SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

OMAR YOVANY FORERO DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA DE SISTEMAS
CALAMAR - GUAVIARE
2021

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

OMAR YOVANY FORERO DIAZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO
PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

TUTORA:

MARIA ALEJANDRA LOPEZ HURTADO
MAGISTER

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA DE SISTEMAS
CALAMAR - GUAVIARE
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Calamar, Guaviare 28 de noviembre de 2021

AGRADECIMIENTOS

Agradecimiento primordial a Dios por traerme hasta este punto y darme la fortaleza para continuar a pesar de los obstáculos los cuales se me han presentado en el camino. A mi familia quienes han sido apoyo moral para nunca desfallecer, para mi madre que siempre será el mayor pilar y motivación para cada día desear más en mi camino hacia el conocimiento.

No puedo dejar por fuera a cada uno de mis tutores los cuales siempre me tendieron la mano cuando el camino se complicaba, ellos entre su gran profesionalismo dedicaron ese espacio para que comprendiera de manera adecuada y sencilla como solucionar los diversos inconvenientes educativos que se presentaban cuando un tema no era bien claro, siempre fue un sueño estar en esta etapa la cual en algún momento la vi inalcanzable. La ingeniería, una rama de la cual muchos hablan, pero pocos tienen el valor de abordarla. Mil gracias a todos los partícipes y acompañantes de este bonito proceso.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BRING YOUR OWN DEVICE (BYOD): es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

DHCP: Es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

IANA: Para poder acceder a una página web basta con introducir el nombre del dominio en el navegador. Este nombre se envía a un servidor que se encarga de "traducirlo" en una dirección IP y dirige al usuario a la página web esperada. Estos nombres y números designados como identificadores únicos se comparan con un conjunto estandarizado de parámetros del protocolo de Internet, permitiendo así la comunicación entre ordenadores. Una de las tareas de la Internet Assigned Numbers Authority (IANA) es administrar estos identificadores, entre muchas otras.

KERNEL: El núcleo o kernel es la parte central de un sistema operativo y es el que se encarga de realizar toda la comunicación segura entre el software y el hardware del ordenador.

Modelo OSI: El modelo de interconexión de sistemas abiertos (OSI, por sus siglas en inglés) es un modelo conceptual, creado por la Organización Internacional de Normalización (ISO), que permite que diversos sistemas de comunicación se comuniquen usando protocolos estándar. En resumidas cuentas, el modelo OSI proporciona a los diferentes sistemas informáticos un estándar para comunicarse entre sí. Se puede entender como un lenguaje universal de comunicación entre sistemas de redes informáticas que consiste en dividir un sistema de comunicación en siete capas abstractas, apiladas en vertical.

MULTICAST: Multicast se refiere a la entrega de datos de forma simultánea a un grupo de nodos receptores como destino, desde un emisor como origen.

NAT: Son las siglas de Network Address Translator, o en español traductor de direcciones de red. Su función es precisamente esa, traducir las direcciones para que sean posibles las conexiones. El NAT es una parte fundamental entre nuestros dispositivos e Internet. Forma parte del router, módem o el equipo que utilicemos para conectarnos a la red.

NSLOOKUP: Es una herramienta de línea de comandos muy práctica y fácil de usar, cuya función básica es encontrar la dirección IP de un equipo determinado o realizar una búsqueda DNS inversa (es decir, encontrar el nombre de dominio de una determinada dirección IP). nslookup se ejecuta en la interfaz de líneas de comando del sistema operativo correspondiente: mientras que los usuarios de Windows iniciarán el servicio a través del símbolo del sistema (CMD), los de Unix lo hacen a través del terminal. Además, en la actualidad existen varios servicios web que permiten usar nslookup también online.

OSPF: Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).

En una red OSPF, los direccionadores o sistemas de la misma área mantienen una base de datos de enlace-estado idéntica que describe la topología del área. Cada direccionador o sistema del área genera su propia base de datos de enlace-estado a partir de los anuncios de enlace-estado (LSA) que recibe de los demás direccionadores o sistemas de la misma área y de los LSA que él mismo genera. El LSA es un paquete que contiene información sobre los vecinos y los costes de cada vía. Basándose en la base de datos de enlace-estado, cada direccionador o sistema calcula un árbol de extensión de vía más corta, siendo él mismo la raíz, utilizando el algoritmo SPF.

POOL: Un pool DHCP son las direcciones comprendidas en un intervalo determinado, por ejemplo, de 192.168.1.10 a 192.168.1.50. Todas las direcciones IP comprendidas en ese intervalo las irá adjudicando el servidor DHCP a medida que los clientes las soliciten.

PROTOCOLOS: Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin.

Protocolo ARP: El Address Resolution Protocol (protocolo de resolución de direcciones) fue especificado en 1982 en el estándar RFC 826 para llevar a cabo la resolución de direcciones IPv4 en direcciones MAC. ARP es imprescindible para la transmisión de datos en redes Ethernet por dos razones: por un lado, las tramas de datos (también tramas Ethernet) de los paquetes IP solo pueden enviarse con ayuda de una dirección de hardware a los hosts de destino, pero el protocolo de Internet no puede obtener estas direcciones físicas por sí mismo. Por el otro, y debido a su limitada longitud, el protocolo IPv4 carece de la posibilidad de almacenar las direcciones de los dispositivos. Con un mecanismo de caché propio, el protocolo ARP también es, aquí, la solución más adecuada.

Red P2P: Es una red donde un grupo de personas o máquinas participan de forma completamente descentralizada. Es decir, es una red donde no hay un punto central de conexión o control, y donde las partes actúan de forma autónoma respondiendo a un protocolo de comunicaciones y consenso común. De esta forma, los integra.

SMB (Server Message Block): Es un protocolo cliente / servidor que gobierna el acceso a archivos y directorios completos, así como a otros recursos de red como impresoras, enrutadores o interfaces abiertas a la red. El intercambio de información entre los diferentes procesos de un sistema (también conocido como comunicación entre procesos) se puede manejar en base al protocolo SMB.

Trama Ethernet: Es la principal responsable de la correcta configuración de las reglas y del éxito de la transmisión de los paquetes de datos. Los datos enviados a través de Ethernet son transportados a través de la trama. Una trama Ethernet tiene un tamaño de entre 64 y 1518 bytes, dependiendo del tamaño de los datos que debe transportar.

VTY: Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15. El número de líneas vty que admite un router Cisco varía según el tipo de router y la versión de IOS. No obstante, la cantidad más frecuente de líneas vty configuradas es cinco. Estas líneas se numeran del 0 al 4 de manera predeterminada, aunque se pueden configurar líneas adicionales. Es necesario establecer una contraseña para todas las líneas vty disponibles. Puede configurarse la misma contraseña para todas las conexiones.

RESUMEN

Se hace énfasis en este documento a los ejercicios planteados para la obtención del título de Ingeniería en Sistemas en donde con los diversos capítulos ofrecidos en la plataforma CISCO y UNAD se ejecute el conocimiento que se ha estado adquiriendo durante el tiempo que conlleva el diplomado en cuestión. Con la certificación CCNP y la implementación de escenarios en los entornos prestos para un desarrollo óptimo de la actividad, se efectúa dentro del software Packet Tracer los ejercicios planteados haciendo énfasis en las distintas configuraciones que se realizan a partir de las topologías dada, se duplica el escenario referente a las pruebas de habilidades CCNA, en donde las configuraciones de redes y enrutamiento han de ser en estado óptimo para la solución de los puntos planteados dentro de la guía haciendo que exista una conmutación para permitir la entrega de la señal desde y hacia el destino requerido.

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

ABSTRACT

Emphasis is placed in this document on the exercises proposed to obtain the degree in Systems Engineering where with the various chapters offered on the CISCO and UNAD platform, the knowledge that has been acquired during the time involved in the diploma in question is executed. With the CCNP certification and the implementation of scenarios in the environments ready for an optimal development of the activity, the exercises proposed are carried out within the Packet Tracer software emphasizing the different configurations that are carried out from the given topologies, the scenario regarding the CCNA skills tests is duplicated, where the network and routing configurations must be in optimal state for the solution of the points raised within the guide making that there is a switching to allow the delivery of the signal to and from the required destination.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

Dentro del presente documento se desarrollará 2 escenarios propuestos con el fin, y se apliquen aquellos conocimientos aprendidos durante las fases propuestas en el diplomado de cisco, demostrando las habilidades que se han ido adquiriendo y el buen manejo que se le da a las herramientas ofrecidas para su fin.

En el desarrollo de las actividades y capítulos predispuestos, definimos los conceptos de una configuración optima y correcta entre los dispositivos, para así tener una conectividad apropiada en las redes creadas, es de resaltar el manejo de aquellos dispositivos que encontramos alojados en el software Cisco Packet Tracer, saber con especificación la topología que se manejara para no presentar percances al momento de la configuración.

Dentro del simulador se han de especificar aquellos comandos que cumplen con los requerimientos solicitados, saber cuál es su funcionalidad y aplicarlos correctamente en la configuración de los hosts al igual que en el desarrollo del esquema de direccionamiento IP de los dispositivos utilizados, verificando en última instancia que la conectividad y el transporte de los datos sea optimo.

