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

WILLIAM CLEMENTE SANCHEZ ORJUELA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA-ECBTI
INGENIERIA DE SISTEMAS
ZIPAQUIRA
2021

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

WILLIAM CLEMENTE SANCHEZ ORJUELA

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

DIRECTOR
MSc JAVIER VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA-ECBTI
INGENIERIA DE SISTEMAS
ZIPAQUIRA
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Zipaquirá 28 de Noviembre de 2021

DEDICATORIA

Quiero dedicar este esfuerzo, este camino emprendido a dios todo poderoso que me dio la fuerza para culminar esta etapa y comenzar nuevos retos.

De igual manera a mi familia, esposa e hija por motivarme y acompañarme en este proceso de aprendizaje y entrega

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Agradezco primeramente a Dios que no ha permitido que me quebrante en momentos de debilidad, que bendice mi vida cada día, a mi familia esposa e hija y mis padres que siempre estuvieron presentes apoyándome y motivándome cuando el camino se volvía oscuro.

A JAVIER RICARDO VASQUEZ, Ingeniero de telecomunicaciones, docente del diplomado, quien con sus conocimientos aporto para el desarrollo del trabajo.

A LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, por darme la oportunidad de estudiar, de generar los espacios virtuales de enseñanza, y brindarme el mejor apoyo logístico para la presentación de este trabajo.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Direccionamiento: Se entiende por redireccionamiento la forma en que se interpretan los bits de un campo de dirección de una instrucción para localizar un operando o una dirección de destino del resultado de la instrucción.

Gateway: es una pieza de hardware o software de red que se utiliza en telecomunicaciones para redes de telecomunicaciones que permite que los datos fluyan de una red discreta a otra

Interfaz: Es un límite compartido a través del cual dos o mas componentes separados de un sistema informático intercambian información, el intercambio puede ser de hardware o software de computadora.

Mac: es un identificador de 48 bits que corresponde en forma única a una tarjeta o dispositivo de red. Se le conoce también como dirección física.

Subred: rango de direcciones lógicas, que cuando una red se vuelve muy grande, conviene dividirla en subredes

Topología de red: es la disposición de una red incluyendo sus nodos y líneas de conexión

RESUMEN

En esta actividad practica se avala el aprendizaje de lo visto en el diplomado de ccna en cada una de sus unidades, por medio de actividades en donde se puso en práctica estos conocimientos en base a ejercicios prácticos, esta practicidad se debe evidenciar en los escenarios 1 y 2 de este trabajo, con los ejercicios que la guía menciona, en los cuales se realiza una configuración de una red pequeña, su esquema de direccionamiento y subnetting, la configuración de sus dispositivos como lo son el router y el switch desde su parte inicial y los ajustes básicos de seguridad de los mismos así como el direccionamiento ip de los equipos de cómputo conectados a estos. Seguido de esto configurar una red con dual stack, protocolo de enrutamiento dinámico OSPF, NAT, ACL y protocolo de tiempo de red, todo esto evidenciado desde la opción CLI de cada dispositivo con los comandos ejecutados.

PALABRAS CLAVE: Subneteo, Direccionamiento, Seguridad, Comunicación, Enrutamiento, NAT

ABSTRACT

In this practical activity the learning of what is seen in the ccna diploma in each of its units is endorsed, through activities where this knowledge was put into practice based on practical exercises, this practicality should be evidenced in scenarios 1 and 2 of this work. , with the exercises mentioned in the guide, in which a small network configuration is carried out, its addressing scheme and subnets, the configuration of its devices such as the router and the switch from its initial part. and the basic security configuration of the same as well as the IP addressing of the computer equipment connected to them. Followed by this, configure a network with double stack, dynamic routing protocol OSPF, NAT, ACL and network time protocol, all this evidenced from the CLI option of each device with the commands executed.

KEYWORDS: Subnetting, Addressing, Security, Communication, Routing, NAT

INTRODUCCIÓN

.

En este trabajo encontrara la resolución de dos ejercicios o escenarios para probar las habilidades técnicas que se han adquirido durante el diplomado CCNA cisco de la Unad, en el cual se estudiaron y se colocaron en práctica temas como el enrutamiento estático, la configuración de dispositivos de comunicaciones como lo son el router y el switch,protocolos de estado de enlace como OSPF,listas de control de acceso, configuraciones dinámicas de direcciones ip o DHCP Y en última instancia la traducción de direcciones de red para ipv4 mediante NAT,

Todos estos procesos guiados por el material educativo, y la orientación del tutor del curso, importantes para una eficaz y efectiva resolución de los escenarios propuestos los cuales aportan en la vida laboral y profesional.

OBJETIVOS

OBJETIVO GENERAL

Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado

OBJETIVOS ESPECÍFICOS

1.Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
2. Configurar los aspectos básicos de los dispositivos de la Red propuesta
3. Configurar los ajustes básicos de seguridad en el R1 y S1
4. Configurar los hosts y verificar la conectividad entre los equipos
5. Configuración de enrutamiento OSPF en enrutadores
6. Configuración NTP
7.Configuracion de NAT dinámica y estática en el enrutador 2
8.Configuracion de DHCP para la VLAN
9.Verificacion y configuración de listas de acceso (ACL)
10.Verificacion de OSPF
11.Configuracion inicial de enrutadores y switches
12.Verificacion de paquetes en la red.

DESARROLLO

1. ESCENARIO 1

Figura 1 Escenario 1

Fuente: Elaboración Propia

Figura 2 Topología Realizada

Fuente: Elaboración Propia

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).

Ip a trabajar 192.168.15.0 el 15 corresponde a los dos últimos de mi cedula.

SUBNETEO

Ip 192.168.15.0 /24

LAN 1: 100 HOST

Identificar mascara de subred: 255.255.255.0

Aplicando formula de host: $2^7 - 2 = 126$

Obteniendo la nueva mascara de red Lan 1: 255.255.255.128/25 en binario 11111111.11111111.11111111.10000000

Salto de red: $256 - 128 = 128$

LAN 2: 50 HOST

Identificar mascara de subred: 255.255.255.0

Aplicando formula de host: $2^6 - 2 = 62$

Obteniendo la nueva mascara de red Lan 2: 255.255.255.192 /26 en binario 11111111.11111111.11111111.11000000

Salto de red: $256 - 192 = 64$

Tabla 1 Direccionamiento

Item	Requerimiento
Direccion de red	192.168.15.0 donde 15 corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100 host ip rango para esta red 192.168.15.1-192.168.15.126
Requerimiento de host Subred LAN2	50 host ip rango 192.168.15.129-192.168.15.190
R1 G0/0/1	192.168.15.1
R1 G0/0/0	192.168.15.129
S1 SVI	192.168.15.2
PC-A	192.168.15.126
PC-B	192.168.15.190

Fuente: Prueba de Habilidades CCNA ll

Tabla 2 Subneteo Ejercicio

Número de subred	Hosts solicitados	Dirección de red	Mascara	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	100	192.168.15.0	/25	192.168.15.1	192.168.15.126	192.168.15.127
1	50	192.168.15.128	/26	192.168.15.129	192.168.15.190	192.168.15.191

Fuente: Elaboración Propia

CONFIGURACIÓN AJUSTES BÁSICOS R1

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

Se adjunta código con la configuración y veracidad del código

Tabla 3 Configuración R1

Tarea Especificación	Especificaciones y Configuración
Desactivar la búsqueda DNS	Router> Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del Router	Router> Router>enable Router#configure terminal Router(config)#Hostname R1
Nombre de dominio	R1> R1>enable R1#configure terminal R1(config)# ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1> R1>enable R1#configure terminal R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1> R1>enable R1#configure terminal R1#line console 0 R1(config-line) #password ciscoconpass R1 (config-line) #login R1 (config-line) ##exit
Establecer la longitud mínima para las contraseñas	R1> R1>enable R1#configure terminal R1(config)#security passwords min-length 10

Crear un usuario administrativo en la base de datos local	R|> R1>enable R1#configure terminal R1(config)# username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1> R1>enable R1#configure terminal R1(config)# line vty 0 15 R1(config-line)#login loca
Configurar VTY solo aceptando SSH	R1> R1>enable R1#configure terminal R1(config)# line vty 0 15 R1(config-line) #login local R1(config-line) # transport input ssh R1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	R1> R1>enable R1#configure terminal R1(config)# service password-encryption
Configure un MOTD Banner	R1> R1>enable R1#configure terminal R1(config)# banner motd "prohibido el acceso no autorizado"
Configurar interfaz G0/0/0	R1> R1>enable R1#configure terminal R1(config)#int g0/0/1 R1(config-if) #description to Lan 1 R1(config-if) #ip address 192.168.15.1 255.255.255.128 R1(config-if) # R1(config-if) #no shutdown R1(config-if) # R1(config-if) #exit

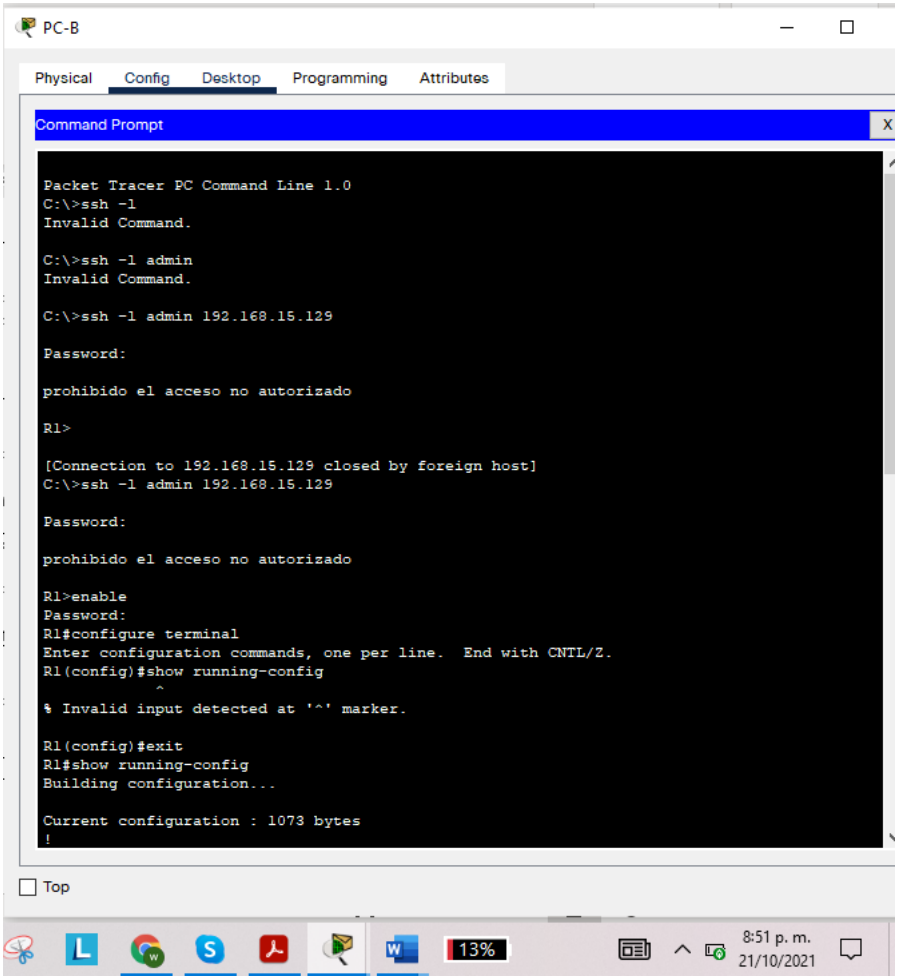
Configurar interfaz G0/0/1	R1(config)#int g0/0/0 R1(config-if) #description to Lan 2 R1(config-if) #ip address 192.168.15.129 255.255.255.192 R1(config-if) #no shutdown R1(config-if) #exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com 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 % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] R1(config)#exit *Mar 1 1:17:30.879: %SSH-5-ENABLED: SSH 1.99 has been enabled R1# %SYS-5-CONFIG_I: Configured from console by console

Fuente: Prueba de Habilidades CCNA ll

EVIDENCIA DE CONEXIÓN SSH DESDE PC-B A R1

Conexión desde PC-B con command prompt a R1 con el comando ssh -L admin dirección ip 192.168.15.129, contraseña admin1pass

Figura 3 Conexión ssh



Fuente: Elaboración Propia

CONFIGURACIÓN AJUSTES BÁSICOS DE S1

Tabla 4 Configuración S1

Tarea Especificación	Especificaciones y Configuración
Desactivar la búsqueda DNS	Switch> Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del Switch	Switch>

