más productiva.

REFERENCIAS

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-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, 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.

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.

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

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 Ingenieria (CONIITI) (pp. 1-6). IEEE.

Nguyen, V. G., & Kim, Y. H. (2016). SDN-based enterprise and campus networks: a case of VLAN management. Journal of Information Processing Systems, 12(3), 511-524.

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx