# SOLUCIÒN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÌAS CISCO

JHON ALEXANDER BARBOSA CARDENAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
DUITAMA
25/11/2021

# SOLUCIÒN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÌAS CISCO

JHON ALEXANDER BARBOSA CARDENAS

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

TUTOR:
ING. RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA *DE SISTEMAS*
DUITAMA
25/11/2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

FLORESTA(BOYACA), 25 noviembre de 2021

AGRADECIMIENTOS

Quiero dedicar este trabajo en primer lugar a Dios en quien creo firmemente y que me ha permitido llegar hasta donde estoy. Este logro sin duda me permitirá conquistar nuevas metas y consolidar mi carrera en todos los aspectos que me he propuesto como persona y profesional.

A mi familia, que son el motor que me permite avanzar en mis retos diarios, quien me acompaña y me apoya en cada uno de los peldaños que alcanzo día tras día.

A mis docentes quienes han sido un apoyo fundamental y que con sus orientaciones, correcciones y acompañamiento me han permitido aprender de mis errores y caminar hacia el conocimiento y la ciencia.

A mi universidad, que me dio la oportunidad de creer en mis sueños. Crecer en mis conocimientos y formarme como un ser integral para servir y mediante mi profesión contribuir a formar un mundo capacitado para resolver los problemas que se nos presentan a diario mediante la puesta al servicio de conocimientos adquiridos en una institución donde la formación es integral, ética e incluyente.

## CONTENIDO

## LISTA DE TABLAS

## LISTA DE TABLAS

Lista de figuras

# GLOSARIO

OSI: Modelo que permite que diversos sistemas de comunicación se comuniquen usando protocolos estándar.

ENRUTAMIENTO: Función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

LAN: Redes de áreas locales.

WAN: Red de área amplia.

TCP/IP: Conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red.

CCNA: Certificación entregada por la compañía Cisco Systems a las personas que hayan superado satisfactoriamente el examen correspondiente sobre infraestructuras de red e Internet.

DNS (Nombre de dominio): son aquellos nombres que le ponemos a las ip para ser más fácil el reconocimiento.

LOOBACK: Es una interface que dirige el tráfico hacia ellos mismos.

IP: Es una dirección única que permite la comunicación entre redes.

OSPF: este es un protocolo de direccionamiento de tipo enlace - estado.

## RESUMEN

Este trabajo se desarrolla con el objetivo de obtener la certificación CCNA.
La metodología utilizada involucra el proceso de enrutamiento para la creación de redes LAN y WAN, utilizando los diferentes protocolos y configuraciones de equipos de acuerdo a lo solicitado.

Inicialmente se diseña el enrutamiento de las redes configurando de manera correcta cada uno de los dispositivos tales como router y switch, utilizando líneas de comandos mediante el estudio del modelo OSI, la arquitectura TCP/IP, utilizando herramientas y protocolos que mejoren el rendimiento de las redes y de esta manera adquirir la destreza para solucionar oportunamente problemas de interconectividad.
En el desarrollo del presente trabajo y siguiendo cada uno de los protocolos establecidos, se van afianzando los niveles de seguridad básicos para posibles ataques de terceros, de manera que se pueda proteger la información y evitar daños en las redes.
En un segundo escenario se realizarán ejercicios con protocolos de enrutamiento con versiones ipv4 y ipv6 para conectar distintos equipos en diferentes subredes y así por tener un mejor dinamismo de la información y seguridad en sus redes.

En síntesis, se desarrollan operaciones básicas de enrutamiento mediante el uso de comandos que generen como resultado los adecuados protocolos y creaciones de red garantizando la seguridad de la misma.



Palabras Clave: OSI, CCNA, LAN, Enrutamiento WAN, Redes, TCP / IP.



## ABSTRACT

This paper develops the objective of knowing the routing process for the creation of LAN and WAN networks, using the different protocols and equipment configurations according to those requested.

Initially, the routing of the networks is designed correctly configuring each of the devices such as router and switch, using command lines through the study of the OSI model, the TCP / IP architecture, using tools and protocols that improve the performance of the networks. networks and acquire the skills to solve interconnectivity problems in a timely manner.
In the development of this work and following each of the established protocols, the basic security levels for possible third-party attacks are being strengthened, so that information can be protected and damage to networks is avoided.
In a second scenario, exercises will be carried out with routing protocols with ipv4

and ipv6 versions to connect different equipment in different subnets and thus have a better dynamism of information and security in their networks.

In fact, basic routing operations are developed through the use of commands that generate the appropriate protocols and network creations as a result, guaranteeing network security

Keywords:OSI,CCNA,LAN,EnrutamientoWAN,Redes,TCP/IP.

# INTRODUCCIÓN

En este trabajo se ilustra la creación de redes utilizando escenarios de simulación mediante el uso de packet tracer con el fin de generar técnicas adecuadas de enrutamiento. Inicialmente se realiza el esquema de direccionamiento con el fin de establecer concretamente las direcciones IP de cada uno de los equipos y subredes.

En el desarrollo del trabajo se configuran los dispositivos de una red pequeña tales como router, switch y equipos y se administran de forma segura; esto permite resolver cualquier problema o dificultad que se presente en cuanto a la conexión de las redes LAN y WAN.

En el desarrollo del trabajo podemos observar la utilización de líneas de comando para la configuración de cada equipo, registrando cada una de las acciones realizadas y que finalmente conducen a los requerimientos de la guía de actividades.

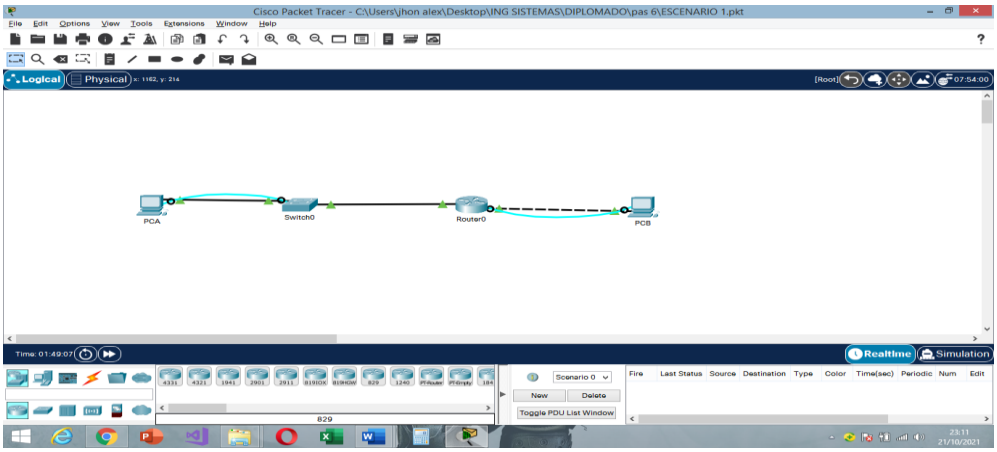
La finalidad del trabajo es identificar cada uno de los pasos para la creación de redes LAN y WAN y configurar los dispositivos de manera adecuada y segura, como también poner en práctica algunos protocolos con las configuraciones básicas de enrutamiento para el buen funcionamiento de las redes y su seguridad

1. ESCENARIO 1

Figura 1. Escenario 1


fuente propia

Figura 2. Simulación de escenario 1




Fuente propia

1.1 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.

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

1.2.1. 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.

ESQUEMA DE DIRECCIONAIENTO IP

IP BASE: 192.168.85.0 /24
Mascara: 255.255.255.0 clase C (R.R.R.H)
LAN 1 = 100 HOST $2^7 = 128$
LAN 1 = 192.168.85.0 255.255.255.128
LAN 1 = 192.168.85.0/25
LAN 2 = 50 HOST $2^6 = 64$ (128+64 =192)
LAN 2 =192.168.85.128 255.255.255.192
LAN 2 = 192.168.85.128/26

1.0.Tabla de direccionamiento

| SUBREDES | DIRECCION DE RED | MASCARA | IP INICIAL | IP FINAL | NUMERO DE SALTO |
|---|---|---|---|---|---|
| LAN 1 = 100HOST | 192.168.85.0 | 255.255.255.128 | 192.168.85.1 | 192.168.85.126 | 128 |
| LAN 2 = 50 HOST | 192.168.85.128 | 255.255.255.192 | 192.168.85.129 | 192.168.85.190 | 64 |

Fuente propia

1. Tabla de direccionamiento

| Item | Requerimiento | Dirección IP |
|---|---|---|
| Dirección de Red | 192.168.85.0 donde X corresponde a los últimos dos dígitos de su cédula. | 192.168.85.0 /24 |
| Requerimiento de host Subred LAN1 | 100 | 192.168.85.0/25 |
| Requerimiento de host Subred LAN2 | 50 | 192.168.85.128/26 |
| R1 G0/0/1 | Primera dirección de host de la subred LAN1 | 192.168.85.1/25 |
| R1 G0/0/0 | Primera dirección de host de la subred LAN2 | 192.168.85.129/26 |

| | | |
|---|---|---|
| S1 SVI | Segunda dirección de host de la subred LAN1 | 192.168.85.2/25 |
| PC-A | Última dirección de host de la subred LAN1 | 192.168.85.126/25 |
| PC-B | Última dirección de host de la subred LAN2 | 192.168.85.190/26 |

Fuente propia

CONFIGURAR LOS ASPECTOS BÁSICOS DE LOS DISPOSITIVOS DE LA RED PROPUESTA.
CONFIGURACION DEL ROUTER

Router>enable----------Modo administrador
Router#configure terminal----------configuracion global
Router(config)#no ip domain-lookup----------desactivar DNS
Router(config)#hostname R1----------Nombre del router
R1(config)#ip domain-name ccna-lab.com----------asignar nombre al dominio
R1(config)#enable secret ciscoenpass----------colocar contraseña cifrada modo privilegiado
R1(config)#line console 0----------configurar línea de consola del router
R1(config-line) #password ciscoconpass----------contraseña de acceso
R1(config-line) #login----------solicitud de autenticación para la contraseña
R1(config-line) #exit----------regresar al modo de configuración global
R1(config)#username admin password admin1pass------se crea contraseña ADMIN
R1(config)#line vty 0 4----------se ingresa a linea vty del router
R1(config-line) #password ciscocisco----------se le asigna contraseña
R1(config-line) #login local----------se autentica la linea vty
R1(config-line) #transport input ssh--------se configura para que solo permita conexión ssh
R1(config-line) #exit---------- se sale de la configuración vty
R1(config)#service password-encryption----se cifran la contraseña
R1(config)#Banner motd # esta configuración fue realizado por jhon alex del curso ccnaI no intente ingresar sin autorización #----------mensaje de advertencia
R1(config)#interface gigabitEthernet 0/0/0----------ingresamos a la interface g0/0/0
R1(config-if) #ip address 192.168.85.129 255.255.255.192-----se le asigna ip
R1(config-if) #description esta es la interfase de la LAN 1----una pequeña descripción
R1(config-if) #no shutdown----------se activa la interface
R1(config-if) #exit----------salimos de la interface
R1(config)#interface gigabitEthernet 0/0/1------ingresamos a la interface g0/0/1
R1(config-if) #ip address 192.168.85.1 255.255.255.128-----le ponemos la dirección ip
R1(config-if) #description esta interface es la de LAN 2----descripción de la interface
R1(config-if) #no shutdown----------se activa la interface
R1(config-if) #exit----------se sale de la interface

R1(config)#ip domain-name ccna-lab.com----------se le asigna nombre al dominio
R1(config)#crypto key generate rsa general-keys modulus 1024s genera una clave cifrada de 1024 bits.