	Switch>enable Switch#configure terminal Switch(config)#Hostname S1 S1(config)#
Nombre de dominio	S1> S1>enable S1#configure terminal S1(config)# ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1> S1>enable S1#configure terminal S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1> S1>enable S1#configure terminal S1(config)#line console 0 S1(config-line) #password ciscoconpass S1 config-line) #login S1 (config-line) #exit
Crear un usuario administrativo en la base de datos local	S|> S1>enable S1#configure terminal S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1> S1>enable S1#configure terminal S1(config)# line vty 0 15 S1(config-line) #login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1> S1>enable S1#configure terminal S1(config)# line vty 0 15 S1(config-line) #login local S1(config-line) # transport input ssh S1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	S1> S1>enable S1#configure terminal S1(config)# service password-encryption
Configurar un MOTD Banner	S1>

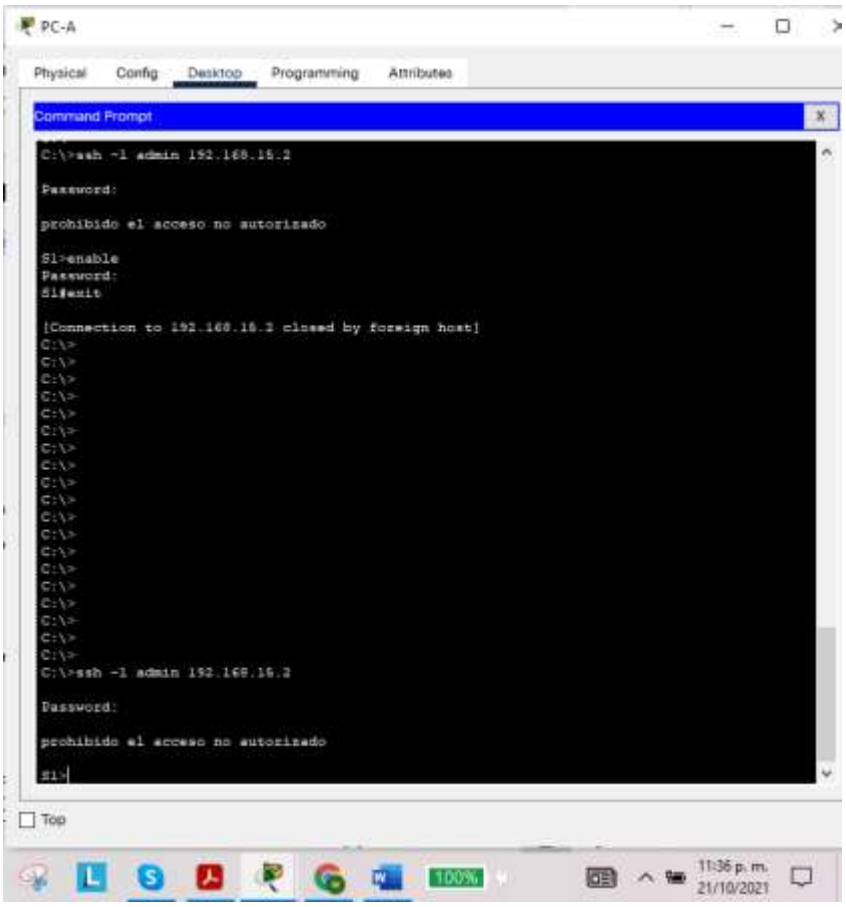
	S1>enable S1#configure terminal S1(config)# banner motd "prohibido el acceso no autorizado"
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable... [OK]
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 1 *Mar 1 5:59:3.643: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if) #ip address 192.168.15.2 255.255.255.128
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.15.1

Fuente: Elaboración Propia

EVIDENCIA DE CONEXIÓN SSH DESDE PC-A A S1

Conexión desde PC-A con command prompt a S1 con el comando ssh -L admin dirección ip 192.168.15.2, user admin,contraseña admin1pass

Figura 4 Conexión ssh



Fuente: Elaboración Propia

PASO 2. CONFIGURAR LOS EQUIPOS

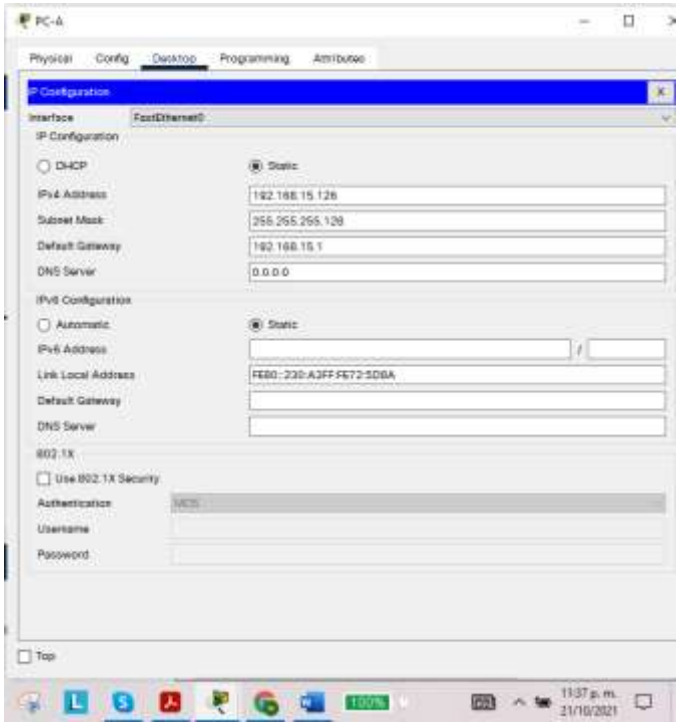
PC-A CONFIGURACIÓN DE RED

Tabla 5 Configuración PC-A

PC-A Configuración de red	
Descripción	PC-A
Direccion Física	0030.A372.5D8A
Direccion Ip	192.168.15.2
Mascara de subred	255.255.255.128
Gateway predeterminado	192.168.15.1

Fuente: Prueba de Habilidades CCNA ll

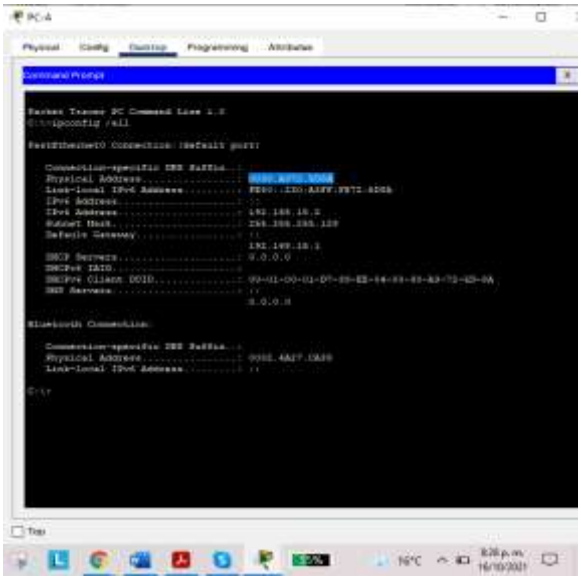
Figura 5 Configuración IP PC-A



Fuente: Elaboración Propia

CONFIGURACIÓN DE RED HOST PC-A, COMANDO IPCONFIG /ALL

Figura 6 comando ipconfig /all



Fuente: Elaboración Propia

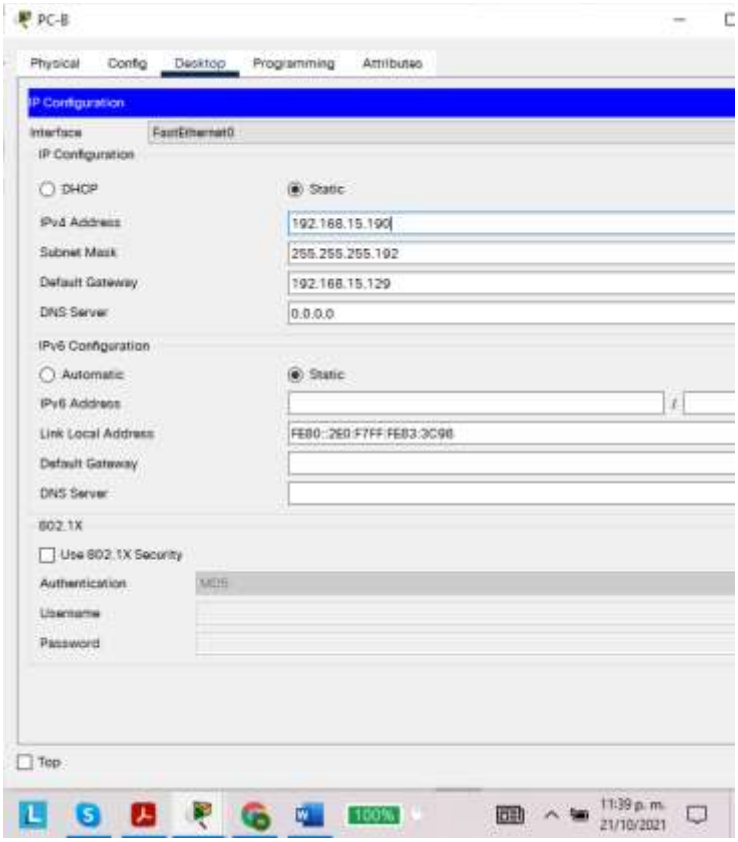
PC-B CONFIGURACIÓN DE RED

Tabla 6 configuración de red PC-B

PC-B Configuración de red	
Descripción	PC-B
Direccion Física	00E0.F783.3C98
Direccion Ip	192.168.15.130
Mascara de subred	255.255.255.192
Gateway predeterminado	192.168.15.129

Fuente: Prueba de Habilidades CCNA ll 1

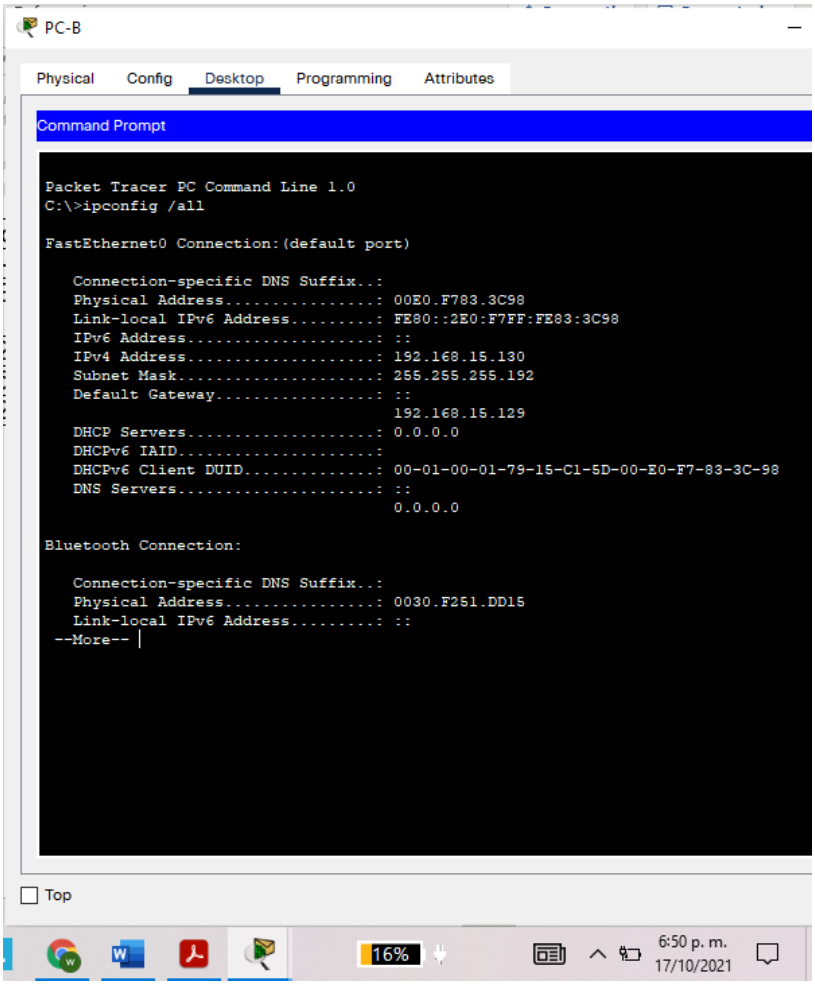
Figura 7 Configuración IP PC-B



Fuente: Elaboración Propia

CONFIGURACIÓN DE RED HOST PC-B COMANDO IPCONFIG /ALL

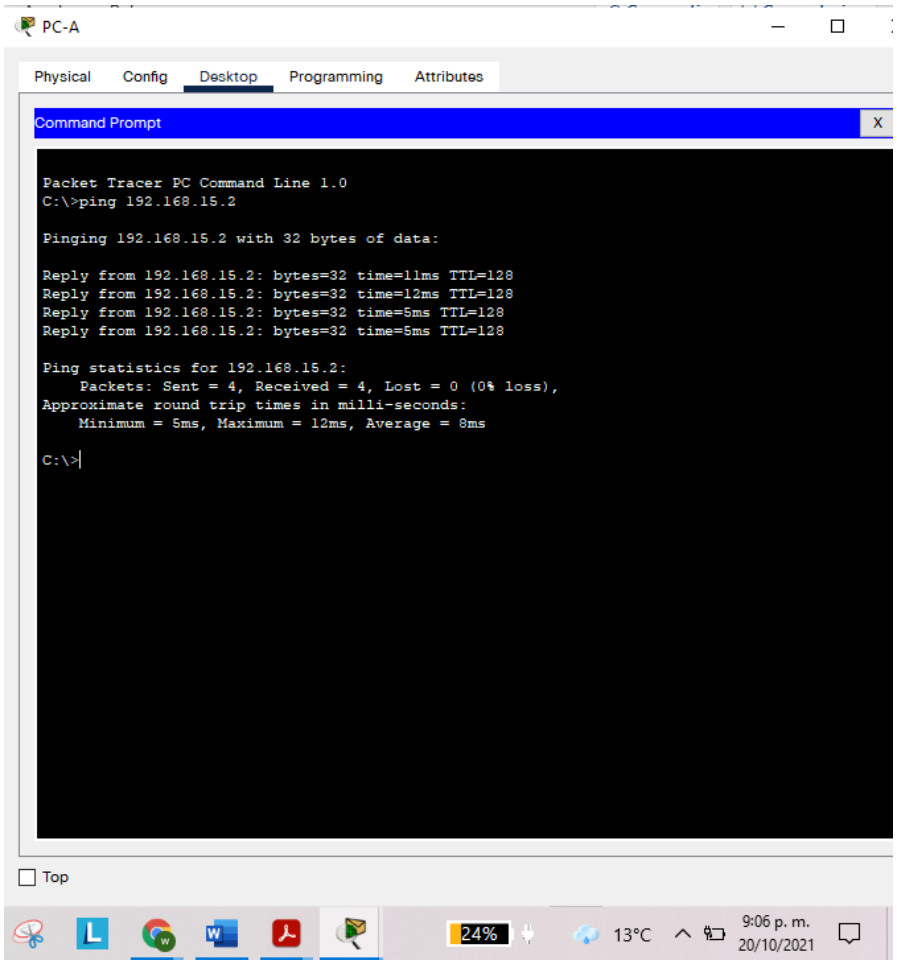
Figura 8 Configuración PC-B ipconfig /all



Fuente: Elaboración Propia

Ping realizado desde la PC-A hasta la vlan del switch

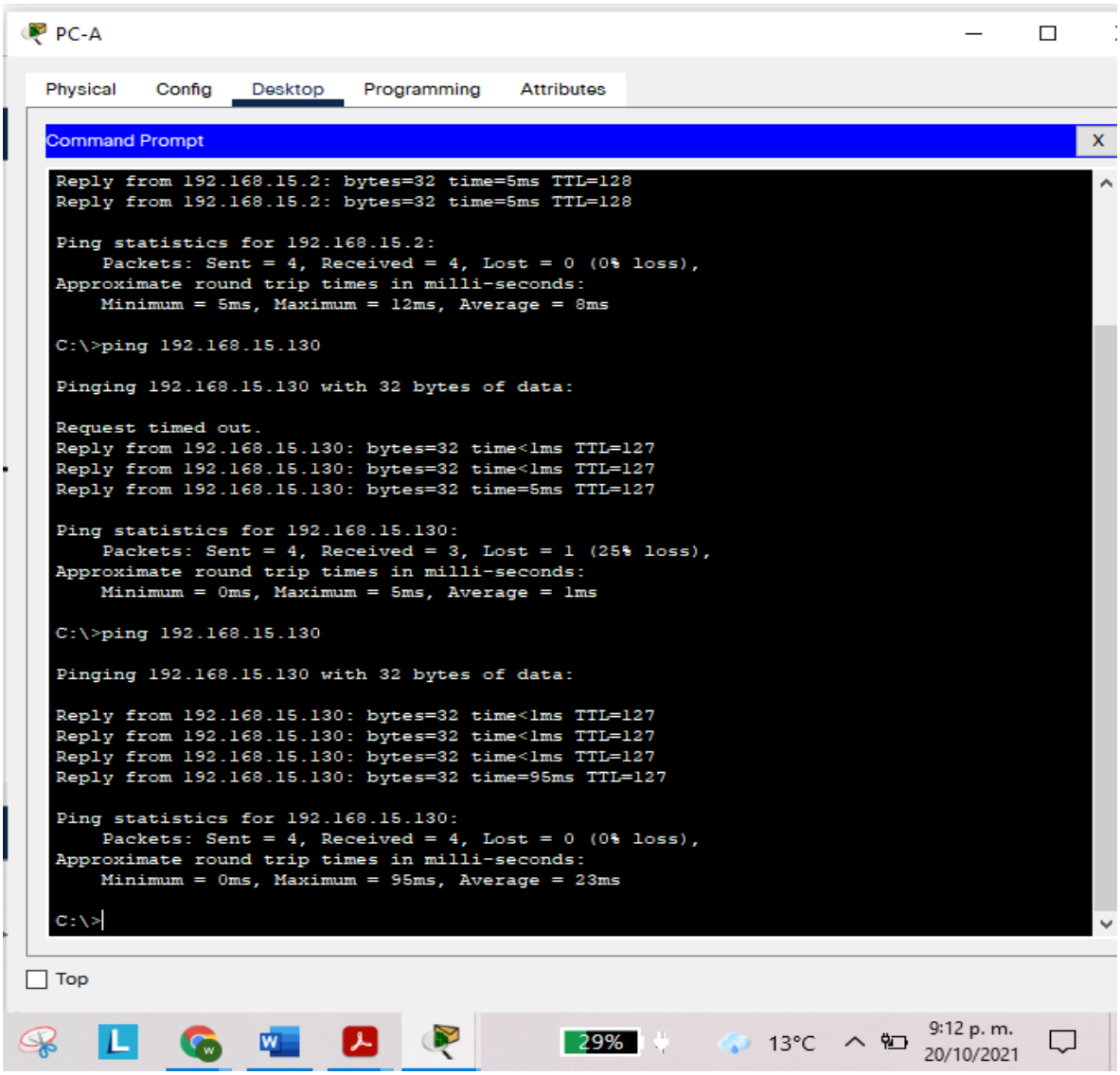
Figura 9 Conexión PC- A con Switch



Fuente: Elaboración Propia

Ping de PC-A a PC-B

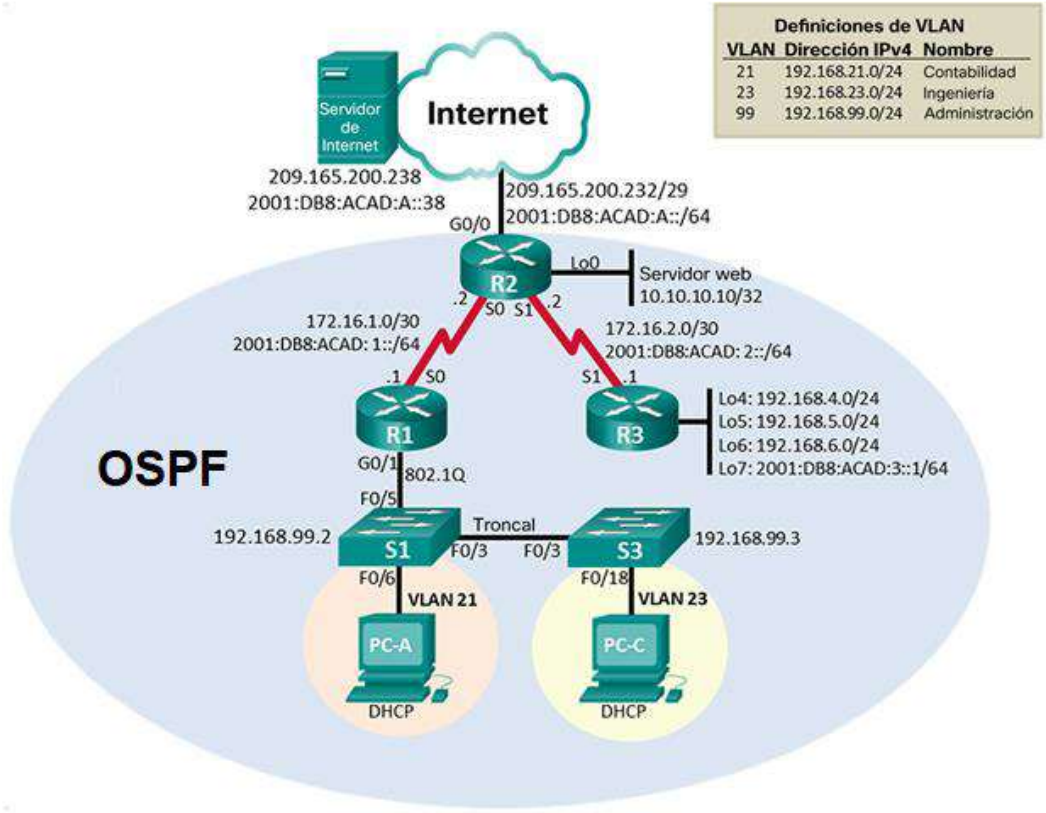
Figura 10 Conexión PC-A a PC-B



Fuente: Elaboración Propia

ESCENARIO 2

Figura 11 Topología Escenario 2



Fuente: Prueba de Habilidades CCNA ll

PARTE 1 INICIALIZAR DISPOSITIVOS

PASO 1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

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

Tabla 7 Inicialización de Dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	**R1** 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 **R2** 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 **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
Volver a cargar todos los routers	Router>enable Router#reload Proceed with reload? [confirm] System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 2010 by cisco Systems, Inc. Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB CISCO1941/K9 platform with 524288 Kbytes of main memory
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	**Switch 0** 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 1** 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 0** Switch>enable

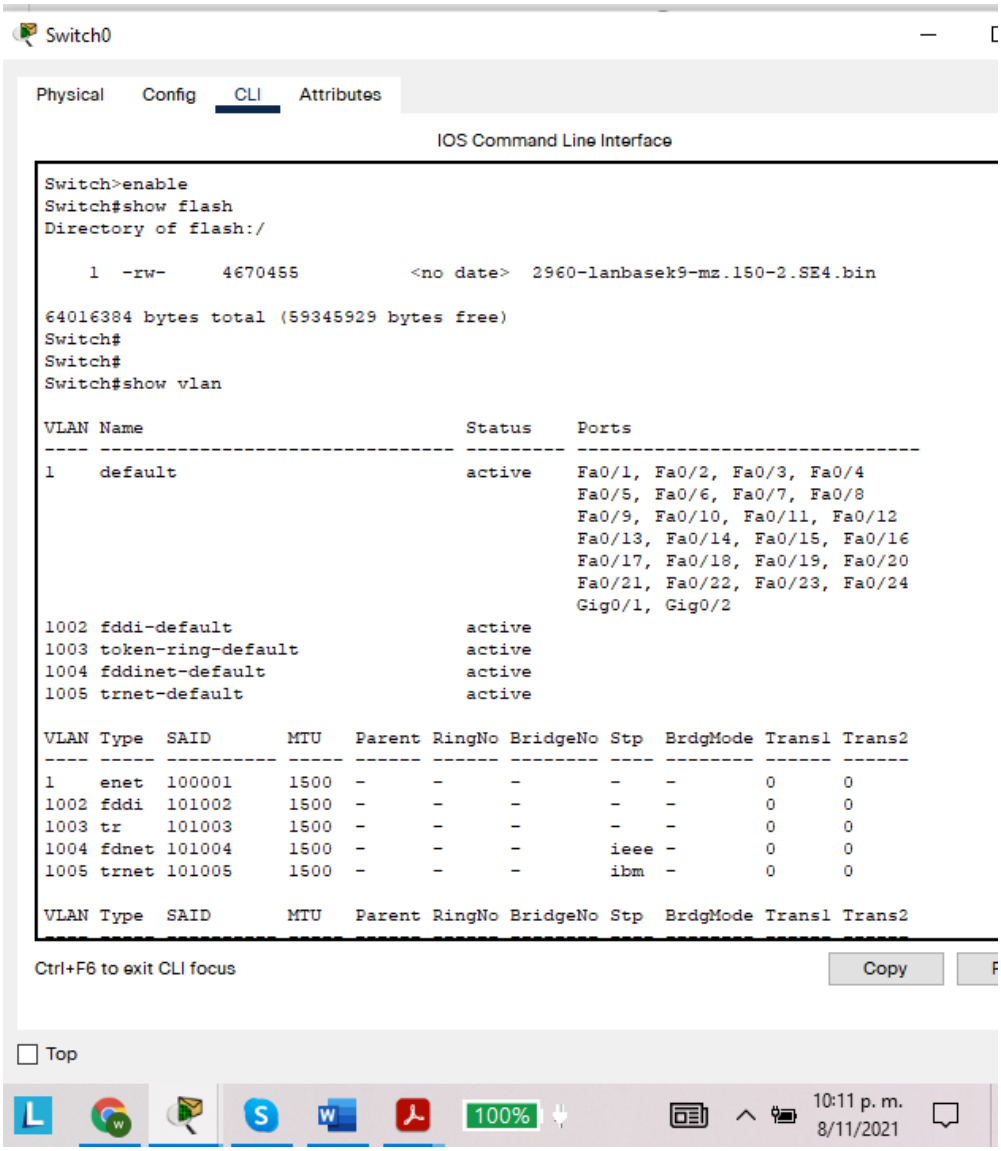
	Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory) **Switch 1** Switch>enable Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory)
Volver a cargar ambos switches	Switch# Switch#reload Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960-24TT starting..
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	**Switch 0** Switch>enable Switch#show flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) Switch#show vlan VLAN Name Status Ports ---- -------------------------------- --------- ------------------------------- 1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2