1. ESCENARIO 1

Figura 1. Escenario 1

Fuente: Prueba de habilidades CCNA II-2021

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 5: 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 swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

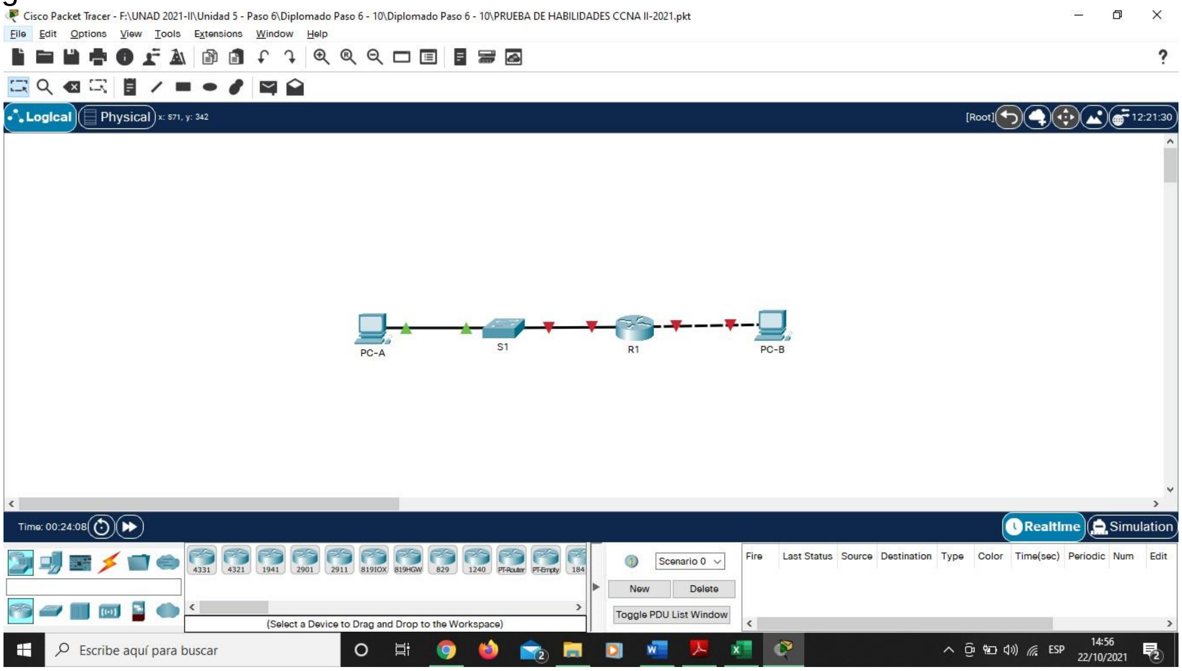
Tabla 1. Subnetting

Dirección IP Suministrada		
192.168.47.0 / 24		
Clase C	**R.R.R.H**	
POSICIONES TOMADAS PARA 100 HOST EN LA LAN1	**0**	**0000000**
	1 PARA SUBRED	**7 BITS PARA HOST**
LAN 1	**192.168.47.0 / 25**	
MASCARA SUBRED	**255.255.255.128**	
PRIMERA RED DISPONIBLE PARA LAN1	**192.168.47.1**	
ULTIMA RED DISPONIBLE PARA LAN1	**192.168.47.126**	
SALTO SEGUNDA SUBRED INCREMENTO EN VARIACION CON LA PRIMERA	**Valor máximo posición octeto (2^8), restando lo que dio en la máscara menos significativa.**	**256-128 = 128**
POSICIONES TOMADAS PARA 50 HOST EN LA LAN2	**00**	**000000**
	2 PARA SUBRED	**6 BITS PARA HOST**
LAN 2	**192.168.47.128 / 26**	
MASCARA SUBRED	**255.255.255.192**	
PRIMERA RED DISPONIBLE PARA LAN2	**192.168.47.129**	
ULTIMA RED DISPONIBLE PARA LAN2	**192.168.47.190**	
IP DISPONIBLE PARA FUTURA SUBRED	**192.168.47.191**	

Fuente: Elaboración Propia

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.

Figura 2. Simulación de escenario 1



Fuente: Elaboración Propia

Tabla 2. Direccionamiento

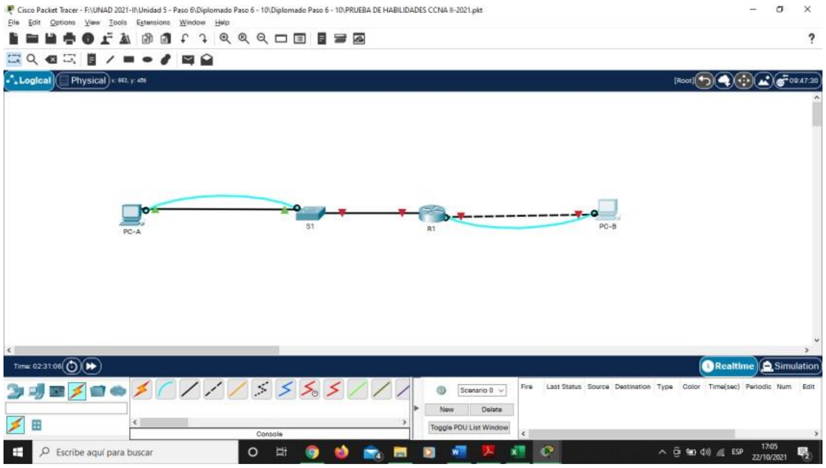
Ítem	**Requerimiento**
Dirección de Red	192.168.47.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	**192.168.47.1 /25**
R1 G0/0/0	**192.168.47.129 /26**
S1 SVI	**192.168.47.2 /25**
PC-A	**192.168.47.126 /25**
PC-B	**192.168.47.190 /26**

Fuente: Elaboración Propia

Parte 3: Configure aspectos básicos

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

Figura 3. Simulación escenario cable consola



Fuente: Elaboración Propia

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuraciones para R1

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
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 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: Escenario 2 Prueba de habilidades CCNA II-2021
En el siguiente proceso podemos ver reflejada la línea de código para desactivar la búsqueda DNS.

Router>enable **Ingreso modo privilegiado**
Router#configure terminal **Configuración de terminal para Router**
Enter configuration commands, one per line. End with CNTL/Z. **Se permite el ingreso a la configuración**
Router(config)#no ip domain-lookup **Desactivamos la búsqueda DNS**
Router(config)#

- Siguiendo las instrucciones ofrecidas en la tabla anterior ejecutaremos la línea de código que nos permitirá cambiar el nombre.

Router(config)#ho R1 **Asignamos nombre al Router**
R1(config)#

- Efectuamos la línea para cambias el Nombre de dominio.

R1>enable **Ingresamos al modo Privilegiado**
R1#configure terminal **Configuración de terminal para Router**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname
R1(config)#ip domain-name ccna-lab.com **Aplica el nombre de Dominio solicitado**
R1(config)#

- Se establece la Contraseña cifrada para el modo EXEC privilegiado.

R1(config)#enable secret ciscoenpass **Habilitar contraseña en el modo privilegiado**

- Se Sigue con las instrucciones para configurar una Contraseña de acceso a la consola.

R1(config)#line console 0 **Modo de configuración de línea de la consola.**
R1(config-line)#password ciscoconpass **Asignación contraseña consola**
R1(config-line)#login **Cumple la función de requerir autenticación al iniciar**

sesión
R1(config-line)#exit

- Se solicita según guía el establecer la longitud mínima para las contraseñas.

  R1(config)#security passwords min-length 10 **Longitud mínima solicita para contraseña**

- Continuando el contexto de la guía se debe crear un usuario administrativo en la base de datos local.

  R1(config)#username admin password admin1pass **Creación Usuario administrativo de datos local**

- Configurar el inicio de sesión en las líneas VTY para que use la base de datos local. Este proceso se realiza con el fin de permitir el acceso a un dispositivo Cisco a través de Telnet.

  R1(config)#line vty 0 4 **Iniciamos sesión en la línea VTY**
  R1(config-line)#password diplomadocisco **Se asigna una contraseña en este apartado para configurar un recurso secundario para ingreso netamente administrativo**
  R1(config-line)#login local **Habilita la base de datos local para la autenticación**
  R1(config-line)#

- Se procede a la Configuracion VTY solo aceptando SSH

  R1(config-line)#transport input SSH **Se define el protocolo que será usado para conectar la línea específica del router.**

- Efectuamos el Cifrado de las contraseñas de texto no cifrado.

  R1(config)#service password-encryption **Lo utilizamos para impedir que agentes externos o no autorizados puedan ver las contraseñas en el archivo de configuración.**

- Se procede con las instrucciones brindadas para Configurar un MOTD Banner

  R1(config)#banner motd #Esta es la configuración aplicada al switch Cisco de la UNAD, cualquier intromisión sin autorización tendrá consecuencias judiciales# **En este espacio dejaremos un mensaje colgado al arranque de la consola**

en R1 para que los usuarios tengan conocimiento de donde ingresaran y las consecuencias que conlleva recalar sin autorización

Observamos en este apartado la configuración que con anterioridad se estableció y en lo subrayado obtenemos el resultado pidiendo así la verificación del usuario y la contraseña asignada al modo privilegiado

Esta es la configuración aplicada al router Cisco de la UNAD, cualquier intromisión sin autorización tendrá consecuencias judiciales

User Access Verification

Password:
R1>enable
Password:
R1#

- El paso siguiente solicitado es Configurar interfaz G0/0/0

R1>enable **Acceso al modo privilegiado**
Password: **Ingreso contraseña asignada**
R1#config terminal **Configuración modo privilegiado**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/0 **Modo configuración interfaz Gigabit Ethernet**
R1(config-if)#ip address 192.168.47.129 255.255.255.192 **Asignación dirección IP**
R1(config-if)#description esta es la interfaz LAN2 **Se describe el nombre de la interfaz LAN configurada**
R1(config-if)#no shutdown **Habilitación interfaz seleccionada**
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line 21ill21colo n Interface GigabitEthernet0/0/0, changed state to up

- Se realiza los mismos pasos que anteriormente se ejecutaron, pero esta vez con la interface G0/0/1.