2. tabla de configuración del router

| Tarea | Especificación | LINEA DE COMANDO |
|---|---|---|
| Desactivar la búsqueda DNS | | Router> enable<br>Router# configure terminal<br>Router(config)#no ip domain-lookup |
| Nombre del router | R1 | Router(config)#hostname R1 |
| Nombre de dominio | ccna-lab.com | R1(config)#ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass | R1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass | R1(config)#line console 0<br>R1(config-line) #password ciscoconpass<br>R1(config-line) #login |
| Establecer la longitud mínima para las contraseñas | 10 caracteres | R1(config)#security password min-length 10 |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin<br>Password: admin1pass | R1(config)#username admin password admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | | R1(config)#line vty 0 4<br>R1(config-line) #password ciscocisco.<br>R1(config-line) #login local |
| Configurar VTY solo aceptando SSH | | R1(config-line) #transport input ssh |
| Cifrar las contraseñas de texto no cifrado | | R1(config)#service password-encryption |
| Configure un MOTD Banner | | R1(config)#Banner motd #esta configuración fue realizado por jhon alex del curso ccnaIIno intente ingresar sin autorización# |

| | | |
|---|---|---|
| Configurar interfaz G0/0/0 | Establezca la descripción<br>Establece la dirección IPv4.<br>Activar la interfaz. | R1(config)#interface gigabitEthernet 0/0/0<br>R1(config-if) #ip address 192.168.85.129 255.255.255.192<br>R1(config-if) #description esta es la interfase de la LAN 1<br>R1(config-if) #no shutdown |
| Configurar interfaz G0/0/1 | Establezca la descripción<br>Establece la dirección IPv4.<br>Activar la interfaz. | R1(config)#interface gigabitEthernet 0/0/1<br>R1(config-if) #ip address 192.168.85.1 255.255.255.128<br>R1(config-if) #description esta interface es la de LAN 2<br>R1(config-if) #no shutdown |
| Generar una clave de cifrado RSA | Módulo de 1024 bits | R1(config-if) #ip domain-name ccna-lab.com<br>R1(config)#crypto key generate rsa general-keys modulus 1024 |

Fuente propia

Las tareas de configuración de S1 incluyen lo siguiente:

CONFIGURACIÓN DEL SWITCH 1(S1)
Switch>enable----------modo administrador
Switch#configure terminal----------configuracion global
Switch(config)#no ip domain-lookup----------desactivación del DNS
Switch(config)#hostname S1----------nombre al switch
S1(config)#ip domain-name ccna-lab.com----------asignar nombre al domino
S1(config)#enable secret ciscoenpass----------asignar contraseña cifrada
S1(config)#line console 0----------configurar linea de consola
S1(config-line) #password ciscoconpass----------crear contraseña de acceso
S1(config-line) #login----------autenticamos la contraseña
S1(config-line) #exit----------volvemos a la configuración global
S1(config)#username admin password admin1pass----se crea usuario y contraseña admin
S1(config)#line vty 0 15----------se ingresa a linea vty de S1
S1(config-line) #password ciscocisco----------se crea contraseña
S1(config-line) #login local----------se autentica modo local
S1(config-line)#transport input ssh----------se configura ssh
S1(config-line)#exit----------se sale del la linea vty
S1(config)#service password-encryption----------se cifran las contraseñas de texto
S1(config)#Banner motd #este es el switch 1 configurado por jhon alex en el curso ccna II NO INGRESE SIN AUTORIZACION#----------mensaje de advertencia
S1(config)#ip domain-name ccna-lab.com----------se asigna nombre al domino
S1(config)#crypto key generate rsa general-keys modulus 1024--------se genera clave sifrada de 1024 bits

S1(config-if)#ip default-Gateway 192.168.85.1----------se ingresa ip por defecto del gateway.

2. tabla de configuración del switch

| Tarea | Especificación | LINEAS DE COMANDOS |
|---|---|---|
| Desactivar la búsqueda DNS. | | Switch>enable<br>Switch#configure terminal<br>Switch(config)#no ip domain-lookup |
| Nombre del switch | S1 | Switch(config)#hostname S1 |
| Nombre de dominio | ccna-lab.com | S1(config)#ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass | S1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass | S1(config)#line console 0<br>S1(config-line) #password ciscoconpass<br>S1(config-line) #login |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin<br>Password: admin1pass | S1(config)#username admin password admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | | S1(config)#line vty 0 15<br>S1(config-line) #password ciscocisco<br>S1(config-line) #login local |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | | S1(config-line) #transport input ssh |
| Cifrar las contraseñas de texto no cifrado | | S1(config-line) #exit<br>S1(config)#service password-encryption |
| Configurar un MOTD Banner | | S1(config)#Banner mod #este es el switch 1 configurado por jhon alex en el curso ccna II NO INGRESE SIN AUTORIZACION# |
| Generar una clave de cifrado RSA | Módulo de 1024 bits | S1(config)#ip domain-name ccna-lab.com<br>S1(config)#crypto key generate rsa general-keys modulus 1024 |

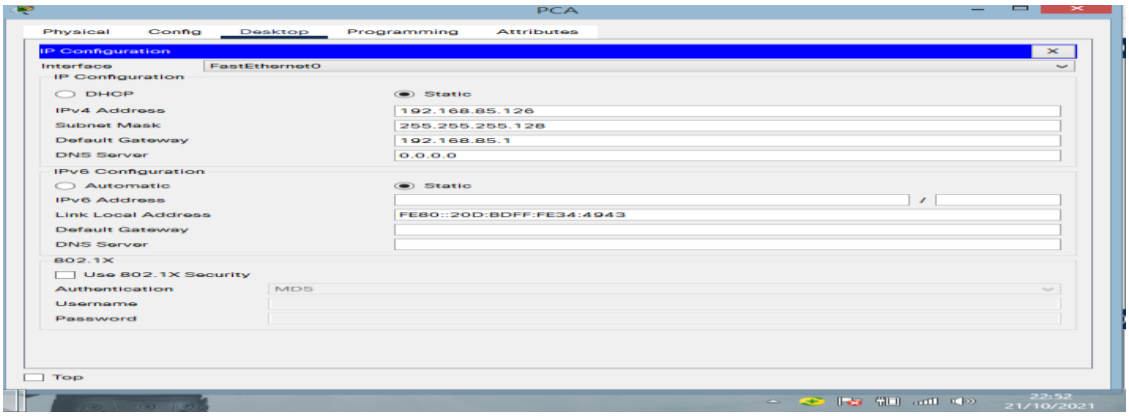
| | | |
|---|---|---|
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento | S1(config)#interface vlan 1<br>S1(config-if) #ip address 192.168.85.2 255.255.255.128<br>S1(config-if) #no shutdown |
| Configuración del Gateway predeterminado | Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento. | S1(config-if) #ip default-gateway 192.168.85.1 |

Fuente propia

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

Figura 3. Pantallazo de configuración de la IP DE LAS PC




Fuente propia

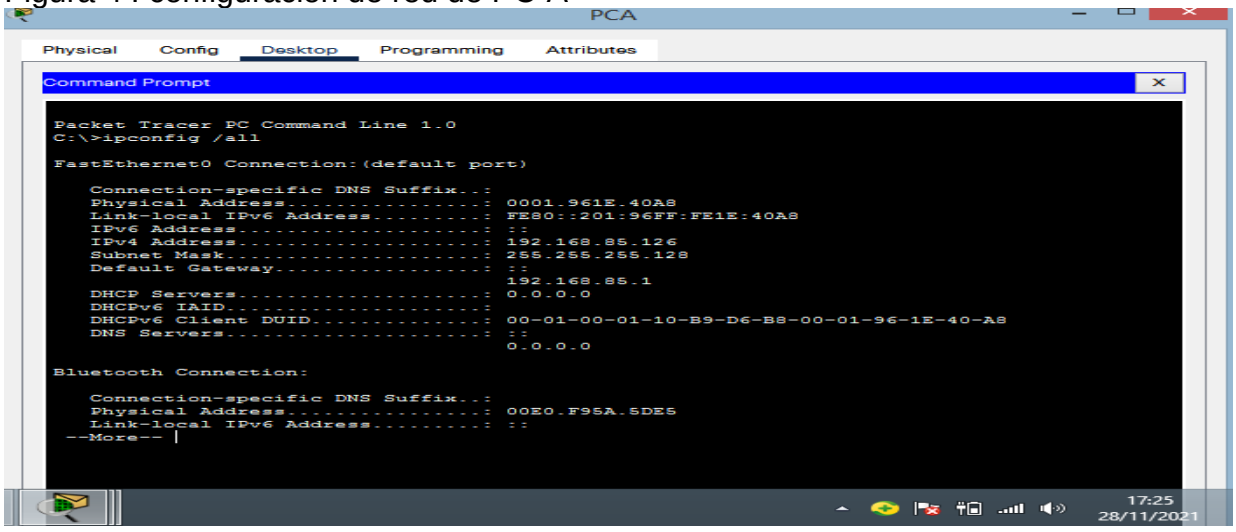
3. tabla de configuración de PC-A

| PC-B Network Configuration | |
|---|---|
| Descripción | Este es el PC A |
| Dirección física | FastEthernet0 Connection☹default port) |

| | |
|---|---|
| | Connection-specific DNS Suffix..:<br>Link-local Ipv6 Address……..: FE80::20D:BDFF:FE34:4943<br>Ipv6 Address…….....: ::<br>Ipv4 Address…….....: 192.168.85.126<br>Subnet Mask…….....: 255.255.255.128<br>Default Gateway…….....: ::<br>192.168.85.1<br><br>Bluetooth Connection:<br><br>Connection-specific DNS Suffix..:<br>Link-local Ipv6 Address……..: ::<br>Ipv6 Address…….....: ::<br>Ipv4 Address…….....: 0.0.0.0<br>Subnet Mask…….....: 0.0.0.0<br>Default Gateway…….....: ::<br>0.0.0.0 |
| Dirección IP | 192.168.85.126 |
| Máscara de subred | 255.255.255.128 |
| Gateway predeterminado | 192.168.85.1 |

