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

LESBY ELENA PEREZ CORCHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
PROGRAMA DE INGENIERIA DE SISTEMAS
COROZAL SUCRE
2021

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

LESBY ELENA PEREZ CORCHO

DIPLOMADO CISCO DE OPCION DE GRADO PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

NANCY AMPARO GUACA (DIRECTORA)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
PROGRAMA DE INGENIERIA DE SISTEMAS
COROZAL SUCRE
2021

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado

Firma del jurado

Sampués, noviembre de 2021

AGRADECIMIENTOS

Agradezco en primera instancia a Dios quien siempre ha permanecido constantemente en cada momento de mi vida y me guía hacia la entereza y el éxito.

Reconocer a mi esposo e hija quienes han sido pacientes y me han brindado su apoyo, comprensión y espacio para poder llevar a un feliz término todo este proceso de aprendizaje, en mi formación.

Agradecer a la familia unadista y compañeros quienes de una u otra manera me han apoyado con su paciencia y sapiencia me han brindado los medios y la orientación en el desarrollo de este proceso de formación.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL: La lista de control de acceso, contiene los hosts a los que se permite o se niega el acceso al dispositivo de red. Estas pueden definir de una de dos maneras: por dirección IPv4 o por dirección IPv6. Es una lista de filtros de tráfico de red y acciones correlacionadas utilizadas para mejorar la seguridad. Bloquea o permite a los usuarios acceder a recursos específicos.

CISCO: Las certificaciones cisco son reconocidas a nivel mundial como un estándar de la industria para diseño y soporte de redes, garantizando altos niveles de conocimientos y confiabilidad. Su línea de cursos va desde la tecnología más básica de redes hasta áreas especializadas y tecnología avanzada tales como seguridad, redes inalámbricas y telefonía IP.

DHCP: Es un protocolo de configuración de host dinámico y un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales. Además de la dirección IP, DHCP también asigna la máscara de subred, la dirección de puerta de enlace predeterminada, la dirección del servidor de nombres de dominio (DNS) y otros parámetros de configuración pertinentes.

Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, dicha agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

Gateway. Es un dispositivo en red que actúa como un punto de entrada de una red a otras redes. Es el enlace que conecta dos ordenadores a Internet. La pasarela actúa como portal entre dos programas y como medio de comunicación entre los protocolos que les permite compartir datos en los mismos dispositivos informáticos o entre diferentes sistemas informáticos.

IPv6: Es un sistema de direccionamiento de 128 bits, es la versión más reciente, utilizado para identificar un dispositivo en redes informáticas. Una dirección IPv6 se representa en ocho campos de números hexadecimales, cada uno de los cuales contiene 16 bits. Se divide en dos partes, cada una de las cuales consta de 64 bits. La primera parte es la dirección de red y la segunda parte la dirección de host.

VLAN: una red de área local virtual, es una red conmutada segmentada lógicamente por función, o aplicación, independientemente de las ubicaciones físicas de los usuarios. Estos son un grupo de hosts que se pueden ubicar en cualquier lugar de una red pero que se comunican como si estuvieran en el mismo segmento físico.

RESUMEN

En esta actividad se desarrolló una práctica para evaluar los conocimientos adquiridos en el curso de prueba de habilidades prácticas CCNA cisco, diseñado en el programa packet tracer 8.0.1, este software permite idear un escenario de la vida real donde se desarrolla la solución de problemas de la actividad final. Se configuran direcciones IP acorde con la topología de red para cada uno de los dispositivos, configuración de los routers, VLANs, puertos troncales, puertos de acceso, encapsulamiento, direcciones IP a los switches, routers, acorde a los lineamientos. en donde nos permitirá lograr un mayor aprendizaje y a la vez acceder a la opción de grado en la facultad de ingeniería de sistemas.

Palabras Claves: CCNA, Cisco, Topología, Red, Sistemas.

ABSTRACT

In this activity a practice was developed to evaluate the knowledge acquired in the CCNA cisco practical skills test course, designed in the packet tracer 8.0.1 program, this software allows to devite a real-life scenario where the problem solving of the final activity is developed. IP addresses are configured according to the network topology for each of the devices, configuration of the routers, VLANs, trunk ports, access ports, encapsulation, IP addresses to the switches, routers, according to the guidelines. where it will allow us to achieve greater learning and at the same time access the degree option in the faculty of systems engineering.

Keywords: CCNA, Cisco, Topology, Network, Systems.

INTRODUCCION

Actualmente se está viviendo en una época donde es fundamental el uso de la tecnología, esta se ha convertido en algo cotidiano, las telecomunicaciones han tomado mucho avance en el desarrollo de la humanidad. Para el crecimiento de cualquier empresa, es indispensable el envío de información digital y a su vez la conectividad de diferentes servidores, debido a que es necesario estar siempre conectados.

Siguiente se desarrollará el escenario 1 y 2, de la actividad final del diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN/WAN, donde se pondrá en práctica lo aprendido durante el curso, dando solución a escenarios propuestos, configurando e interconectando entre sí cada uno de los dispositivos que forman parte del escenario, aplicando los diferentes comandos asignados.

Esta prueba de habilidades tiene como finalidad realizar un recorrido por las temáticas vistas en el diplomado, buscando así afianzar las competencias adquiridas demostrando las destrezas y conocimientos obtenidos. Para ello se trabajará en el simulador aplicado para el desarrollo de los dos escenarios en la plataforma CISCO denominado Packet Tracer, el cual permite configuraciones básicas de switches y routers, además, la configuración de interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, seguridad, aplicación de redes virtuales VLAN, direccionamiento dinámico, establecimiento de listas de control de acceso y traducción de direcciones de red NAT. Por lo que nos permitirá la organización de ideas y adquirir mucho más conocimiento en cuanto a las tecnologías de hoy, con habilidades y destrezas en el diseño e implementación de redes informáticas para un acceso seguro, con control y gestión de la información.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

Fuente propia

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

Objetivos

Parte 1: Construir en el simulador la Red
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

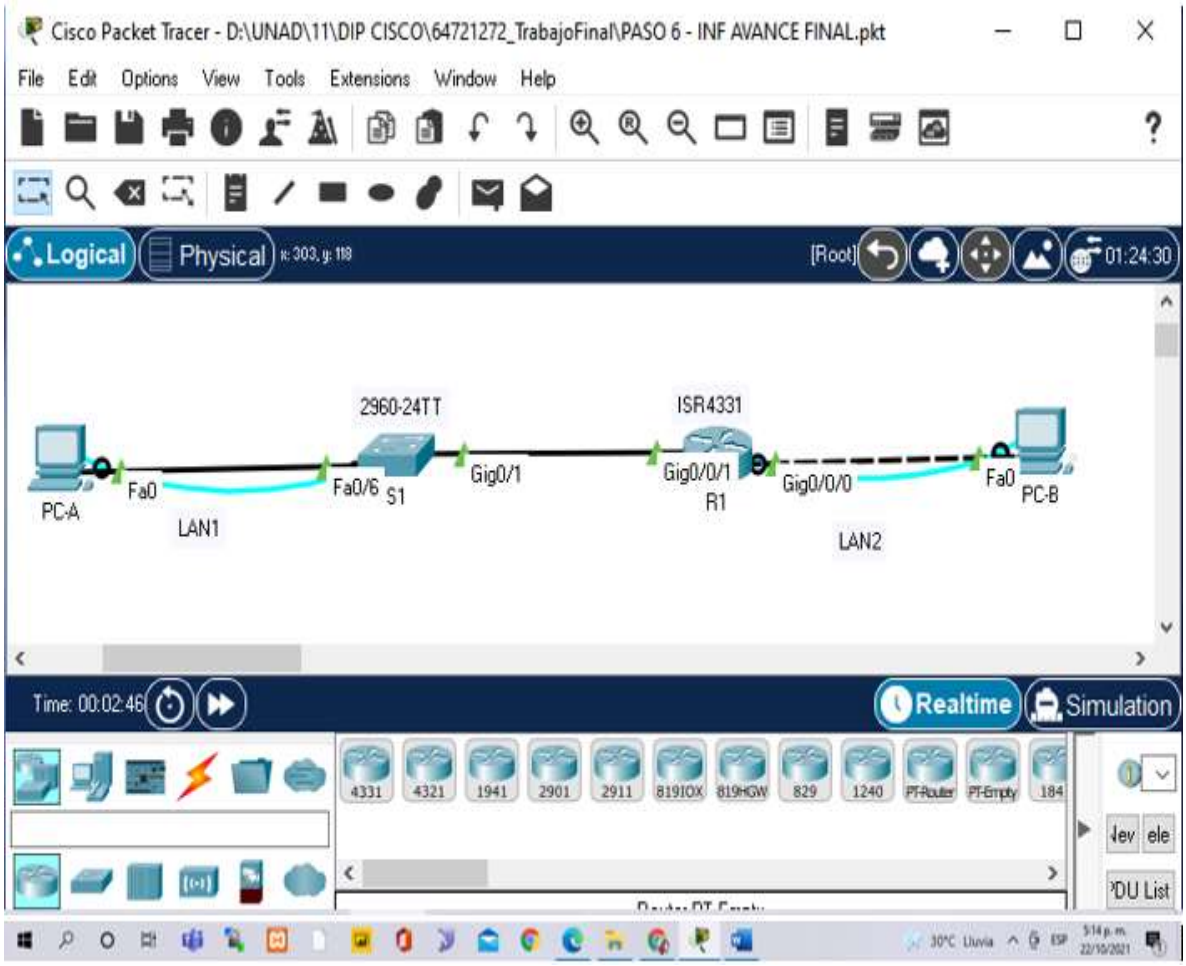
Aspectos básicos/situación

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

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

Se empieza por realizar la topología, conectando cada uno de los equipos de cómputo como lo plantea a figura 1. Así: (figura 2)

Figura 2. Simulacion de Escenario 1



Fuente propia

Parte 2: Desarrolle el esquema de direccionamiento IP

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

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

Tabla 1. de Direccionamiento

Ítem	Requerimiento
Dirección de red	192.168.72.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.72.1/25 Primera dirección de host de la subred LAN1
R1 G0/0/0	192.168.72.129/26 Primera dirección de host de la subred LAN2
S1 SVI	192.168.72.2/25 Segunda dirección de host de la subred LAN1
PC-A	192.168.72.126/25 Ultima dirección de host de la subred LAN1
PC-B	192.168.72.190/26 Ultima dirección de host de la subred LAN2

Fuente propia.

Descripción de la tabla 1.

Para desarrollar el esquema de direccionamiento IP, empecé por crear la subred de mayor tamaño LAN1 (100 Hosts), luego la de menor tamaño LAN2 (50 hosts), y por ultimo los demás requerimientos de direccionamiento según lo pide la tabla, de la siguiente manera:

Tabla 2. Esquema de Direccionamiento.

Sub red	Dirección IP	Mas cara	Primera IP	Ultima IP	Broadcast
LAN 1	192.168.72.0	25	192.168.72.1	192.168.72.126	192.168.72.127
LAN 2	192.168.72.128	26	192.168.72.129	192.168.72.190	192.168.72.191

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 3. Configuración del Router 1 (R1)

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router# configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass R1(config)#
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10 R1(config)#
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#
Configure MOTD Banner	R1(config)#banner motd ##CCNA – acceso restringido a Router## R1(config)#
Configurar interfaz G0/0/0 Establezca la descripción Establece la dirección IPv4 Activar la interfaz	R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 192.168.72.129 255.255.255.192 R1(config-if)#description interfaz LAN2 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#

Configurar interfaz G0/0/1 Establezca la descripción Establece la dirección IPv4 Activar la interfaz	R1(config)#interface gigabitEthernet 0/0/1 R1(config-subif)#ip address 192.168.72.1 255.255.255.128 R1(config-if)#description interfaz LAN1 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#Ip domain-name ccna-lab.com R1(config)#crypto key generate rsa R1(config)#exit R1#wr

Fuente propia

Descripción de la tabla No. 3. Se realizo la configuración del Router teniendo en cuenta el escenario 1, mediante conexión de consola y se demuestra en la figura 3 y 4, por medio de los siguientes comandos

Comandos ejecutados	Explicación comandos
Router>enable	Inicio al modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R1	Asigno el nombre R1 al Router
R1(config)#ip domain-name ccna-lab.com	Asigno el nombre de dominio
R1(config)#enable secret ciscoenpass	Asigno contraseña modo privilegiado
R1(config)#line console 0	Ingreso a la línea consola
R1(config-line)#password ciscoconpass	Asigno contraseña al acceso a consola
R1(config-line)#login	Habilito la contraseña
R1(config-line)#exit	Salida de la línea de consola
R1(config)#security passwords min-length 10	Establezco contraseña de long 10
R1(config)#username admin password admin1pass	Creo usuario adm base local
R1(config)#line vty 0 4	Configure inicio de sesión en líneas VTY
R1(config-line)#login local	Habilito inicio sesión vty
R1(config-line)#transport input ssh	Configure VTY aceptando SSH
R1(config-line)#login local	Habilito configuración vty con SSH
R1(config-line)#exit	Salida de la configuración vty
R1(config)#service password-encryption	Cifrado de la contraseña
R1(config)#banner motd ##CCNA - Acceso Restringido a Router##	Asigno mensaje acceso restringido
R1(config)#interface gigabitEthernet 0/0/0	Configuro interfaz serial 0
R1(config-if)#ip address 192.168.72.129 255.255.255.192	Establezco dir IpV4

```
R1(config-if)#description interfaz LAN2      Establezco descripción interfaz LAN2
R1(config-if)#no shutdown                                  Activo la interfaz
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#exit                                          Salgo de conf interfaz LAN2
R1(config)#interface gigabitEthernet 0/0/1          Configuro interfaz serial 1
R1(config-if)#ip address 192.168.72.1 255.255.255.128      Establezco dir IPV4
R1(config-if)#description interfaz LAN1      Establezco descripción interfaz LAN1
R1(config-if)#no shutdown                                  Activo la interfaz
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1(config-if)#exit                                          Salgo de conf interfaz LAN1
R1(config)#ip domain-name ccna-lab.com                      Activo clave cifrado
R1(config)#crypto key generate rsa                  Genero 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            Designo cifrado de 1024bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#exit                                     Salgo de la activación cifrado
*Mar 1 0:58:53.732: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
R1#wr                                                       Guardo configuración
Building configuration...
[OK]
R1#
```

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4. Configuración del Switch 1 (S1)

Tarea	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com S1(config)#
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass S1(config)#
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit S1(config)#
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Configurar un MOTD Banner	S1(config)#banner motd ##CCNA - Acceso restringido a switch## S1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)# ip domain-name ccna-lab.com S1(config)#crypto key generate rsa S1(config)#
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 conforme a la tabla de direccionamiento	S1(config)#interface Vlan1 S1(config-if)#ip address 192.168.72.2 255.255.255.128 S1(config-if)#no shutdown S1(config-if)#exit

	S1(config)#
Configuración del Gateway predeterminado Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.	S1(config)#ip default-gateway 192.168.72.1 S1(config)#exit S1#wr Building configuration... [OK] S1#

Fuente propia.

Descripción de la tabla No. 4. Se realiza la configuración del Switch teniendo en cuenta el escenario 1, mediante conexión de consola, y se demuestra en la figura 5 y 6, ejecutando los siguientes comandos:

Comandos ejecutados	Explicación de comandos
Switch>enable	Inicio al modo privilegiado
Switch#configure terminal	Ingreso al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
Switch(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Switch(config)#hostname S1	Asigno nombre R1 al Router
S1(config)#ip domain-name ccna-lab.com	Asigno nombre de dominio
S1(config)#enable secret ciscoenpass	Asigno contraseña modo privilegiado
S1(config)#line console 0	Ingreso a la línea de consola
S1(config-line)#password ciscoconpass	Asigno contraseña al acceso a consola
S1(config-line)#login	Habilito la contraseña
S1(config-line)#exit	Salgo de la línea consola
S1(config)#username admin password admin1pass	Creo usuario adm base local
S1(config)#line vty 0 15	Configuro inicio de sesión en línea vty
S1(config-line)#login local	Habilito inicio sesión vty
S1(config-line)#transport input ssh	Configuro vty aceptando SSH
S1(config-line)#login local	Habilito configuración vty con SSH
S1(config-line)#exit	Salgo de configuración vty
S1(config)#service password-encryption	Cifro la contraseña de texto
S1(config)#banner motd ##CCNA - Acceso restringido al Switch##	Asigno mensaje de Acceso restringido
S1(config)#ip domain-name ccna-lab.com	Activo clave de cifrado
S1(config)#crypto key generate rsa	Genero 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	Designo cifrado de 1024bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S1(config)#interface Vlan1 Configuro interfaz de administración(SVI)
*Mar 1 1:16:15.906: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip address 192.168.72.2 255.255.255.128 Asigno dirección IPV4
S1(config-if)#no shutdown Activo la interfaz
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#exit Salgo de configuración de interfaz
S1(config)#ip default-gateway 192.168.72.1 Configuro dirección IP gateway
S1(config)#exit Salgo de configuración gateway
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#wr Guardo configuración
Building configuration...
[OK]
S1#

Paso 2. Configurar los equipos

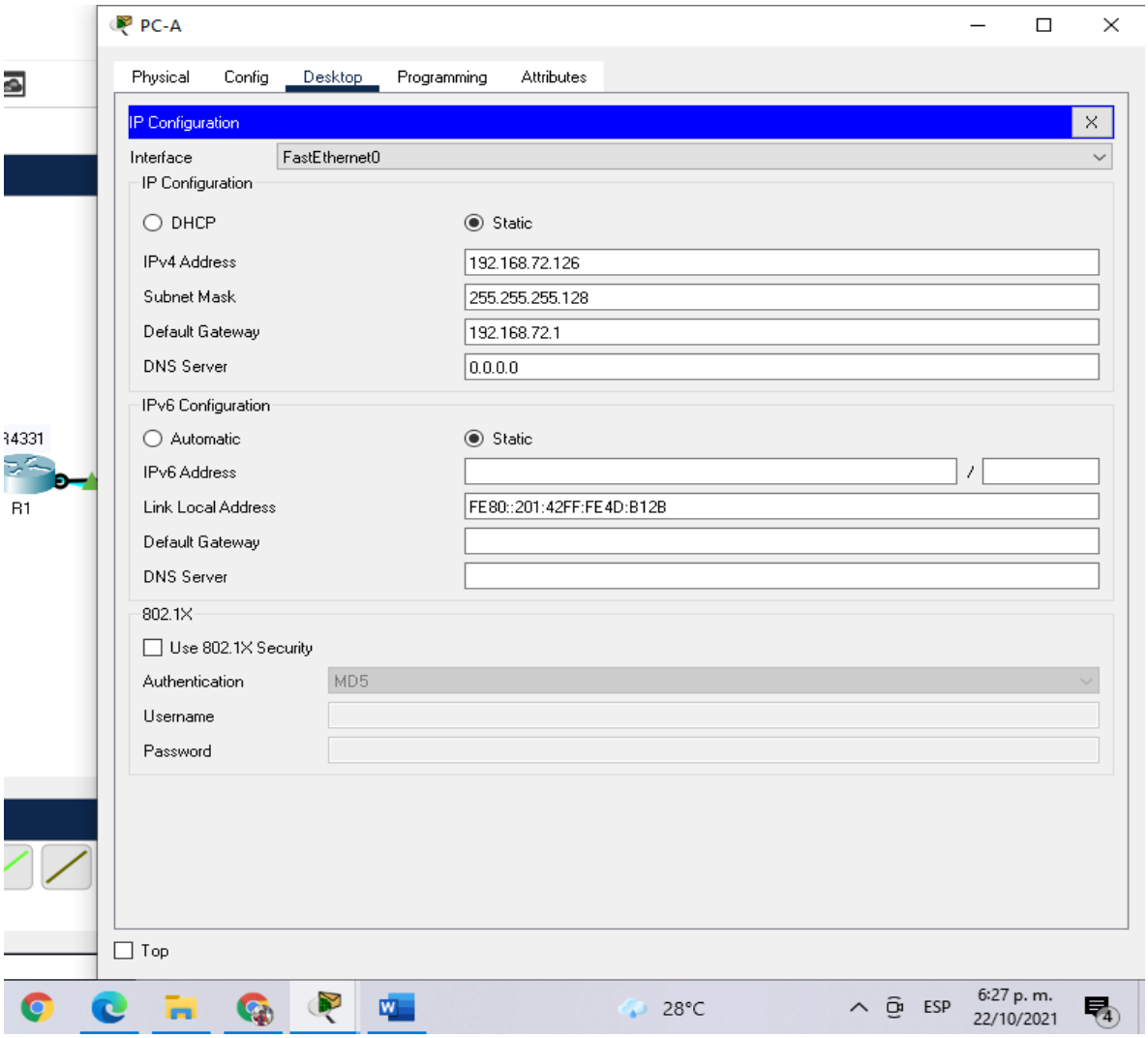
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all

Tabla 5. Configuración de Equipo Host PC-A

PC-A Network Configuración	
Descripción	PC-A
Dirección física	0001.424D.B12B
Dirección IP	192.168.72.126
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.72.1

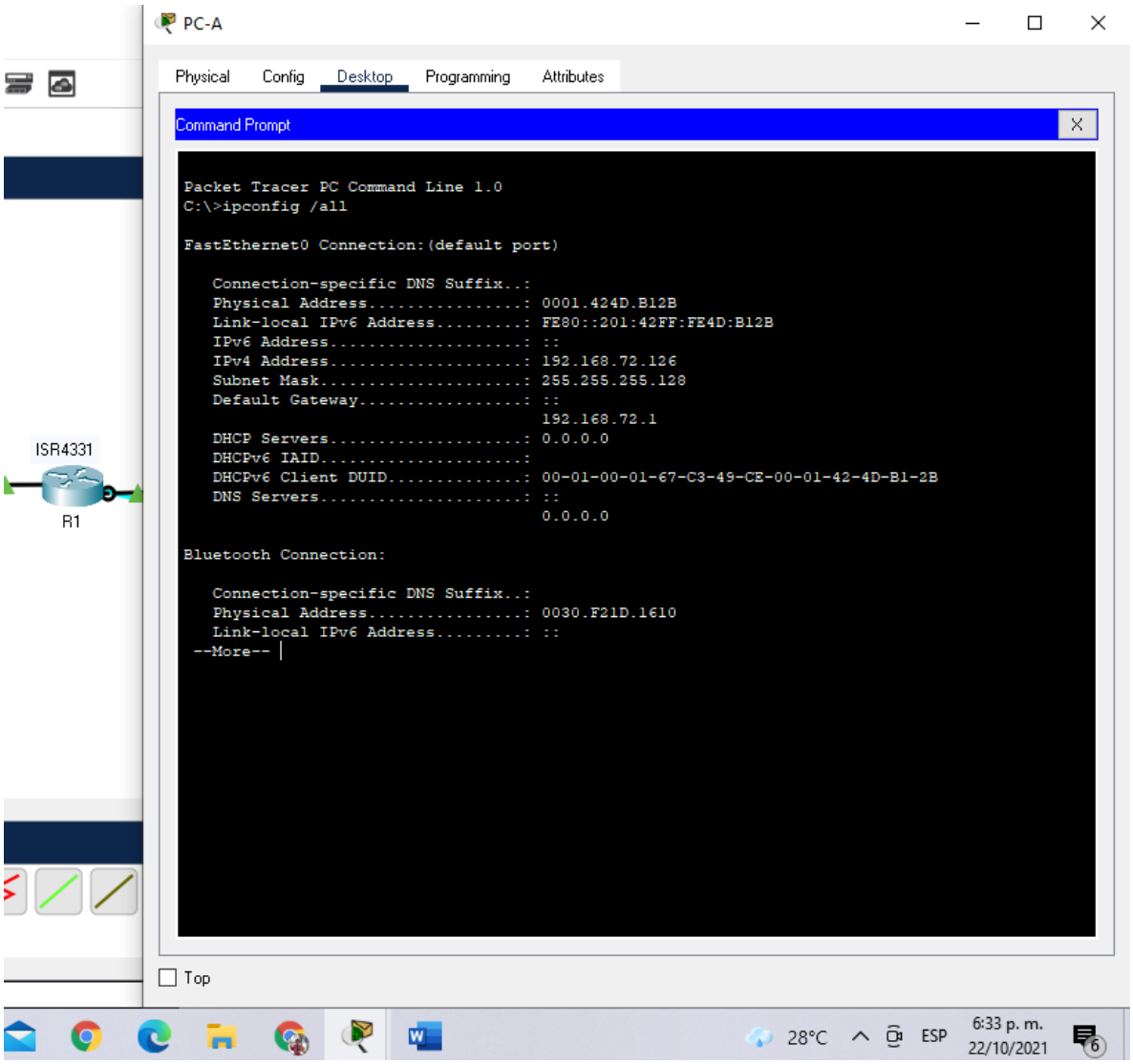
Fuente propia.

Figura 3. Configuración Host PC-A



Fuente propia

Figura 4. Configuración Host PC-A. Comando Ipconfig/all



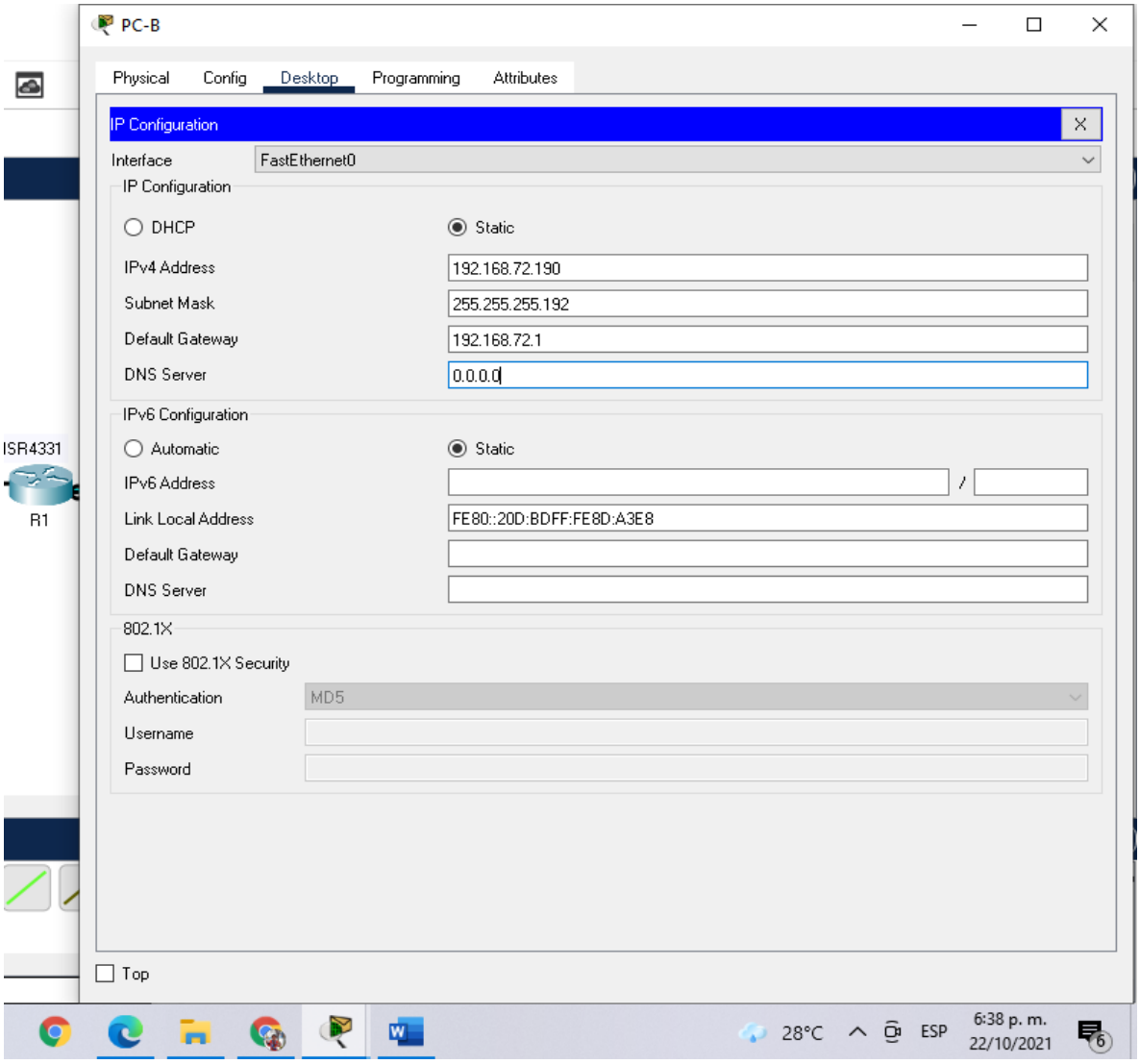
Fuente propia.

Tabla 6. Configuración de Equipo Host PC-B

PC-B Network Configuración	
Descripción	PC-B
Dirección física	000D.BD8D.A3E8
Dirección IP	192.168.72.190
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.72.1

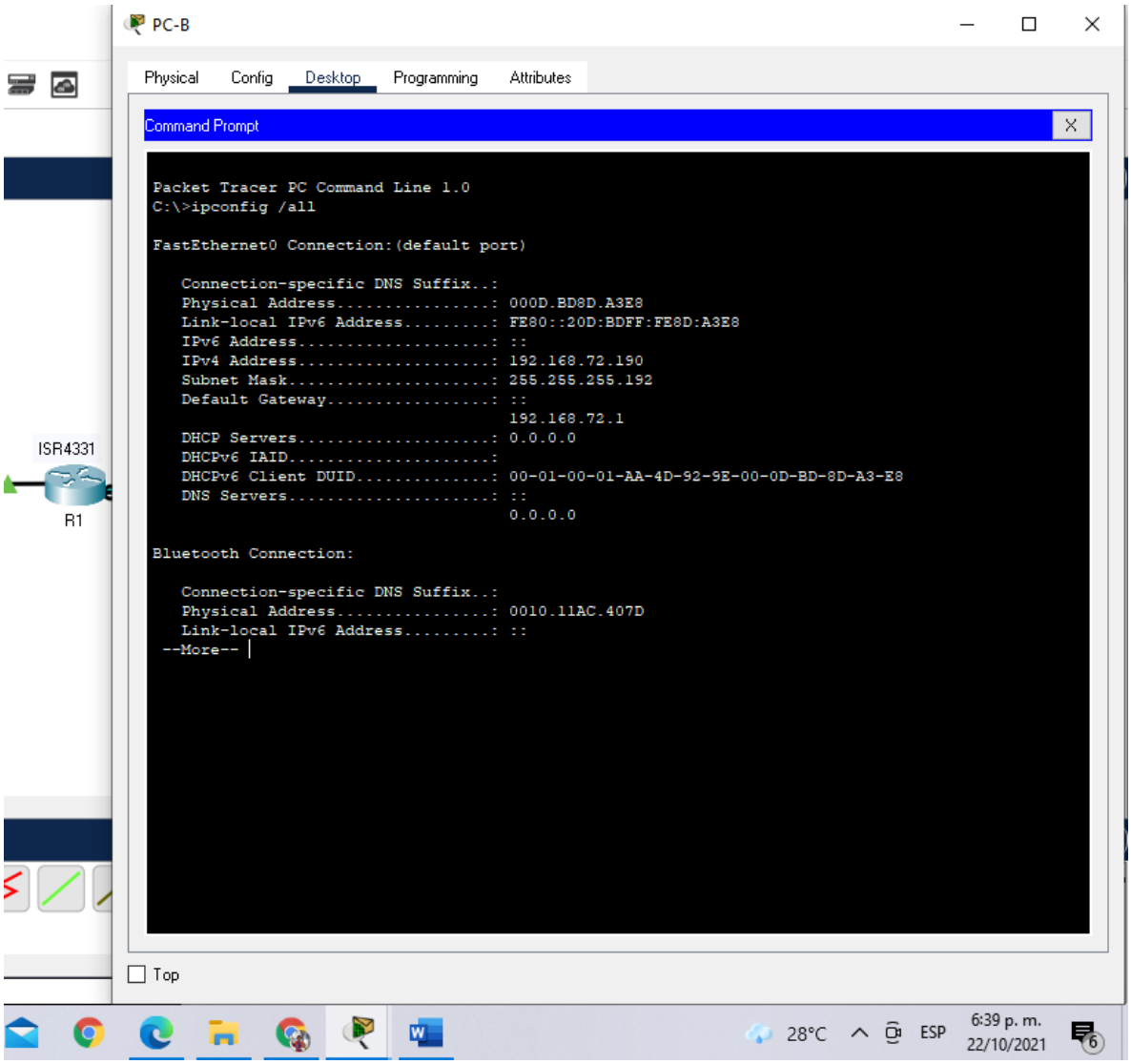
Fuente propia

Figura 5. Configuración Host PC-B



Fuente propia

Figura 6. Configuración Host PC-B. Comando ipconfig/all

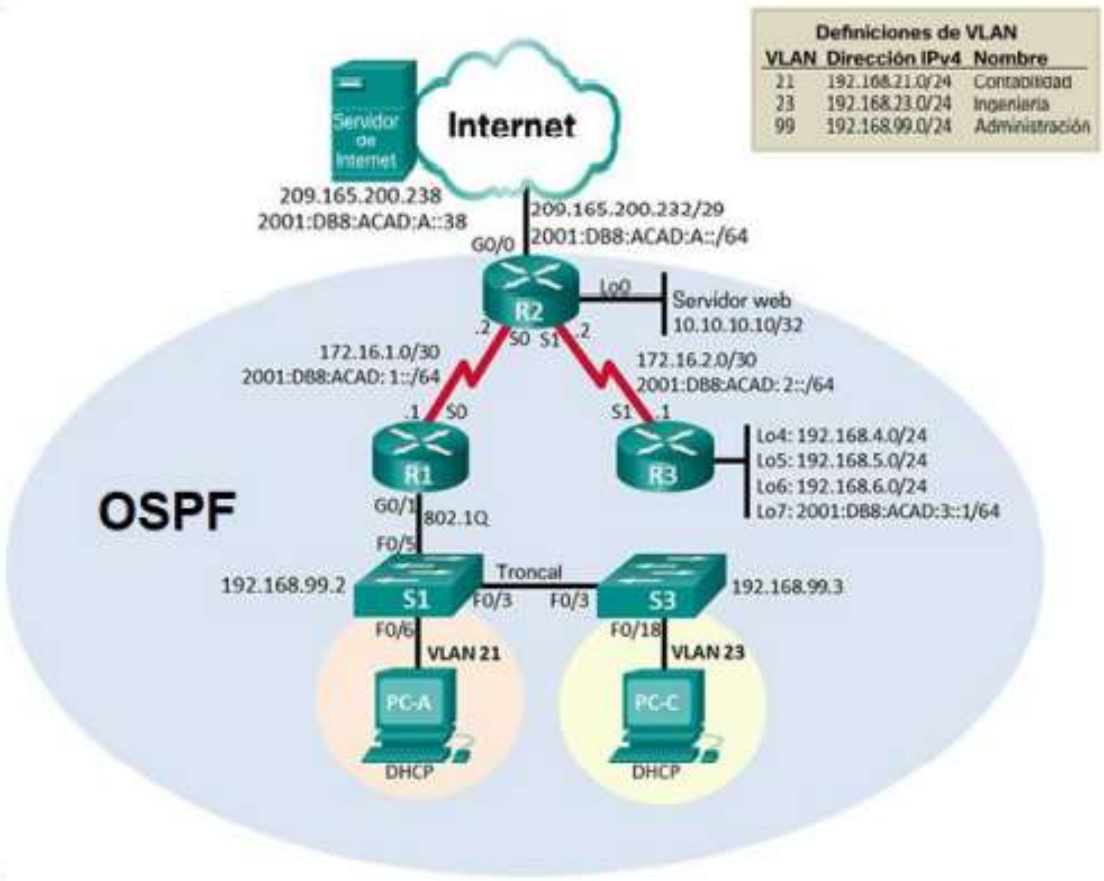


Fuente propia.

2. ESCENARIO 2

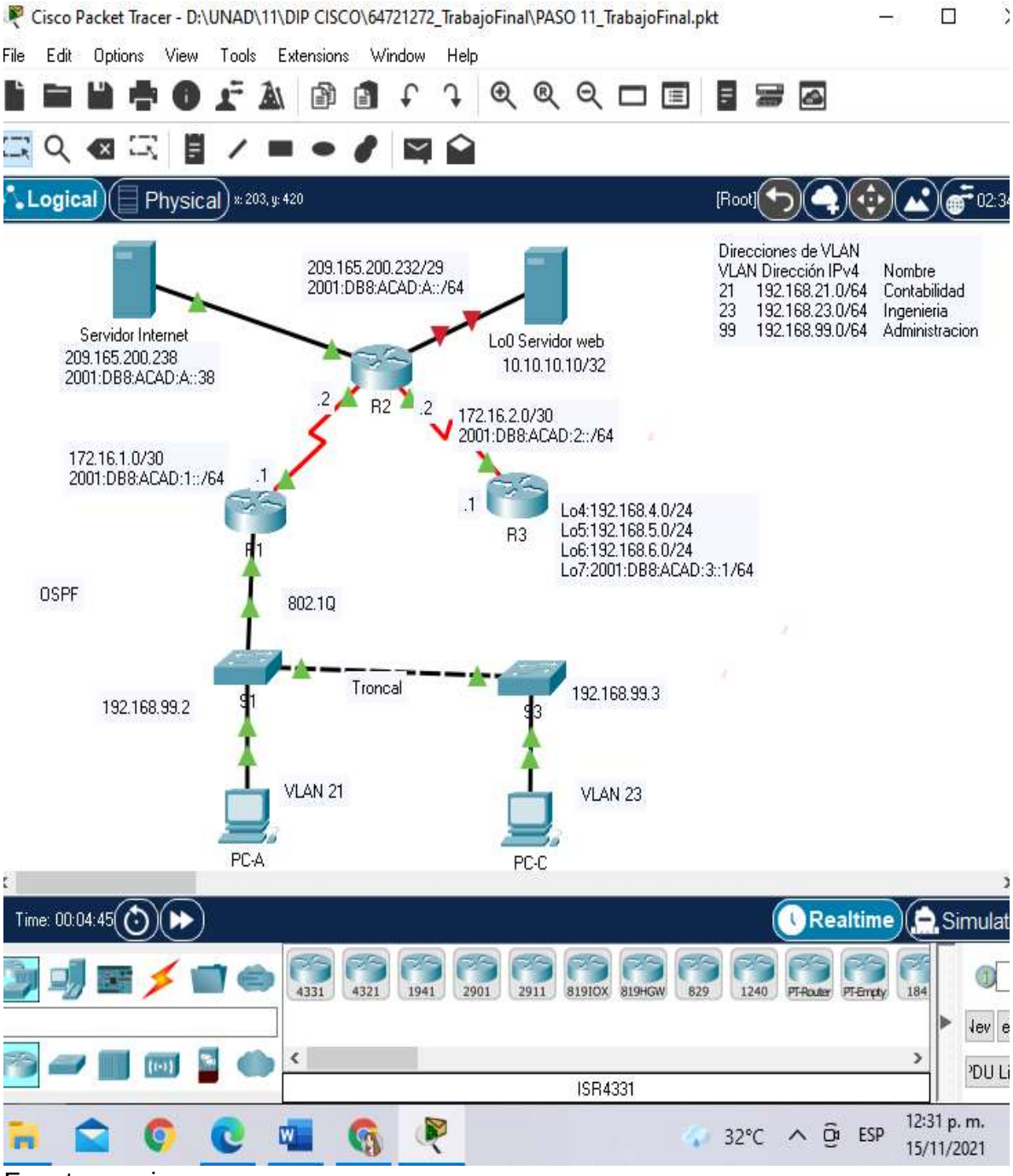
Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de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

Figura 7. Escenario 2



Fuente propia.

Figura 8. Simulación Escenario 2.



Fuente propia.

Parte 1: Inicializar dispositivos

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

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

Tabla 7. Inicialización y cargue de los routers y los switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Configuración R1, R2 y R3 Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router#
Volver a cargar todos los routers	Configuración R1, R2 y R3 Router#reload Proceed with reload? [confirm] Router>
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Configuración Switches S1 y S3 Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch>enable Switch#delete vtp Delete filename [vtp]? Delete flash:/vtp? [confirm] %Error deleting flash:/vtp (No such file or directory) Switch#
Volver a cargar ambos switches	Configuración Switches S1 y S3 Switch#reload Proceed with reload? [confirm] Switch>

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Configuración Switches S1 y S3 Switch# Switch#show vlan brief

Fuente propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 8. Configuración de la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Mascara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado Ipv6	2001:DB8:ACAD:A::1

Fuente propia

Paso 2: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Parte 2 - P2. Configuración R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrado	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Configure MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	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 propia
Nota: Todavía no configure G0/1.

Código de configuración R1 - tabla 9	Descripción del código
Router>enable	Inicio al modo privilegiado
Router#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R1	Asigno nombre R1 al router
R1(config)#enable secret class	Asigno contraseña modo privilegiado
R1(config)#line console 0	Ingreso a línea de consola
R1(config-line)#password cisco	Asigno contraseña al acceso de consola
R1(config-line)#login	Habilito la contraseña
R1(config-line)#exit	Salgo de la línea de consola
R1(config)#line vty 0 4	Configure inicio de sesión en líneas VTY
R1(config-line)#password cisco	Asigno contraseña acceso telnet
R1(config-line)#login	Habilito la contraseña
R1(config-line)#exit	Salida configuración vty y telnet
R1(config)#service password-encryption	Cifrado de contraseña
R1(config)#banner motd #***se prohibe el acceso no autorizado***#	Asigno mensaje acceso restringido
R1(config)#Ipv6 unicast-routing	Habilito el routing IPv6 en el router
R1(config)#interface serial 0/0/0	Configuro interfaz S0/0/0
R1(config-if)#description conexion a R2	Establezco la descripción a R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Establezco dirección Ipv4
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64	Establezco dirección Ipv6
R1(config-if)#clock rate 128000	Establezco frecuencia de reloj
R1(config-if)#no shutdown	Activo la interfaz
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down	
R1(config-if)#exit	Salgo de la interfaz

R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 Configuro la ruta IPv4
R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2 Configuro la ruta IPv6
R1(config)#exit Salgo de la interfaz
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Parte 2 – P3. Configuración 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	
Configure MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	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 S0/0/1	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 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
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de G0/0 Configurar una ruta IPv6 predeterminada de G0/0

Fuente propia.