	1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 ---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ----- - 1 enet 100001 1500 - - - - - 0 0 1002 fddi 101002 1500 - - - - - 0 0 1003 tr 101003 1500 - - - - - 0 0 1004 fdnet 101004 1500 - - - ieee - 0 0 1005 trnet 101005 1500 - - - ibm - 0 0 VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 ---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ----- - Remote SPAN VLANs --- Primary Secondary Type Ports **Switch 1** Switch>enable Switch#show flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) Switch#show vlan VLAN Name Status Ports ---- --- 1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8

	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2 1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 ---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ----- - 1 enet 100001 1500 - - - - - 0 0 1002 fddi 101002 1500 - - - - - 0 0 1003 tr 101003 1500 - - - - - 0 0 1004 fdnet 101004 1500 - - - ieee - 0 0 1005 trnet 101005 1500 - - - ibm - 0 0 VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 ---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ----- - Remote SPAN VLANs ---------- --- Primary Secondary Type Ports ------- --------- ---------- ---------- --

Fuente: Prueba de Habilidades CCNA ll

Figura 12 Comando show Flash y show vlan



Fuente: Elaboración 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 del servidor de internet

Elemento o tarea de configuración	Especificación
Dirección ipv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Prueba de Habilidades CCNA ll

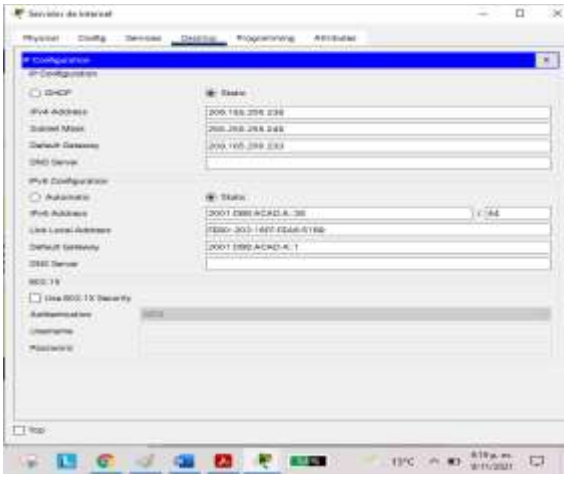
Tabla 9 Subneteo de red

Id address:	**209.165.200.232**
Network Address:	209.165.200.232
Usable Host Ip Range:	209.165.200.233-209.165.200.238
Broadcast Address:	209.165.200.239
Total Number of Hosts:	8
Number of Usable:	6
Subnet mask:	255.255.255.248

Wildcard Mask:	0.0.0.7
Binary subnet Mask:	11111111.11111111.11111111.11111000
Ip Type: **Ip Addres**	PUBLICIP-CLASS C
Ip Addres	**2001.db8:a cad:a::38/64**
Full Ip Address:	2001:0db8:acad:000a:0000:0000:0000:0038
Total Ip Addresses	8.446.744.073.709.551.616
Network:	2001:0db8:acad:000a:: /64 2001:0db8:acad:000a:0000:0000:0000:0000
Ip Range	2001:db8:acad:a::1 2001:0db8:acad:000a:0000:0000:0000:0001 2001:db8:acad:a:ffff:ffff:ffff:ffff 2001:0db8:acad:000a:ffff:ffff:ffff:ffff
Ip Type:	GLOBAL UNICAST

Fuente: Prueba de Habilidades CCNA ll

Figura 13 Configuración de servidor



Fuente: Elaboración Propia

PASO 2: CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10 Configuración R1

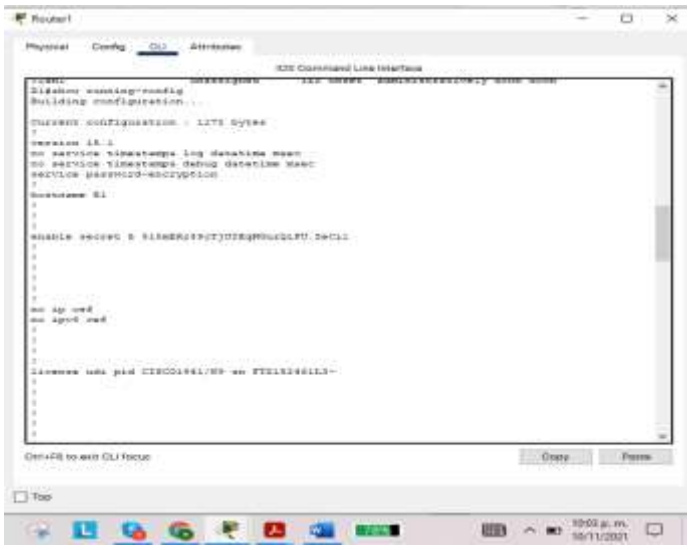
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ip domain-lookup
Nombre del router	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ip domain-lookup Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1>enable R1# R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#enable secret class
Contraseña de acceso a la consola	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#

Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
	R1(config)

Mensaje MOTD	R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd "prohibido el acceso no autorizado" R1(config)#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#int se0/0/0 R1(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#ipv6 route::/0 se0/0/0 ^ % Invalid input detected at '^' marker. R1(config)#ipv6 route ::/0 se0/0/0 R1(config)#

Fuente: Prueba de Habilidades CCNA ll

Figura 14 Cambio de nombre y Encriptación de password



Fuente: Elaboración Propia

Figura 15 Banner Password Cisco y Class

Fuente: Elaboración Propia

PASO 3: CONFIGURAR R2

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configuración R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Este comando (ip http server) no es compatible con Packet Tracer
Mensaje MOTD	R2(config)#banner motd "prohibido el acceso no autorizado"
Interfaz S0/0/0	R2(config)#int se0/0/0 R2(config-if)#description Connection R1 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)#no shutdown R2(config-if)#

	%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up R2(config-if)#ex %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
Interfaz S0/1/0	R2(config)#int se0/1/0 R2(config-if)#Description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description Connection to Internet 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 shutdowen ^ % Invalid input detected at '^' marker. R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 description simulacion servidor web R2(config-if)#

	%LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#
Rutas predeterminadas	R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Fuente: Prueba de Habilidades CCNA ll

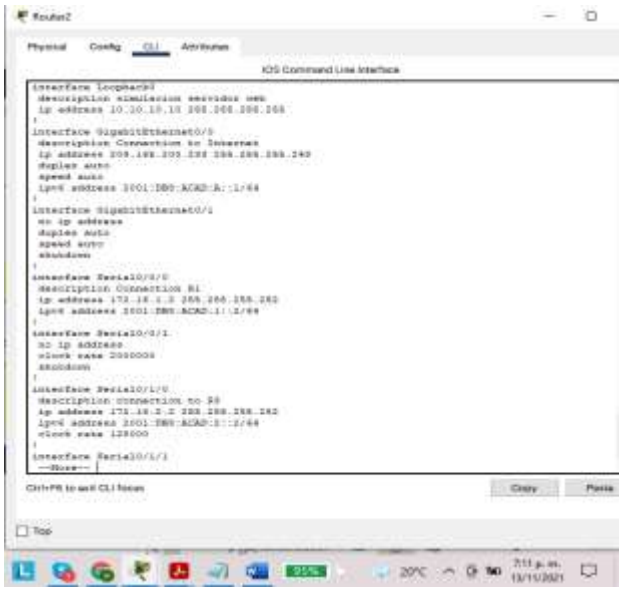
Figura 16 Configuración contraseña cisco, nombré del router

Fuente: Elaboración Propia

Figura 17 Configuración de interfaces

Fuente: Elaboración Propia

Figura 18 Configuración de banner



Fuente: Elaboración Propia

PASO 4: CONFIGURAR R3

La configuración del R3 incluye las siguientes tareas:

Tabla 12 Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ip domain-lookup Router(config)#
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "prohibido el acceso no autorizado" R3(config)#
Interfaz S0/0/1	R3#configure Terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)#int se0/1/0 R3(config-if)#description connection R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252

	R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 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)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	int loopback 5 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)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#int loopback 6 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)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 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)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#EXIT
Rutas predeterminadas	R3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)#ip route 0.0.0.0 0.0.0.0 se0/1/0 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/1/0 R3(config)#end R3# %SYS-5-CONFIG_I: Configured from console by console R3#

Fuente: Prueba de Habilidades CCNA ll

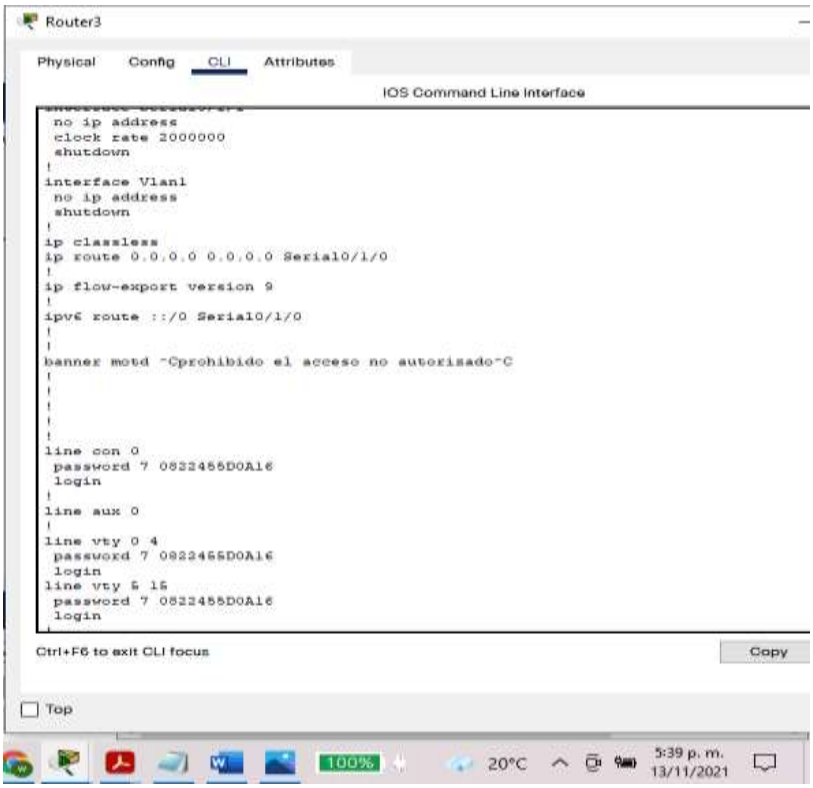
Figura 19 show run encriptación y clave cisco

Fuente: Elaboracion Propia **1**

Figura 20 Interfaces

Fuente: Elaboración Propia

Figura 21 enrutamiento, Banner y líneas



Fuente: Elaboración Propia 2

PASO 5: CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

Tabla 13 Configuracion S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 S1(config)#

Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S1(config)#
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit S1(config)#
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Mensaje MOTD	S1(config)#banner motd "Se prohibe el acceso no autorizado" S1(config)#