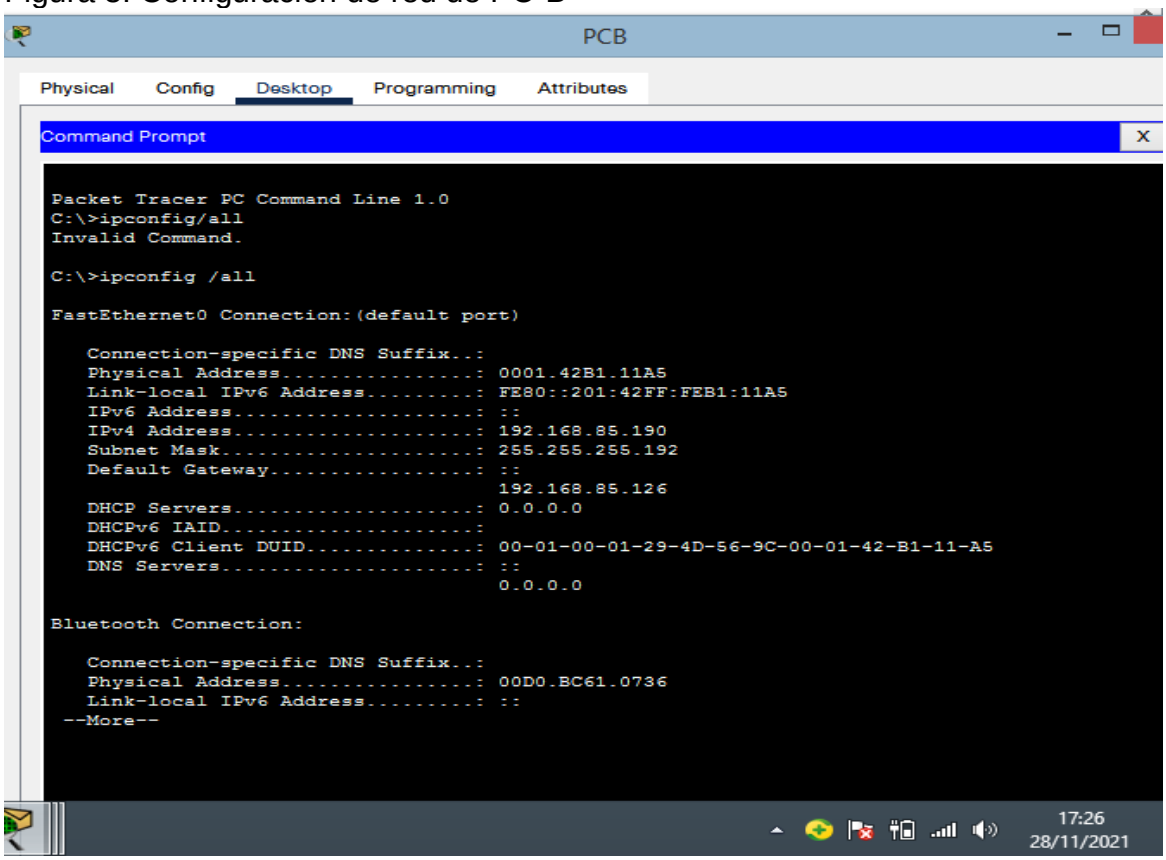
Fuente propia

Figura 4 . configuracion de red de PC-A




Fuente propia

Figura 5. Configuracion de red de PC-B




Fuente propia

configuración de la ip de la PC-B

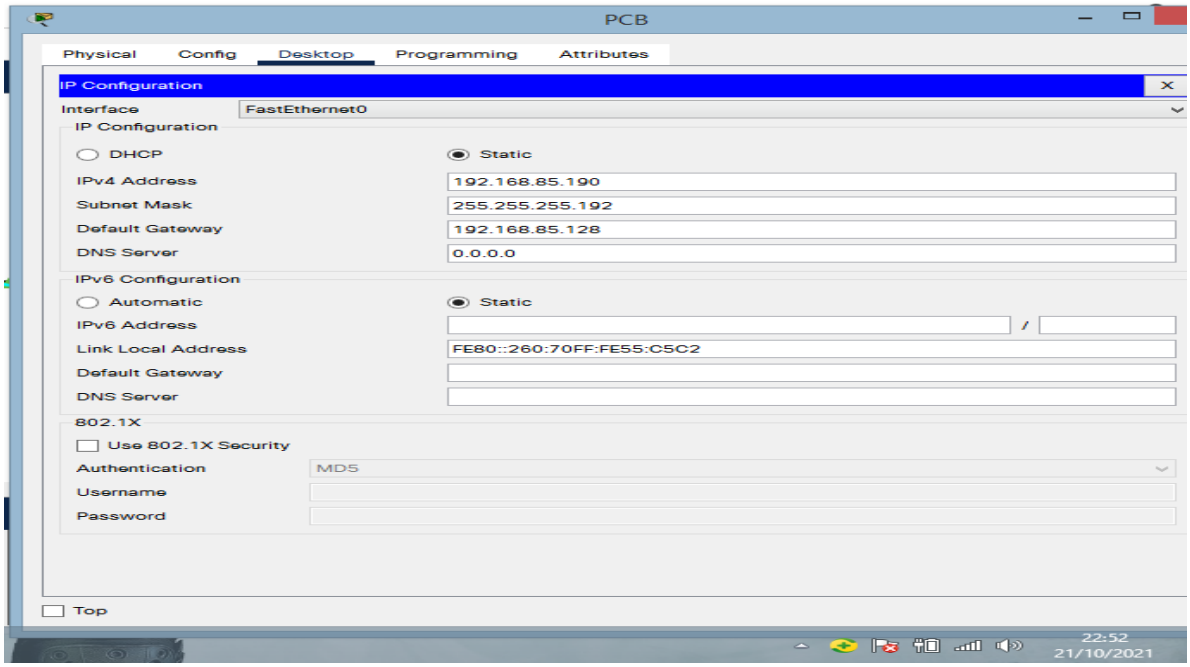
4. tabla de configuración de la pcb

| PC-B Network Configuration | |
|---|---|
| Descripción | Este es el PC B |
| Dirección física | FastEthernet0 Connection:(default port)<br><br>Connection-specific DNS Suffix..:<br>Link-local IPv6 Address.....:<br>FE80::260:70FF:FE55:C5C2<br>IPv6 Address.....: ::<br>IPv4 Address.....: 192.168.85.190<br>Subnet Mask.....: 255.255.255.192<br>Default Gateway.....: ::<br>192.168.85.128<br><br>Bluetooth Connection: |

| | |
|---|---|
| | Connection-specific DNS Suffix..:<br>Link-local IPv6 Address.....: ::<br>IPv6 Address.....: ::<br>IPv4 Address.....: 0.0.0.0<br>Subnet Mask.....: 0.0.0.0<br>Default Gateway.....: ::<br>0.0.0.0 |
| Dirección IP | 192.168.85.190 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 192.168.85.128 |

Fuente propia

Figura 6. Pantallazo de configuración de la IP DE LAS PC




Fuente propia

ESCENARIO 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de

acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 7. topología escenario 2

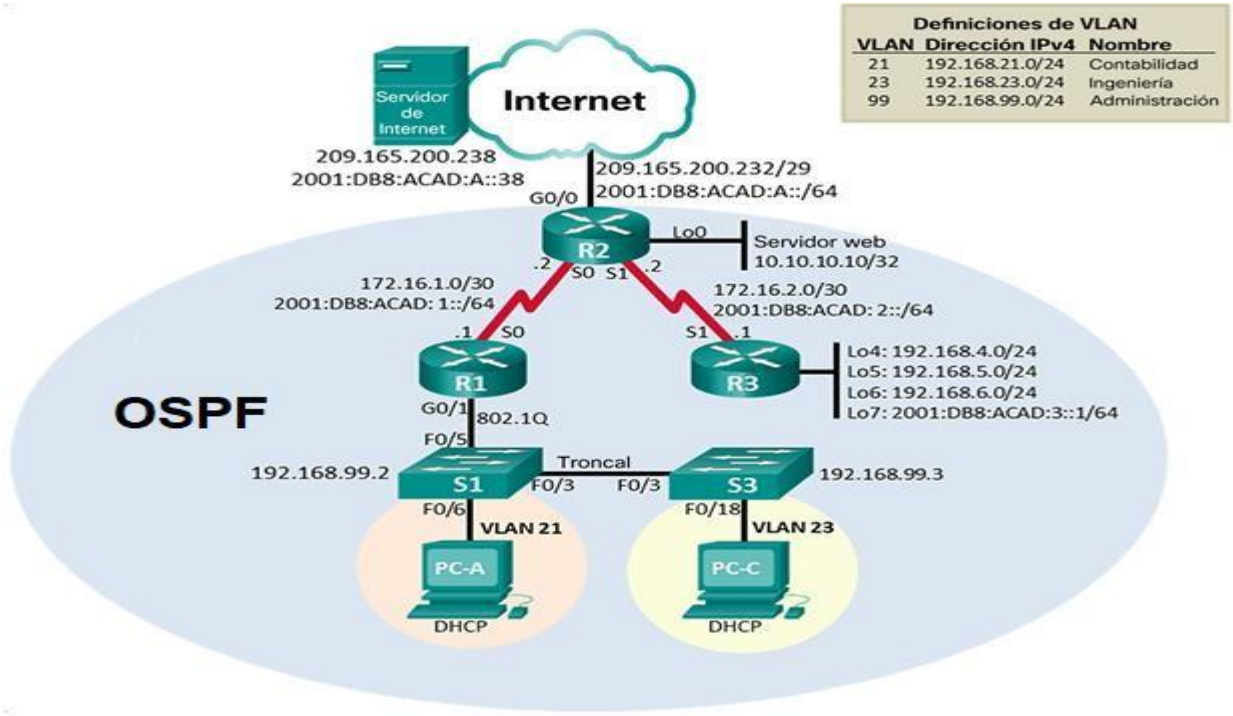
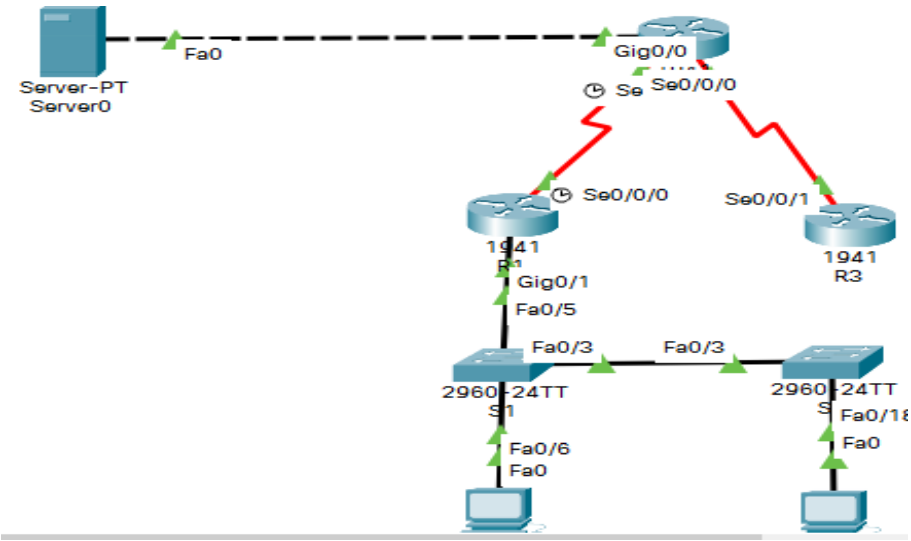



Figura 8. Topologia en packect tracer




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.

5. Tabla de reinicio de dispositivos

| TAREA | COMANDO DE IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | R1(config)#erase startup-config |
| Volver a cargar todos los routers | R1#reload |

| | |
|---|---|
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | erase startup-config<br>delete vlan brief |
| Volver a cargar ambos switches | reload |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | Show vlan brief<br>Show flash |

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):

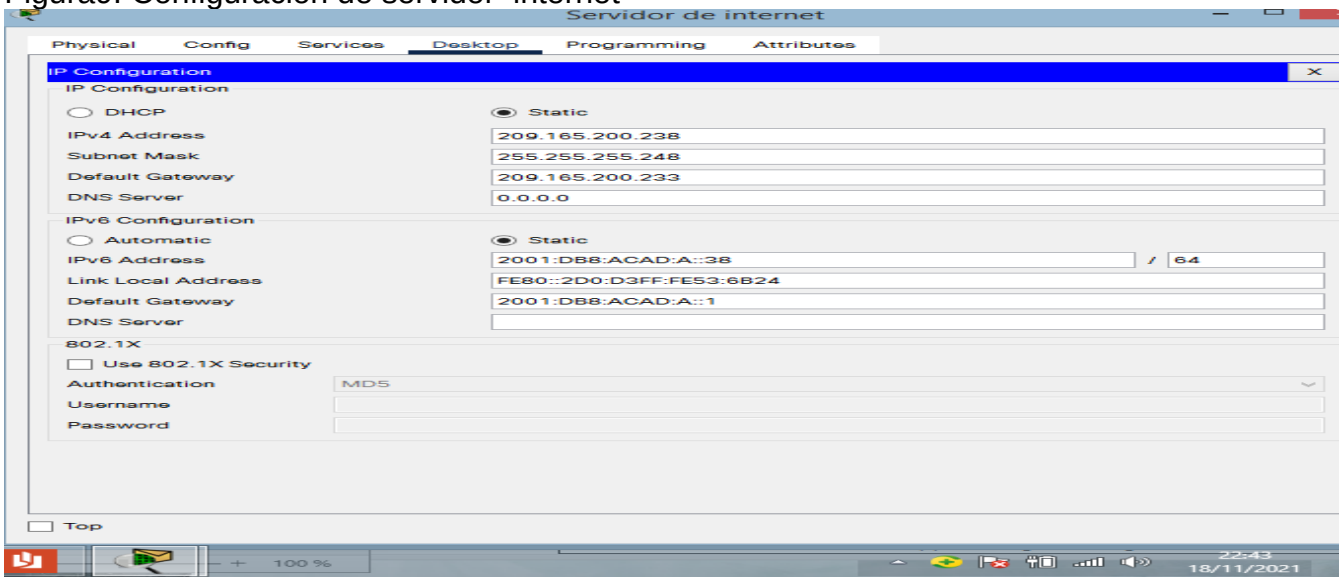
6 tabla de configuración de servidor internet

| Elemento o tarea de configuración | ESPECIFICACIÓN |
|---|---|
| Dirección IPv4 | 209.165.200.238 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.233 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38/64 |

| | |
|---|---|
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:A::1 |

Fuente propia

Figura9. Configuración de servidor internet




Fuente propia

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

7.Tabla configuración de R1

| Elemento o tarea de configuración | ESPECIFICACIÓN |
|---|---|
| Desactivar la búsqueda DNS | Comando para desactivar la búsqueda DNS<br><br>Router#no ip domain-lookup |
| Nombre del router | Comando para asignarle nombre a nuestro dispositivo<br>Router(config)#hostname R1 |
| Contraseña de exec privilegiado cifrada | Asignamos mediante el siguiente comando la contraseña del modo privilegiado<br>R1(config)#enable secret class |
| Contraseña de acceso a la consola | Líneas de comando para asignar la contraseña del acceso de consola |

| | |
|---|---|
| | R1(config)#line console 0<br>R1(config-line) #password cisco<br>R1(config-line) #login<br>R1(config-line) #exit |
| Contraseña de acceso Telnet | Líneas de comando para asignarle la contraseña para el acceso a telnet<br>R1(config)#line vty 0 4<br>R1(config-line) #password cisco<br>R1(config-line) #login |
| Cifrar las contraseñas de texto no cifrado | Comando para cifrar las contraseñas.<br>R1(config-line) #service password-encryption |
| Mensaje MOTD | Mensaje de pantalla “Se prohíbe el acceso no autorizado”<br>R1(config)#banner motd # Se prohíbe el acceso no autorizado. # |

| | |
|---|---|
| Interfaz S0/0/0 | Establezca la descripción<br>Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones<br>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones<br>Establecer la frecuencia de reloj en 128000<br>Activar la interfaz:<br>R1(config)# int s 0/0/0<br>R1(config-if) #description conectividad a R2<br>R1(config-if) #ip address 172.16.1.1 255.255.255.252<br>R1(config-if) # ipv6 address2001:db8:acad:1::1/64<br>R1(config-if) #clock rate 128000<br>This command applies only to DCE interfaces<br>R1(config-if)#no shutdown |
| Rutas predeterminadas | Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0:<br>R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0<br>R1(config)#ipv6 route ::/0 serial0/0/0 |

Fuente propia

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

8. Tabla configuración R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Comando para desactivar búsqueda DNA<br>Router(config)#ip domain lookup |
| Nombre del router | Comando para asignar nombre al equipo<br>Router (config)#hostname R2 |
| Contraseña de exec privilegiado cifrada | Asignamos mediante el siguiente comando la contraseña del modo privilegiado<br>R2(config)#enable secret class |
| Contraseña de acceso a la consola | Líneas de comando para asignar la contraseña del acceso de consola<br>R2(config)#line console 0<br>R2(config-line) #password cisco<br>R2(config-line) #login<br>R2(config-line) #exit |
| Contraseña de acceso Telnet | Líneas de comando para asignarle la contraseña para el acceso a telnet<br>R2(config)#line vty 0 4<br>R2(config-line) #password cisco<br>R2(config-line) #login |
| Cifrar las contraseñas de texto no cifrado | Comando para cifrar las contraseñas.<br>R2(config-line) #service password-encryption |
| Habilitar el servidor HTTP | Comando para habilitar el servidor, aunque este comando no funciona en el packet tracer este es el comando:<br>R2(config)#ip http server |
| Mensaje MOTD | Comando para emitir un mensaje:<br>R2(config)#banner motd# Se prohíbe el acceso no autorizado. # |

| | |
|---|---|
| Interfaz S0/0/0 | Establezca la descripción<br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br>Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz<br>*R2(config)#int s0/0/0*<br>*R2(config)# description connection to R1*<br>*R2(config)#ipaddress172.16.1.2 255.255.255.252*<br>*R2(config)#ipv6address 2001:DB8:ACAD:1::2/64*<br>*R2(config)# no shutdown* |
| Interfaz S0/0/1 | Establecer la descripción<br>Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.<br>Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000.<br>Activar la interfaz<br>*R2(config)#int s0/0/1*<br>*R2(config)# description connection to R3*<br>*R2(config)#ipaddress172.16.2.2 255.255.255.252*<br>*R2(config)#ipv6address 2001:DB8:ACAD:2::2/64*<br>*R2(config)# no shutdown* |

| | |
|---|---|
| Interfaz G0/0 (simulación de Internet) | Establecer la descripción.<br>Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.<br>Establezca la dirección Ipv6. Utilizar la primera dirección disponible en la subred.<br>Activar la interfaz:<br>*R2(config)#int g0/0*<br>*R2(config)# description connection to internet*<br>*R2(config)#ipaddress209.165.200.233 255.255.255.252*<br>*R2(config)#ipv6address 2001:DB8:ACAD:A::1/64*<br>*R2(config)# no shutdown* |
| Interfaz loopback 0 (servidor web simulado) | Establecer la descripción. Establezca la dirección Ipv4.<br>*R2(config)#int loopback0*<br>*R2(config)# description simulated web server*<br>*R2(config)# ip Address10.10.10.10 255.255.255.255* |

| | |
|---|---|
| Ruta predeterminada | Configure una ruta Ipv4 predeterminada de G0/0.<br>Configure una ruta Ipv6 predeterminada de G0/0.<br>*R2(config)# ip router 0.0.0.0 0.0.0.0 g0/0*<br>*R2(config)#ipv6 route ::/0 g0/0* |

Fuente propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

9.Tabla configurar R3

| Elemento o tarea de configuración | ESPECIFICACIÓN |
|---|---|
| Desactivar la búsqueda DNS | Comando para desactivar búsqueda DNA<br>*Router(config)#ip domain lookup* |
| Nombre del router | Comando para asignar nombre al equipo<br>*Router (config)#hostname R3* |
| Contraseña de exec privilegiado cifrada | Asignamos mediante el siguiente comando la contraseña del modo privilegiado<br>*R3(config)#enable secret class* |
| Contraseña de acceso a la consola | Líneas de comando para asignar la contraseña del acceso de consola<br>*R3(config)#line console 0*<br>*R3(config-line)#password cisco*<br>*R3(config-line) #login*<br>*R3(config-line) #exit* |
| Contraseña de acceso Telnet | Líneas de comando para asignarle la contraseña para el acceso a telnet<br>*R3(config)#line vty 0 4*<br>*R3(config-line) #password cisco*<br>*R3(config-line) #login* |
| Cifrar las contraseñas de texto no cifrado | Comando para cifrar las contraseñas y tener más seguridad<br>R3(config-line) #service password-encryption |
| Mensaje MOTD | Comando para emitir un mensaje:<br>R3(config)#banner motd# Se prohíbe el acceso no autorizado. # |

| | |
|---|---|
| Interfaz S0/0/1 | Establecer la descripción<br>Establezca la dirección Ipv4. Utilizar la siguiente dirección disponible en la subred.<br>Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz<br>*R3(config)#int s0/0/1*<br>*R3(config)# description connection to R2*<br>*R3(config)#ipaddress172.16.2.1 255.255.255.252*<br>*R3(config)#ipv6address 2001:DB8:ACAD:2::1/64*<br>*R3(config)# no shutdown* |
| Interfaz loopba 4 | Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.<br>*R3(config)# int loopback4*<br>*R3(config-if) # ip address 192.168.4.1 255.255.255.0* |
| Interfaz loopback 5 | Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.<br>*R3(config)# int loopback5*<br>*R3(config-if) # ip address 192.168.5.1 255.255.255.0* |
| Interfaz loopback 6 | Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.<br>*R3(config)# int loopback6*<br>*R3(config-if) # ip address 192.168.6.1 255.255.255.0* |
| Interfaz loopback 7 | Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>*R3(config)# int loopback7*<br>*R3(config-if) # ip address 192.168.7.1 255.255.255.0* |

| | |
|---|---|
| Rutas predeterminadas | Comandos para asignar rutas predeterminadas<br>*R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1*<br>*R3(config)#ipv6 route::/0 s0/0/1* |

Fuente propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

10 Tabla configuración S1

| Elemento o tarea de configuración | Especif icación |
|---|---|
| Desactivar la búsqueda DNS | Comando para desactivar búsqueda DNA<br>*switch(config)#ip domain lookup* |
| Nombre del switch | Comando para asignar nombre al equipo<br>*switch(config)#hostname S1* |
| Contraseña de exec privilegiado cifrada | Asignamos mediante el siguiente comando la contraseña del modo privilegiado<br>*S1(config)#enable secret class* |
| Contraseña de acceso a la consola | Líneas de comando para asignar la contraseña del acceso de consola<br>*S1(config)#line console 0*<br>*S1(config-line) #password cisco*<br>*S1(config-line) #login*<br>*S1(config-line) #exit* |
| Contraseña de acceso Telnet | Líneas de comando para asignarle la contraseña para el acceso a telnet<br>*S1(config)#line vty 0 4*<br>*S1(config-line) #password cisco*<br>*S1(config-line) #login* |
| Cifrar las contraseñas de texto no cifrado | Comando para cifrar las contraseñas y tener más seguridad<br>*S1(config-line) #service password-encryption* |
| Mensaje MOTD | Comando para emitir un mensaje:<br>*S1(config)#banner motd# Se prohíbe el acceso no autorizado. #* |

Fuente propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

11 tabla configuración S3

| Elemento o tarea de configuración | ESPECIFICACIÓN |
|---|---|
| Desactivar la búsqueda DNS | Comando para desactivar búsqueda DNA<br>switch(config)#ip domain lookup |
| Nombre del switch | Comando para asignar nombre al equipo<br>switch(config)#hostname S3 |
| Contraseña de exec privilegiado cifrada | Asignamos mediante el siguiente comando la contraseña del modo privilegiado<br>S3(config)#enable secret class |
| Contraseña de acceso a la consola | Líneas de comando para asignar la contraseña del acceso de consola<br>S3(config)#line console 0<br>S3(config-line) #password cisco<br>S(config-line) #login<br>S3(config-line) #exit |
| Contraseña de acceso Telnet | Líneas de comando para asignarle la contraseña para el acceso a telnet<br>S3(config)#line vty 0 4<br>S3(config-line) #password cisco<br>S3(config-line) #login |
| Cifrar las contraseñas de texto no cifrado | Comando para cifrar las contraseñas y tener más seguridad<br>S3(config-line) #service password-encryption |
| Mensaje MOTD | Comando para emitir un mensaje:<br>S3(config)#banner motd# Se prohíbe el acceso no autorizado. # |

Fuente propia

Paso 7: Verificar la conectividad de la red

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

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

12 Tabla verificación de conectividad

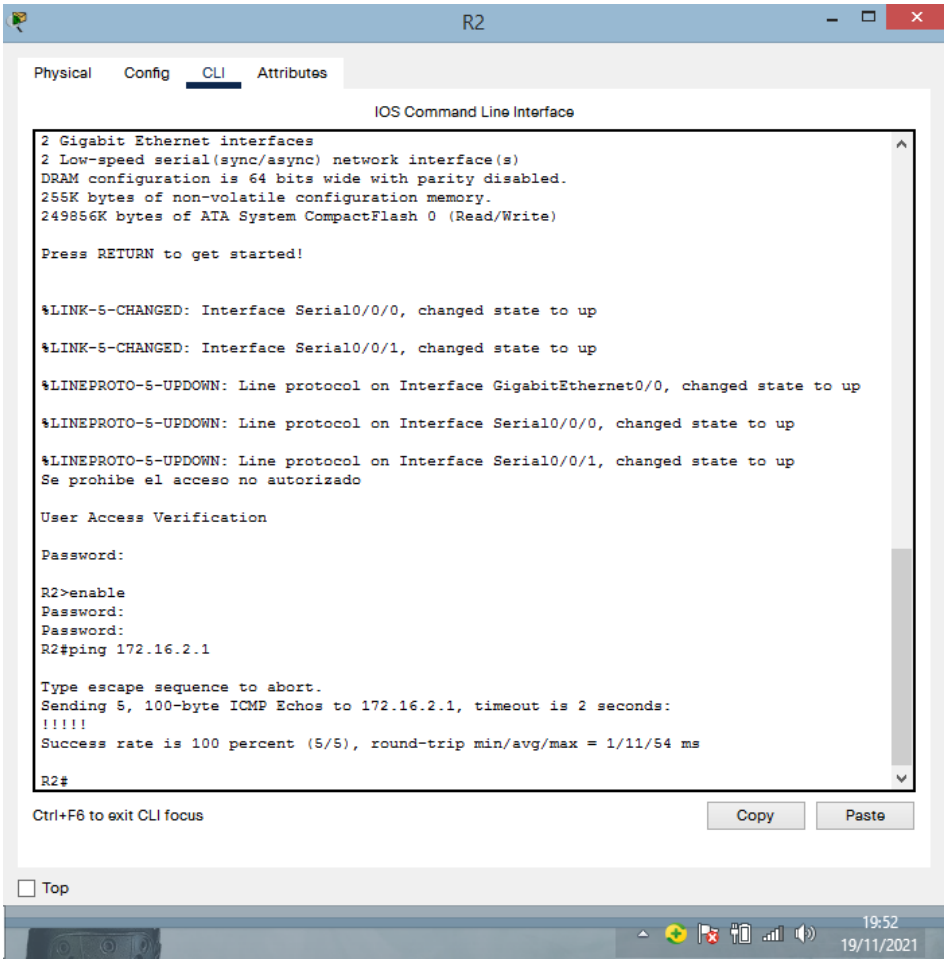
| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | EXITOSO |
| R2 | R3, S0/0/1 | 172.16.2.1 | EXITOSO |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | EXITOSO |