R1(config)#interface G0/0/1
R1(config-if)#description Esta es la Interfaz LAN1
R1(config-if)#ip address 192.168.47.1 255.255.255.128
R1(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line 22ill22colo n Interface GigabitEthernet0/0/1, changed state to up

- Acto seguido se desea generar una clave RSA

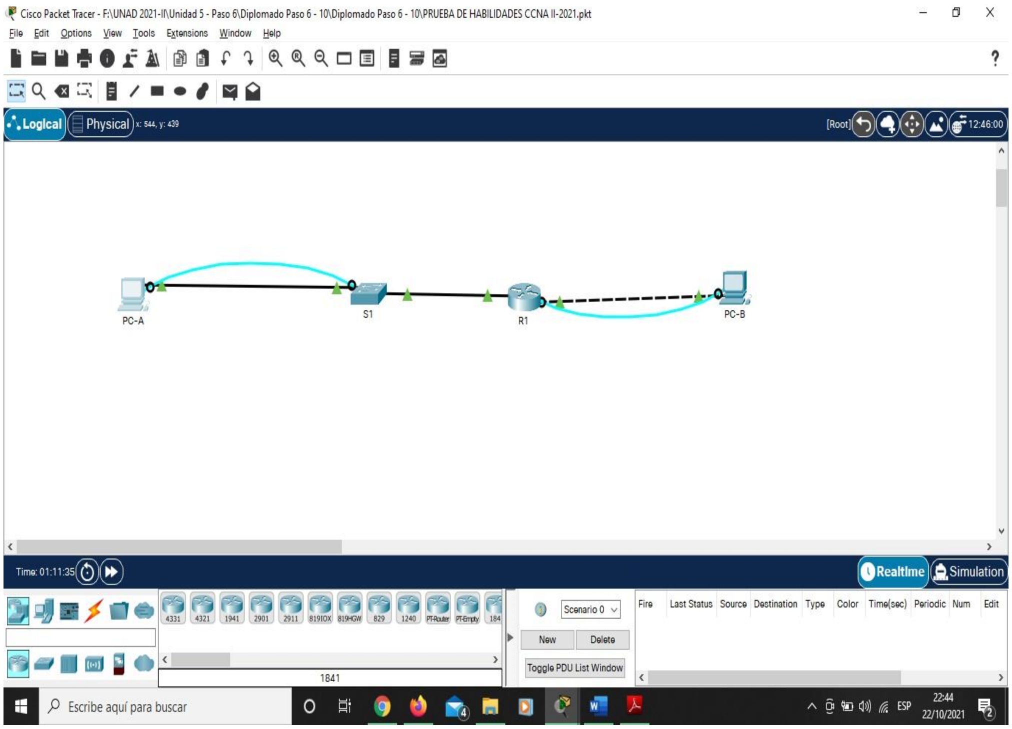
  R1(config)#ip domain name ccna-lab.com **configura el nombre de dominio IP**
  R1(config)#crypto key generate rsa **habilitar el servidor SSH en el switch y generar la claves RSA.**
  The name for the keys 22ill be: R1.ccna-lab.com
  Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater 22il 512 may take a few minutes.

  How many bits in the modulus [512]: 1024 **Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo en este caso se opto por la 1024 dado que esta aunque tarda es mas segura.**

  % Generating 1024 bit RSA keys, keys 22ill be non-exportable…[OK]

  R1(config)#exit **Salimos a la entra principal del modo privilegiado**
  R1#wr **Por medio de este comando guardamos la configuración realizada**
  Building configuration…
  [OK]
  R1#

Figura 4. Conexión establecida



Fuente: Elaboración Propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4. Configuraciones para S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	
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 que use la base de datos local	
Configurar las líneas VTY para que	

acepten únicamente las 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 de direccionamiento.

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

- Desactivación búsqueda DNS.

  Switch>enable **Habilitación modo privilegiado**
  Switch#configure terminal **Configuración interfaz**
  Enter configuration commands, one per line. End with CNTL/Z.
  Switch(config)#no ip domain-lookup **Desactivamos la traducción de nombres a dirección del dispositivo.**

- Nombramos el switch con los datos dados.

  Switch(config)#ho S1 **Proceso para asignar nombre al Switch**
  S1(config)#

- Configuramos el nombre de dominio.

  S1(config)#ip domain-name ccna-lab.com **Comando para asignar el dominio solicitado**

- Contraseña cifrada para el modo EXEC privilegiado.

  S1(config)#enable secret ciscoenpass **Esta práctica tiene como objetivo configurar una contraseña para la conexión de consola al modo de usuario y también configurar contraseñas para las sesiones de terminal virtual**

- Asignamos la contraseña de acceso a la consola.

  S1(config)#line console 0 **Habilita el modo de configuración de la consola, el cero representa la primera interfaz.**
  S1(config-line)#password ciscoconpass **Asigna contraseña de acceso**

S1(config-line)#login

- Creamos un usuario administrativo en la base de datos local

  S1(config-line)#exit **Salimos a la configuración inicial**
  S1(config)#username admin password admin1pass **Creamos el nuevo usuario**

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

  S1(config)#line vty 0 15 **Iniciamos sesión en la línea VTY**
  S1(config-line)#password diplomadocisco **Se asigna una contraseña en este apartado para configurar un recurso secundario para ingreso netamente administrativo**
  S1(config-line)#login local **Habilita la base de datos local para la autenticación**

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

  S1(config-line)#transport input SSH **Comando usado para solo conexiones SSH**.

- Cifrar las contraseñas de texto no cifrado

  S1(config)#service password-encryption **Lo utilizamos para impedir que agentes externos o no autorizados puedan ver las contraseñas en el archivo de configuración.**

- Configurar un MOTD Banner

  S1(config)#banner motd #Esta es la configuración aplicada al switch Cisco de la UNAD, cualquier intromisión sin autorización tendrá consecuencias judiciales#

  Se aplica un banner para que al inicio de la consola aparezca lo ingresado

- Generar una clave de cifrado RSA

  S1(config)#ip domain name ccna-lab.com **Configura el nombre de dominio IP**
  S1(config)#crypto key generate rsa **Habilitar el servidor SSH en el switch y**

generar las claves 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 **Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo en este caso se opto por la 1024 dado que esta aunque tarda es mas segura**
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

- Configuramos la interfaz de administración (SVI)

S1(config)#int vlan 1 **Habilitamos el modo configuración de la interfaz VLAN1**
*Mar 1 1:56:19.651: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip address 192.168.47.2 255.255.255.128 **Se establece la dirección IPV4 de la tabla de direcciones la segunda disponible.**
S1(config-if)#no shutdown **Subimos la interface**
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

- Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento

S1(config-if)#exit
S1(config)#ip default-gateway 192.168.47.1 **Se asigna el Gateway predeterminado conforme a la tabla de direcciones.**
S1(config)#exit
S1#wr **Guardamos las configuraciones realizadas**
Building configuration...
[OK]
S1#

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**.

Se procede a verificar las configuraciones realizadas mediante el comando siguiente en la PC-A

C:\>ipconfig /all
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address. 0005.5ED6.C9E8
Link-local IPv6 Address. ....: FE80::205:5EFF:FED6:C9E8
IPv6 Address. ....: ::
IPv4 Address. ....: 192.168.47.126
Subnet Mask.................... : 255.255.255.128
Default Gateway. ....: ::0.0.0.0
DHCP Servers. ....: 0.0.0.0
DHCPv6 IAID.....................:
DHCPv6 Client DUID..............: 00-01-00-01-8C-51-79-67-00-05-5E-D6-C9-E8
DNS Servers.................... : ::0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address................: 0007.EC1A.4B03
Link-local IPv6 Address. ....: ::
IPv6 Address. ....: ::
IPv4 Address. ....: 0.0.0.0
Subnet Mask.................... : 0.0.0.0
Default Gateway. ....: ::0.0.0.0
DHCP Servers. ....: 0.0.0.0
DHCPv6 IAID.....................:
DHCPv6 Client DUID..............: 00-01-00-01-8C-51-79-67-00-05-5E-D6-C9-E8
DNS Servers.................... : ::0.0.0.0

Tabla 5. Asignación de Direcciones PC-A

PC-A Network Configuration	
Descripción	**Este es la Pc A configurada**
Dirección física	**0005.5ED6.C9E8**
Dirección IP	**192.168.47.126 /25**
Máscara de subred	**255.255.255.128**
Gateway predeterminado	**192.168.47.1**

Fuente: Elaboración propia

Se procede a verificar las configuraciones realizadas mediante el comando siguiente en la PC-B

C:\>ipconfig /all

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address................. 0060.3E7C.04D9
Link-local IPv6 Address........ : FE80::260:3EFF:FE7C:4D9
IPv6 Address...................: ::
IPv4 Address...................: 192.168.47.190
Subnet Mask. .... : 255.255.255.192
Default Gateway................ : ::192.168.47.129
DHCP Servers...................: 0.0.0.0
DHCPv6 IAID.....................:
DHCPv6 Client DUID..............: 00-01-00-01-35-41-2C-73-00-60-3E-7C 04-D9
DNS Servers. .... : ::0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address................: 0007.EC64.7A32
Link-local IPv6 Address........ : ::
IPv6 Address...................: ::
IPv4 Address...................: 0.0.0.0
Subnet Mask. .... : 0.0.0.0
Default Gateway................ : ::0.0.0.0
DHCP Servers...................: 0.0.0.0
DHCPv6 IAID.....................:
DHCPv6 Client DUID..............: 00-01-00-01-35-41-2C-73-00-60-3E-7C 04-D9
DNS Servers. .... : ::0.0.0.0

Tabla 6. Asignación de Direcciones PC-B

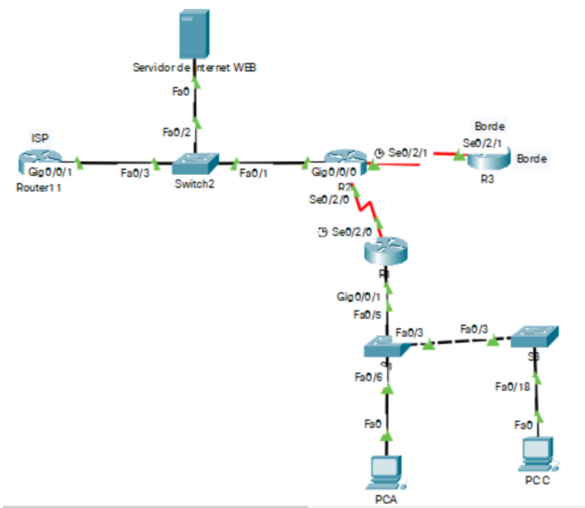
PC-B Network Configuration	
Descripción	**Este es la Pc B**
Dirección física	**0060.3E7C.04D9**
Dirección IP	**192.168.47.190 /26**
Máscara de subred	**255.255.255.192**
Gateway predeterminado	**192.168.47.129**

Fuente: Elaboración Propia

2. ESCENARIO 2

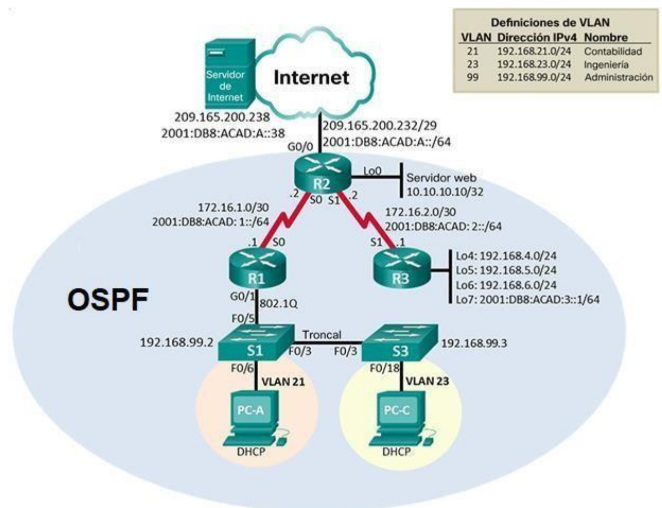
TOPOLOGÍA

Figura 5. Topología 2 realizada



Fuente: Elaboración Propia

Figura 6. Topología 2 ofrecida



Fuente: Prueba de habilidades CCNA II-2021

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 7. Inicializar los dispositivos