Código de configuración R2 – tabla 10	Descripción del código
Router>enable	Inicio al modo privilegiado
Router#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R2	Asigno el nombre R2 al Router
R2(config)#enable secret class	Asigno contraseña modo privilegiado
R2(config)#line console 0	Ingreso a la línea de consola
R2(config-line)#password cisco	Asigno contraseña acceso a consola
R2(config-line)#login	Habilito contraseña
R2(config-line)#exit	Salgo de la línea de consola
R2(config)#line vty 0 4	Configure inicio de sesión en líneas VTY
R2(config-line)#password cisco	Asigno contraseña acceso vty
R2(config-line)#login	Habilito contraseña
R2(config-line)#exit	Salgo de la línea vty
R2(config)#service password-encryption	cifrado de contraseña
R2(config)#ip http server	Habilitar el servidor http
^	Comando inhabilitado en el simulador
% Invalid input detected at '^' marker.	
R2(config)#banner motd #***se prohíbe el acceso no autorizado***#	Asigno mensaje acceso restringido
R2(config)#Ipv6 unicast-routing	Habilito el routing IPv6 en el router
R2(config)#interface serial 0/0/0	Configuro interfaz serial 0
R2(config-if)#description conexión a R1	Descripción conexión al R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252	Establezco dirección Ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64	Establezco dirección Ipv6
R2(config-if)#no shutdown	Activo la interfaz
R2(config-if)#exit	Salgo de la configuración interfaz serial 0

```
R2(config)#interface serial 0/0/1                          Configuro interfaz serial 1
R2(config-if)#description conexión a R3                    Descripción conexión al R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252       Establezco dirección Ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64           Establezco dirección Ipv6
R2(config-if)#clock rate 128000                            Establecer frecuencia de reloj
R2(config-if)#no shutdown                                  Activo la interfaz
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit                                         Salgo de la configuración interfaz serial 1
R2(config)#interface gigabitEthernet 0/0                   Configuro interfaz g 0
R2(config-if)#description conexión servidor                Descripción conexión al servidor
R2(config-if)#ip address 209.165.200.233 255.255.255.248   Establezco dir. Ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64           Establezco dirección Ipv6
R2(config-if)#no shutdown                                  Activo la interfaz
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line Conexión 31 n Interface GigabitEthernet0/0,
changed state to up
R2(config-if)#exit                                         Salgo de la configuración g 0
R2(config)#interface loopback 0                            Configuro interfaz L0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line Conexión 31 n Interface Loopback0, changed
state to up
R2(config-if)#description conexión servidor web            Descripción conexión servidor
R2(config-if)#ip address 10.10.10.10 255.255.255.255       Establezco dir. Ipv4
R2(config-if)#exit                                         Salgo de la configuración L0
R2(config)#ip route  0.0.0.0 0.0.0.0 172.16.1.1            Asigno ruta predeterminada Ipv4
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:1::1              Asigno ruta predeterminada Ipv6
R2(config)#ip route  0.0.0.0 0.0.0.0 172.16.2.1            Asigno ruta predeterminada Ipv4
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:2::1              Asigno ruta predeterminada Ipv6
R2(config)#ip route  0.0.0.0 0.0.0.0 209.165.200.238       Asigno ruta predet. Ipv4
R2(config)#ipv6 route ::/0 2001:DB8:ACAD:A::38             Asigno ruta predeterminada Ipv6
R2(config)#exit                                            Salgo de la configuración
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11. Parte 2 – P4. 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 S0/0/1	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 loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de G0/0 Configurar una ruta IPv6 predeterminada de G0/0

Fuente propia.

Código de configuración R3 – tabla 11	Descripción del código
Router>enable	Inicio al modo privilegiado
Router#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
Router(config)#no ip domain-lookup	Desactivo la búsqueda DNS
Router(config)#hostname R3	Asigno el nombre R3 al Router
R3(config)#enable secret class	Asigno contraseña modo privilegiado
R3(config)#line console 0	Ingreso a la línea de consola
R3(config-line)#password cisco	Asigno contraseña acceso a consola
R3(config-line)#login	Habilito contraseña
R3(config-line)#exit	Salgo de la línea de consola
R3(config)#line vty 0 4	Configuro inicio de sesión en líneas VTY
R3(config-line)#password cisco	Asigno contraseña acceso telnet
R3(config-line)#login	Habilito contraseña
R3(config-line)#exit	Salgo de la línea vty
R3(config)#service password-encryption	cifrado de contraseña
R3(config)#banner motd #***se prohibe el acceso no autorizado***#	Asigno mensaje acceso restringido
R3(config)#Ipv6 unicast-routing	Habilito el routing IPv6 en el router
R3(config)#interface serial 0/0/1	Configuro interfaz serial 1
R3(config-if)#description conexion a R2	Descripción conexión al R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252	Establezco dirección Ipv4
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64	Establezco dirección Ipv6
R3(config-if)#no shutdown	Activo la interfaz
R3(config-if)#	
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up	
R3(config-if)#exit	Salgo de la configuración interfaz serial 1
R3(config)#	
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up	
R3(config)#interface loopback 4	Configuro interfaz Lo4
R3(config-if)#	
%LINK-5-CHANGED: Interface Loopback4, changed state to up	
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up	
R3(config-if)#description interfaz virtual(prueba 4)	Descripción conexión int Lo4
R3(config-if)#ip address 192.168.4.1 255.255.255.0	Establezco dirección Ipv4
R3(config-if)#exit	Salgo de la configuración interfaz Lo4
R3(config)#interface loopback 5	Configuro interfaz Lo5
R3(config-if)#	
%LINK-5-CHANGED: Interface Loopback5, changed state to up	
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up	
R3(config-if)#description interfaz virtual(prueba 5)	Descripción conexión int Lo5

R3(config-if)#ip address 192.168.5.1 255.255.255.0 Establezco dirección Ipv4
R3(config-if)#exit Salgo de la configuración interfaz Lo5
R3(config)#interface loopback 6 Configuro interfaz Lo6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
R3(config-if)#description interfaz virtual(prueba 6) Descripción conexión int Lo6
R3(config-if)#ip address 192.168.6.1 255.255.255.0 Establezco dirección Ipv4
R3(config-if)#exit Salgo de la configuración interfaz Lo6
R3(config)#interface loopback 7 Configuro interfaz Lo7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#description interfaz virtual(prueba 7) Descripción conexión int Lo7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 Establezco dirección Ipv6
R3(config-if)#exit Salgo de la configuración interfaz Lo7
R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 Asigno ruta predeterminada Ipv4
R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2Asigno ruta predeterminada Ipv6
R3(config)#exit Salgo de la configuración
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Parte 2 – P5. 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 propia.

Código de configuración S1 – tabla 12 Descripción del código

Switch>enable Inicio al modo privilegiado
Switch#configure terminal Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivo la búsqueda DNS
Switch(config)#hostname S1 Asigno el nombre S1 al Switch
S1(config)#enable secret class Asigno contraseña modo privilegiado
S1(config)#line console 0 Ingreso a la línea de consola
S1(config-line)#password cisco Asigno contraseña acceso consola
S1(config-line)#login Habilito contraseña
S1(config-line)#exit Salgo de la línea de consola
S1(config)#line vty 0 4 Configure inicio de sesión en línea VTY
S1(config-line)#password cisco Asigno contraseña acceso telnet
S1(config-line)#login Habilito contraseña
S1(config-line)#exit Salgo de la línea vty
S1(config)#service password-encryption cifrado de contraseña
S1(config)#banner motd #***se prohibe el acceso no autorizado***#
Asigno mensaje acceso restringido
S1(config)#exit Salgo de la configuración
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Parte 2 – P6. 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 propia.

Código de configuración S3 – tabla 13 Descripción del código

Switch>enable Inicio al modo privilegiado
Switch#configure terminal Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup Desactivo la búsqueda DNS
Switch(config)#hostname S3 Asigno el nombre S3 al Switch
S3(config)#enable secret class Asigno contraseña modo privilegiado
S3(config)#line console 0 Ingreso a la línea de consola
S3(config-line)#password cisco Asigno contraseña acceso a consola
S3(config-line)#login Habilito contraseña
S3(config-line)#exit Salgo de la línea de consola
S3(config)#line vty 0 4 Configure inicio de sesión en línea VTY
S3(config-line)#password cisco Asigno contraseña acceso a telnet
S3(config-line)#login Habilito contraseña
S3(config-line)#exit Salgo de la línea vty
S3(config)#service password-encryption cifrado de contraseña
S3(config)#banner motd #***se prohíbe el acceso no autorizado***#
Asigno mensaje acceso restringido
S3(config)#exit Salgo de configuración
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#

Paso 7: Verificar la conectividad de la red

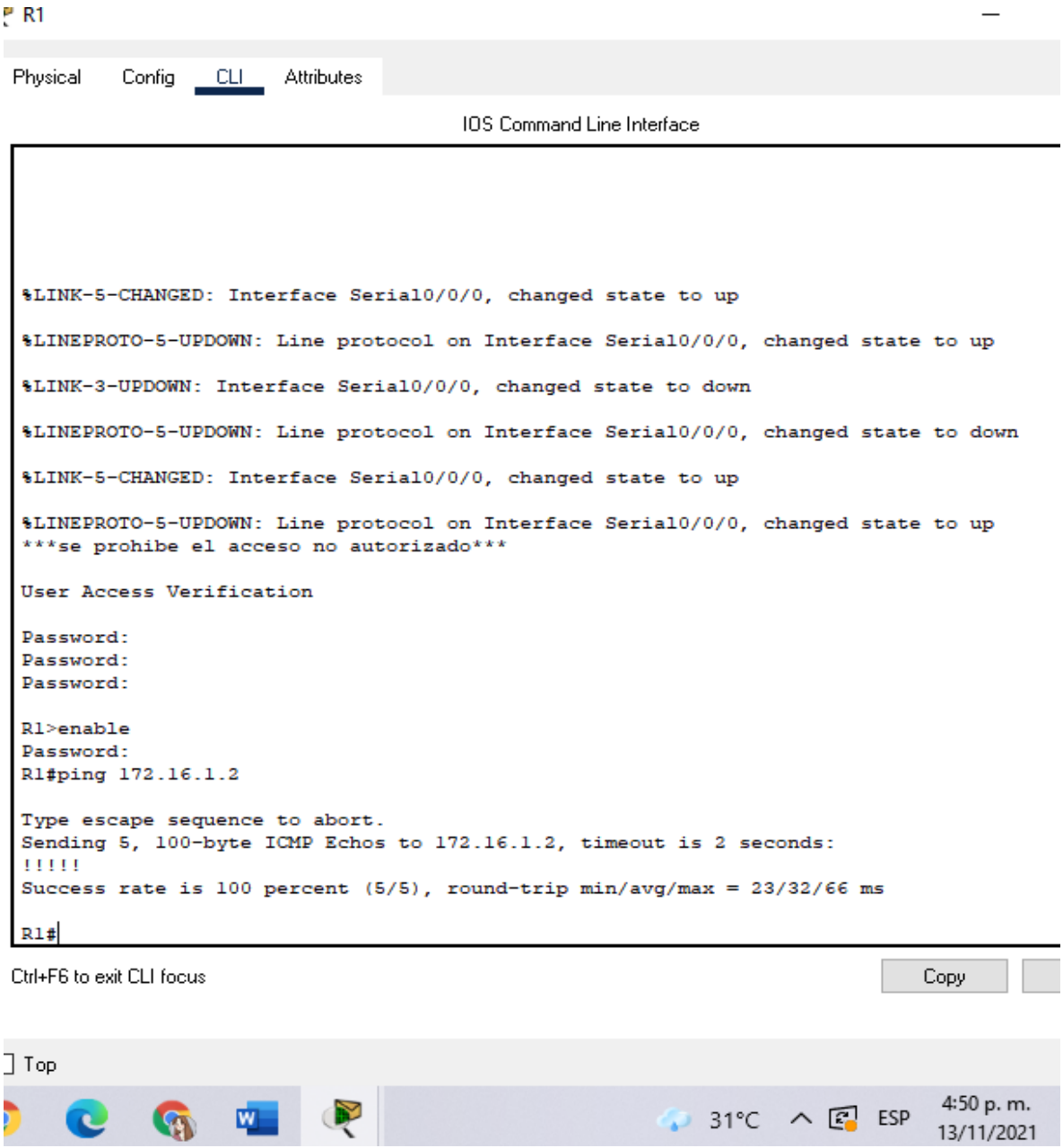
Utilice el comando ping para probar la conectividad entre los dispositivos de red.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Parte 2 – P7. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	100% (5/5)
R2	R3, S0/0/1	172.16.2.1	100% (5/5)
PC de Internet	Gateway predeterminado	209.165.200.233	Ok

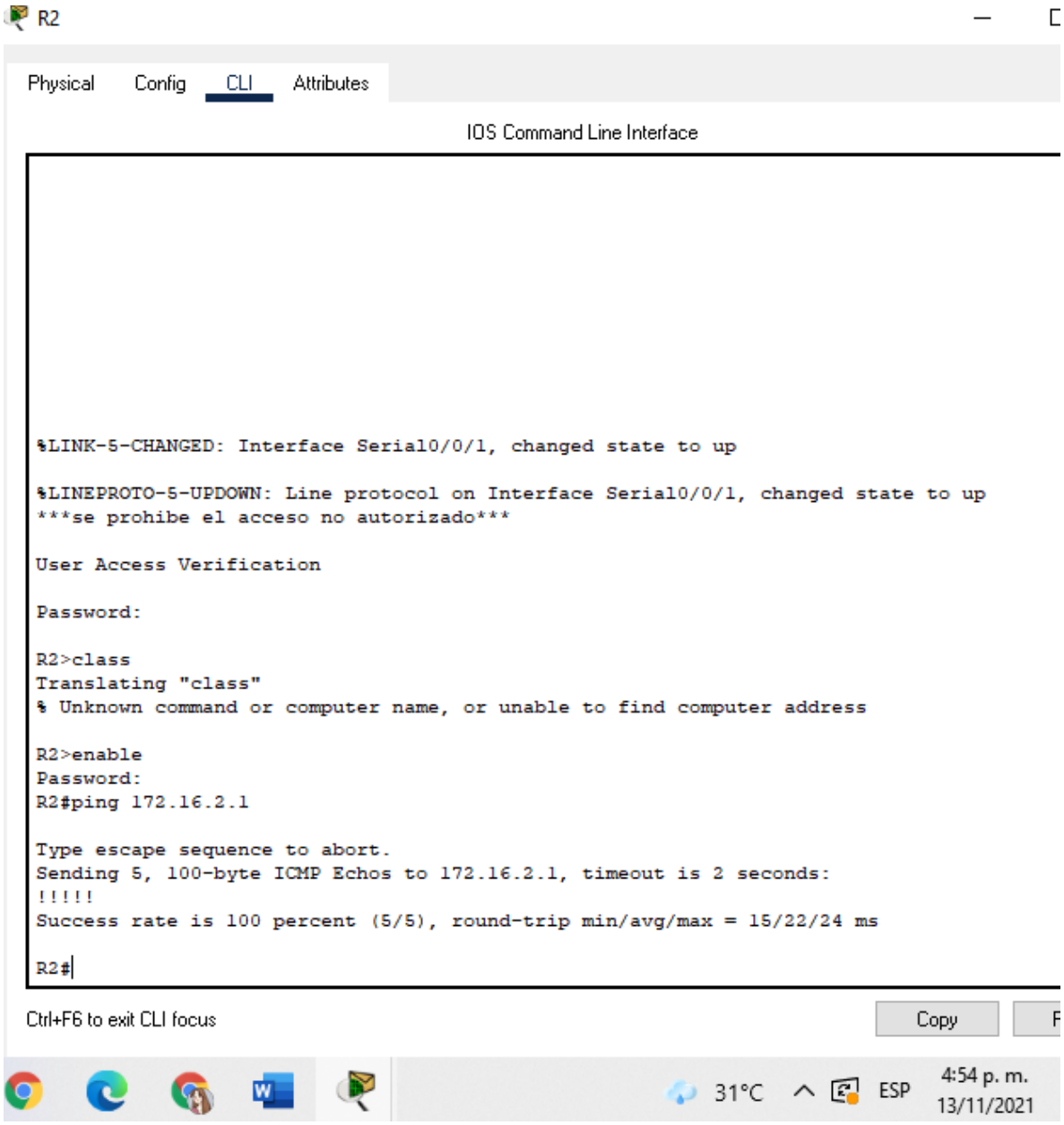
Fuente propia.

Figura 9. Prueba de conectividad desde R1 a R2, S0/0/0 (172.16.1.2)



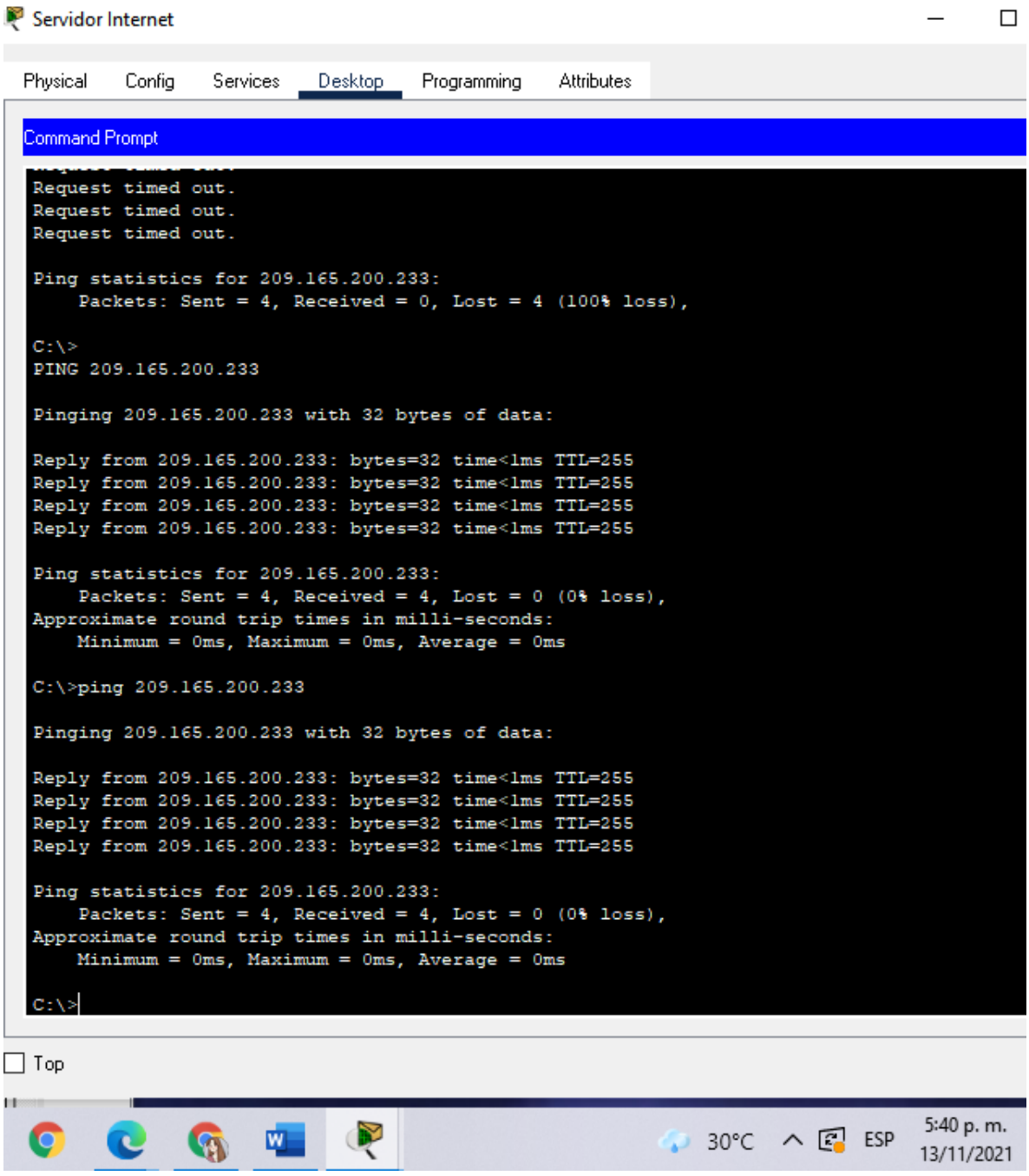
Fuente propia

Figura 10. Prueba de conectividad desde R2 a R3, S0/0/1 (172.16.2.1)



Fuente propia.

Figura 11. Prueba de conectividad desde PC internet a Gateway Predeterminado (209.165.200.233)



Fuente propia.

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. Parte 3 – P1. Configuración switch 1, VLAN y routing

Elemento o tarea de configuración	Especificación
Crear la base de datos 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 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	
Apagar todos los puertos sin usar	

Fuente propia.

Código de configuración S1 – tabla 15	Descripción del código
S1>enable	Inicio al modo privilegiado
Password:	Ingreso contraseña modo privilegiado
S1#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
S1(config)#vlan 21	Ingreso a configuración vlan21
S1(config-vlan)#name contabilidad	Nombro la vlan Contabilidad
S1(config-vlan)#exit	Salgo de la configuración
S1(config)#vlan 23	Ingreso a configuración vlan23
S1(config-vlan)#name Ingenieria	Nombro la vlan Ingeniería
S1(config-vlan)#exit	Salgo de la configuración
S1(config)#vlan 99	Ingreso a configuración vlan99
S1(config-vlan)#name Administracion	Nombro la vlan Administración
S1(config-vlan)#exit	Salgo de la configuración

S1(config)#interface vlan 99 Configuro vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2 255.255.255.0 Asigno dir. Ipv4 vlan 99
S1(config-if)#no shutdown Activo la interfaz
S1(config-if)#exit Salgo de la configuración vlan 99
S1(config)#ip default-gateway 192.168.99.1 Asigno Gateway predeterminado
S1(config)#interface fastEthernet 0/3 Ingreso a la interfaz F0/3
S1(config-if)#switchport mode trunk Configuración enlace troncal en int f0/3
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S1(config-if)#switchport trunk native vlan 1 Configuración enlace troncal vlan 1
S1(config-if)#exit Salgo de la configuración f0/3
S1(config)#interface fastEthernet 0/5 Ingreso a la interfaz F0/5
S1(config-if)#switchport mode trunk Configuración enlace troncal en int f0/5
S1(config-if)#switchport trunk native vlan 1 Configuración enlace troncal vlan 1
S1(config-if)#exit Salgo de la configuración f0/5
S1(config)#interface range fastEthernet 0/1-2, f0/4, f0/7-24
Configuración puertos de acceso en demás rangos
S1(config-if-range)#switchport mode Access Configuración acceso permanente
S1(config-if-range)#exit Salgo de la configuración
S1(config)#interface fastEthernet 0/6 Ingreso a la interfaz F0/6
S1(config-if)#switchport mode access Configuración acceso permanente
S1(config-if)#switchport access vlan 21 Configuración acceso vlan 21
S1(config-if)#exit Salgo de la configuración f0/6
S1(config)#interface range fastEthernet 0/1-2, f0/4, f0/7-24
Configuración rango interfaz y apagar los no utilizados
S1(config-if-range)#shutdown Apagar las interfaces
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down ……%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#
S1(config-if-range)#exit Salgo de la configuración
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Parte 3 – P2. Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos 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	Asigne la primera dirección IP de la subred como el gateway predeterminado
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente propia.

Código de configuración S3 – tabla 16	Descripción del código
S3>enable	Inicio al modo privilegiado
Password:	Ingreso contraseña modo privilegiado
S3#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
S3(config)#vlan 21	Ingreso a configuración vlan21
S3(config-vlan)#name Contabilidad	Nombro la vlan Contabilidad
S3(config-vlan)#exit	Salgo de la configuración
S3(config)#vlan 23	Ingreso a configuración vlan23
S3(config-vlan)#name Ingenieria	Nombro la vlan Ingeniería
S3(config-vlan)#exit	Salgo de la configuración
S3(config)#vlan 99	Ingreso a configuración vlan99
S3(config-vlan)#name Administracion	Nombro la vlan Administración
S3(config-vlan)#exit	Salgo de la configuración
S3(config)#interface vlan 99	Configuro vlan 99
S3(config-if)#	
%LINK-5-CHANGED: Interface Vlan99, changed state to up	

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
S3(config-if)#ip address 192.168.99.3 255.255.255.0 Asigno dir. Ipv4 vlan 99
S3(config-if)#exit Salgo de la configuración vlan 99
S3(config)#ip default-gateway 192.168.99.1 Asigno Gateway predeterminado
S3(config)#interface fastEthernet 0/3 Ingreso a la interfaz F0/3
S3(config-if)#switchport mode trunk Configuración enlace troncal en int f0/3
S3(config-if)#switchport trunk native vlan 1 Configuración enlace troncal vlan 1
S3(config-if)#exit Salgo de la configuración f0/3
S3(config)#interface range fastEthernet 0/1-2, f0/4-17, f0/19-24
Configuración puertos de acceso en demás rangos
S3(config-if-range)#switchport mode Access Configuración acceso permanente
S3(config-if-range)#exit Salgo de la configuración
S3(config)#interface fastEthernet 0/18 Ingreso a la interfaz F0/18
S3(config-if)#switchport mode access Configuración acceso permanente
S3(config-if)#switchport access vlan 21 Configuración acceso vlan 21
S3(config-if)#exit Salgo de la configuración
S3(config)#interface range fastEthernet 0/1-2, f0/4-17, f0/19-24
Configuración rango interfaz y apagar los no utilizados
S3(config-if-range)#shutdown Desactivar la interfaz
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down…….. %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S3(config-if-range)#exit Salgo de la configuración de rango
S3(config)#exit Salgo de la configuración
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Parte 3 – P3. Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23

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

Fuente propia.

Código de configuración R1 – tabla 17 Descripción del código

R1>enable Inicio al modo privilegiado
Password: Ingreso contraseña modo privilegiado
R1#configure terminal Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/1.21 Configuro interfaz g1.21
R1(config-subif)#encapsulation dot1Q 21 Configuración de encapsulamiento21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Asignación dir. Ipv4
R1(config-subif)#description LAN de Contabilidad VLAN 21 Desc. conex vlan21
R1(config-subif)#no shutdown Activo la interfaz
R1(config-subif)#exit Salgo de la configuración
R1(config)#interface gigabitEthernet 0/1.23 Configuro interfaz g1.23
R1(config-subif)#encapsulation dot1Q 23 Configuración de encapsulamiento23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 Asignación dir. Ipv4
R1(config-subif)#description LAN de Ingenieria VLAN 23 Desc. conex vlan23
R1(config-subif)#no shutdown Activo la interfaz
R1(config-subif)#exit
R1(config)#interface gigabitEthernet 0/1.99 Configuro interfaz g1.99
R1(config-subif)#encapsulation dot1Q 99 Configuración de encapsulamiento99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Asignación dir. Ipv4
R1(config-subif)#description LAN de Administracion VLAN 99 Desc. conex vlan99
R1(config-subif)#no shutdown Activo la interfaz
R1(config-subif)#exit Salgo de la configuración
R1(config)#interface gigabitEthernet 0/1 Configuro interfaz g1
R1(config-if)#no shutdown Activo la interfaz
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up
R1(config-if)#exit Salgo de la configuración interfaz
R1(config)#exit Salgo de la configuración
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

Paso 4: Verificar la conectividad de la red

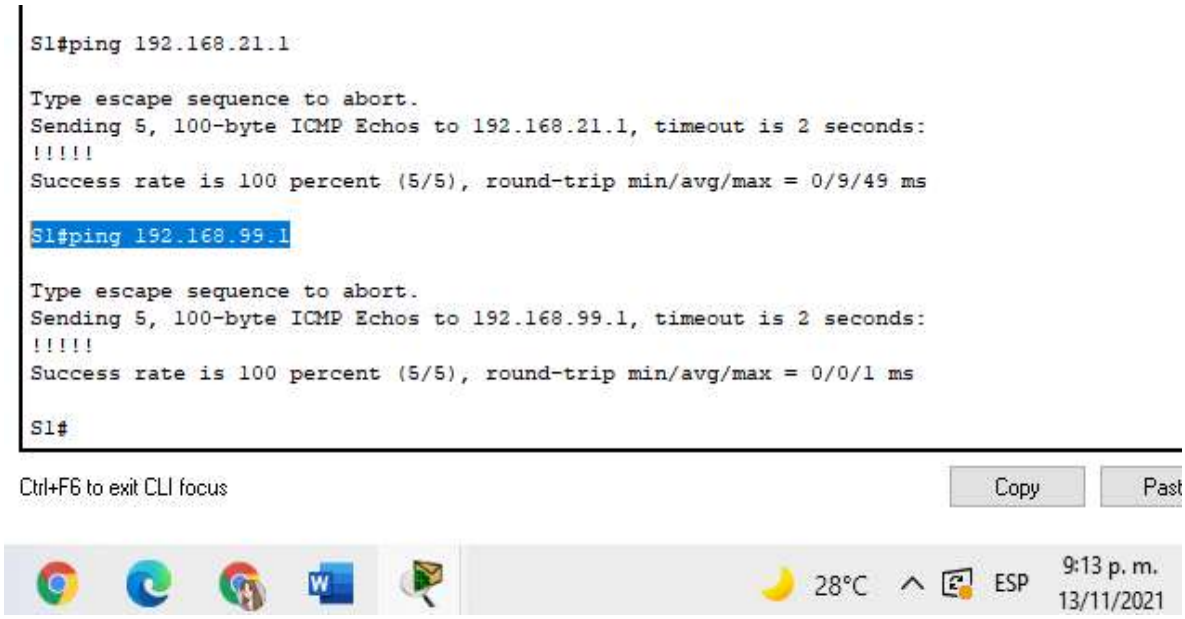
Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 18. Parte 3 – P4. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	100 % (5/5)
S3	R1, dirección VLAN 99	192.168.99.1	100 % (5/5)
S1	R1, dirección VLAN 21	192.168.21.1	100 % (5/5)
S3	R1, dirección VLAN 23	192.168.23.1	100 % (5/5)

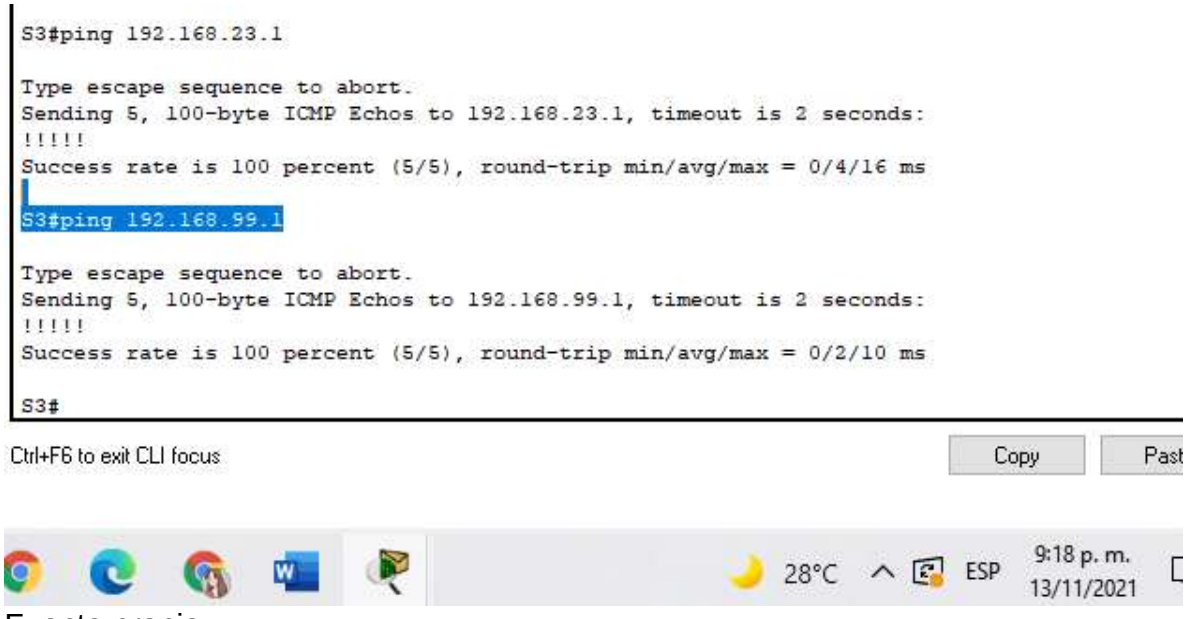
Fuente propia.

Figura 12. Parte 3 – P4. Prueba de conectividad desde S1 a R1, Vlan 99 y 21



Fuente propia

Figura 13. Parte 3 – P4. Prueba de conectividad desde S3 a R1, Vlan 99 y 23



Fuente propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Parte 4 – P1. Configuración OSPF en el R1

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

Fuente propia.

Código de configuración OSPF en R1 – tabla 19. Descripción del código