Fuente propia

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

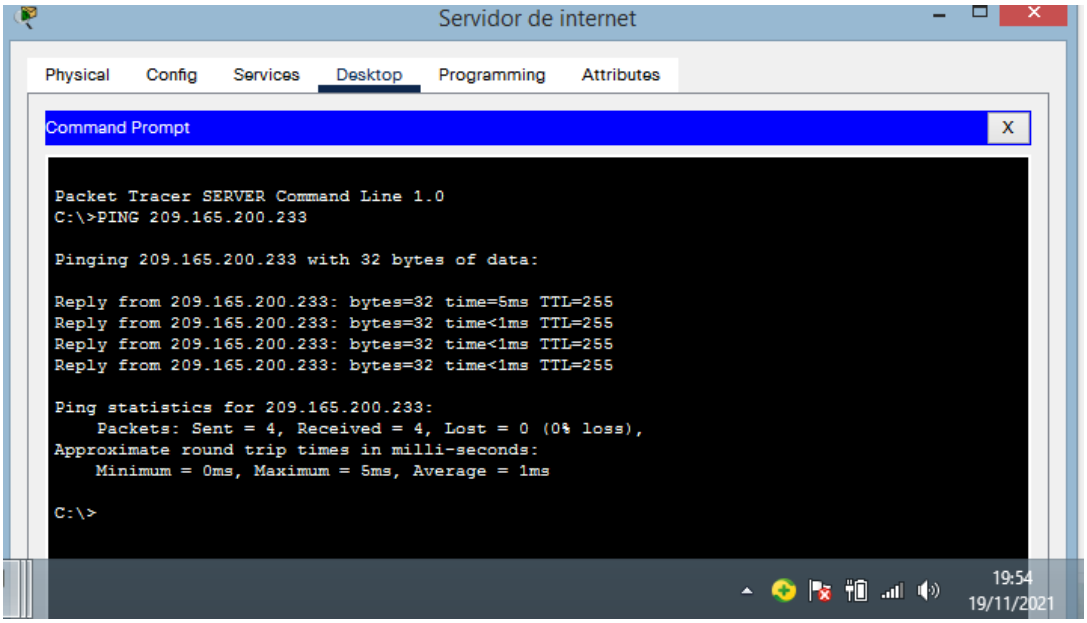
Ping R2 a R3

Figura 10  verificación de conectividad




Fuente propia

Figura 11. Verificación de conectividad




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:

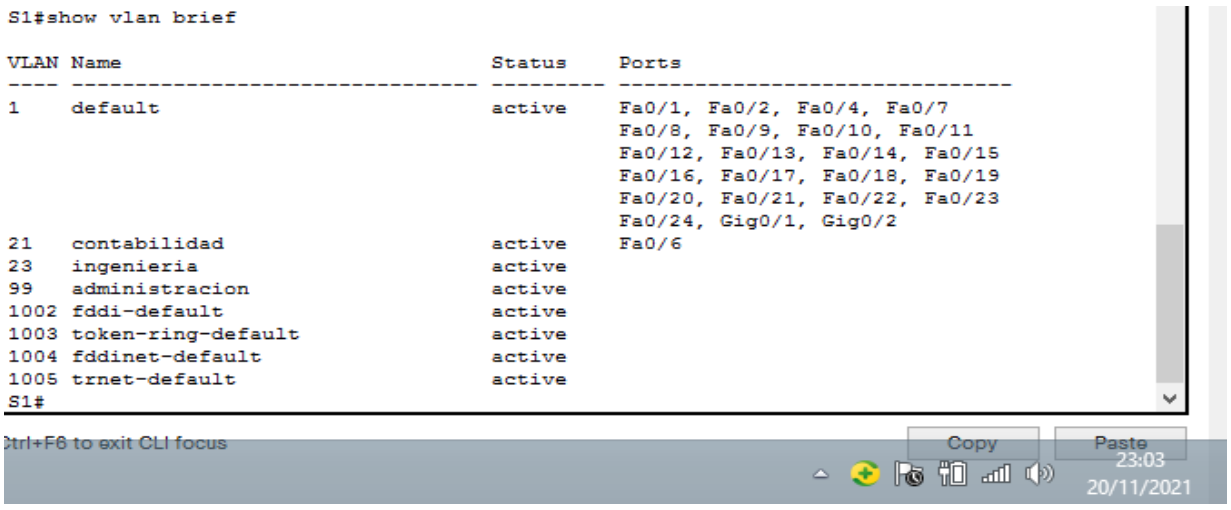
13. Tabla config. Seguridad de switch

| Elemento o tarea de configuración | *ESPECIFICACIÓN* |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican:<br>*S1(config)#vlan 21*<br>*S1(config-vlan) # name contabilidad*<br>*S1(config)#vlan 23*<br>*S1(config-vlan) # name ingeniería*<br>*S1(config)#vlan 99*<br>*S1(config-vlan) # name administración* |

| | |
|---|---|
| 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:<br>*S1(config)#int vlan99*<br>*S1(config-vlan) #ip address 192.168.99.2 255.255.255.0*<br>*S1(config-vlan) # no shutdown* |
| Asignar el 34ateway predeterminado | Asigne la primera dirección Ipv4 de la subred como el 34ateway predeterminado.<br>*S1(config)#ip default-gatewey 192.168.99.1* |
| Forzar el enlace troncal en la interfaz F0/3 | Utilizar la red VLAN 1 como VLAN nativa<br>*S1(config)# int f0/3*<br>*S1(config-if)#switchport mode trunk* |
| Forzar el enlace troncal en la interfaz F0/5 | Utilizar la red VLAN 1 como VLAN nativa<br>*S1(config)# int f0/5*<br>*S1(config-if)#switchport mode trunk* |
| Configurar el resto de los puertos como puertos de acceso | Utilizar el comando interface range:<br>*S1(config)#int range f0/1-2, f0/4 f0/7-24, g0/1-2*<br>*S1(config)#switchport mode Access* |
| Asignar F0/6 a la VLAN 21 | *S1(config)#int f0/6*<br>*S1(config-if) #switchport Access vlan 21*<br>*S1(config-if) #switchport mode Access* |
| Apagar todos los puertos sin usar | *S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2*<br>*S1(config)# shutdown* |

Fuente propia

Figura12. Pantallazo de verificación de configuración de vlan




Fuente propia

Paso 2: Configurar el S3

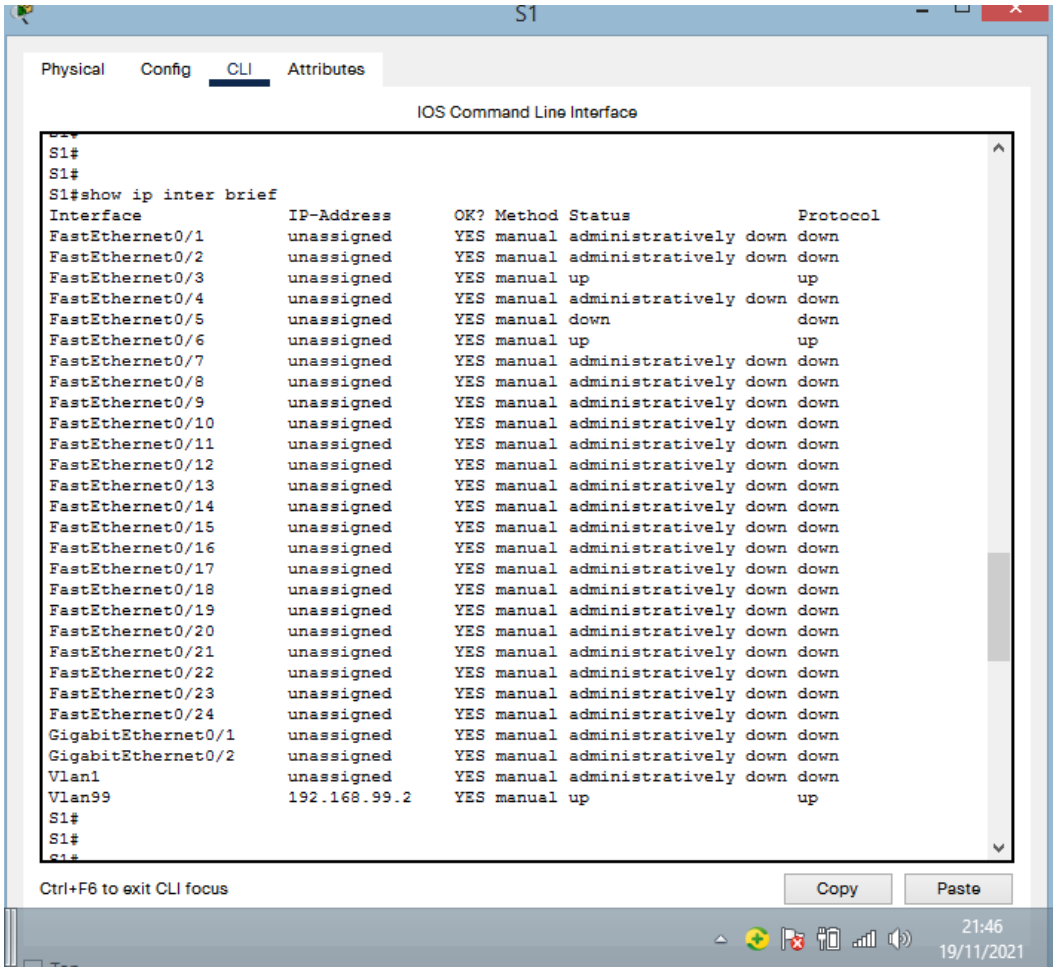
La configuración del S3 incluye las siguientes tareas:

38.Tabla configuración de S3

| Elemento o tarea de configuración | ESPECIFICACIÓN |
|---|---|
| Crear la base de datos de VLAN | Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.<br>*S3(config)#vlan 21*<br>*S3(config-vlan) # name contabilidad*<br>*S3(config)#vlan 23*<br>*S3(config-vlan) # name ingeniería*<br>*S3(config)#vlan 99*<br>*S3(config-vlan) # name administración* |
| 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.<br>*S3(config)#int vlan99*<br>*S3(config-vlan) #ip address 192.168.99.3 255.255.255.0*<br>*S3(config-vlan) # no shutdown* |
| Asignar el 35ateway predeterminado. | Asignar la primera dirección IP en la subred como 35ateway predeterminado.<br>*S1(config)#ip default-gatewey 192.168.99.1* |
| Forzar el enlace troncal en la interfaz F0/3 | Utilizar la red VLAN 1 como VLAN nativa<br>*S1(config)# int f0/3*<br>*S1(config-if)#switchport mode trunk* |
| Configurar el resto de los puertos como puertos de acceso | Utilizar el comando interface range:<br>*S1(config)#int range f0/1-2,f0/4 f0/7-24, g0/1-2*<br>*S1(config)#switchport mode access* |
| Asignar F0/18 a la VLAN 21 | *S1(config)#int f0/18*<br>*S1(config-if)#switchport Access vlan 21*<br>*S1(config-if)#switchport mode access* |
| Apagar todos los puertos sin usar | *S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2*<br>*S1(config)# shutdown* |