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

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

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 8. Configuración Computadora Internet

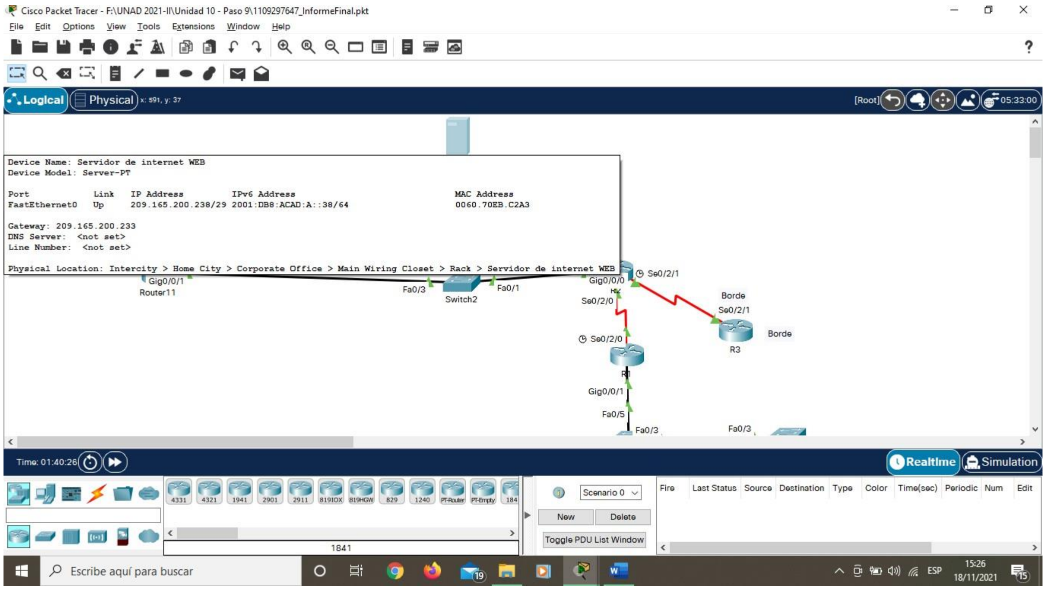
Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/29
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1 /64

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

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

- **Se anexa pantallazo de configuración para la computadora de Internet, en donde observamos la asignación de direcciones a esta.**

Figura 7. Asignación de Direcciones



Fuente: Elaboración Propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Instrucciones 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	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 de topología 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 S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

- Procedemos con la configuración del router con los ítems solicitados en la tabla.

`r1(config)#ho R1` **Asignamos el nombre para el router**
`R1(config)#enable` secret class **habilita la contraseña Mod-Privilegiado**
`R1(config)#line console 0` **Modo de configuración de línea de la consola**
`R1(config-line)#password cisco` **Asignación contraseña consola**
`R1(config-line)#login` **Cumple la función de requerir autenticación al iniciar sesión**
`R1(config-line)#line vty 0 4` **Iniciamos sesión en la línea VTY** `R1(config-line)#password cisco` **Se asigna una contraseña en este apartadopara configurar un recurso secundario para ingreso netamente administrativo**
`R1(config-line)#login` **Cumple la función de requerir autenticación al iniciar sesión**
`R1(config-line)#service password-encryption` **Lo utilizamos para impedir que agentes externos o no autorizados puedan ver las contraseñas en el archivo de configuración.**
`R1(config)#banner motd #se prohibe el acceso no autorizado#` **En este espacio dejaremos un mensaje colgado al arranque de la consola en R1 para que los usuarios tengan conocimiento de donde ingresaran y las consecuencias que conlleva recalar sin autorización**

`R1(config)#ipv6 unicast-routing` **Nos brinda la posibilidad de habilitar el routing IPv6 en el router. De este modo se hace necesario antes de poder configurar cualquier protocolo de routing IPv6**

`R1(config)#int s0/2/0` **Ingreso a la interfaz serial**

`R1(config-if)#ip address 172.16.1.1 255.255.255.252` **Asignamos la dirección IPv4 para la interfaz**

`R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64` **Asignamos la dirección IPv6 para la interfaz**

`R1(config-if)#clock rate 128000` **Establecemos la velocidad en bps**

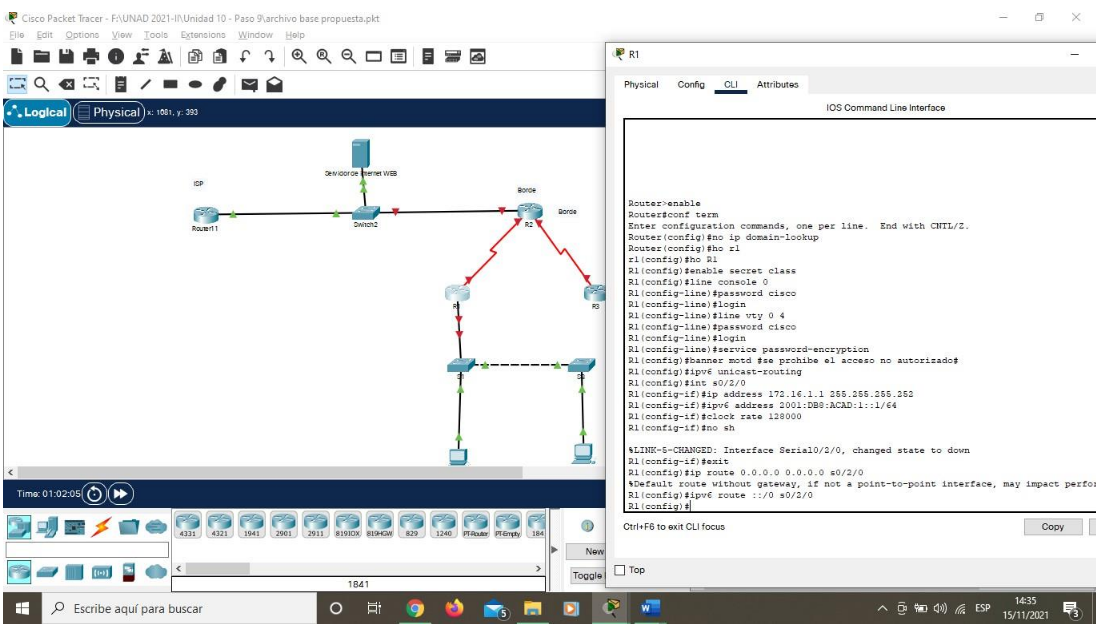
`R1(config-if)#no sh` **Habilitamos la interfaz**

```
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
R1(config-if)#exit
```

`R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0` **configuración rutas predeterminadas**

```
%Default route without gateway, if not a point-to-point
interface, may impact performance
R1(config)#ipv6 route ::/0 s0/2/0
R1(config)#
```

Figura 8. Configuración R1



Fuente: Elaboración Propia

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Instrucciones R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
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	
Habilitar el servidor HTTP	Esta versión no funciona para ninguno
Mensaje MOTD	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 G0/0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección 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: Escenario 2 Prueba de habilidades CCNA II-2021

- **Se procede en este apartado a seguir con las instrucciones dadas en la tabla anterior, es claro que vamos a realizar un procesos similar al ejecutado en R1 a diferencia de nuevas instrucciones.**

```
Router>enable
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ho R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config)#ip http server
```
Como se menciona en la tabla, esta versión es no funcional para este escenario trabajado siguiendo instrucciones.

```
^
% Invalid input detected at '^' marker.
```

Para cada interfaz se asigna lo solicitado de tal fin que cada una obtenga el resultado deseado

R2(config)#int s0/2/0
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#int s0/2/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#description conexión entre R2 y R1 **Se le asigna una descripción a la interfaz**
R2(config-if)#no sh

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line 36ateway36o n Interface Serial0/2/0, changed state to up

R2(config-if)#int s0/2/1
R2(config-if)#ip address 172.16.2.1 255.255.255.252
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to down
R2(config-if)#exit
R2(config)#int g0/0/0
R2(config-if)#description interface hacia internet
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#int G0/0/0
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64
R2(config-if)#no sh

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line 36ateway36o n Interface GigabitEthernet0/0/0, changed state to up

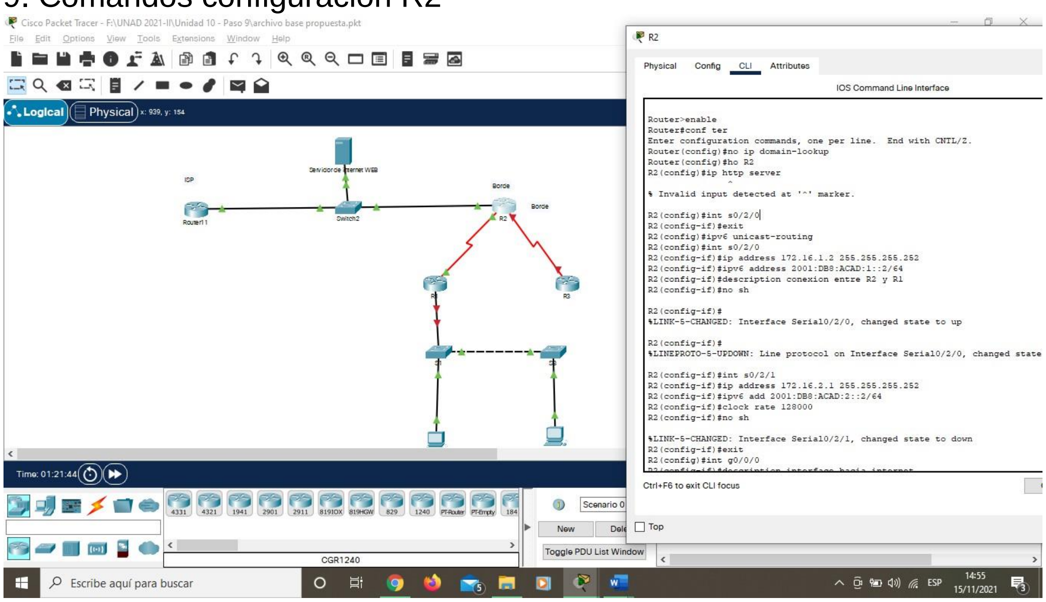
- **Para este proceso se verifica en la topología presentada y es de observar que se cuenta con Direcciones LoopBack que han de ser configuradas según requerimientos**

```
R2(config-if)#exit
R2(config)#int loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line 37ateway37o n Interface Loopback0,
changed state to up

R2(config-if)#description servidor WEB
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
```