```
R1>enable                                                    Inicio al modo privilegiado
Password:                                                    Ingreso contraseña modo privilegiado
R1#configure terminal                                        Inicio al modo de configuración
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1                                     Configuración OSPF
R1(config-router)#router-id 1.1.1.1                          Configuración router R1
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0          Anuncio red 172.16.1.0
R1(config-router)#network 172.168.21.0 0.0.0.255 area 0Anuncio red 172.16.1.21
R1(config-router)#network 172.168.23.0 0.0.0.255 area 0Anuncio red 172.16.1.23
R1(config-router)#network 172.168.99.0 0.0.0.255 area 0Anuncio red 172.16.1.99
R1(config-router)#passive-interface gigabitEthernet 0/1.21 Establezc int21 Pasiva
R1(config-router)#passive-interface gigabitEthernet 0/1.23 Establezc int23 Pasiva
R1(config-router)#passive-interface gigabitEthernet 0/1.99 Establezc int99 Pasiva
R1(config-router)#exit                                       Salgo de la configuración router
R1(config-router)#no auto-summary          Desactivo la sumarización automática
                                           El comando no aceptado en el simulador
R1(config-router)#exit                                       Salgo de la configuración router
R1(config)#exit                                              Salgo de la configuración
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Parte 4 – P2. Configuración OSPF en el 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 propia.