Fuente: Prueba de Habilidades CCNA II

Figura 22 Configuración Switch

Fuente: Elaboración Propia

PASO 6: CONFIGURAR EL S3

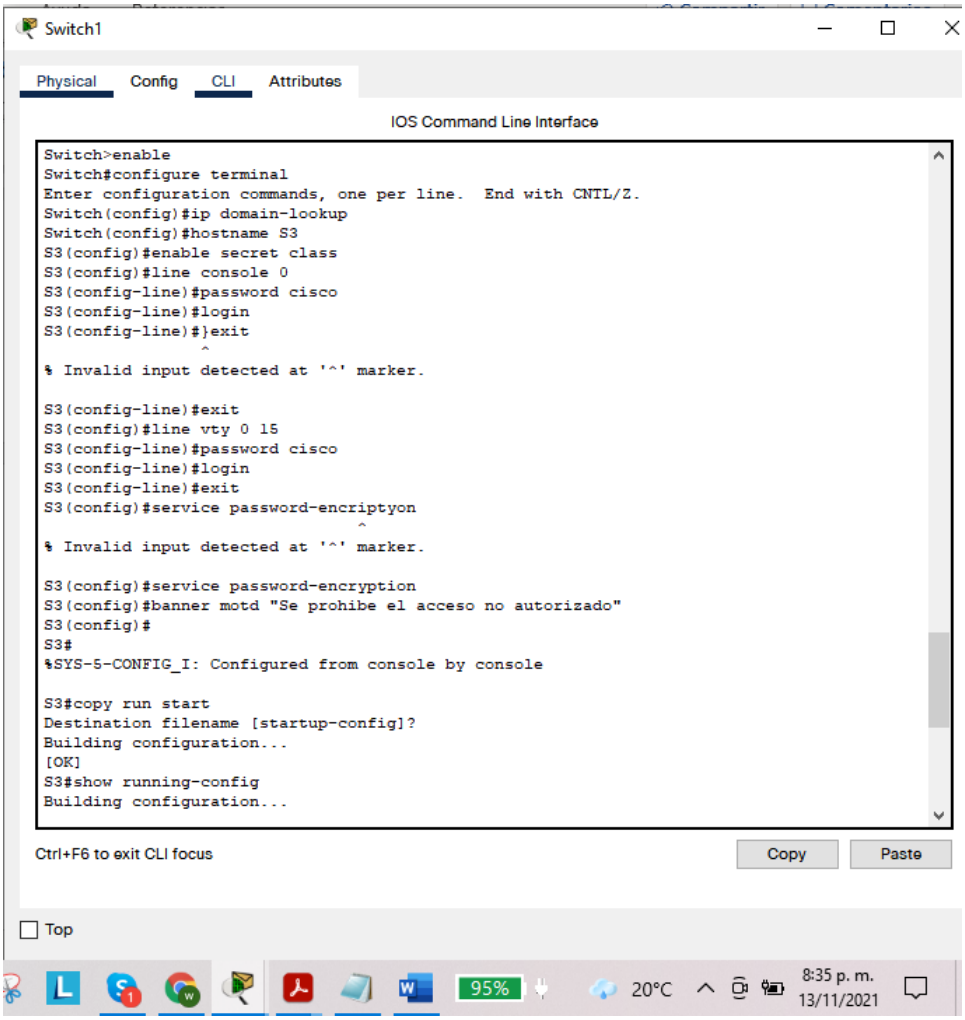
La configuración del S3 incluye las siguientes tareas:

Tabla 14 Configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 S3(config)#
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#
Contraseña de acceso a la consola	S3(config)#line console 0 S3config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption S3(config)#
Mensaje MOTD	S3(config)#banner motd "Se prohibe el acceso no autorizado" S3(config)#

Fuente: Prueba de Habilidades CCNA ll

Figura 23 Configuración S3



Fuente: Elaboración Propia

PASO 7. VERIFICAR LA CONECTIVIDAD DE LA RED

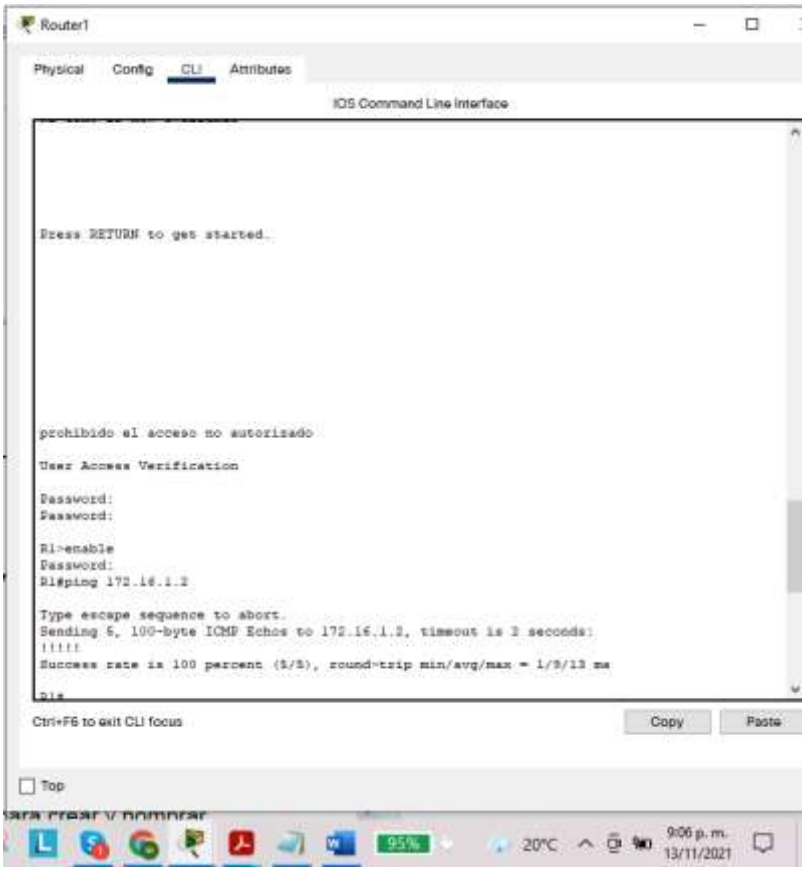
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla.

Tabla 15 Conectividad de la red

Desde	A	Direccion ip	Resultados de ping
R1	R2,S0/0/0	172.16.1.2	Successful
R2	R3,S0/1/0	172.16.2.1	Successful
Servidor de Internet	Gateway predeterminado	209.165.200.233	Successful

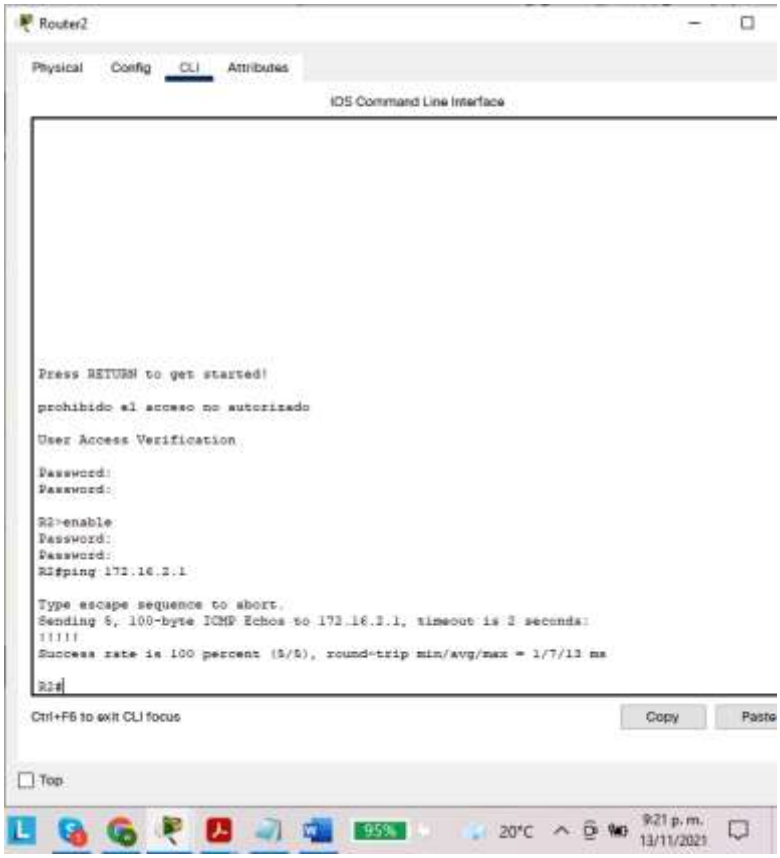
Fuente: Elaboración Propia 3

Figura 24 ping de R1 a R2



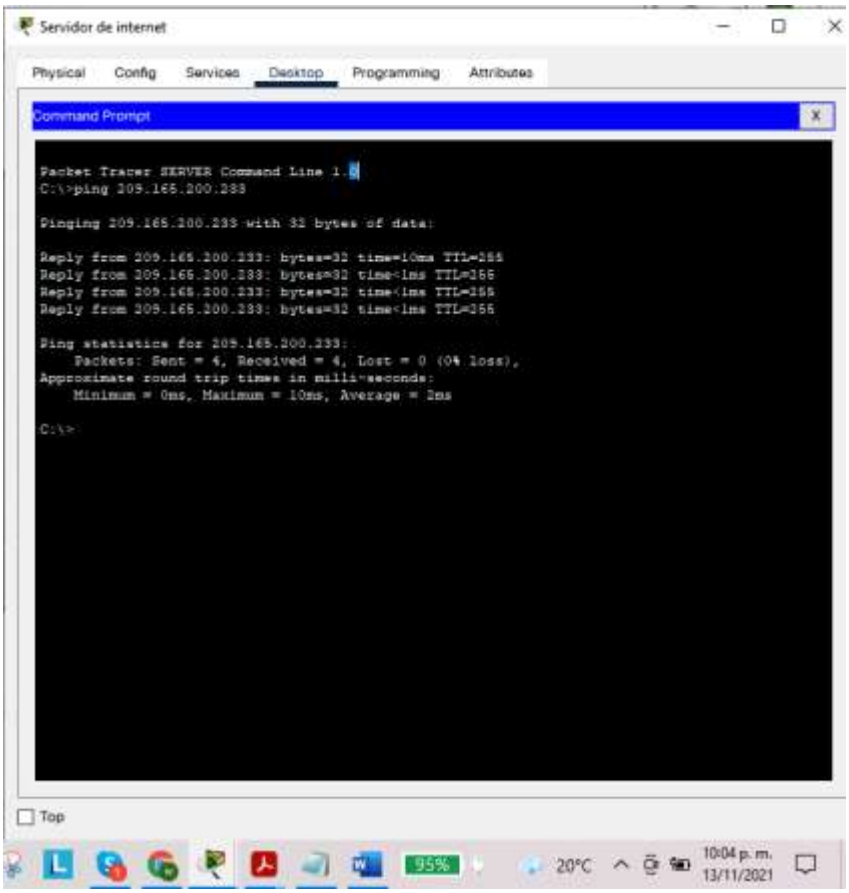
Fuente: Elaboración Propia

Figura 25 ping R2 con R3



Fuente: Elaboración Propia

Figura 26 conexión de servidor con Gateway predeterminado



Fuente: Elaboración Propia

PASO 1: CONFIGURAR S1

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

La configuración del S1 incluye las siguientes tareas:

Tabla 16 Configuración de seguridad del S1, vlan

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#end S1# %SYS-5-CONFIG_I: Configured from console by console S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#end S1# %SYS-5-CONFIG_I: Configured from console by console S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#end S1# %SYS-5-CONFIG_I: Configured from console by console
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-if)#ip address 192.168.99.1 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit S1(config)#interface vlan 99

	S1(config-if)#no ip address 192.168.99.1 255.255.255.0 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	. S1(config)#ip default-gateway 192.168.99.1 S1(config)#
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int fa0/3 S1(config-if)#switchport mode trunk 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
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int fa0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#
Apagar todos los puertos sin usar	S1#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %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

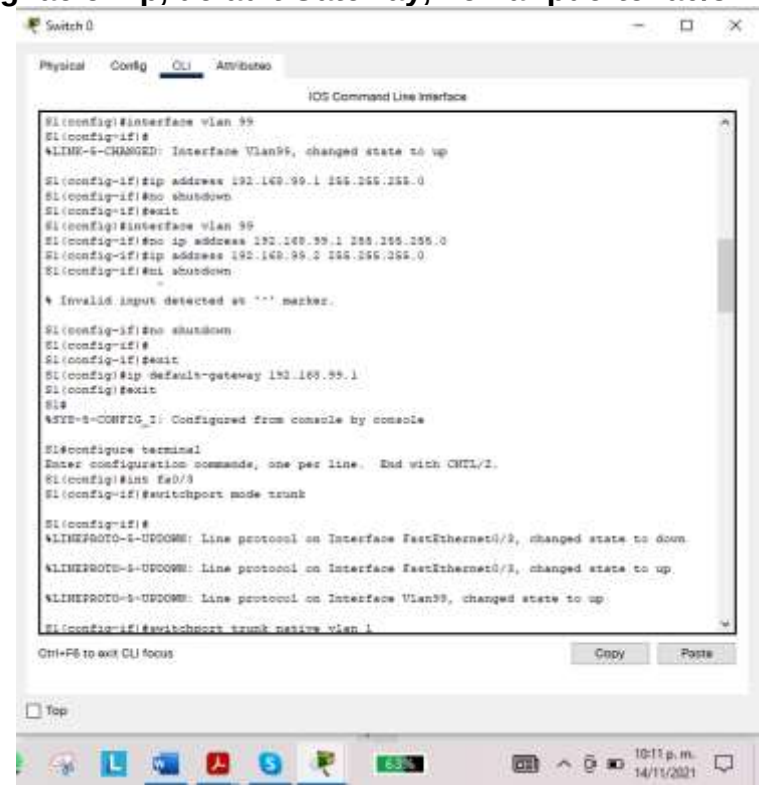
	%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down S1(config-if-range)#