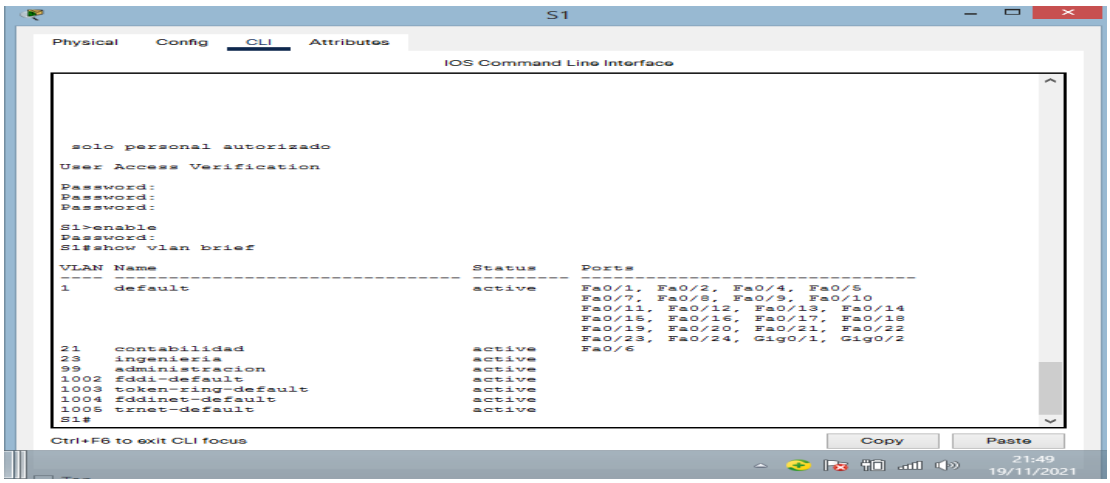
Fuente propia

Figura 13. Pantallazo de comprobación




Fuente propia

Figura 14 pantallazo de comprobación




Fuente propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

15 Tabla de configuración de router 1

| Elemento o tarea de configuración | Especifi cación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | Descripción: LAN de Contabilidad Asignar la VLAN 21<br>Asignar la primera dirección disponible a esta interfaz<br>*R1(config)# int g0/1.21*<br>*R1(config-if) #description vlan 21*<br>*R1(config-if)#encapsulation dot1Q 21*<br>*R1(config-if)#ip address192.168.21.1 255.255.255.0* |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | Descripción: LAN de Ingeniería Asignar la VLAN 23<br>Asignar la primera dirección disponible a esta interfaz<br>*R1(config)# int g0/1.23*<br>*R1(config-if)#description vlan 23*<br>*R1(config-if)#encapsulation dot1Q 23*<br>*R1(config-if)#ip address192.168.23.1 255.255.255.0* |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | Descripción: LAN de Administración Asignar la VLAN 99<br>Asignar la primera dirección disponible a esta interfa<br>*R1(config)# int g0/1.99*<br>*R1(config-if) #description vlan 99*<br>*R1(config-if)#encapsulation dot1Q 99*<br>*R1(config-if) #ip address192.168.99.1 255.255.255.0* |
| Activar la interfaz G0/1 | *R1(config-if) #int g0/1*<br>*R1(config-if) #no shutdown* |

Fuente propia

Paso 4: Verificar la conectividad de la red

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

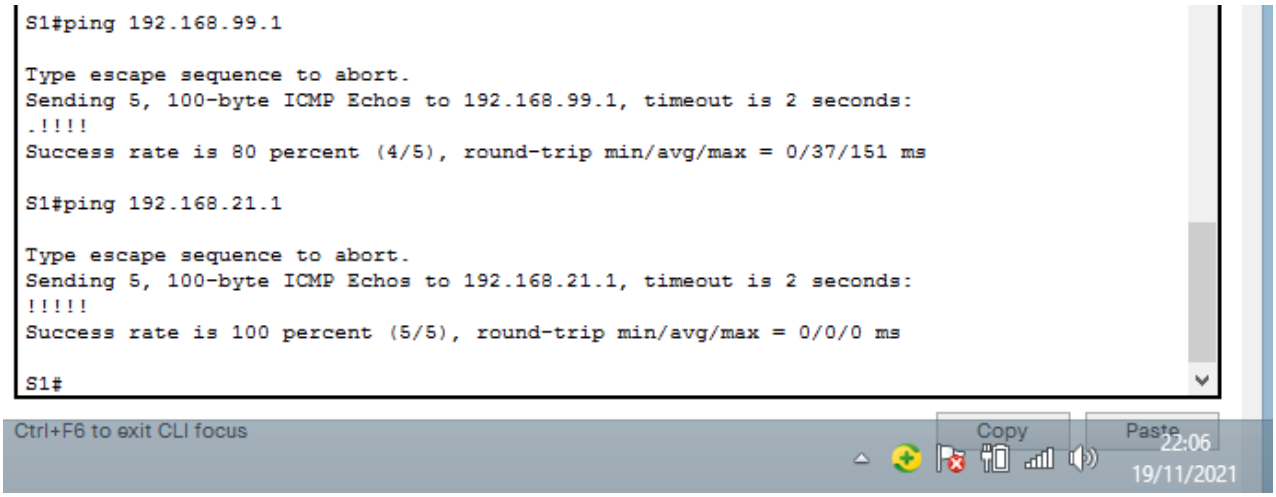
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

16. tabla de comprobación de conectividad de red

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | EXITOSO |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | EXITOSO |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | EXITOSO |
| S3 | R1, dirección VLAN 23 | 192.168.21.1 | EXITOSO |

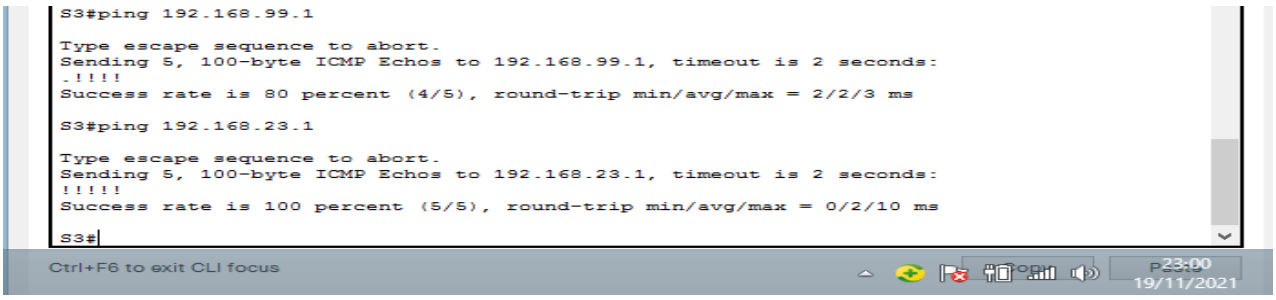
Fuente propia

Figura 15 pantallazo de comprobación




Fuente propia

Figura 16 pantallazo comprobación




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 17 configuración de ospf en R1

| ELEMENTO O TAREA DE CONFIGURACIÓN | Especificación |
|---|---|
| Configurar OSPF área 0 | *R1(config)#route ospf 1* |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente.<br>R1(config-ospf)#network 172.16.1.0 0.0.0.3 area0<br>R1(config-ospf)#network 192.168.21.0 0.0.0.255 area0<br>R1(config-ospf)#network 192.168.23.0 0.0.0.255 area0<br>R1(config-ospf) #network 192.168.99.0 0.0.0.255 area0 |
| Establecer todas las interfaces LAN como pasivas | R1(config)# passive-interface g0/1.21<br>R1(config)# passive-interface g0/1.23<br>R1(config)# passive-interface g0/1.99 |
| Desactive la sumarización automática | No aplica |

Fuente propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18 configuración ospf en R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2(config)# router ospf 1 |
| Anunciar las redes conectadas directamente | Nota: Omitir la red G0/0.<br>R2(config-ospf)#network 10.10.10.10 0.0.0.0 area0<br>R2(config-ospf)#network 172.16.1.0 0.0.0.3 area0<br>R2(config-ospf)#network 172.16.2.0 0.0.0.3 |

| | |
|---|---|
| | area0 |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config)# passive-interface loopback0 |
| Desactive la sumarización automática. | No aplica |

Fuente propia

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Configuración de ospf v3

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | *R3(config)#router ospf 1* |
| Anunciar redes IPv4 conectadas directamente | *R3(config-ospf)#network172.16.2.0 0.0.0.3 area0*<br>*R3(config-ospf)#network192.168.4.0 0.0.0.255 area0*<br>*R3(config-ospf)#network192.168.5.0 0.0.0.255 area0*<br>*R3(config-ospf)#network192.168.6.0 0.0.0.255 area0* |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | *R3(config)#passive-interface loopback4*<br>*R3(config)#passive-interface loopback5*<br>*R3(config)#passive-interface loopback6* |
| Desactive la sumarización automática. | No aplica |

Fuente propia

Paso 4: Verificar la información de OSPF

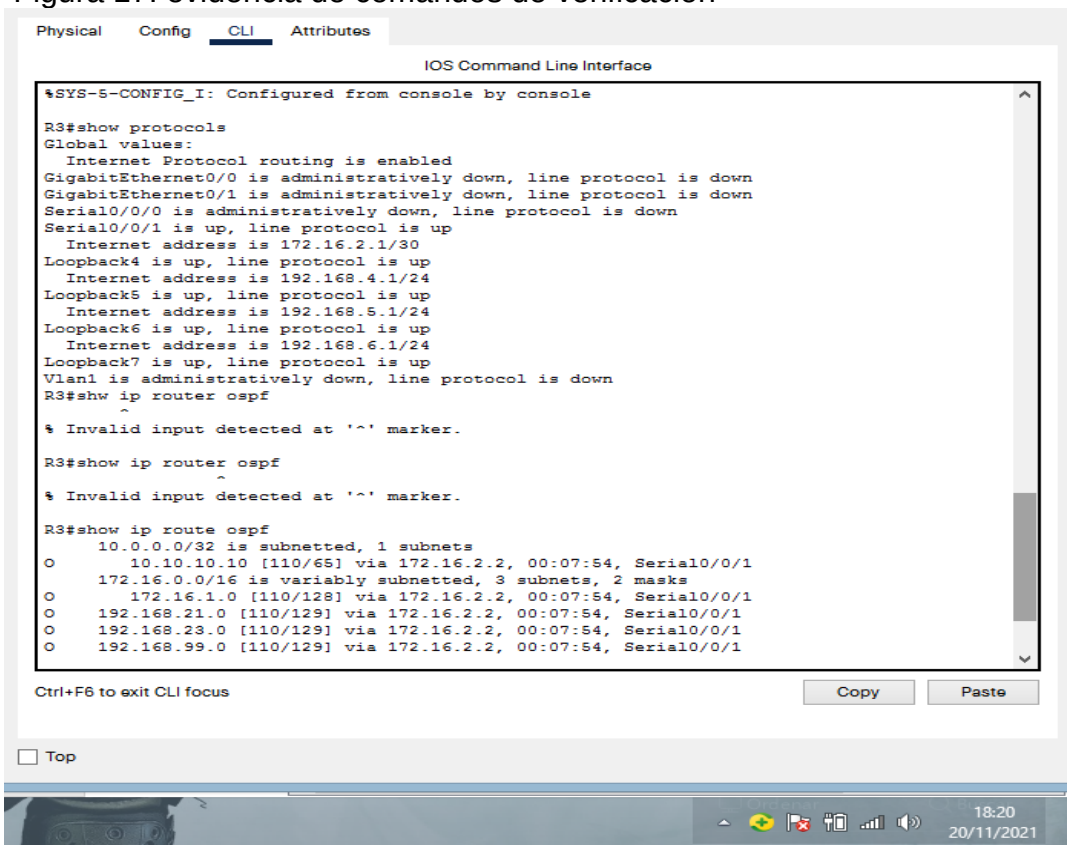
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 20 comandos de verificación

| PREGUNTA | RESPUESTA |
|---|---|
| ¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router? | R3#show protocols |
| ¿Qué comando muestra solo las rutas OSPF? | R3#show ip route ospf |
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución? | R3#show running-config\| section ospf |

Fuente propia

Figura 17. evidencia de comandos de verificación




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 21 configuración de R1 como servidor de DHCP

| Elemento o tarea de configuración | ESPECIFICACIÓN |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | *R1(config)# ip dhcp excluded-address 192.168.21.1 192.168.21.20* |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | *R1(config)# ip dhcp excluded-address 192.168.23.1 192.168.23.20* |
| Crear un pool de DHCP para la VLAN 21 | Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de |

| | |
|---|---|
| | dominio: ccna-sa.com<br>Establecer el ateway predeterminado<br>R1(config)#ip dhcp pool ACCT<br>R1(config)#network 192.168.21.0 255.255.255.0<br>R1(config)#defaul-router 192.168.21.1<br>R1(config)#dns-server 10.10.10.10 |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>Servidor DNS:<br>10.10.10.10 Nombre de<br>dominio: ccna-sa.com<br>Establecer el ateway predeterminado<br>R1(config)#ip dhcp pool ENGNR<br>R1(config)#network 192.168.23.0 255.255.255.0<br>R1(config)#defaul-router 192.168.23.1<br>R1(config)#dns-server 10.10.10.10 |

Fuente propia

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

La configuración del R2 incluye las siguientes tareas:

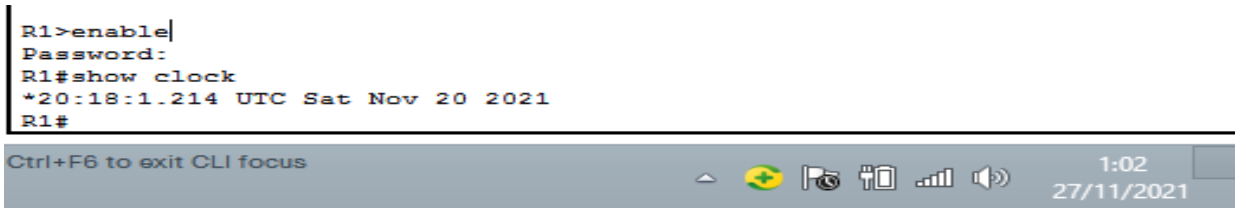
Tabla 22. Configuración NAT

| 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<br>R2(config)#username webuser privilege 15 secret 5 cisco12345 |
| Habilitar el servicio del servidor HTTP | Aunque cisco packet tracer no soporta este código lo incluyo:<br>IP HTTP SERVER |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | *Ip http autentication local* |
| Crear una NAT estática al servidor web. | Direccion global interna: 209.165.200.238<br>R2(config)# ip nat outside |

| | |
|---|---|
| | R2(config-if)#duplex auto<br>R2(config-if)#speed auto |
| Asignar la interfaz interna y externa para la NAT estática | R2(config)# int g0/0<br>R2(config-if)#ip address 209.165.200.233 255.255.255.248<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 |
| Configurar la NAT dinámica dentro de una ACL privada | Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1<br>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3<br>*R2(config)#acces-list 1 permit 192.168.21.0 0.0.0.255*<br>*R2(config)#acces-list 1 permit 192.168.23.0 0.0.0.255*<br>*R2(config)#acces-list 1 permit 192.168.4.0 0.0.3.255* |
| Defina el pool de direcciones IP públicas utilizables. | Nombre del conjunto: INTERNET<br>El conjunto de direcciones incluye:<br>209.165.200.225 – 209.165.200.228<br>R2(config)#Ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248 |
| Definir la traducción de NAT dinámica | *R2(config)# ip nat inside source list 1 pool INTERNET* |