- **Se asigna una Ruta predeterminada**

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
%Default route without Gateway, if not a point-to-point
interface, may impact performance
R2(config)#ipv6 route ::/0 G0/0/0
R2(config)#
```

Figura 9. Comandos configuración R2



Fuente: Elaboración propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11. Instrucciones configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
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	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/2/1	Establecer la descripción Establezca la dirección Ipv4. Utilizar la siguiente direccióndisponible 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 direccióndisponible en la subred.
Interfaz loopback 5	Establezca la dirección Ipv4. Utilizar la primera direccióndisponible en la subred.
Interfaz loopback 6	Establezca la dirección Ipv4. Utilizar la primera direccióndisponible en la subred.
Interfaz loopback 7	Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones.

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

- **Siguiendo las distintas instrucciones el proceso siguiente nos permitirá realizar la configuración pertinente para el Router 3**

Router>enable **Habilitación modo privilegiado**
Router#conf term **Configuración interfaz**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup **Desactivamos la traducción de nombres a dirección del dispositivo.**
Router(config)#ho R3 **Proceso para asignar nombre al Router**
R3(config)#enable secret class **Esta práctica tiene como objetivo configurar una contraseña para la conexión de consola al modo de usuario y también configurar contraseñas para las sesiones de terminal virtual**
R3(config)#line console 0 **Habilita el modo de configuración de la consola, el cero representa la primera interfaz.**
R3(config-line)#password cisco **Asigna contraseña de acceso**

```
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #Se 39ateway el acceso no autorizado#
R3(config)#ipv6 unicast-routing
R3(config)#int s0/2/1
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no sh

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line 39ateway39o n Interface Serial0/2/1,
changed state to up
```

Asignación de Direcciones Loopback

```
R3(config)#int loopback 4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line 39ateway39o n Interface Loopback4,
changed state to up
```

```
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#exit
R3(config)#int loopback 5

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line 40ateway40o n Interface Loopback5,
changed state to up

R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#exit
R3(config)#int loopback 6

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line 40ateway40o n Interface Loopback6,
changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface loopback 7

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line 40ateway40o n Interface Loopback7,
changed state to up

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
```

- **Se asigna una Ruta predeterminada**

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1
%Default route without 40ateway, if not a point-to-point
interface, may impact performance
R3(config)#ipv6 route ::/0 S0/2/1
R3(config)#
```

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuración S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del switch	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	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

A continuación, el proceso a seguir es el de la configuración básica del switch en donde por medio de la tabla, e instrucciones personalizadas se les asigna datos específicos.

```
S1>enable
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#)banner motd #Se prohibe el acceso no autorizado#
^
% Invalid input detected at '^' marker.
S1(config)#banner motd #Se prohibe el acceso no autorizado#
S1(config)#
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Instrucciones configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del switch	S3
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	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

Como en instrucciones anteriormente realizadas continuamos con configuraciones básicas para el Switch 3, asignación de contraseñas, cifrado y banner motd

```
S3>enable
S3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Se prohibe el acceso no autorizado#
S3(config)#exit
S3#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

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 14. Veracidad de los Ping

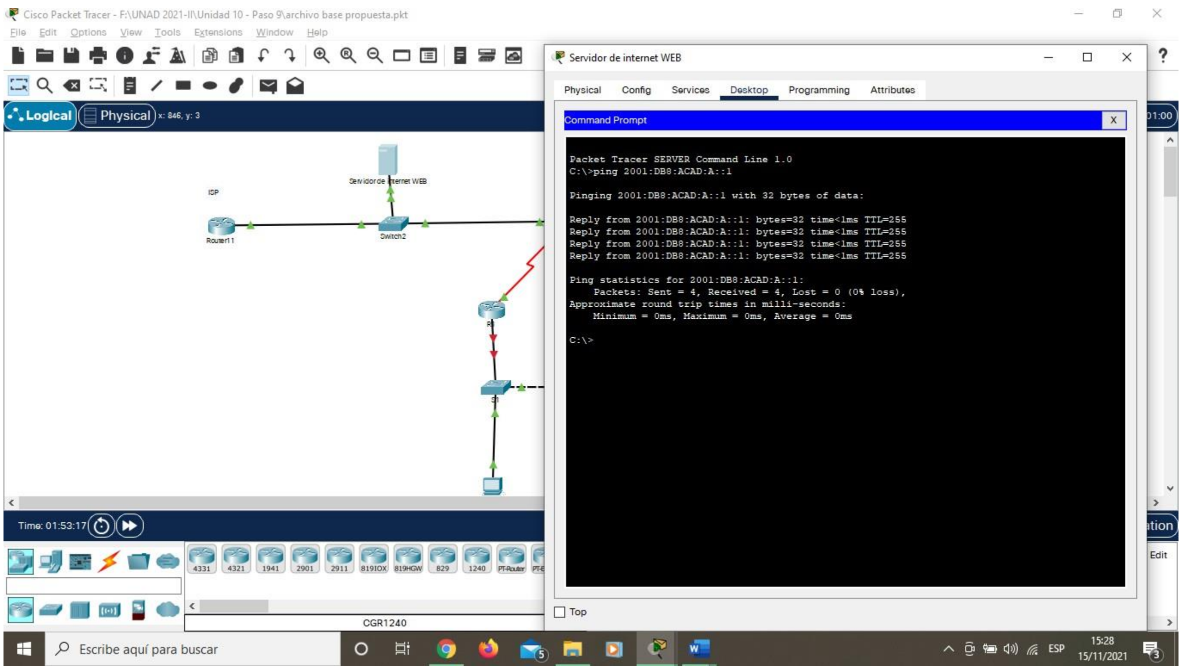
Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	Exitosos
R2	R3, S0/2/1	172.16.2.2	Exitosos
PC de Internet	Gateway predeterminado	2001:DB8:ACAD:A::1	Exitosos

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
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 = 1/10/19 ms


R2#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/15/17 ms


C:\>ping 2001:DB8:ACAD:A::1

Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
```

```
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 10. Veracidad de los Ping



Fuente: Elaboración Propia

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

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 15. Configuración S1 asignación direcciones VLAN

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 de administración.	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 el Gateway predeterminado.
Forzar el enlace troncal en la interfazF0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfazF0/5	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	
Apagar todos los puertos sin usar	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ho S1
```
`S1(config)#Vlan 21` **Ingreso a las VLAN**

`S1(config-vlan)#name contabilidad` **Asignacion de nombres según tabla de equivalencias en la topología del escenario #2**

```
S1(config-vlan)#vlan 23
S1(config-vlan)#name 45ateway45o
S1(config-vlan)#vlan 99
```

S1(config-vlan)#name 46ateway46o n46ón
S1(config-vlan)#exit
S1(config)#int vlan 99 **Ingresamos a la Vlan para de este modo configurar la Ip solicitada según tabla de configuración**
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip add 192.16.99.2 255.255.255.0 **asignación dirección de Vlan 99**
S1(config-if)#no sh
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#sw mode trunk **Ingreso al modo Trunk**

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line 46ateway46o n Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line 46ateway46o n Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line 46ateway46o n Interface Vlan99, changed state to up

S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#sw mode trunk **permite realizar un enlace troncal de todas y cada una de las VLANs**
S1(config-if)#switchport trunk native vlan 1 **Asignacion VLAN nativa**
S1(config-if)#exit
S1(config)#int f0/3
S1(config-if)#sw trunk native vlan 1
S1(config-if)#exit
S1(config)#int range f0/1- f0/2 **configuramos interfaces simultáneamente**
S1(config-if-range)#sw mode 46atewa
S1(config-if-range)#int range f0/7- f0/24
S1(config-if-range)#sw mode 46atewa
S1(config-if-range)#exit
S1(config)#int f0/6
S1(config-if)#sw acc vlan 21 **Asignación interfaz F0/6 a la Vlan 21**

```
S1(config-if)#
```

`S1(config)#int range f0/7 - f0/24` **establecemos el rango de los puertos sin usar y los apagamos**

```
S1(config-if-range)#no sh
S1(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
```

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuración S3 Redes VLAN

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 nombre a 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 de topología
Asignar el Gateway predeterminado.	Asignar la primera dirección IP en la subred como Gatewaypredeterminado.
Forzar el enlace troncal en la interfaz	Utilizar la red VLAN 1 como VLAN nativa

F0/3	
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

- **Se procede con la configuración requerida en la tabla**

```
Switch>en
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ho s3
s3(config)#ho S3
S3(config)#vlan 21  Se asignan los nombres requeridos para las VLANs
S3(config-vlan)#name contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name 49ccess49lo
S3(config-vlan)#vlan 99
S3(config-vlan)#name 49ccess49lo n49ón
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line 49ccess49lo n Interface Vlan99, changed
state to up

S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no sh
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1  Gateway predeterminado
S3(config)#int f0/3
S3(config-if)#sw mode trunk
S3(config-if)#sw trunk native vlan 1
S3(config-if)#exit
S3(config)#int range f0/1 - f0/2
```

S3(config-if-range)#sw mode 50ccess **Con este comando, la interfaz cambia al modo de acceso permanente.**
S3(config-if-range)#int ran f0/7 - f0/24
S3(config-if-range)#sw MODE ACCess
S3(config-if-range)#exit
S3(config)#int f0/18
S3(config-if)#sw acc vlan 21 **Asignación interface F0/18 a la VLAN 21**
S3(config-if)#exit
S3(config)#int range f0/7 - f0/17 **Se establece el rango de los puertos que se apagaran**
S3(config-if-range)#sh