Fuente: Prueba de Habilidades CCNA ll

Figura 27 Creación de la base de datos Vlan

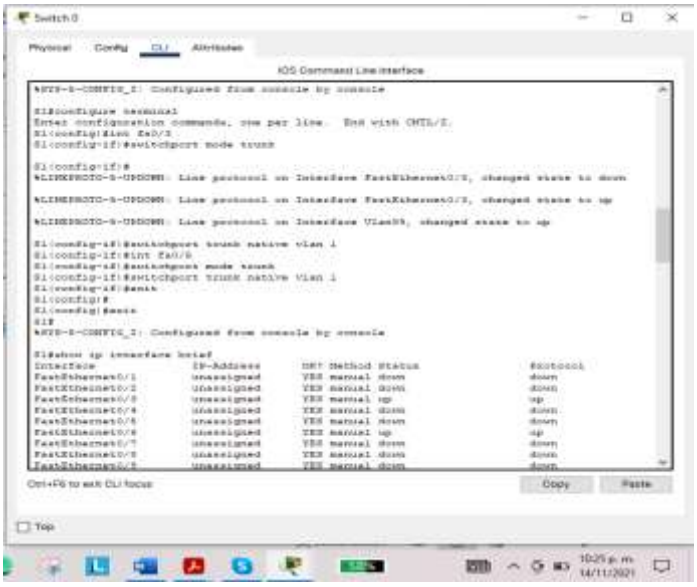
Fuente: Elaboración Propia

Figura 28 Asignación ip, default Gateway, Forzar puerto fa0/3



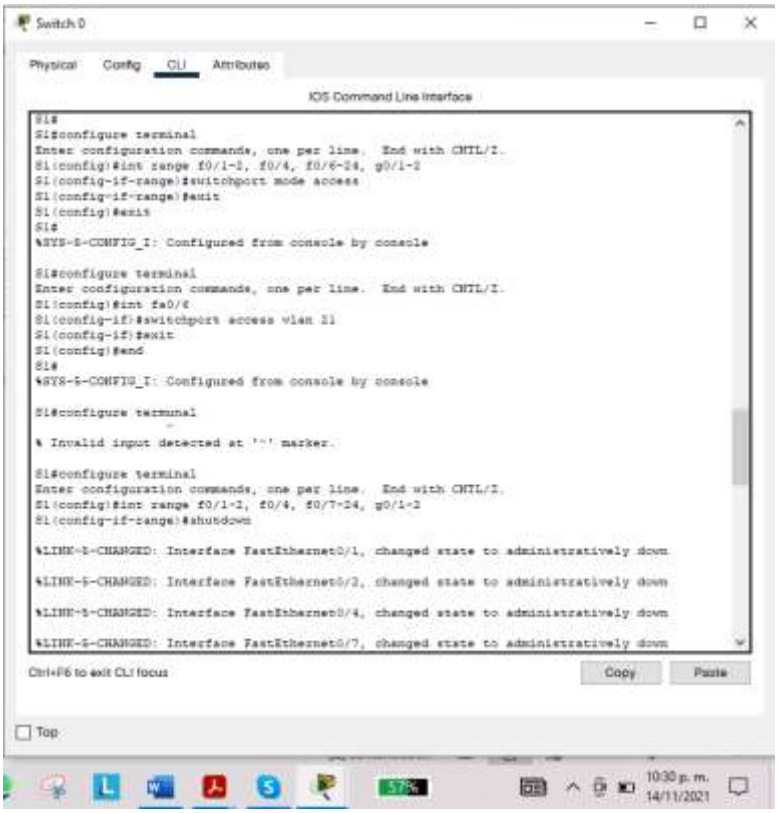
Fuente: Elaboración Propia

Figura 29 Vlan nativa



Fuente: Elaboración Propia

Figura 30 Interfaces Apagadas



Fuente: Elaboracion Propia

PASO 2: CONFIGURAR EL S3

La configuración del S3 incluye las siguientes tareas:

Tabla 17 Configuración de S3, VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3>enable Password: S3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23

	S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)# S3(config-vlan)#exit S3(config)# S3# %SYS-5-CONFIG_I: Configured from console by console
Asignar la dirección IP de administración.	S3(config)#int 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 S3(config-if)#
Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#
Asignar F0/18 a la VLAN 23	S3(config)#int fa0/18 S3(config-if)#switchport access vlan 23 S3(config-if)# S3# %SYS-5-CONFIG_I: Configured from console by console
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2,f0/4-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

	%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down %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 FastEthernet0/19, 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

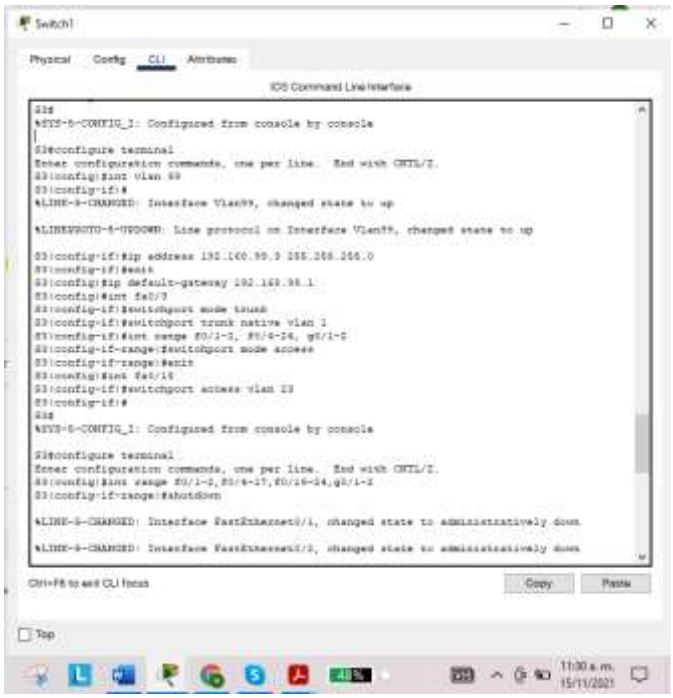
	%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

Fuente: Prueba de Habilidades CCNA ll

Figura 31 Creación de base de datos VLAN

Fuente: Elaboracion Propia

Figura 32 Interfaz vlan 99,default-gateway,puertos e interfaces



Fuente: Elaboracion Propia

PASO 3: CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#

Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown 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

Fuente: Prueba de Habilidades CCNA ll

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 19 Verificación de conexion

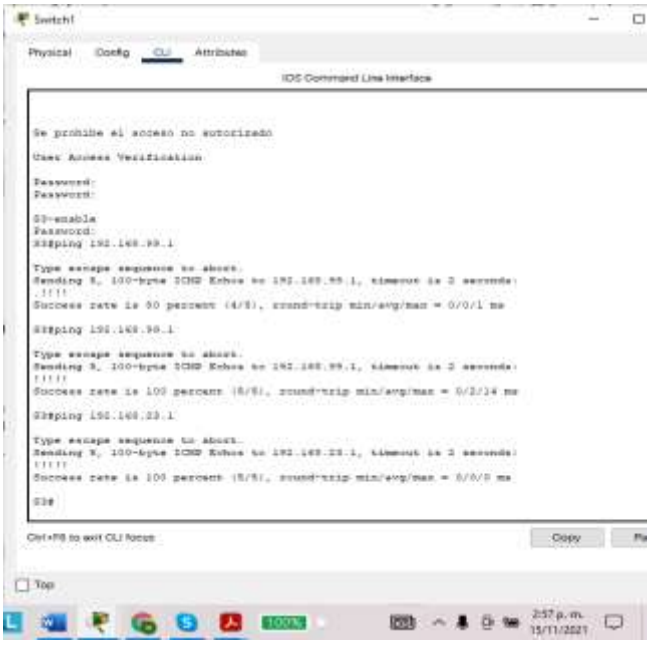
Desde	A	Dirección Ip	Resultados de ping
S1	R1,dirección VLAN 99	192.168.99.1	Success
S3	R1,dirección VLAN 99	192.168.99.1	Success
S1	R1,dirección VLAN 21	192.168.21.1	Success
S3	R1,dirección VLAN 23	192.168.23.1	Success

Fuente: Prueba de Habilidades CCNA ll

Figura 33 Conexión S1 vlan 99

Fuente: Elaboracion Propia

Figura 34 conexión S3 a vlan 99

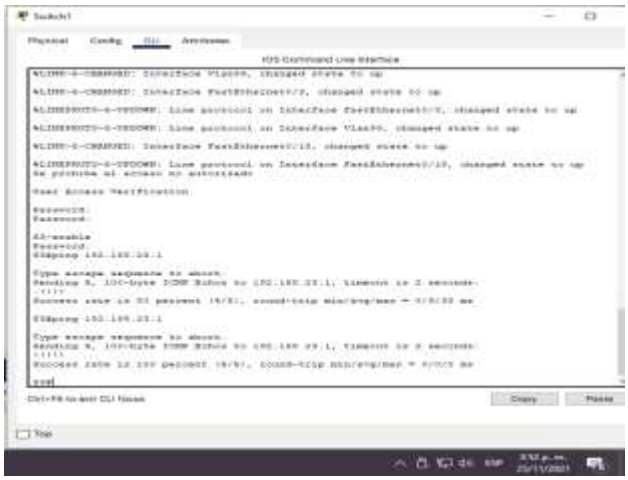


Fuente: Elaboracion Propia

Figura 35 Conexión Vlan 21

Fuente: Elaboracion Propia

Figura 36 Conexión



Fuente: Elaboracion 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:

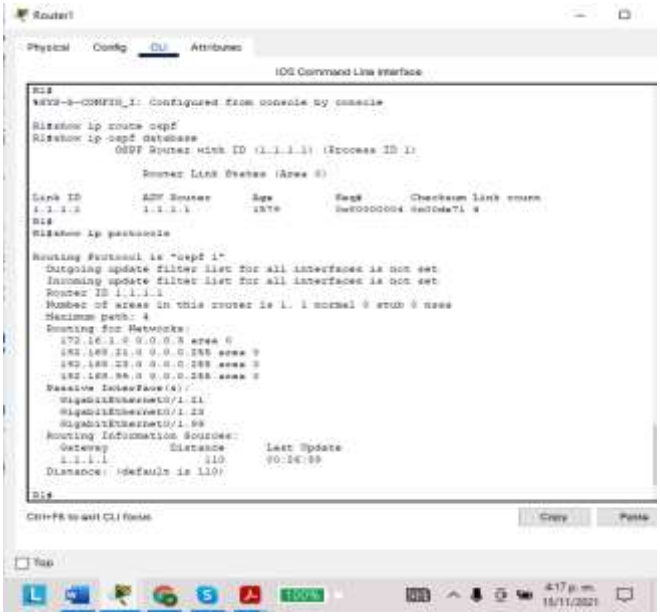
Tabla 20 R1 OSPF

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1 R1(config-router)# R1#
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0

	R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99 R1(config-router)# passive-interface g0/1
Desactive la sumarización automática	En ospf no se utiliza auto-summary

Fuente: Prueba de Habilidades CCNA ll

Figura 37 Configuración OSPF R1



Fuente: Elaboracion Propia

Figura 38 ingreso de ip directas

Fuente: Elaboracion Propia

PASO 2. CONFIGURAR OSPF EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 21 Ospf R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 2
Anunciar las redes conectadas directamente	R2(config-router)#net 10.10.10.10 0.0.0.0 area 0 R2(config-router)#net 172.16.1.0 0.0.0.3 area 0 R2(config-router)#net 172.16.1.0 0.0.0.3 area 0 07:02:01: %OSPF-5-ADJCHG: Process 2, Nbr 1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done % Incomplete command. R2(config-router)#net 172.16.2.0 0.0.0.3 area 0 R2(config-router)#
Establecer todas las interfaces LAN como pasivas	R2(config)#router ospf 2 R2(config-router)#passive-interface Loopback 0
Desactive la sumarización automática	En ospf no se utiliza auto-summary

Fuente: Prueba de Habilidades CCNA ll

PASO 3: CONFIGURAR OSPFV3 EN EL R2 (ERROR ESTO DEBE SER PARA LAS REDES BAJO IPV6.)