Código de configuración OSPF en R2 – tabla 20.	Descripción del código
R2>enable	Inicio al modo privilegiado
Password:	Ingreso contraseña modo privilegiado
R2#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
R2(config)#router ospf 1	Configuración OSPF
R2(config-router)#router-id 2.2.2.2	Configuración router R2
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0	Anuncio red 10.10.10.10
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0	Anuncio red 172.16.1.0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0	Anuncio red 172.16.2.0
R2(config-router)#passive-interface loopback 0	Establezco int Lo0 Pasiva
R2(config-router)#exit	Salgo de la configuración del R2
R2(config-router)#no auto-summary	Desactivo la sumarización automática
	El comando no aceptado en el simulador
R2(config-router)#exit	Salgo de la configuración del router
R2(config)#exit	Salgo de la configuración
R2#	
%SYS-5-CONFIG_I: Configured from console by console	
R2#	

Paso 3: Configurar OSPFv3 en el R2

Código de configuración OSPFv3 en R2	Descripción del código
R2>enable	Inicio al modo privilegiado
Password:	Ingreso contraseña modo privilegiado
R2#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
R2(config)#ipv6 router ospf 1	Configuro router dirección ipv6
R2(config-rtr)#router-id 4.4.4.4	Configuración router R2
R2(config-rtr)#exit	Salgo de la configuración
R2(config)#interface gigabitEthernet 0/0	Configuración interfaz g0
R2(config-if)#ipv6 ospf 1 area 0	Habilito ipv6 en el router
R2(config-if)#exit	Salgo de la configuración
R2(config)#interface serial 0/0/0	Configuración interfaz S0
R2(config-if)#ipv6 ospf 1 area 0	Habilito ipv6 en el router
R2(config-if)#exit	Salgo de la configuración
R2(config)#interface serial 0/0/1	Configuración interfaz S1
R2(config-if)#ipv6 ospf 1 area 0	Habilito ipv6 en el router
R2(config-if)#exit	Salgo de la configuración
R2(config)#exit	Salgo de la configuración
R2#	
%SYS-5-CONFIG_I: Configured from console by console	
R2#	

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Parte 4 – P3. Configuración OSPF en R3

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 propia.

Código de configuración OSPF en R3 – tabla 21. Descripción del código

```
R3>enable                                          Inicio al modo privilegiado
Password:                                          Ingreso contraseña modo privilegiado
R3#configure terminal                              Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1                           Configuración ospf router R3
R3(config-router)#router-id 3.3.3.3                Configuración router R3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0   Anuncio red 172.16.2.0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 Anuncio red 192.168.4.0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 Anuncio red 192.168.5.0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 Anuncio red 192.168.6.0
R3(config-router)#passive-interface loopback 4     Establezco int Lo4 Pasiva
R3(config-router)#passive-interface loopback 5     Establezco int Lo5 Pasiva
R3(config-router)#passive-interface loopback 6     Establezco int Lo6 Pasiva
R3(config-router)#passive-interface loopback 7     Establezco int Lo7 Pasiva
R3(config-router)#exit                             Salgo de la configuración del router
R3(config-router)#no auto-summary                  Desactivo la sumarizacion automática
                                                   El comando no aceptado en el simulador
R3(config-router)#exit                             Salgo de la configuración del router
R3(config)#exit                                    Salgo de la configuración
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

Paso 4: Verificar la información de OSPF

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

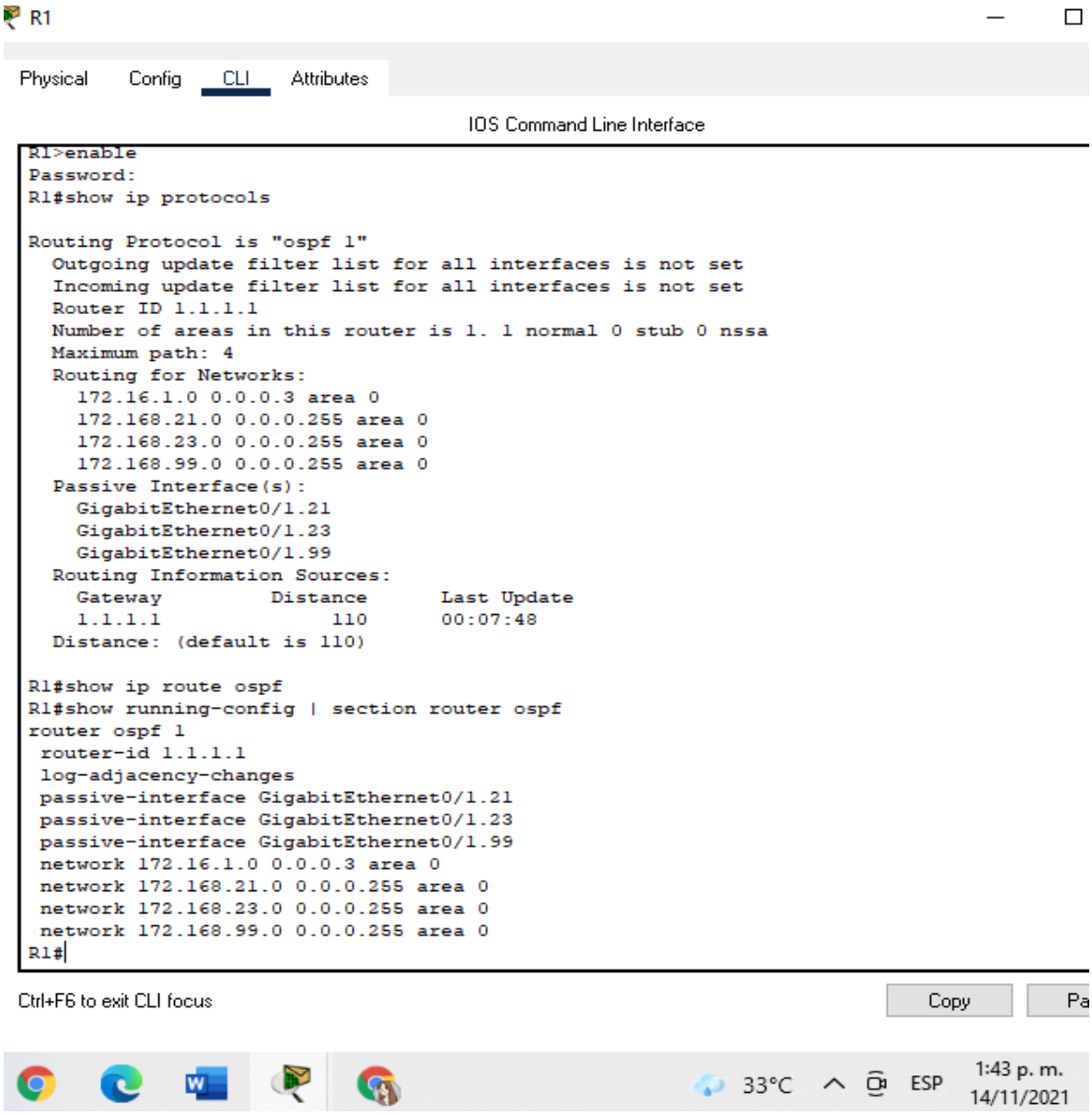
Tabla 22. Parte 4 – P4. Verificando la información de OSPF

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?	Desde el modo privilegiado en R1, R2 y R3 se aplica el siguiente comando: R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Desde el modo privilegiado en R1, R2 y R3 se aplica el siguiente comando: R2#show ip route ospf

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Desde el modo privilegiado en R1, R2 y R3 se aplica el siguiente comando: R3#show running-config | section router ospf

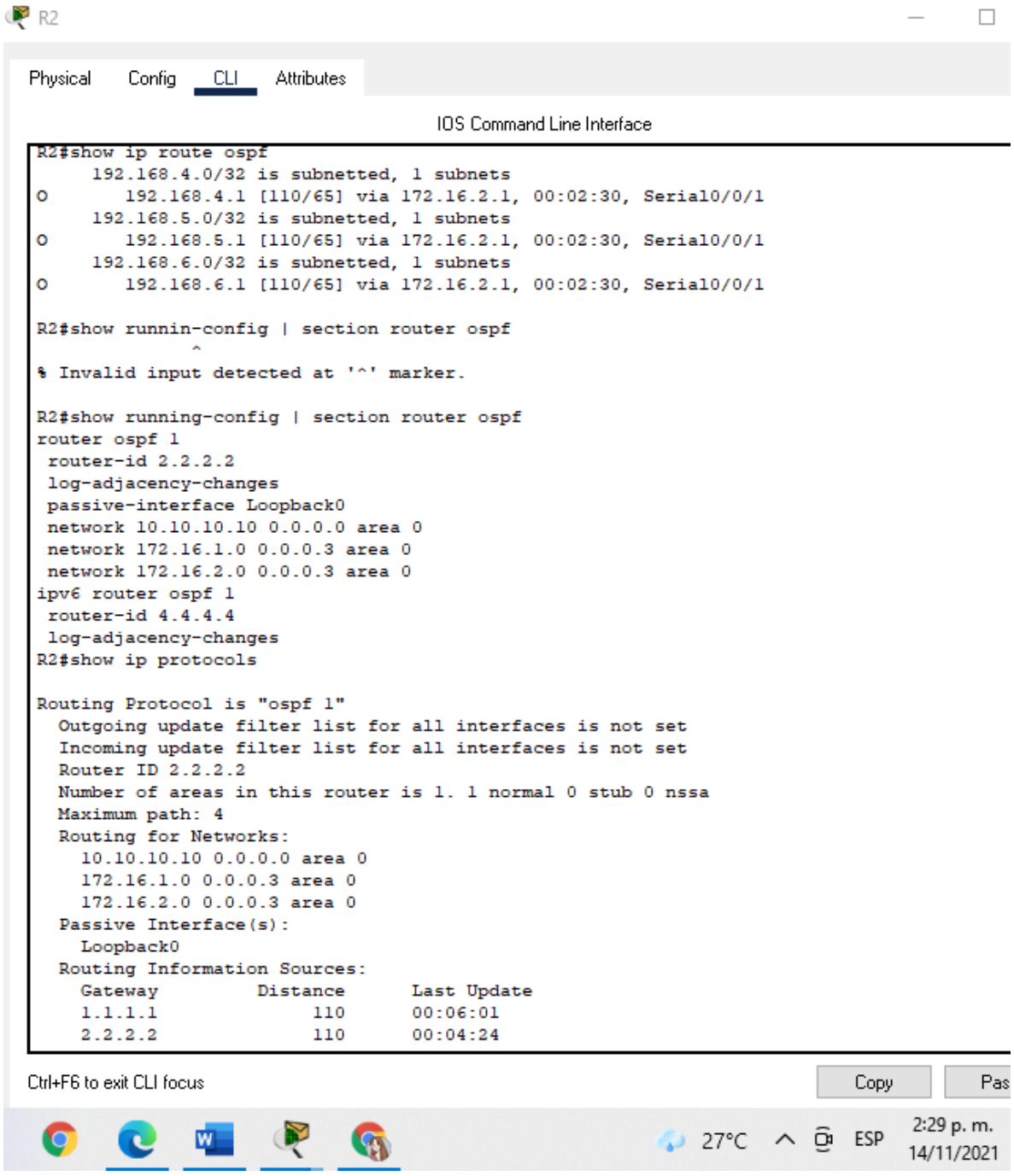
Fuente propia.

Figura 14. Parte 4 – P4. Verificando la información de OSPF en R1



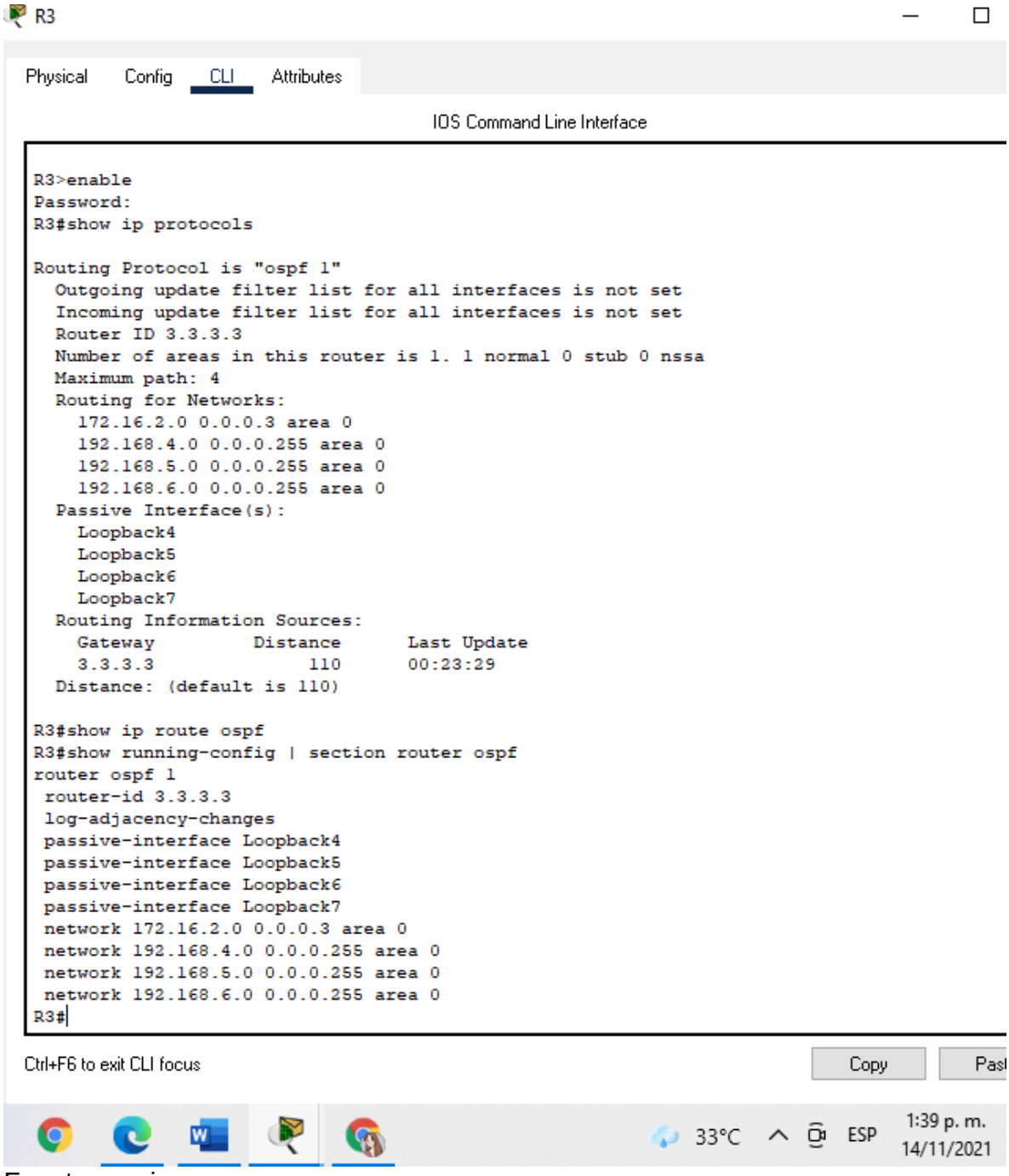
Fuente propia.

Figura 15. Parte 4 – P4. Verificando la información de OSPF en R2



Fuente propia.

Figura 16. Parte 4 – P4. Verificando la información de OSPF en R3



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 23. Parte 5 – P1. Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
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 propia.

Código config. DHCP y NAT para IPv4 -tabla 23 Descripción código

R1#configure terminal Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservo 20 dir. IP en la VLAN 21 para config. estáticas
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Reservo 20 dir. IP en la VLAN 23 para config. estáticas
R1(config)#ip dhcp pool ACCT Creo un pool DHCP (ACCT) para la VLAN 21
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Anuncio red 192.168.21.0
R1(dhcp-config)#default-router 192.168.21.1 Establezco la ruta predeterminada
R1(dhcp-config)#dns-server 10.10.10.10 Establezco servidor DNS
R1(dhcp-config)#domain-name ccna-sa.com Establezco nombre dominio
R1(dhcp-config)#exit Salgo de la configuración
R1(config)#ip dhcp pool ENGNR Creo un pool DHCP (ENGNR) para la VLAN 23
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Anuncio red 192.168.23.0
R1(dhcp-config)#default-router 192.168.23.1 Establezco la ruta predeterminada
R1(dhcp-config)#dns-server 10.10.10.10 Establezco servidor DNS
R1(dhcp-config)#domain-name ccna-sa.com Establezco nombre dominio

R1(dhcp-config)#exit Salgo de la configuración
R1(config)#exit Salgo de la configuración
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Parte 5 – P2. Configuración de NAT estática y dinámica en el 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: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	

Fuente propia.

Configuración de la NAT estática y dinámica -tabla 24. Descripción código

R2>enable Inicio al modo privilegiado
Password: Ingreso contraseña modo privilegiado
R2#configure terminal Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 password cisco12345
Creación cuenta usuario con privilegio
R2(config)#ip http server Habilito servicio servidor http
Comando inhabilitado en el simulador
R2(config)#ip http authentication local Configuración del servidor http
Comando inhabilitado en el simulador
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Creo una NAT estática en el servidor web
R2(config)#interface gigabitEthernet 0/0 Configuración interfaz g0
R2(config-if)#ip nat outside Asignación como interfaz externa
R2(config-if)#exit Salgo de la configuración
R2(config)#interface s0/0/ Configuración interfaz s0
R2(config-if)#ip nat inside Asignación como interfaz interna
R2(config-if)#exit Salgo de la interfaz s0
R2(config)#interface s0/0/1 Configuración interfaz s1
R2(config-if)#ip nat inside Asignación como interfaz interna
R2(config-if)#exit Salgo de la interfaz s1
R2(config)#interface loopback 0 Configuración interfaz Lo0
R2(config-if)#ip nat inside Asignación como interfaz interna
R2(config-if)#exit Salgo de la configuración
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 Lista de acceso permitida
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Lista de acceso permitida
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255 Lista 3de acceso permitida
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248 Defino pool de direcciones IP utilizables
R2(config)#ip nat inside source list 1 pool INTERNET Traducción NAT dinámica
R2(config)#exit Salgo de la configuración
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

Paso 3: Verificar el protocolo DHCP y la NAT estática

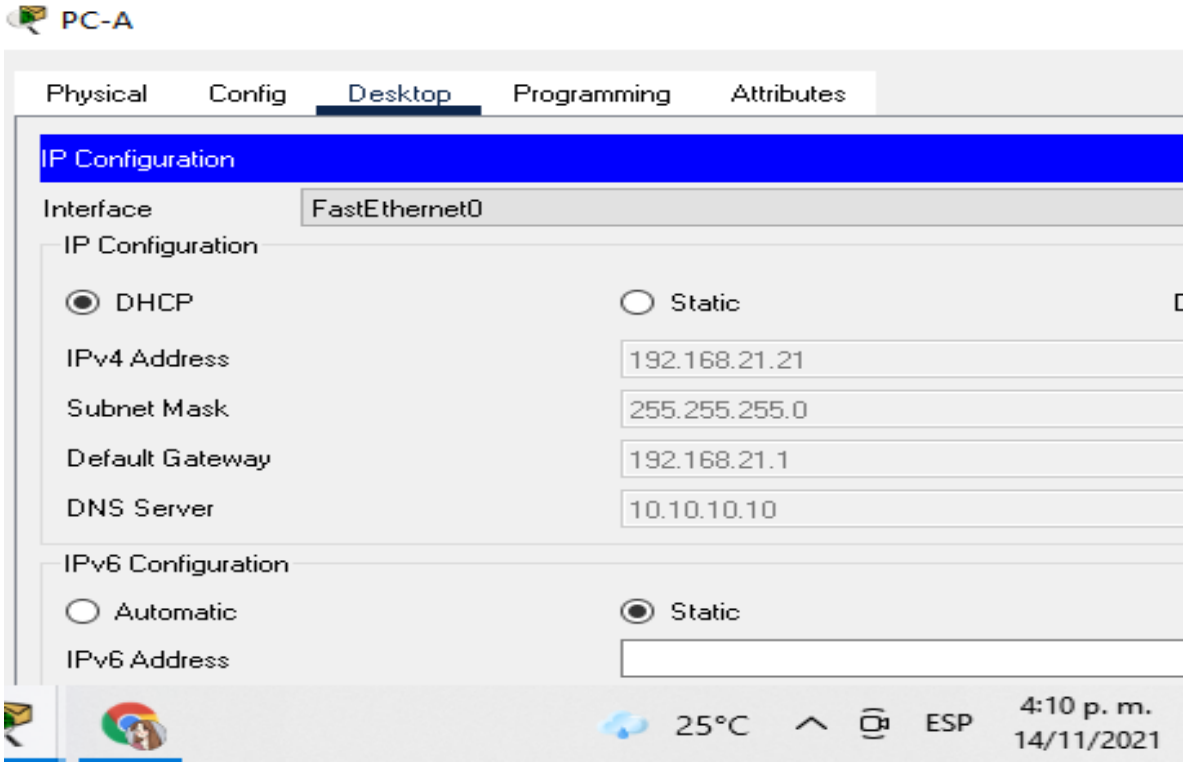
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 25. Parte 5 – P3. Verificando el protocolo DHCP y la NAT estática

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

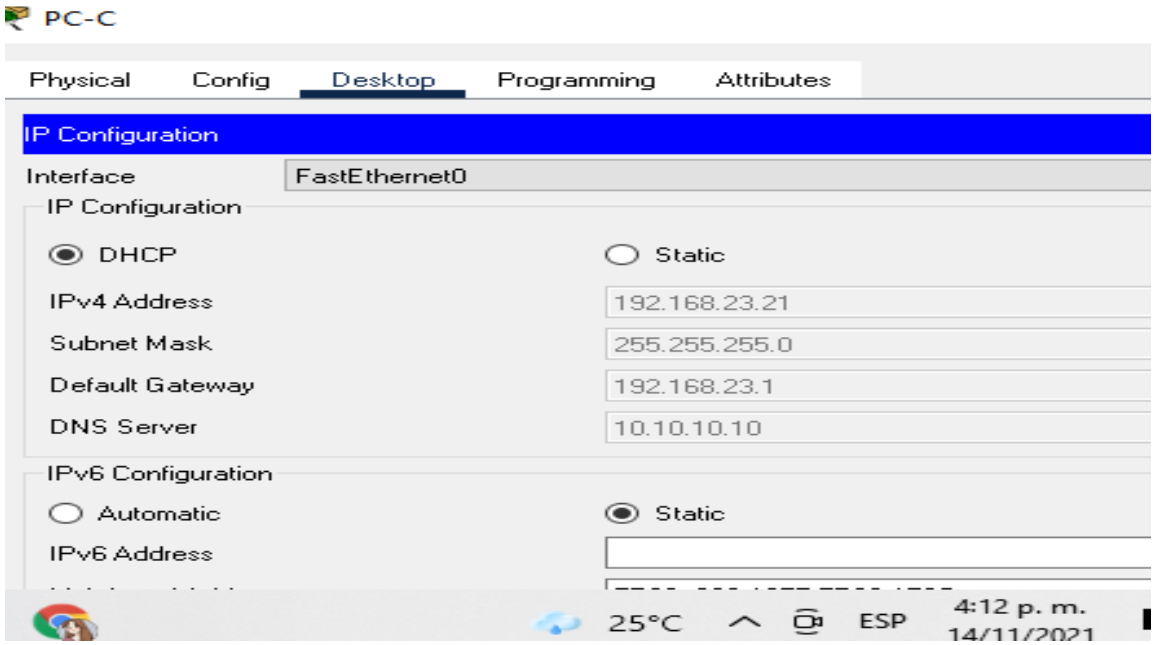
Fuente propia.

Figura 17. Parte 5 – P3. Verificando que la PC-A adquiera información de IP del servidor de DHCP



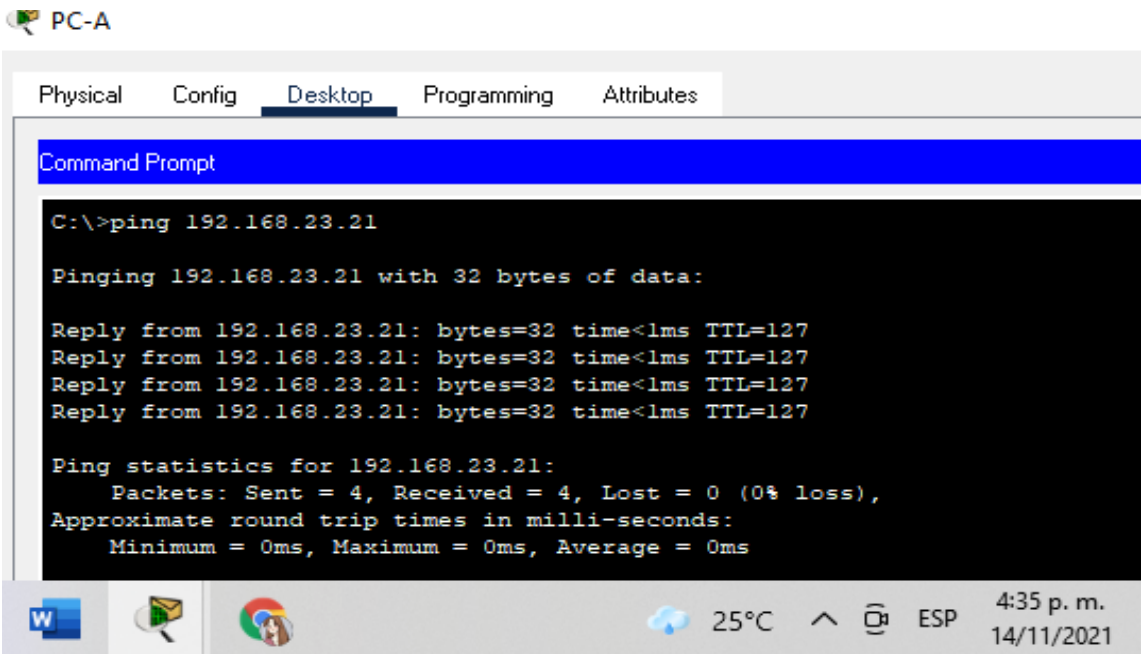
Fuente propia.

Figura 18. Parte 5 – P3. Verificando que la PC-C adquiera información de IP del servidor de DHCP



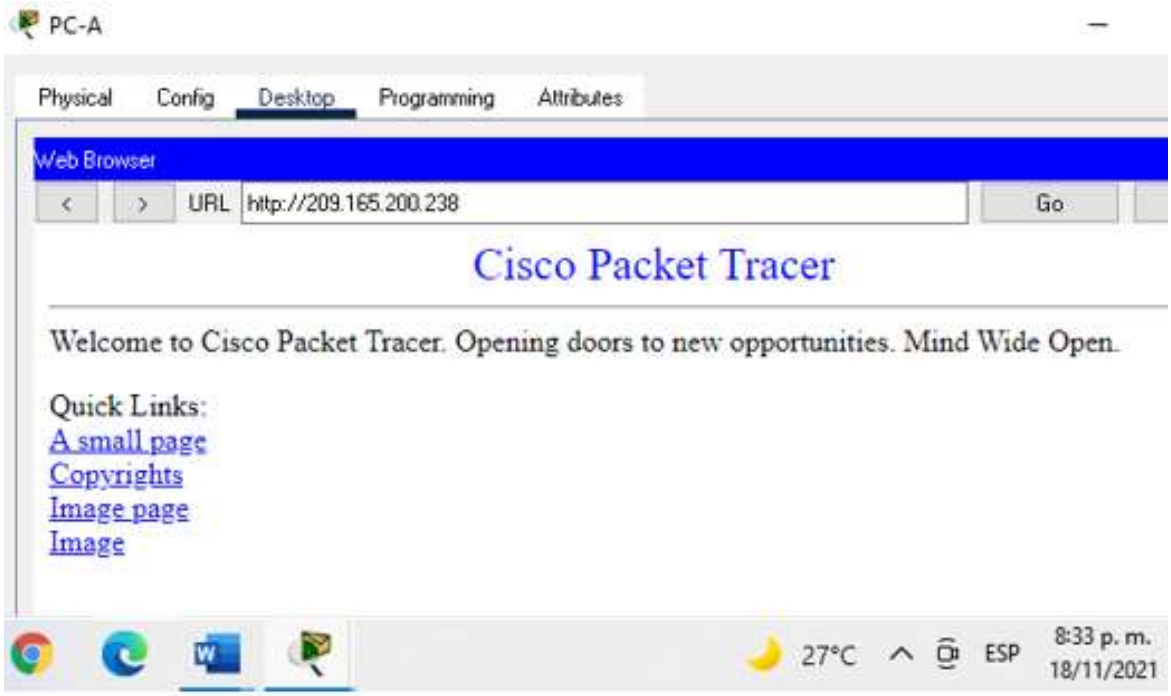
Fuente propia.

Figura 19. Parte 5 – P3. Verificando que la PC-A pueda hacer ping a la PC-C



Fuente propia.

Figura 20. Parte 5 – P3. Verificando el acceso al servidor web (209.165.200.238)



Fuente propia

Nota: En este caso, al insertar la IP 209.165.200.238 no tiene acceso ya que la simulación del router no permite la habilitación del protocolo HTTP, aunque se visualiza la información configurada en el archivo index.html del servidor.

Parte 6: Configurar NTP

Tabla 26. Parte 6. Configurar NTP en R2 y R1.

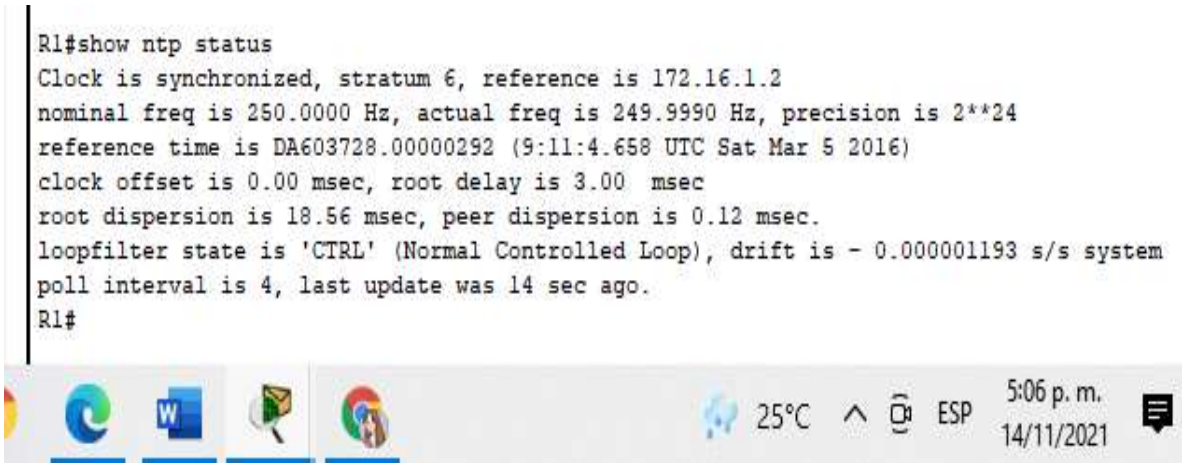
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración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

Fuente propia.

Código Configuración NTP en R2 – tabla 26.	Descripción del código
R2>enable	Inicio al modo privilegiado
Password:	
R2#clock set 09:00:00 05 March 2016	Asigno fecha y hora en R2
R2#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
R2(config)#ntp master 5	Configuro R2 como maestro NTP estrato 5
R2(config)#exit	Salgo de la configuración R2

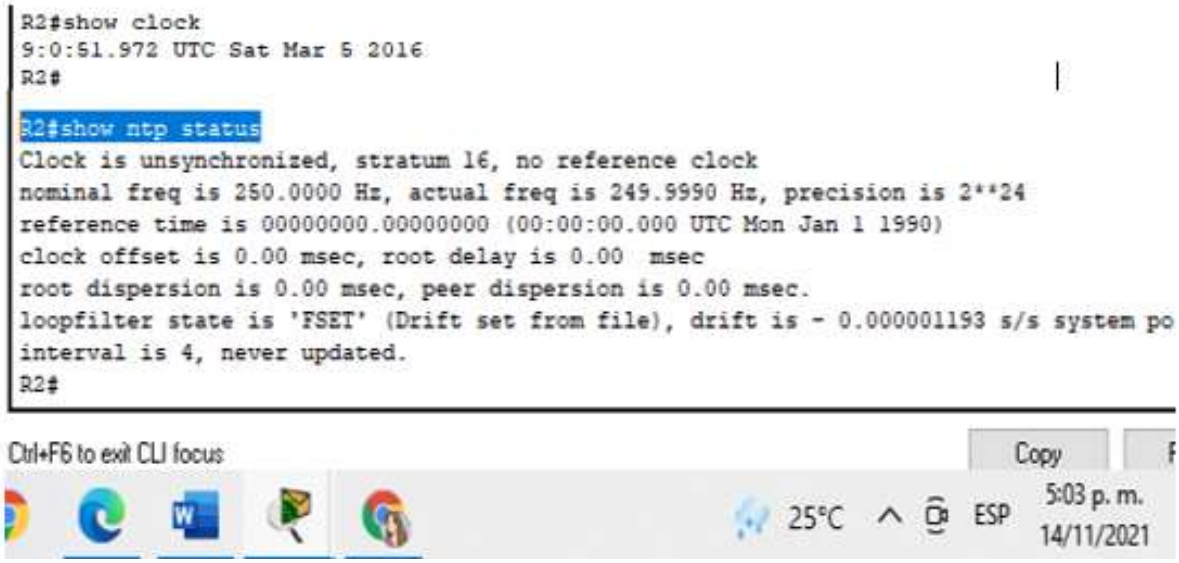
Código Configuración NTP en R1 – tabla 26.	Descripción del código
R1>enable	Inicio al modo privilegiado
Password:	
R1#configure terminal	Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.	
R1(config)#ntp server 172.16.1.2	Configuro R1 como cliente NTP
R1(config)#ntp update-calendar	Configuro R1 actual. calendario hora NTP
R1(config)#exit	Salgo de la configuración
R1#	
%SYS-5-CONFIG_I: Configured from console by console	
R1#	

Figura 21. Parte 6. Verificando configuración de NTP en R1



Fuente propia

Figura 22. Parte 6. Verificando configuración de NTP en R2



Fuente propia

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. Parte 7- P1. Configurar y verificar ACL, restringiendo acceso a VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
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 propia.

Codificación ACL en R2 – tabla 27. Descripción del código

R2#configure terminal Inicio al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
Configuro lista acceso de R1 con telnet a R2
R2(config-std-nacl)#permit host 172.16.1.1 Permite acceso al host
R2(config-std-nacl)#exit Salgo configuración
R2(config)#line vty 0 4 Ingreso a la línea vty
R2(config-line)#access-class ADMIN-MGT in Restringe conexión entre vty det
R2(config-line)#transport input telnet Permite acceso a telnet en línea vty
R2(config-line)#exit Salgo configuración vty
R2(config)#exit Salgo configuración
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#telnet 172.16.1.2 Se verifica que funcione

Figura 23. Parte 7- P1. Verificando ACL, restringiendo acceso a VTY en R2

Fuente propia.

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

Tabla 28. Parte 7- P2. Comando de CLI en R2

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Se utiliza el comando show access-lists
Restablecer los contadores de una lista de acceso	Con el comando clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Se usa el comando show ip interface | include Access show running-config | include access
¿Con qué comando se muestran las traducciones 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. Rta. Con el comando show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Se utiliza el comando clear ip nat translation

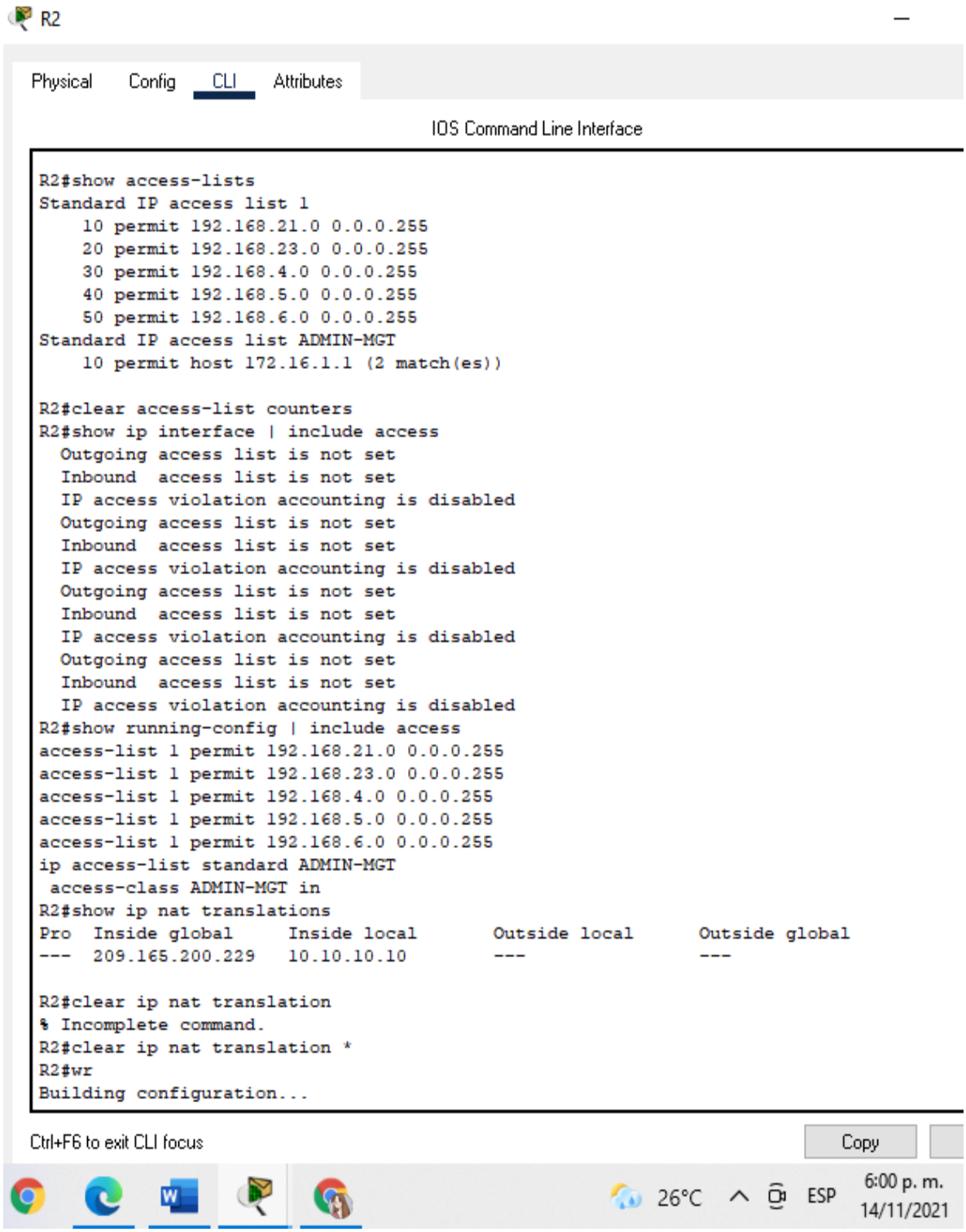
Fuente propia.

Código mostrar en R2 – tabla 28. Descripción del código

R2#show access-lists Muestra coincidencia en lista de acceso
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.0.255
40 permit 192.168.5.0 0.0.0.255
50 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
R2#clear access-list counters Restablece contadores de una lista de acceso
R2#show ip interface | include access Muestra qué ACL se aplica a una interfaz

Outgoing access list is not set
Inbound access list is not set
IP access violation accounting is disabled
Outgoing access list is not set
Inbound access list is not set
IP access violation accounting is disabled
Outgoing access list is not set
Inbound access list is not set
IP access violation accounting is disabled
Outgoing access list is not set
Inbound access list is not set
IP access violation accounting is disabled
R2#show running-config | include access Muestra la dirección que se aplica
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
access-list 1 permit 192.168.5.0 0.0.0.255
access-list 1 permit 192.168.6.0 0.0.0.255
ip access-list standard ADMIN-MGT
access-class ADMIN-MGT in
R2#show ip nat translations Muestra las traducciones NAT
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.229 10.10.10.10 --- ---
R2#clear ip nat translation * Elimina las traducciones de NAT dinámicas
R2#wr Guardo la configuración
Building configuration...
[OK]

Figura 24. Parte 7- P2. Comando de CLI en R2



Fuente propia.

CONCLUSIONES

La plataforma de CISCO Network Academy permite abordar las temáticas a través de módulos, simulaciones, pruebas y prácticas de laboratorio detallada que conlleva a un aprendizaje con efectividad, con las TIC's.

De la anterior actividad se puede detallar que los escenarios propuestos me permitieron dar solución a la configuración de un router, un switch y equipos, además de diseño del esquema de direccionamiento IPv4 para las LAN. Por otra parte, la aplicación de los códigos en cada parte y pasos asignados, verificar el funcionamiento de cada uno de ellos, esta actividad es muy significativa gracias a la metodología aplicada en estos ejercicios, puesto que permite poner aprueba mi capacidad de análisis de entender cuál era las mejores opciones para resolver los escenarios propuestos.

La plataforma de CISCO Network Academy permite abordar las temáticas de CCNA a través de módulos, simulaciones, pruebas y prácticas de laboratorio con información puntual y detallada que conlleva a un aprendizaje con efectividad y a preparar a los profesionales en campos relacionados directamente con las TIC's.

En los entornos de creación y gracias a la tecnología de Cisco, es posible el acceso generalizado y seguro a la información desde diferentes dispositivos y en diversos lugares, con una mejora considerable de la productividad y la implementación de nuevos servicios.

Además nos permitió trabajar dos escenarios con una práctica exigente, abordando las temáticas de las unidades CCNA1 Y CCNA2 , focalizando así el estudio hacia el análisis, la investigación y desarrollo de las habilidades y destrezas en el diseño e implementación de una red, profundizando en OSPF, NAT y ACL, tomando como referencia los dispositivos de tecnología CISCO, lo cual permitió seguridad, conectividad, control de acceso en los protocolos IPv4 e IPv6, enrutamiento con redes virtuales VLAN, listas de acceso y otras. Conllevando con esto a un aprendizaje autónomo y con efectividad como futuros profesionales en las TIC´s.

REFERENCIAS BIBLIOGRAFICAS

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.

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

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

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

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

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

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

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

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

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

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

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

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.

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.

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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