```
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to
administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down
S3(config-if-range)#int range f0/19 - f0/24
S3(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
S3(config-if-range)#
```

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración subinterfaz R1 802.1Q

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

	Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 enG0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

- **Se procede directamente con la configuracion preestablecida en la tabla para la configuración, descripción, asignación VLAN y Direccionamiento IP de las subinterfaces 802.1Q. 21 23 99.**

```
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0/1.21
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1.21, changed state to up

R1(config-subif)#description LAN contabilidad
R1(config-subif)#enc dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0/1.23
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1.23, changed state to up

R1(config-subif)#desc Lan ingenieria
R1(config-subif)#en dot1q 23
```

R1(config-subif)#ip add 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0/1.99
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up

R1(config-subif)#description LAn administracion
R1(config-subif)#en dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0/1
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#int g0/0/1.21 **Configuración Subinterfaz**
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, changed state to up

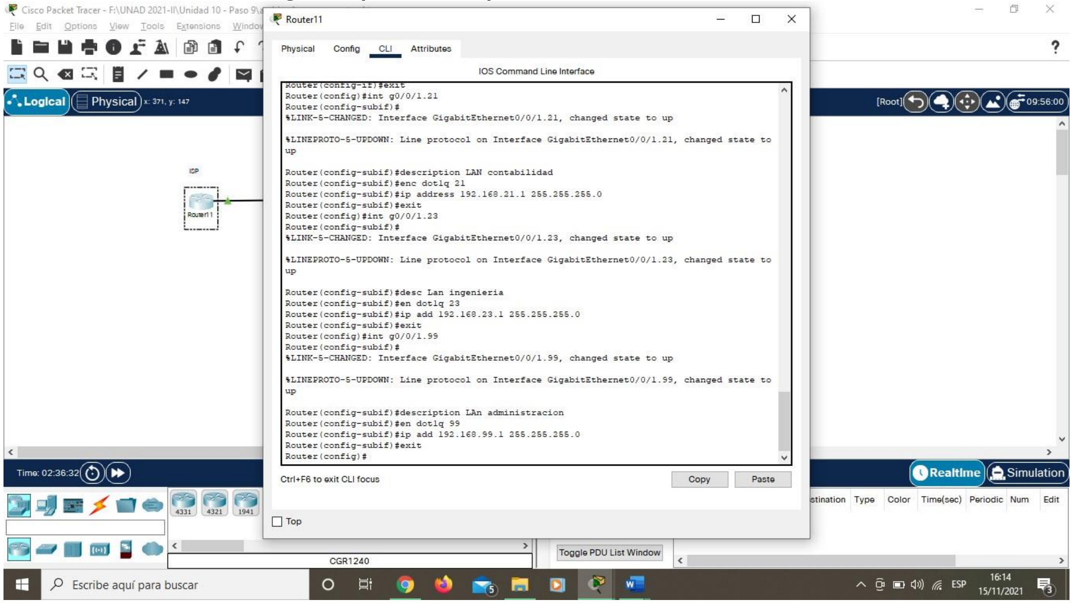
Router(config-subif)#description LAN contabilidad
Router(config-subif)#enc dot1q 21 **protocolo que permite que el router tenga enlace troncal.**
Router(config-subif)#ip address 192.168.21.1 255.255.255.0

```
Router(config-subif)#exit
Router(config)#int g0/0/1.23
```
ingreso configuración interfaz Giga

```
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to up

Router(config-subif)#desc Lan ingenieria
Router(config-subif)#en dot1q 23
Router(config-subif)#ip add 192.168.23.1 255.255.255.0
```
Asignación direcciones para la interfaz predispuesta en línea de código

```
Router(config-subif)#exit
Router(config)#int g0/0/1.99
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up

Router(config-subif)#description LAn administracion
Router(config-subif)#en dot1q 99
Router(config-subif)#ip add 192.168.99.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

Figura 11. Veracidad Códigos aplicados para Subinterfaz



Fuente: Elaboración Propia

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 18. Conectividad de la Red

Desde	A	Dirección IP	Resultados de ping-+
S1	R1, dirección VLAN 99	192.168.99.1	(5/5)
S3	R1, dirección VLAN 99	192.168.99.1	(5/5)
S1	R1, dirección VLAN 21	192.162.21.1	(5/5)
S3	R1, dirección VLAN 23	192.162.23.1	(5/5)

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

S1#ping 192.168.99.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2
seconds:
¡!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/9/19 ms
```

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 = 0/0/0
ms
```

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 = 0/0/1
ms
```

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 = 0/0/1
ms
```

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 19. Instrucciones OSPF R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadasdirectamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 47
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)#passive-interface g0/0/1
```

Se establecen las interfaces configuradas 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
R1(config-router)#
```

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

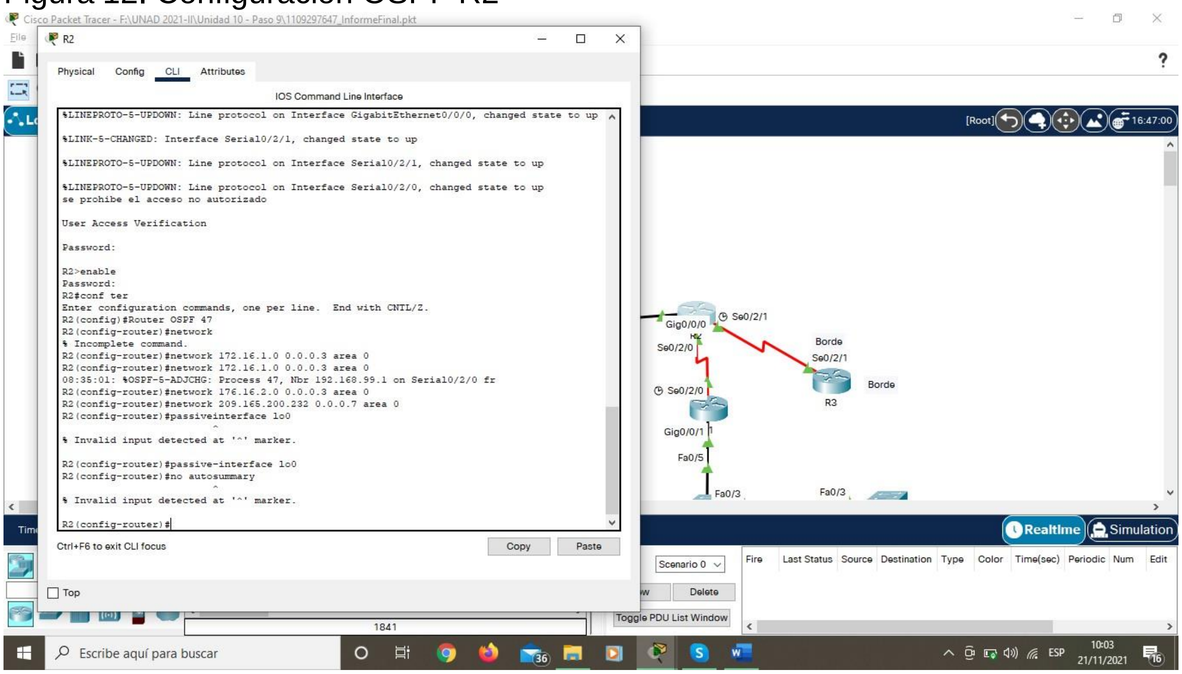
Tabla 20. Instrucciones OSPF R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
R2>enable
Password:
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Router OSPF 47
R2(config-router)#network
% Incomplete command.
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
08:35:01: %OSPF-5-ADJCHG: Process 47, Nbr 192.168.99.1 on
Serial0/2/0 fr
R2(config-router)#network 176.16.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.232 0.0.0.7 area 0
R2(config-router)#passive-interface lo0
R2(config-router)#no autosummary
^
% Invalid input detected at '^' marker.
```

Figura 12. Configuración OSPF R2



Fuente: Elaboración Propia

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Instrucciones OSPFV3 R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

- **Existe un error en la guía y la versión 3 es para IPV6, estipulado que se demarca en la tabla que debemos en R2 anunciar Ipv4 cuando la OSPFv3 es para IPv6, mas sin embargo se deja la evidencia del proceso realizado.**

```
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router Ospf 47
R2(config-rtr)#router-id 1.1.1.1
R2(config-rtr)#int s0/2/0
R2(config-if)#ipv6 ospf 2 area 0
R2(config-if)#
10:14:37: %OSPFv3-5-ADJCHG: Process 2, Nbr 1.1.1.1 on Serial0/2/0
from LOADING to FULL, Loading Done

R2(config-if)#int g0/0/0
R2(config-if)#ipv6 ospf 2 area 0
R2(config-if)#
```

No podemos establecer las interfaces de la Loopback como pasivas debido a que esta no tiene direcciones bajo Ipv6

```
R2(config-if)#no autosummary
^
% Invalid input detected at '^' marker.
```

Se opta por verificar las direcciones que contienen loopback IPV6 y se encontró que el router 3 contiene estas especificaciones e igualmente procedemos a la configuración pertinente

```
R3#conf term
```

```
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 47
R3(config-rtr)#router-id 2.2.2.2
R3(config-rtr)#exit
```

Esto debe ser para las redes IPV6

```
R3(config)#int s0/2/1
R3(config-if)#ipv6 ospf 47 area 0
R3(config-if)#int loop7
R3(config-if)#ipv6 ospf 47 area 0
R3(config-if)#exit
R3(config)#router ospf 47
R3(config-router)#
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3(config)#ipv6 router ospf 47
R3(config-rtr)#passive-interface lo4
R3(config-rtr)#passive-interface lo5
R3(config-rtr)#passive-interface lo6
R3(config-rtr)#exit
R3(config)#exit
R3#
```

En cuanto a la instrucción de sumarización, en este protocolo no se realiza y se coloca la wildcard, en ipv6 no se realiza.

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 22. Comandos Utilizados OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show Ip Protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Debug ip OSPF

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
R2#show ip protocols

Routing Protocol is "ospf 47"
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:
172.16.1.0 0.0.0.3 area 0
176.16.2.0 0.0.0.3 area 0
209.165.200.232 0.0.0.7 area 0
Passive Interface(s):
Loopback0
Routing Information Sources:
Gateway Distance Last Update
10.10.10.10 110 00:25:39
192.168.99.1 110 00:27:03
Distance: (default is 110)
```