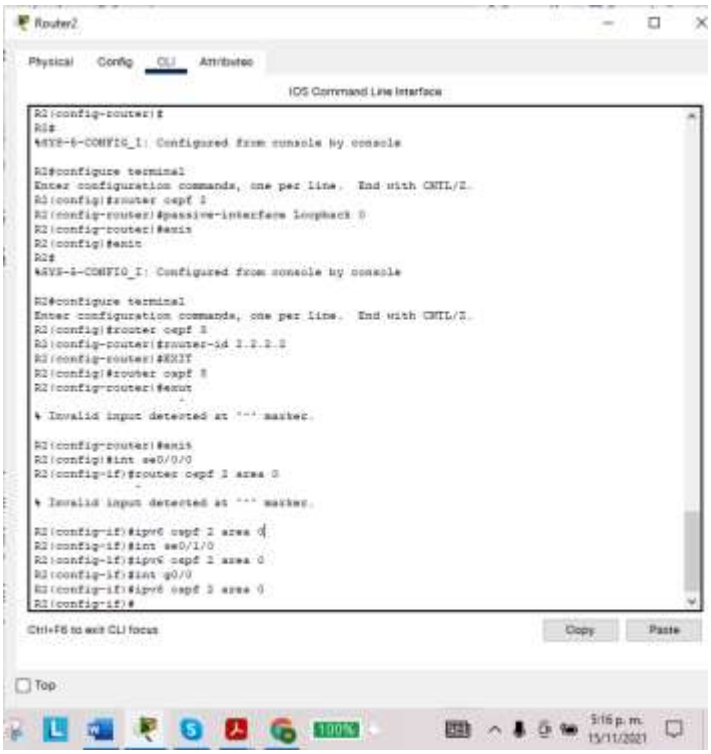
La configuración del R3 incluye las siguientes tareas:

Tabla 22 Ospf ipv6

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 3 R2(config-router)#router-id 2.2.2.2 R2(config)#int se0/0/0 R2(config-if)#router ospf 2 area 0 ^ % Invalid input detected at '^' marker. R2(config-if)#ipv6 ospf 2 area 0 R2(config-if)#int se0/1/0 R2(config-if)#ipv6 ospf 2 area 0 R2(config-if)#int g0/0 R2(config-if)#ipv6 ospf 2 area 0 R2(config-if)#
Anunciar las redes IPV4 conectadas directamente	ERROR ESTO DEBE SER PARA LAS REDES BAJO IPV6.)
Establecer todas las interfaces LAN IPV4 (LOOPBACK) como pasivas	ERROR ESTO DEBE SER PARA LAS REDES BAJO IPV6.)
Desactive la sumarización automática	En ospf no se utiliza auto-summary

Fuente: Prueba de Habilidades CCNA ll

Figura 39 Ospfv3 Ipv6



Fuente: Elaboracion Propia

PASO 4. CONFIGURAR OSPF EN EL R3

Tabla 23 Ospf R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)#router ospf 3 R3(config-router)#
Anunciar las redes IPV4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#

	00:29:56: %OSPF-5-ADJCHG: Process 3, Nbr 10.10.10.10 on Serial0/1/0 from LOADING to FULL, Loading Do R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces LAN IPV4 (LOOPBACK) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#
Desactive la sumarización automática	En ospf no se utiliza auto-summary

Fuente: Prueba de Habilidades CCNA ll

Figura 40 Ospf R3

Fuente: Elaboracion Propia

PASO 5: 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 24 Verificación ospf

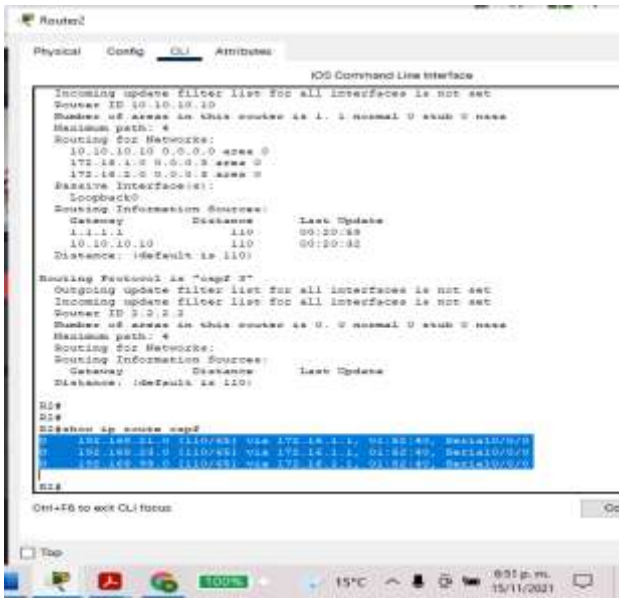
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show running-config

Fuente: Prueba de Habilidades CCNA ll 2

Figura 41 show protocols

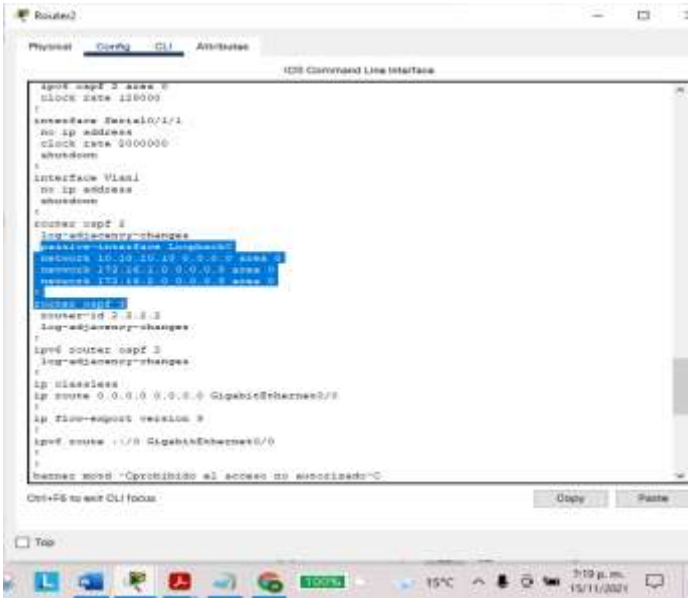
Fuente: Elaboracion Propia

Figura 42 show ip route ospf



Fuente: Elaboracion Propia

Figura 43 show ip protocols



Fuente: Elaboracion Propia

PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 25 Dhcp

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 R1(config)#
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(config)#exit
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(config)#exit R1#

Fuente: Prueba de Habilidades CCNA ll

Figura 44 DHCP R1

Fuente: Elaboracion Propia

PASO 2: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Tabla 26 Nat R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2>enable Password: R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#username webuser privilege 15 secret cisco12345 R2(config)#
Habilitar el servicio del servidor HTTP	Comando invalido R2(config)#ip http server ^ % Invalid input detected at '^' marker.

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación Crear una NAT estática al servidor web.	Comando invalido R2(config)#ip http authentication local ^ % Invalid input detected at '^' marker. Comando invalido R2#ip http secure-server ^ % Invalid input detected at '^' marker.
Asignar la interfaz interna y externa para la NAT estática	R2(config)# R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238 R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside ^ % Invalid input detected at '^' marker. R2(config-if)# R2(config-if)# R2(config-if)#ip nat inside R2(config-if)#int s0/1/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#
Configurar la NAT dinámica dentro de una ACL privada	R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 NETmask 255.255.255.248

	R2# %SYS-5-CONFIG_I: Configured from console by console
Definir la traducción de NAT dinámica	R2# R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#exit R2# %SYS-5-CONFIG_I: Configured from console by console

Fuente: Prueba de Habilidades CCNA ll

Figura 45 Interfaces de entrada y salida NAT

Fuente: Elaboracion Propia

Figura 46 Listas de acceso y ruta nat estatica

Fuente: Elaboracion Propia

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

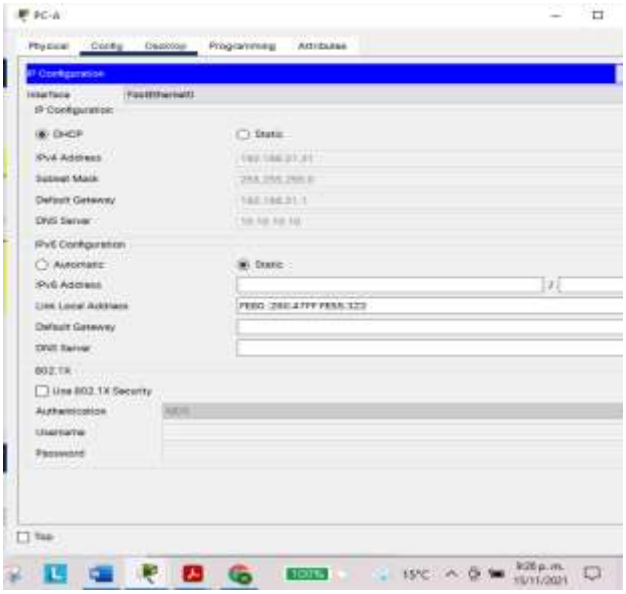
Tabla 27 Verificación de Protocolo Dhcp y Nat

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al	Exitoso cuando se realiza desde los equipos de cómputo, ya que la lógica

servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	seria ingresar desde el equipo pc-a o pc-c al servidor de internet no desde el mismo equipo o computadora de internet, y con el usuario y contraseña no funcionaría porqué los comandos de configuración del http para la utilización de la base de datos local fueron rechazados