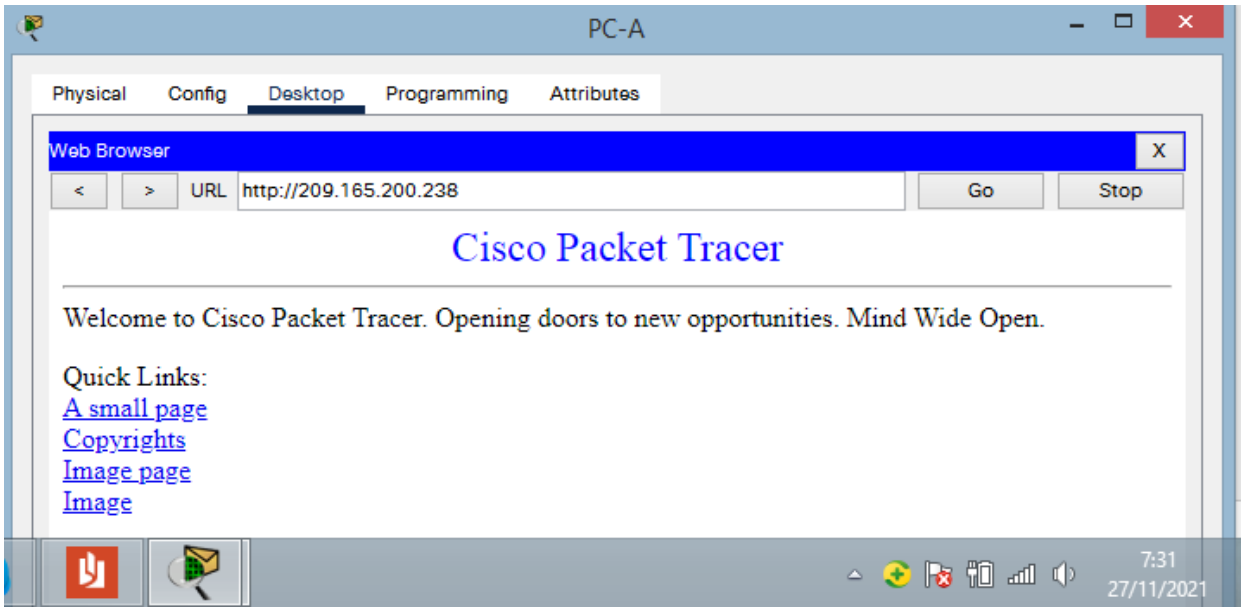
Fuente propia

Figura 18. Comando show clock



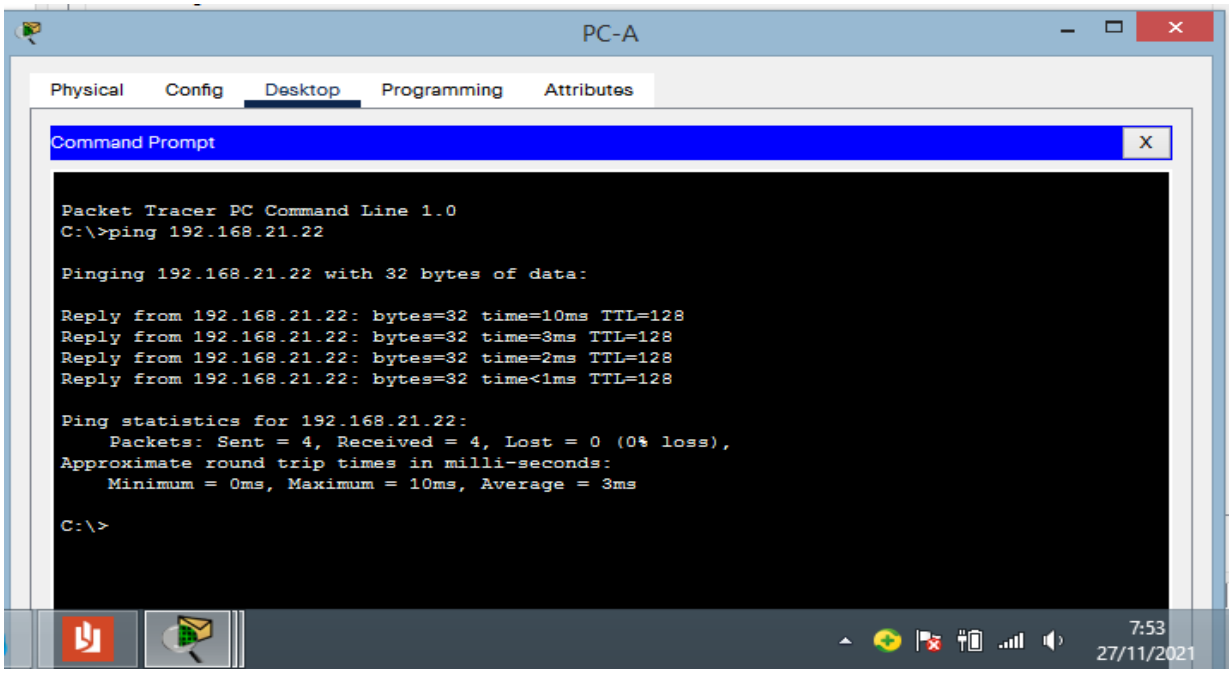

Fuente propia

Figura 19. acceso a http://209.165.200.238



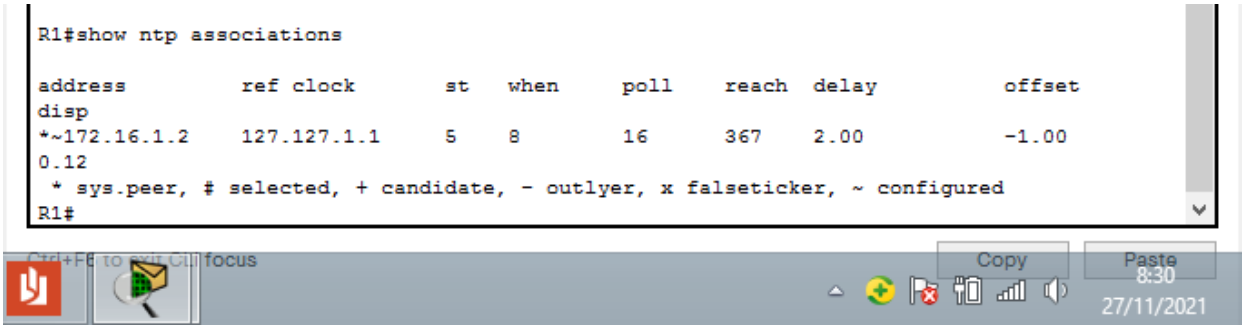

Fuente propia

Figura 20 ping entre pc



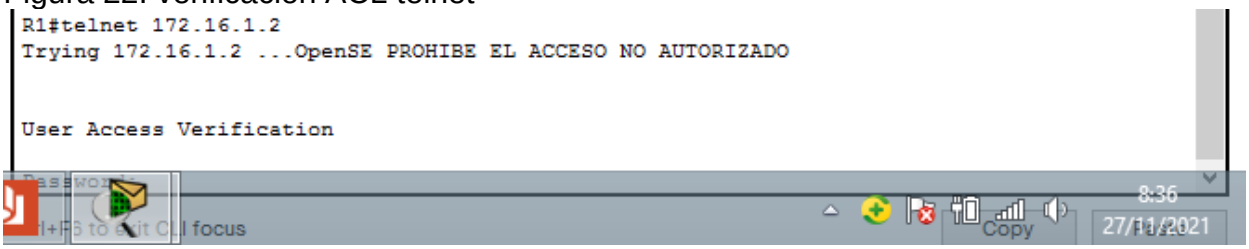

Fuente propia

Figura 21. comando show ntp associations



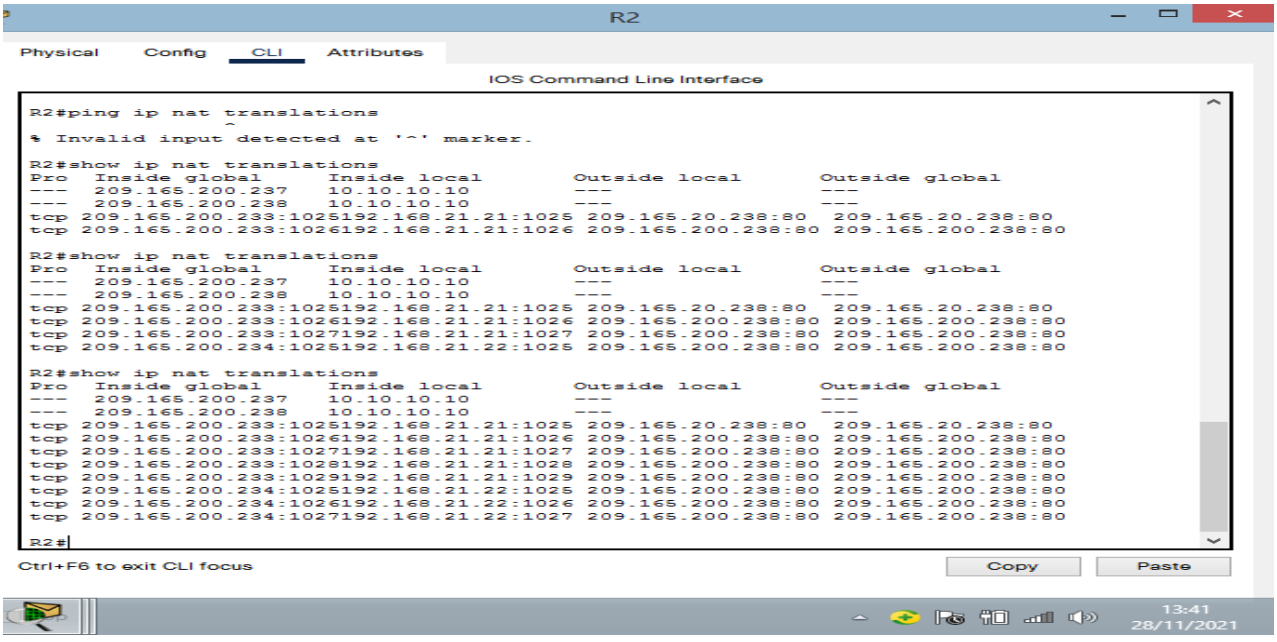

Fuente propia

Figura 22. verificacion ACL telnet



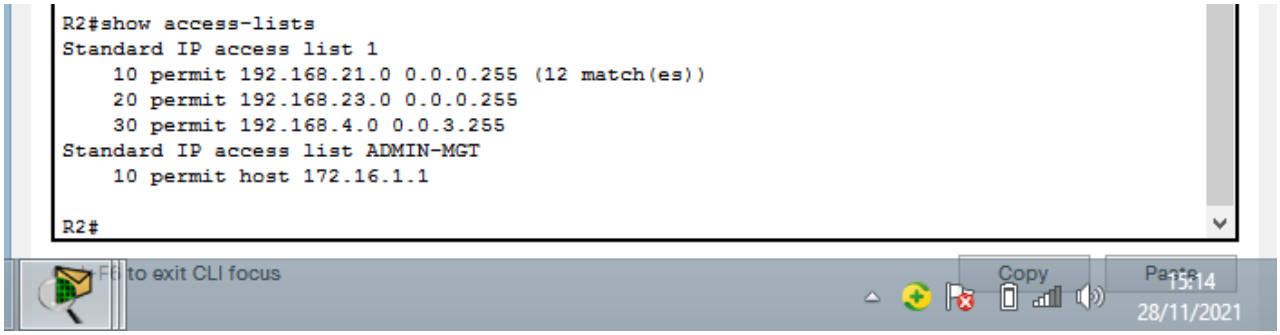

Fuente propia

Figura 24. Verificación de NAT




Fuente propia

Figura 24 verificación de contador y ACL realizando match

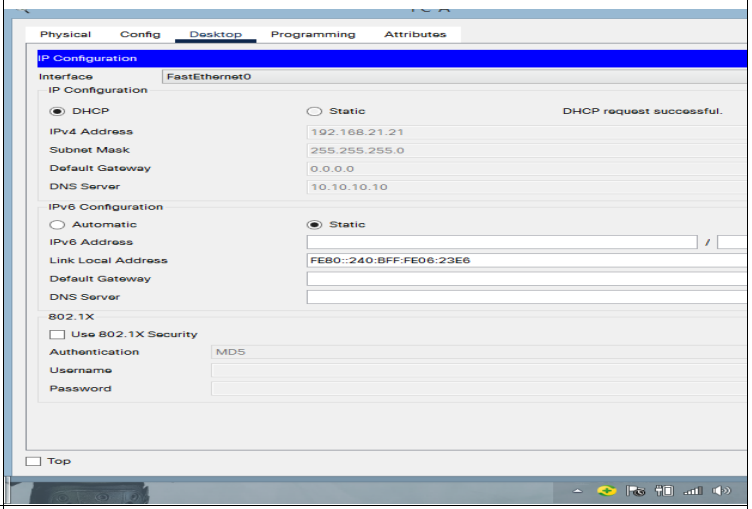


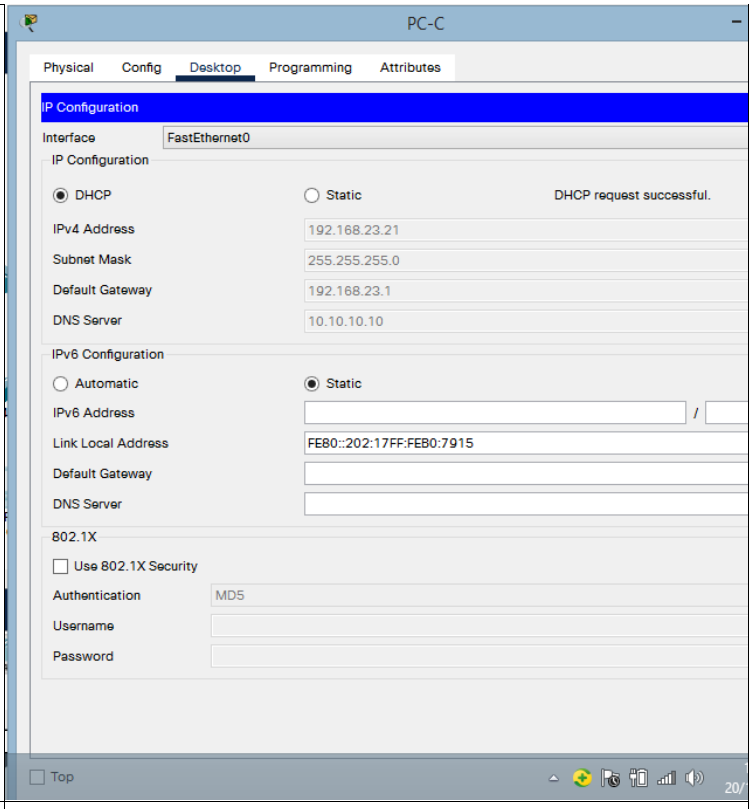
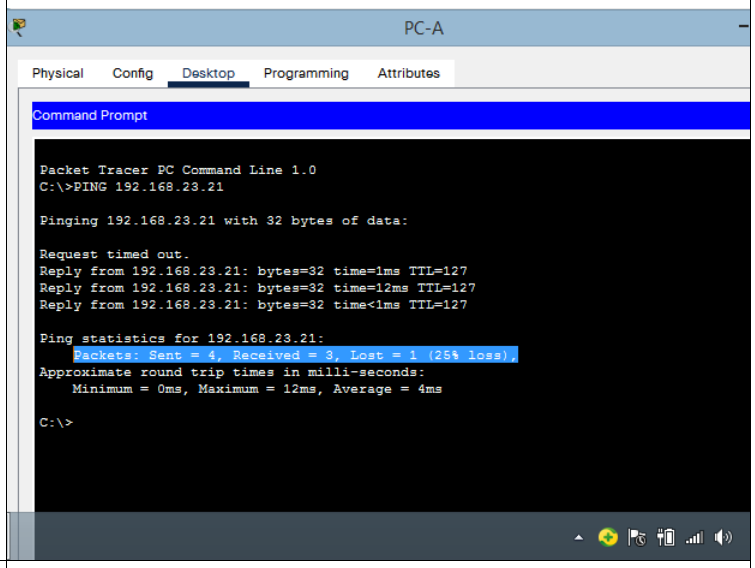

Fuente propia

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 23. Verificación de protocolo DHCP y NAT

| *PRUEBA* | RESULTADOS |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP |  |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | |

| | |
|---|---|
| |  |
| Verificar que la PC-A pueda hacer ping a la PC-C<br>Nota: Quizá sea necesario deshabilitar el firewall de la PC. |  |
| 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 | |

Fuente propia

Parte 6: Configurar NTP

Tabla 24. Configuración NTP

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | R2(config)#clock set 21:3:15<br>20 nov 2021 |
| Configure R2 como un maestro NTP. | Nivel de estrato: 5<br>R2(config)# ntp manster 5 |
| Configurar R1 como un cliente NTP. | Servidor: R2<br>R1(config)# ntp server 172.16.1.2 |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | *R1(config)#ntp update-calendar* |
| Verifique la configuración de NTP en R1. | *R1# show ntp status* |

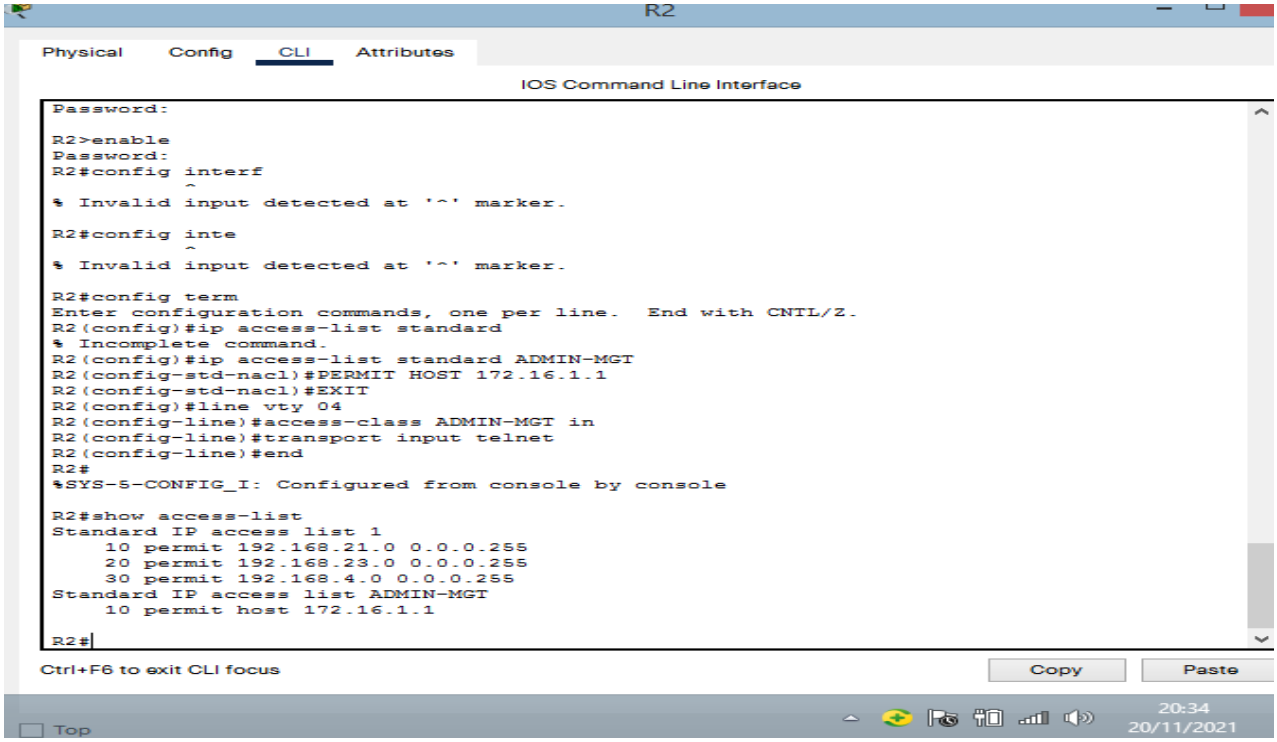
Fuente propia

Parte 7: Configurar y verificar las listas de control de acceso (ACL) Paso 1: Restringir el acceso a las líneas VTY en el R2

| 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<br>R1(config)#ip Access-list standard ADMIN-MGT |
| Aplicar la ACL con nombre a las líneas VTY | R2(config)#line vty 0 4<br>R2(config-line)#access-class ADMIN-MGT in |
| Permitir acceso por Telnet a las líneas de VTY | R2(config)#line vty 0 4<br>*R2(cinfig-line)#transport input telnet* |
| Verificar que la ACL funcione como se espera | *R2# show acces-list* |

Fuente propia

Figura 17 evidencia de verificación de restricción



Fuente propia

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

Tabla 26. Comando de verificación

| Descripción del comando | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | show ip acces-list |
| Restablecer los contadores de una lista de acceso | Clear Access-list counters |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | Show ip interface s0/0/0 |
| ¿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. |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | clear ip nat translation |

Fuente propia

## CONCLUSIONES

Mediante el desarrollo del trabajo se logró conocer los pasos adecuados para la creación de redes LAN y WAN mediante procesos de enrutamiento y protocolos que generen seguridad en la adecuada formulación de las mismas.

De igual forma se pusieron en práctica las diferentes líneas de comando que conducen a las buenas prácticas de configuración teniendo en cuenta aspectos como los posibles ataques y amenazas en cuanto a seguridad por parte de terceros.

Uno de los aprendizajes importantes radica en la capacidad como estudiantes de crear operaciones básicas que permitan realizar el direccionamiento correcto utilizando las fórmulas de enrutamiento acertadas que permitan generar la capacidad de resolver problemas de conectividad y que den como resultado un excelente entendimiento entre el servicio y la buena comunicación.

Se adquiere habilidades para realizar la configuración de diferentes equipos como switches, routers, servidores, utilizando los diferentes protocolos y configuraciones básicas de enrutamiento.

## BIBLIOGRÁFIA


Comandos básicos para trabajar con Packet Tracer « EL portafolio de las redes. (wordpress.com)

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

BAREÑO, Gutiérrez, R., 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 Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)* (pp. 1-5). IEEE.

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

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

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.

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched

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