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 23. Instrucciones R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP enla VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	

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: Escenario 2 Prueba de habilidades CCNA II-2021

```
R1>enable
Password:
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
```
Proceso para excluir un rango de direcciones Vlan21
```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```
Proceso para excluir un rango de direcciones Vlan21
```
R1(config)#ip DHCP pool ACCT
```
Crea un conjunto de ip con el nombre elegido e ingresa al modo de configuracion DHCP
```
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
```
se establece el Gateway predeterminado

```
R1(dhcp-config)#
```

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. NAT estática y dinámica en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.233**
Asignar la interfaz interna y externa para laNAT estática	
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	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
R2>enable
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
```

R2(config)#username webuser privilege 15 password cisco12345 **se crea una cuenta de usuario para una base de datos local**

R2(config)#

Este comando no nos lo toma

```
R2(config)#ip http server
^
% Invalid input detected at '^' marker.

R2(config)#
```

Este comando podemos observar que tampoco nos la toma para la bases de datos local

```
R2(config)#ip http authentication local
^

% Invalid input detected at
'^' marker.
```

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233 **creamos la dirección NAT estática al servidor web**

- **Por medio de la configuración privilegiada se realiza el proceso de asignar la interfaz interna y externa para la NAT estática.**

```
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0/0
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
R2(config-if)#int lo 0
R2(config-if)#ip nat inside
```

```
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g0/0/0
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
R2(config-if)#int lo 0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.68.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255

R2(config)#
```

`R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248` **Definimos el pool de direcciones con las indicaciones ofrecidas en la tabla**

```
R2(config)#ip nat inside source list 1 pool INTERNET
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

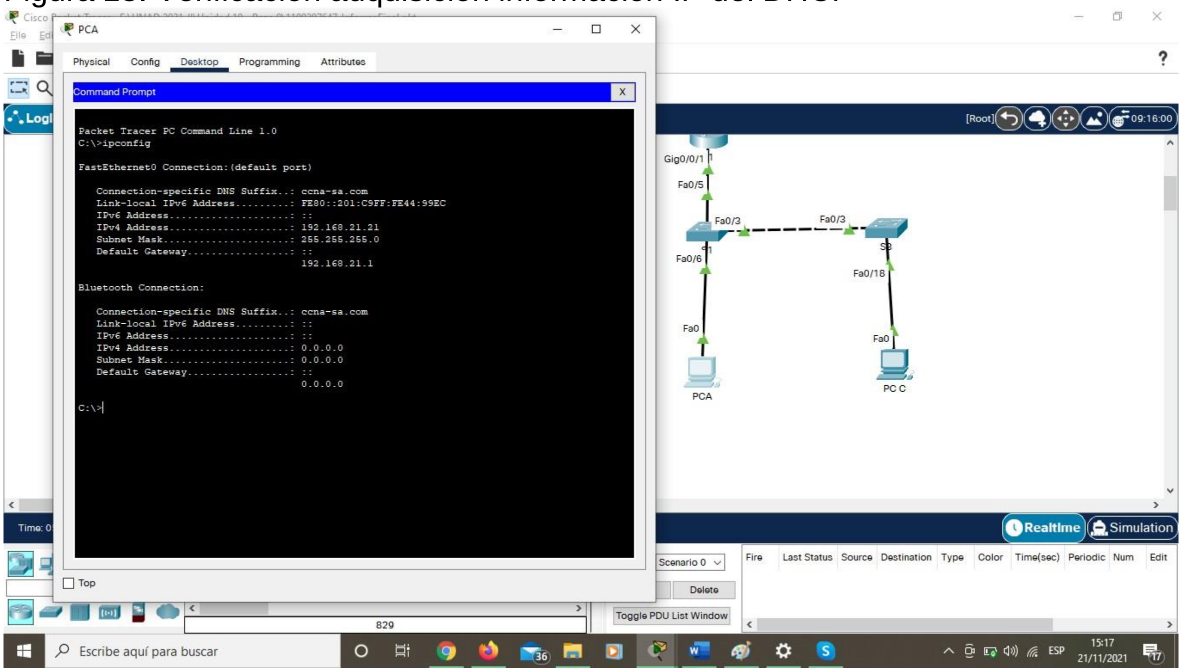
Tabla 25. Instrucciones verificación Protocolo DHCP y NAT

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

Verificar que la PC-A pueda hacer ping ala PC-C **Nota:** Quizá sea necesario deshabilitar elfirewall de la PC.	
Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

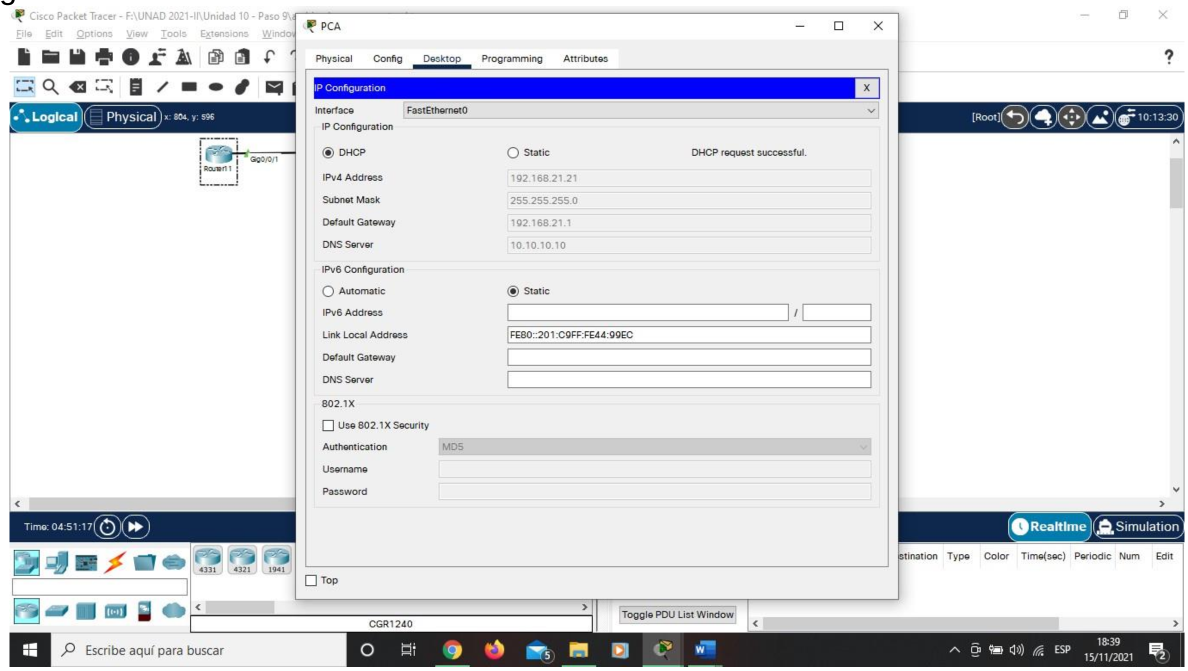
Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

Figura 13. Verificación adquisición información IP del DHCP



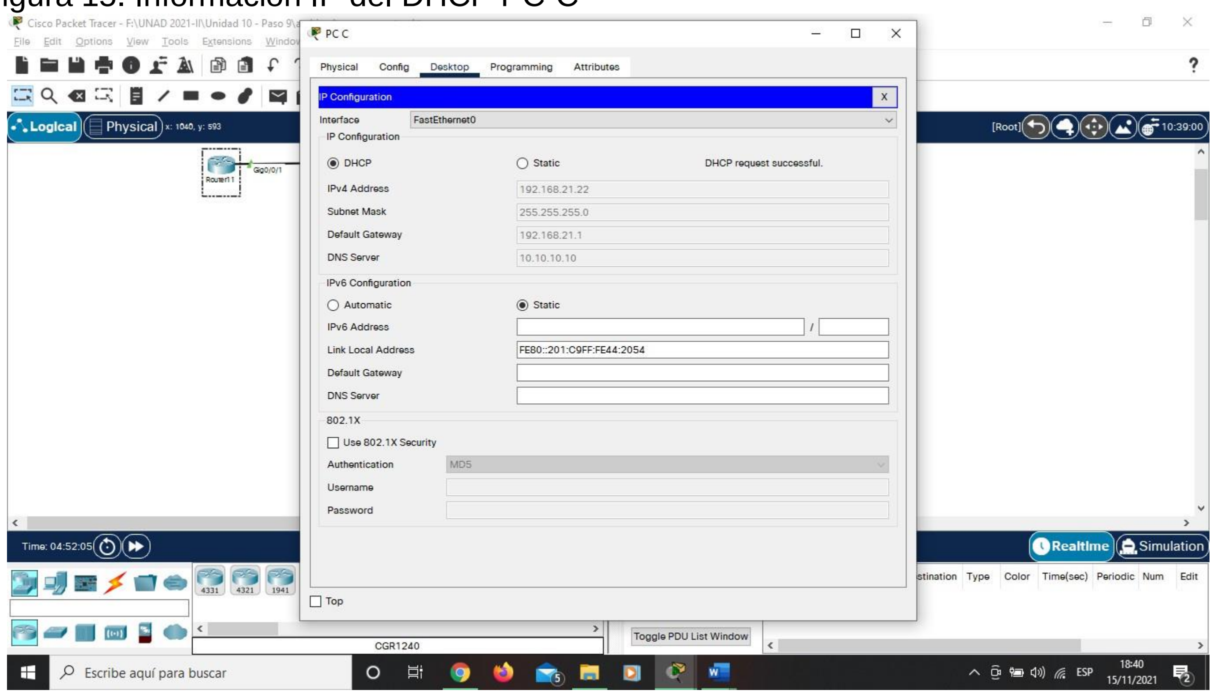
Fuente: Elaboración Propia

Figura 14. Información IP del DHCP PC-A



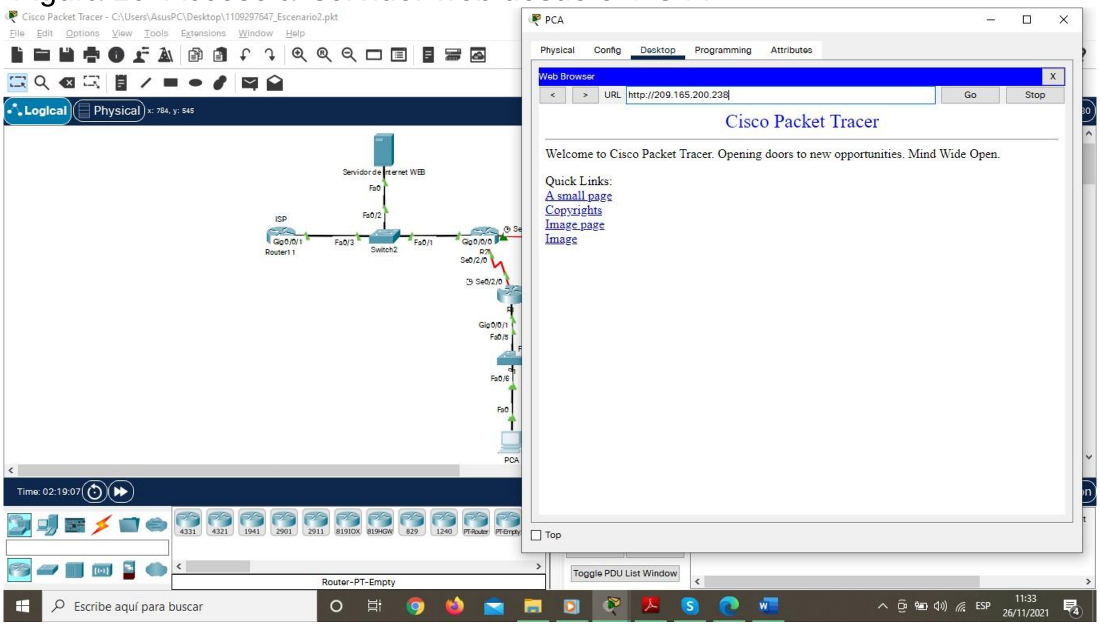
Fuente: Elaboración propia

Figura 15. Información IP del DHCP PC-C



Fuente: Elaboración propia

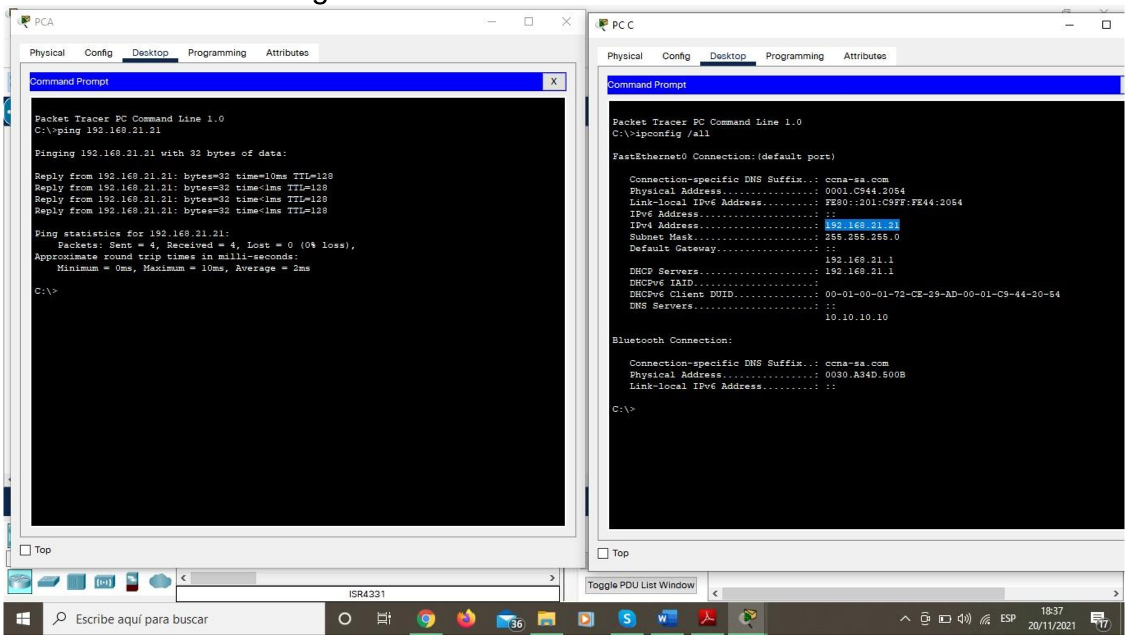
Figura 16. Acceso al servidor web desde el PC-A



Fuente: Elaboración Propia