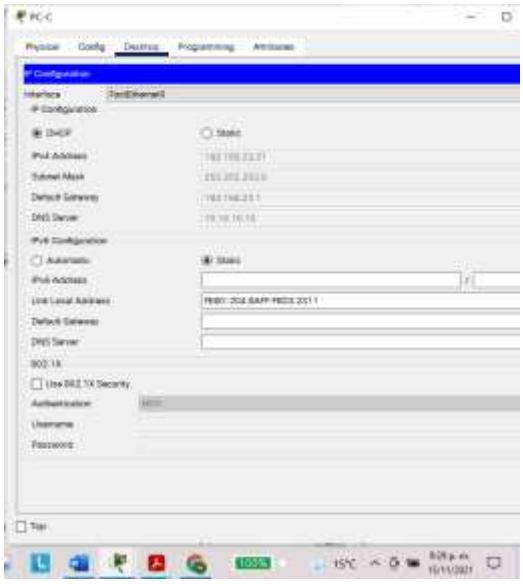
Fuente : Prueba de Habilidades CCNA ll

Figura 47 Información de ip del servidor dhcp en el pc-a



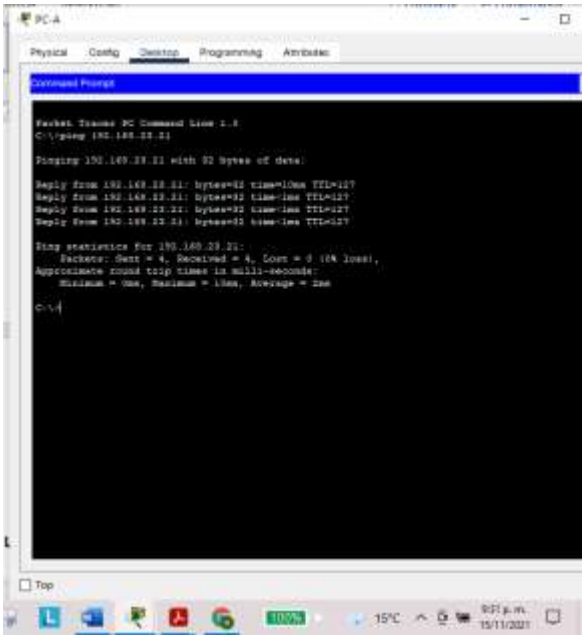
Fuente: Elaboracion Propia

Figura 48 Información de ip del servidor dhcp en el pc-b



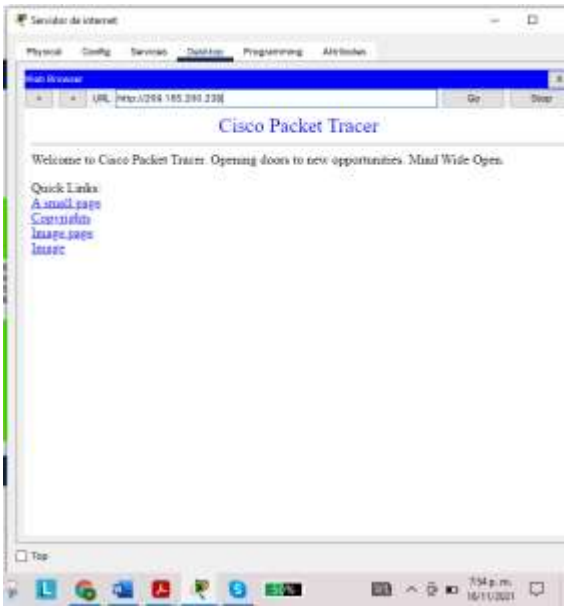
Fuente: Elaboracion Propia

Figura 49 ping de pc-a a pc-b



Fuente: Elaboracion Propia

Figura 50 Acceso al servidor web



Fuente: Elaboracion Propia

ARTE 6: CONFIGURAR NTP

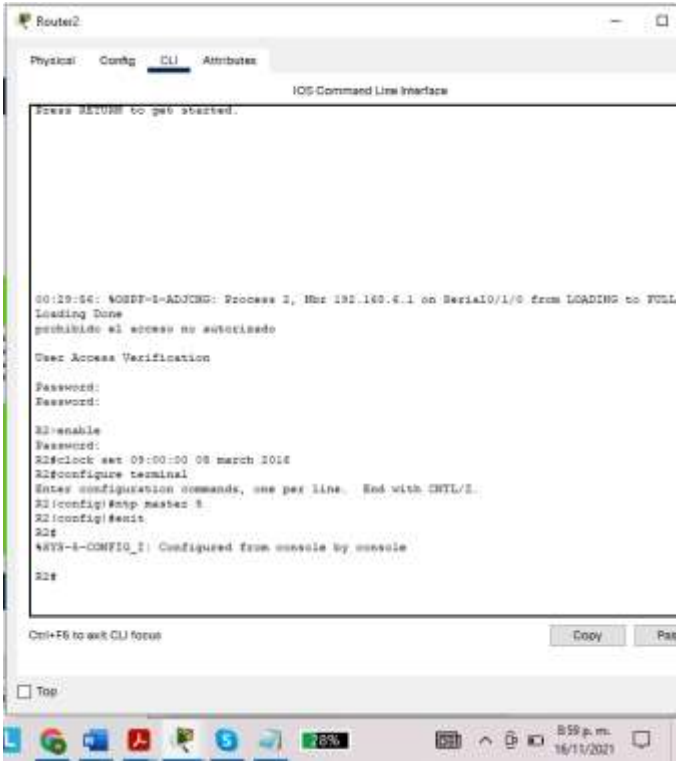
Tabla 28 NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2>enable Password: R2#clock set 09:00:00 05 march 2016 R2#
Configure R2 como un maestro NTP.	R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ntp master 5 R2(CONFIG)#EXIT
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2 R1(CONFIG)#
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(CONFIG)#

Verifique la configuración de NTP en R1	R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 127.127.1.1 5 3 16 17 16.00 726219285937.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured R1#

Fuente: Prueba de Habilidades CCNA ll

Figura 51 Ntp R1



Fuente: Elaboracion Propia

Figura 52 Ntp R1

Fuente: Elaboracion Propia

PASO 1: RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

Tabla 29 Configuración de listas de control

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(CONFIG)#IP ACCESS-LIST STANDARD ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2>enable Password: R2#config ter R2#config terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255

	R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Permitir acceso por Telnet a las líneas de VTY	R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit R2(config)#exit R2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#line vty 0 15 R2(config-line)# R2(config-line)#access-class ADMIN-MGT in R2(config-line)#trasnport input telnet ^ % Invalid input detected at '^' marker. R2(config-line)#transport input telnet R2(config-line)#exit
Verificar que la ACL funcione como se espera	Conexión de telnet de R1 a R2 R1>enable Password: R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Openprohibido el acceso no autorizado User Access Verification Password: Password: R2> Conexión de R3 a R2 Conexión nula R3#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host R3#

Fuente: Prueba de Habilidades CCNA ll

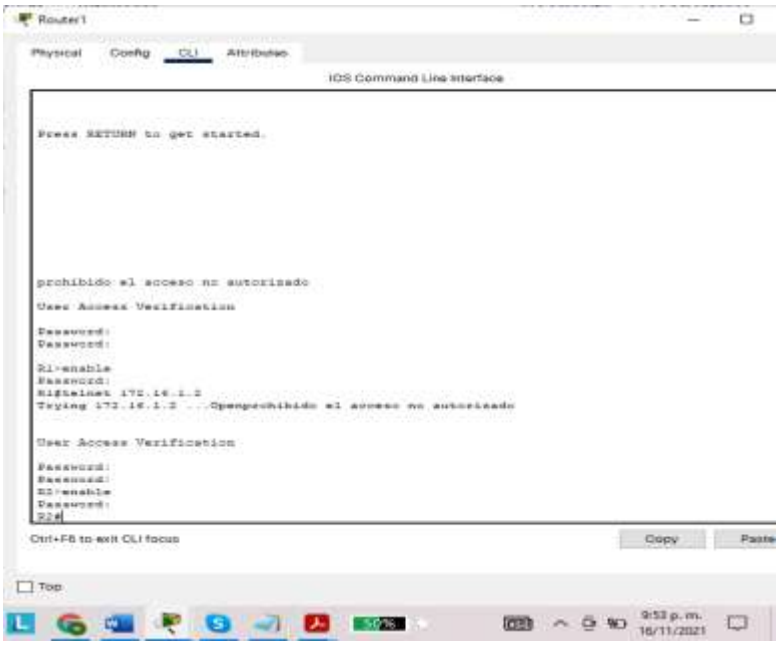
Figura 53 Nombre a la lista de acceso y aplicar ACL

Fuente: Elaboracion Propia

Figura 54 Acceso líneas vty y transport telnet

Fuente: Elaboracion Propia

Figura 55 Verificación de funcionamiento ACL R1 a R2



Fuente: Elaboración Propia

Figura 56 Verificación de funcionamiento ACL R3 a R2

Fuente: Elaboración Propia

PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

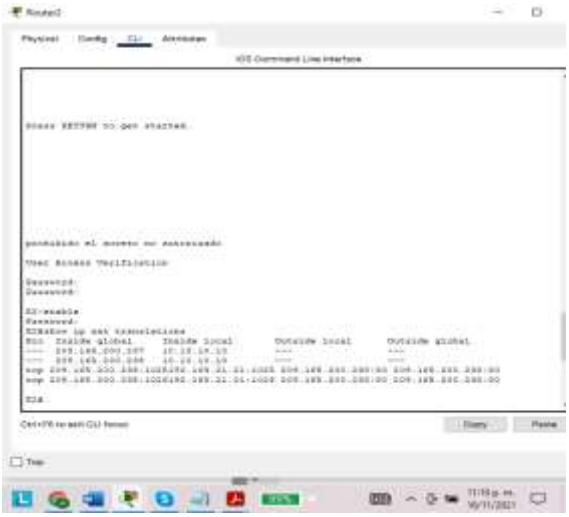
Tabla 30 Comandos de Cli

Descripción del comando	**Entrada del estudiante (comando**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 (8 match(es)) 20 permit 192.168.23.0 0.0.0.255 (6 match(es)) 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) 20 DENY ANY (16 MATCH(ES))
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# **show ip interface** GigabitEthernet0/0 is up, line protocol is up (connected) Internet address is 209.165.200.233/29 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default SPLIT HORIZON IS ENABLED
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- --- 209.165.200.238 10.10.10.10 --- --- tcp 209.165.200.235:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80

	tcp 209.165.200.235:1026192.168.21.21:1026 209.165.200.238:80 209.165.200.238:80 R2#
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * R2# R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- --- 209.165.200.238 10.10.10.10 --- --- tcp 209.165.200.235:1025192.168.23.21:1025 209.165.200.238:80 209.165.200.238:80 R2#clear ip nat translation * R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- --- --- 209.165.200.238 10.10.10.10 --- --- R2#

Fuente: Prueba de habilidades CCNA II

Figura 57 muestra de traducciones NAT

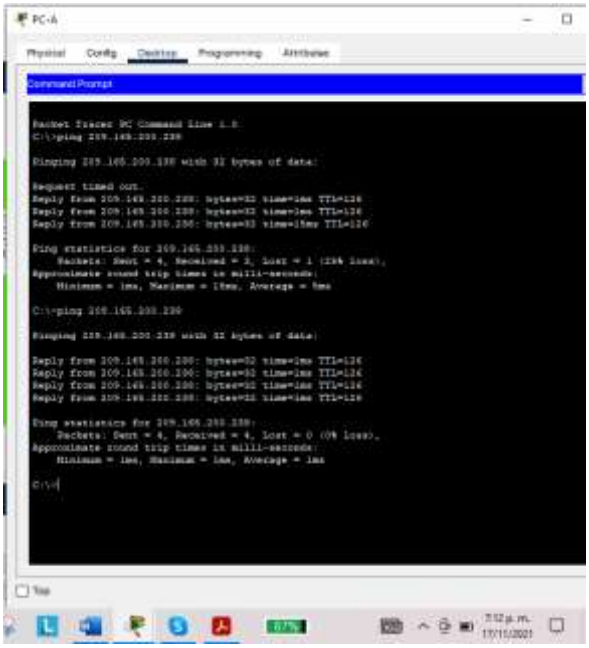


Fuente: Elaboración Propia

Figura 58 Eliminar traducciones NAT

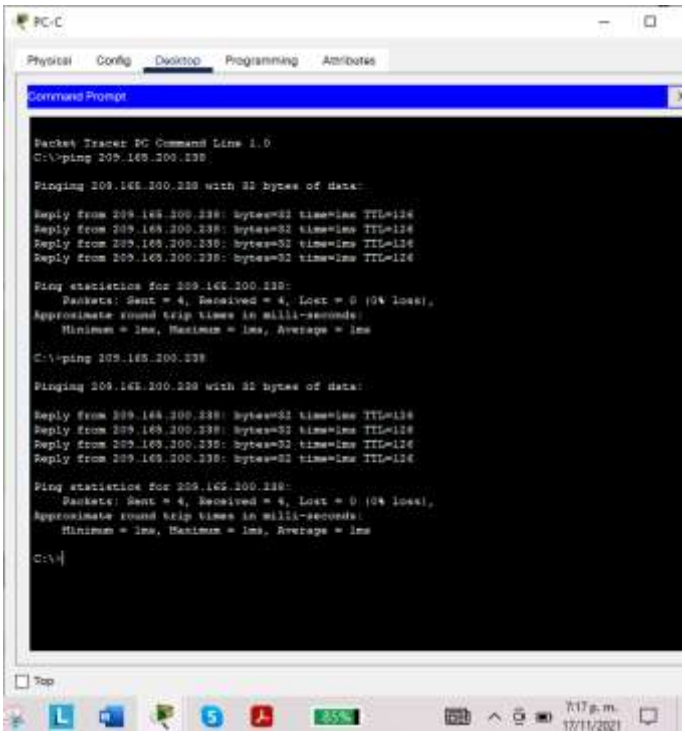
Fuente: Elaboración Propia

Figura 59 Ping de PCA a Servidor de Internet



Fuente: Elaboración Propia

Figura 60 Ping de PC-C a Servidor de Internet



Fuente: Elaboración Propia

Figura 61 Prueba de acceso al Servidor Web desde PC-A

Fuente: Elaboración Propia

CONCLUSIONES

Los conocimientos adquiridos para configuración de los dispositivos sientan bases importantes para la vida laboral en este campo, ya que enriquecen no solo el conocimiento, sino que nos ayudan a escalar profesionalmente, mejorando la condición intelectual y de vida de cada uno de nosotros. Podemos concluir que los dispositivos de comunicaciones requieren obligatoriamente de una configuración de acceso, ya que se resguarda la seguridad del entorno de red donde estén brindando su utilidad y a su vez se genera una confiabilidad con los procesos de comunicaciones.

En la red del escenario 2 se pone en práctica la configuración OSPF, su lógica a la hora de asociar las redes vecinas, las direcciones que se tiene que colocar para que el enrutamiento sea éxito, clave para ser eficaz en lo que pide el cliente que es la comunicación de la red desde los equipos de cómputo. Se puso en práctica y se comprendió el funcionamiento del protocolo DHCP, ya que posee funciones importantísimas dentro de una red facilitando el manejo administrativo de la red, evitando conflictos derivados de una mala configuración de los enrutadores, a su vez genera una configuración más dinámica ya que sincroniza con la escalabilidad de cualquier red empresarial, quitando carga al proceso y al administrador de la red.

BIBLIOGRAFÍA

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

CISCO. (2019). *Configuración de un sistema operativo de red. Fundamentos de Networking*. Obtenido de Configuración de un sistema operativo de red. Fundamentos de Networking: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. (2019). *División de redesIP en subredes*. Obtenido de División de redesIP en subredes: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

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

Vesga, J. (2019). *Introducción al Laboratorio Remoto SmartLab [OVI]*. Obtenido de Introducción al Laboratorio Remoto SmartLab [OVI]: http://hdl.handle.net/10596/24167