```
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<1ms 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 = 0ms, Average = 0ms
```

Figura 17. Verificación Ping a PC-C



Fuente: Elaboración Propia

Parte 6: Configurar NTP

Tabla 26. Indicaciones Configuración NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

R2>enable
R2#clock set 09:00:00 05 march 2016 **Se ajusta la hora y fecha establecida**
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5 **Configuramos el NTP maestro con nivel 5**
R2(config)#exit
R2#

```
%SYS-5-CONFIG_I: Configured from console by console

R2#sh clock
9:0:26.704 UTC Sat Mar 5 2016
R2#



R1#sh clock
*4:37:10.288 UTC Mon Mar 1 1993
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp  server  172.16.1.2
```

Se procede a configurar R1 para actualizaciones periódicas de calendario con hora NTP

```
R1(config)#ntp upd
R1(config)#ntp update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clock set 09:00:00 05 mar
% Incomplete command.
R1#clock set 09:00:00 05 march 2016
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp master 5
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show clock
9:1:8.390 UTC Sat Mar 5 2016
R1#



se prohibe el acceso no autorizado

User Access Verification

Password:

R1>enab
```

```
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Opense prohibe el acceso no autorizado


User Access Verification

Password:
R2>enable
Password:
Password:
R2#
```

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 27. Restricción acceso líneas VTY en R2

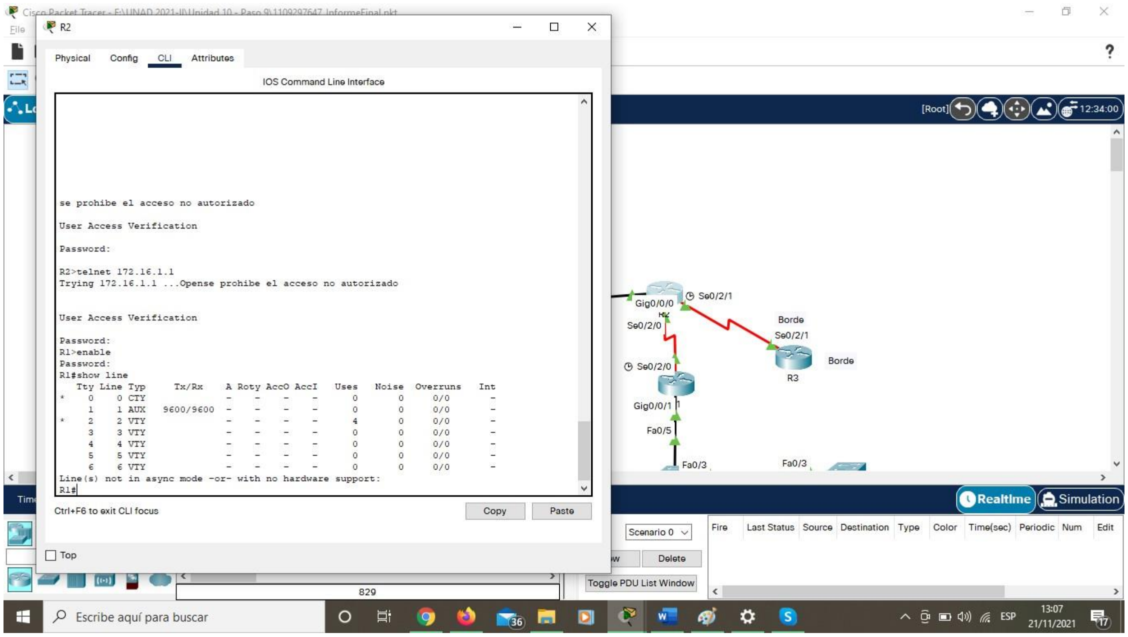
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

```
R2>enable
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
```
se configura la lista de acceso para permitir comunicación de R1 con R2 solamente

```
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#deny any

R2(config)#line vty 0 4
R2(config-line)#ip a
R2(config-line)#ip access-class ADMIN-MGT in

R2(config-line)#transport input telnet
```

Figura 18. Verificación Acceso telnet a PC-C



Fuente: Elaboración Propia

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

Tabla 28. Comandos aplicados a la configuración

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
Restablecer los contadores de una listade acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la direcciónen que se aplica?	Show ip access-lists

¿Con qué comando se muestran lastraducciones NAT?	**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. Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

Fuente: Escenario 2 Prueba de habilidades CCNA II-2021

CONCLUSIONES

Este proceso nos permitió conocer diversas herramientas predispuesta para los distintos escenarios, así mismo emprender el conocimiento hacia nuevas tecnologías y configuraciones más efectivas.

El escenario ofrecido para esta primera actividad nos ayuda a afianzar nuestro manejo en los diversos entornos y dispositivos que se encuentran alojados en Packet Tracer.

Hemos tomado nuevos recursos para identificar los hosts que manejaremos en las distintas subredes de este modo aplicamos la función del subnetting para dividir una red IP física en redes más pequeñas de tal modo que cada una de estas trabaje a nivel transporte y admisión de paquetes, como una red individual.

Al culminar este escenario se pudo dar solución al problema planteado y así demostrar las habilidades obtenidas con los capítulos vistos al momento en CISCO que son fundamentales para comprender el manejo de las redes y sus respectivas configuraciones.

BIBLIOGRÁFIA

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In International Conference on Knowledge Management in Organizations. (2021, July). (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. 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. (2013).

BAREÑO Raúl, G., & Sevillano, A. M. L. 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) (2017, October). (pp. 1-5). IEEE.

CISCO. Capa de aplicación. Fundamentos de Networking. (2019). Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html #10

CISCO. Configuración de un sistema operativo de red. Fundamentos de Networking. (2019). Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. Conceptos de Routing. Principios de Enrutamiento y Conmutación. (2019). Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#1

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

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

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

Froom, R., Frahim, E. CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide

BIBLIOGRÁFIA

CCNP SWITCH. (2015). 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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

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

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. 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). (2019, October). (pp. 1-6). IEEE.

Teare, D., Vachon B., Graziani, R. CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE. (2015). 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

UNAD. Principios de Enrutamiento [OVA]. (2017). Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm