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

JONATHAN ANDRES RINCON RUIZ

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

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

JONATHAN ANDRES RINCON RUIZ

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

DIRECTORA
NANCY AMPARO GUACA

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

NOTA ACEPTACION

Firma Del Presidente Jurado

Firma Del Jurado

Firma Del Jurado

Mariquita, 27 noviembre 2021

DEDICATORIA

Le dedico este informe a Dios por permitirme culminar mi profesión como ingeniero de sistemas, por poner en mi vida personas vestidas de ángeles, que me han ayudado en este proceso, para mi es de gran importancia ser muy agradecido con Dios, por su favor y su bendición que me ha acompañado durante todo este tiempo, me ha puesto personas correctas en mi vida, que me han apoyado económicamente, intelectualmente y extensamente, donde me han facilitado, la vida al dedicarme a mis estudios, también le dedico este logro a mi amada esposa y a su familia que me han ayudado, me han apoyado, a mis padre por la educación que me dieron, por aconséjame en no dejar mis estudios medios, por enseñarme con esfuerzo y dedicación si se puede cumplir los sueños. También me encuentro profundamente agradecido y le dedico parte de este informe al Ingeniero Raúl Bareño Gutiérrez, por su acompañamiento, por transmitir sus diversos conocimientos, es de admirar su trabajo que me ayudaron al pasar este último peldaño en culminar este informe de grado.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

GUI: Una interfaz fácil de utilizar que proporciona una interacción entre un usuario y un SO a través de un entorno gráfico

Consola: Un puerto físico de un dispositivo Cisco que proporciona acceso al dispositivo a través de un canal de administración exclusivo, también conocido como acceso fuera de banda

Ipconfig: Comando de Windows que muestra los parámetros de configuración IP en una PC

Gateway predeterminado: Un router que se encarga de redirigir los paquetes que recibe a su puerto de destino.

también Un dispositivo que permite que los dispositivos de una red se comuniquen con los dispositivos de otras redes

Un dispositivo que permite que los hosts de una red se comuniquen con los hosts de otras redes

Topología física: Los diseños y las conexiones reales de los dispositivos de una red

Dirección física: Una dirección de capa 2 que permite que las NIC se comuniquen entre sí

Dirección lógica: Una dirección de capa 3 que identifica la red y el host específico de esa red

Routing: El proceso de envío de paquetes a hosts en una red remota

Siguiente salto: El router de destino que indica el ingreso de interfaz saliente en la tabla de routing

RAM: Memoria volátil que almacena la configuración en ejecución y las tablas que genera el dispositivo

ROM: Memoria no volátil que contiene instrucciones y un IOS limitado para el router

NVRAM: Memoria no volátil que almacena la configuración de inicio de un dispositivo

Nombre de host: Una forma de identificar un dispositivo de red

Memoria flash: Memoria no volátil que almacena los archivos de IOS y otros archivos del sistema

Dirección de red: Un número decimal con puntos que representa una única dirección IP

Dirección de host: Cualquier dirección IP en una red IP que puede asignarse a una interfaz

Dirección de difusión: Un número decimal con puntos que representa a todos los hosts en una dirección IP.

Dirección de unidifusión: La dirección IP de un solo host en una red

Dirección de multidifusión: Una dirección IP que representa un grupo seleccionado de hosts

Direccionamiento con clase: Intervalos específicos de direcciones IP que componen las clases de direcciones en las que se define la cantidad de direcciones de red y host disponibles

División en subredes: El proceso de subdivisión de una red en grupos más pequeños de dispositivos o subredes.

Dominio de difusión: Un área dentro de cual se compartirá una transmisión por difusión

Subred: La subdivisión de una red que se crea para conservar las direcciones o bien para satisfacer los requisitos específicos de la red

VLSM: Permite la creación de subredes de distintos tamaños de la misma dirección de red

Fórmula 2^n: Calcula la cantidad de subredes creadas para n bits que se pidieron prestados

Fórmula 2^n-2: Calcula la cantidad de hosts por subred para n bits restantes en el campo de host

Segmento: Un bloque de datos de la aplicación que se crea para facilitar el transporte de red

TCP: Un protocolo confiable orientado a la conexión que utiliza un establecimiento de comunicación trilateral

Nombre de dominio: El nombre que se utiliza para identificar de manera única a un sitio web y se utiliza en lugar de la dirección IP

Dispositivo intermediario: Un dispositivo que transmite el tráfico de red y conecta distintas redes

RESUMEN

En el primer escenario del informe del curso de especialización cisco CCNA I Y CCNA II (LAN / WAN) se realiza una topología de subredes, la propuesta indicada por el curso es utilizar las técnicas VLSM y subnetting, para crear dos redes LAN, dividiendo la red 192.168.10.0/24, realizar configuración básica de los dispositivos de red de la primera capa y tercera de capa del modelo OSI, verificar la conectividad y la comunicación entre los dispositivos de red, en este ejercicio se realizó una configuración básica de seguridad y conectividad para evitar ciber ataque a la red

En el segundo escenario se realiza la configuración de una red pequeña, que admita la conectividad de los protocolos IPv4 y IPv6, también se realiza las siguientes configuraciones; seguridad de dispositivos de red, creación de vlan entre los switch y router, se realiza la conexión de dispositivos utilizando el el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), se creó listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Todas esas configuraciones se realizaron por el CLI

Palabras claves: Cisco, direccionamiento, ipv4, cli, lan, ospf.

ABSTRACT

In the first scenario of the report of the Cisco CCNA I and CCNA II (LAN / WAN) specialization course, a subnet topology is performed, the proposal indicated by the course is to use VLSM and subnetting techniques to create two LAN networks, dividing the network 192.168.10.0/24, perform basic configuration of the network devices of the first and third layer of the OSI model, verify connectivity and communication between network devices, in this exercise a basic security and connectivity configuration was performed to avoid cyber-attack on the network.

In the second scenario, the configuration of a small network is carried out, which supports the connectivity of the IPv4 and IPv6 protocols, the following configurations are also carried out; security of network devices, creation of vlan between the switches and routers, the connection of devices is made using the dynamic routing protocol OSPF, the dynamic host configuration protocol (DHCP), the translation of dynamic and static network addresses (NAT), I created access control lists (ACL) and the network time protocol (NTP) server / client. All those configurations were made by the CLI

Keywords: Cisco, address, ipv4, cli, lan, ospf.

INTRODUCCIÓN

En la actualidad el internet o la utilización de redes de datos es de gran importancia, ayudando a la comunidad a ser más competente a agilizar la respuesta y las demandas de cada sector ayudando al éxito de las organizaciones considerándose como un recurso más crítico para el mundo entero.

En el mundo actual, la informática se ha convertido en una parte integral del sector empresarial para actividades profesionales, no solo para actividades profesionales, sino también para actividades personales. A medida que las tecnologías han evolucionado, las redes entraron en escena y, poco a poco, desde la tecnología de red cableada inicial pasamos a esta tecnología de red inalámbrica. Ahora, si pensamos, entonces podemos saber que las redes impactan todo.

El objetivo principal de este informe es en ponen en práctica lo aprendiendo del curso CCNA I y CCNA II. De manera aprendida, se crea dos redes de computadoras utilizando varios protocolos de comunicación y configuración de subredes, estos protocolos se pueden utilizar para configurar rápidamente dispositivos finales, asignando direcciones IP de forma dinámica proporcionando medios de transmisión de datos. Otro protocolo de red de gran importancia es el OSPF, este protocolo ayuda a encontrar la ruta más recomendada y rápida entre nodos, de esa manera se reduce el tráfico en la red, se ejecutó este protocolo en el segundo escenario utilizando ambas versiones para IPv4 y IPv6. Se realiza configuración básica de dos dispositivos de red, teniendo en cuenta la ciber seguridad de cada dispositivo de red.

Se en este documento se realiza la aplicación del proceso NAT, simulando la conexión de los dispositivos a la internet, configurando direcciones ip privadas convirtiendo a dirección pública.

También se ejecutó listas de control de acceso (ACL), para poder denegar el acceso no deseado a la red a algunos dispositivos y a la vez permitir el acceso a otros, de esa manera filtramos el control de acceso a los diferentes dispositivos

DESARROLLO

ESCENARIO 1

Topología

Figura 1 Topología de red escenario 1

Fuente: Propia

Aspectos básicos

En este proyecto se va a realizar la administración y asignación de dos subredes IPv4, en la se muestra en la topología de la figura 1, asignación de direcciones IPv4 al R1, S1, la configuración de los pc y el último paso confirmar la conectividad entre los dispositivos, la tarea es utilizar las técnicas 2^n y 2^2-2, para sacar la cantidad de redes y la cantidad de host de la siguiente red 192.168.10.0. el requerimiento es que en la LAN 1 tenga (100 host) y LAN 2 (50 host)

Tabla de subredes

Tabla 1 Tablas de subredes

Descripción de la subred	Dirección de subred
LAN 1 G0/0/1	192.168.10.1/25
LAN 2 G0/0/0	192.168.37.129/26

Fuente: Propia

Tabla VLSM

Tabla 2 Tabla de subnetting VLSM

LAN	PCS	DIRECCION DE RED	MASCARA	PRIMER IP	ULTIMA IP	BROADCAST	#H
LAN 1	100	192.168.10.0	255.255.255.128	192.168.10.1	192.168.10.126	192.168.10.127	128
LAN 2	50	192.168.10.128	255.255.255.192	192.168.10.129	192.168.10.190	192.168.10.191	64

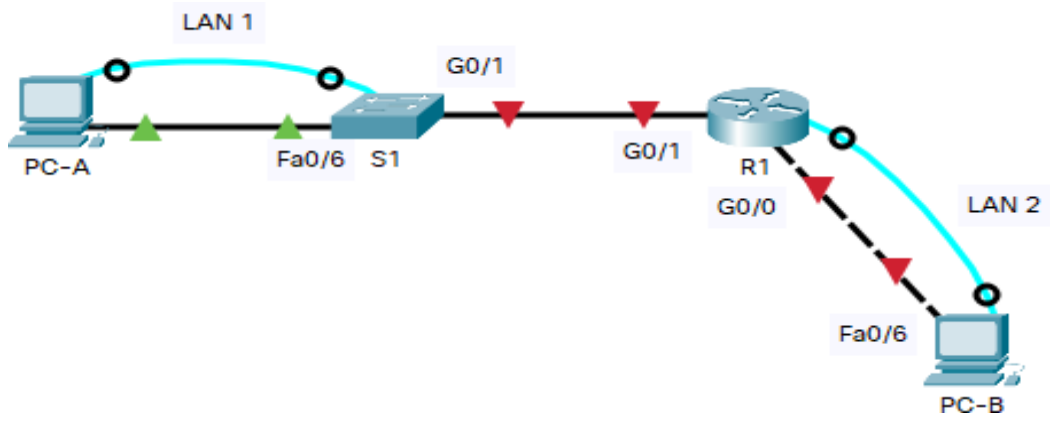
Fuente: Propia

Tabla 3 Tabla de direccionamiento

Ítem	descripción
Dirección red	192.168.10.0
# host Subred LAN1	100
# host Subred LAN2	50
R1 G0/0/1	192.168.10.1/25
R1 G0/0/0	192.168.10.129/26
S1 SVI	192.168.10.2/25
PC-A	192.168.10.126/25
PC-B	192.168.10.190/26

Fuente: Propia

Figura 2 Topología de red en Packet tracer



Fuente: Propia

Configuraciones básicas
Paso 1: configuración básica del R1 IPv4

Se realiza una configuración teniendo en cuenta la tabla 3 de direccionamiento, primero que todo la configuración se realiza por medio de consola del pc asignado para cada red como se encuentra en la figura 2, entonces por medio de consola se realiza las siguientes configuraciones

Router(config)#no Ip domain-lookup	Desactivar la búsqueda DNS
Router(config)#hostname R1	Cambiar nombre del router
R1(config)#ip domain-name ccna-lab.com	Asignarle nombre de dominio

R1(config)#enable secret ciscoenpass	Añadir contraseña cifrada para el modo EXEC privilegiado
R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login	Añadir contraseña de acceso a la consola
R1(config)#security passwords min-length 10	Se establece longitud mínima para las contraseñas 10 caracteres
R1(config)#username admin password admin1pass	Crear un usuario administrativo en la base de datos local
R1(config)#line vty 0 4 R1(config-line)#password ciscocisco R1(config-line)#login local	Configuración de inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#transport input ssh	Configuración VTY solo aceptando SSH
R1(config-line)#service password-encryption	Cifrar las contraseñas de texto no cifrado
R1(config)#banner motd #Solo acceso para los Los administradores de la red #	Añadiendo un banner motd
R1(config)#int g0/0/0 R1(config-if)#Description LAN 2	Acceder a la interfaz G0/0/0 Asignar una descripción a la Interfaz
R1(config-if)#Ip address 192.168.10.129 255.255.255.192	Asignar Dirección IPv4
R1(config-if)#no shu	Encender la interfaz
R1(config)#int g0/0/1	Acceder a la interfaz G0/0/1
R1(config-if)#Description LAN 1	Asignar una descripción

R1(config-if)#Ip address 192.168.10.1 255.255.255.128	Asignar Dirección IPv4
R1(config-if)#no shu	Encender la interfaz
R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	Generar una clave de cifrado RSA

Paso 2 configuración básica de switch S1

Se realiza una configuración básica en el switch S1 teniendo en cuenta la tabla 3 de direccionamiento, primero que todo la configuración se realiza por medio de consola del pc asignado para cada red como se encuentra en la figura 2, entonces por medio de consola se realiza las siguientes configuraciones

Switch(config)#no ip domain-lookup	Desactivar la búsqueda DNS.
Switch(config)#host S1	Nombre del switch
S1(config)#ip domain-name ccna-lab.com	Nombre de dominio
S1(config)#Enable secret ciscoenpass	Contraseña cifrada para el modo EXEC privilegiado
S1(config)#Line console 0	Acceder a la consola 0
S1(config-line)#Password ciscoconpass	Colocar la contraseña
S1(config-line)#login	Toca loguearse para que sirva
S1(config)#username admin password admin1pass	Crear un usuario administrativo en la base de datos local
S1(config)#Line vty 0 15 S1(config-line)#Password ciscocisco S1(config-line)#Login local	Configurar el inicio de sesión en las líneas VTY para que use la base de datos local
S1(config-line)#transport input ssh	Configurar las líneas VTY para que acepten únicamente las conexiones SSH
S1(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
S1(config)#Banner motd #Solo acceso a personal Autorizado#	Configurar un MOTD Banner
S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	Generar una clave de cifrado RSA
S1(config)#Int vlan1	Acceder a la interfaz virtual
S1(config-if)#Ip add 192.168.10.2 255.255.255.128	Añadir dirección IPv4

S1(config-if)#no shut Activar la interfaz
S1(config-if)#Ip default-gateway 192.168.10.1 Configuración El Gateway predeterminado

Paso 3 Asignar direcciones IPv4 a los pc

Tabla 4 Descripción de Dirección ip PC – A

PC-A Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0000.0C2D.8327
Dirección IP	192.168.10.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.10.1

Fuente: Propia

Tabla 5 Descripción de Dirección ip PC – B

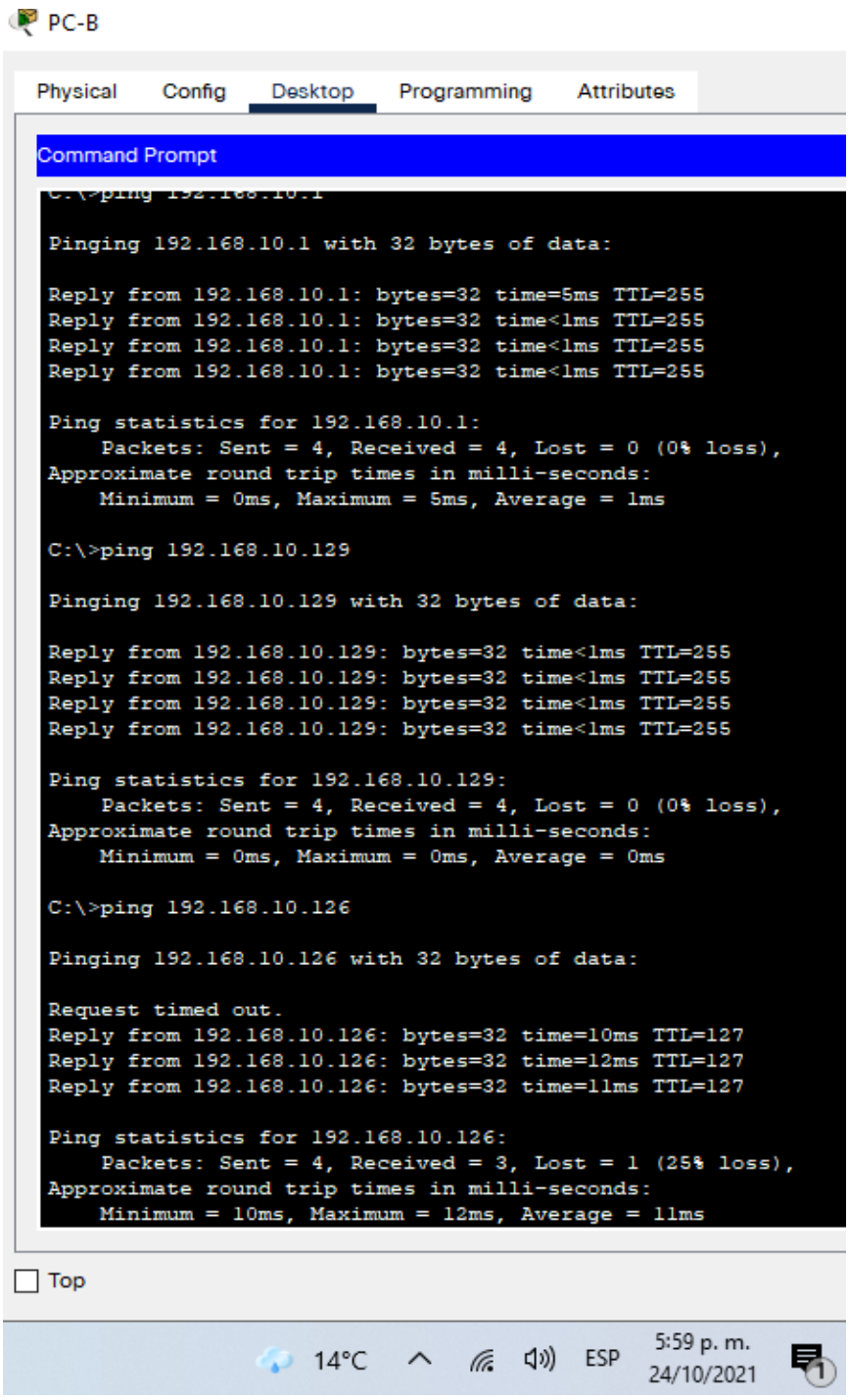
PC-B Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0050.0F23.EB10
Dirección IP	192.168.10.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.10.129

Fuente: Propia

Paso 4 verificación de conexión y configuración

Este es el último paso del escenario 1, se realiza la verificación, configuración y conectividad de todos los dispositivos, donde es de gran importancia, constatar la comunicación o vinculación de cada dispositivo a la red, donde se configuro por medio de consola, la manera que realizamos esa verificación de conexión es utilizando una solicitud del comando ping, enviamos un mensaje a un host de destino, por medio de su dirección ip.

Figura 3 Pantallazo de verificación de conexión -PING-



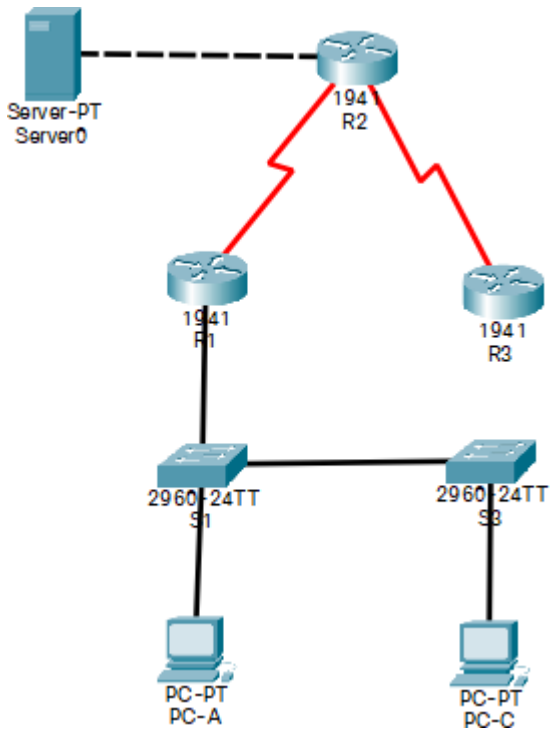
Fuente: Propia

ESCENARIO 2

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

Topología

Figura 4 Teología escenario 2



Fuente: Propia

Parte 1: Inicializar dispositivos

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

Eliminar el archivo startup-config de todos los routers y volver cargar el dispositivo

R1

Router#erase startup-config

Router#reload

R2

Router#erase startup-config

Router#reload

R3
Router#erase startup-config
Router#reload

S1

Switch#erase startup-config	Eliminar el archivo startup-config
Switch#delete flash:vlan.dat	eliminar la base de datos de VLAN anterior
Switch#reload	Volver a cargar ambos switches
Switch# show flash	Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

S3

Switch#erase startup-config	Eliminar el archivo startup-config
Switch#delete flash:vlan.dat	eliminar la base de datos de VLAN anterior
Switch#reload	Volver a cargar ambos switches
Switch# show flash	Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Parte 2: Configurar los parámetros básicos de los dispositivos
Paso 1: Configurar la computadora de Internet

Tabla 6 configuración de la computadora de internet

Direcciones	Elementos de configuración
209.165.200.238	Dirección IPv4
255.255.255.248	Máscara de subred para IPv4
209.165.200.233	Gateway predeterminado
2001:DB8:ACAD:A::38/64	Dirección IPv6/subred
2001:DB8:ACAD:A::1	Gateway predeterminado IPv6

Fuente: Propia

Paso 2: Configurar R1

se realiza la configuración básica del R1 que incluyen los siguientes códigos

Router(config)#No ip domain-look	Desactivar la búsqueda DNS
Router(config)#hostname R1	Nombre del router
R1(config)#enable secret class	Contraseña de exec privilegiado cifrada
R1(config)#line console 0	Acceso a la consola local
R1(config-line)#password cisco	Contraseña de acceso a la consola
R1(config-line)#login	Se active la contraseña local de consola

Contraseña de acceso Telnet

R1(config-line)#line vty 0 4	Modo de configuración de vty
R1(config-line)#password cisco	Contraseña de acceso
R1(config-line)#login	Se activa el acceso
R1(config-line)#service password-encryption	Cifrar las contraseñas
R1(config)#banner motd #se prohibe el acceso no autorizado#	Mensaje MOTD
R1(config)#unicast-routing	Habilitar IPv6
R1(config)#int s0/0/0	Acceder a la Interfaz S0/0/0
R1(config-if)#description RED S0/0/0 R1	Establezca la descripción
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Establecer la dirección IPv4
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64	Establecer la dirección IPv6
R1(config-if)#clock rate 128000	Frecuencia de reloj en 128000
R1(config-if)#NO SHUtdown	Activar la interfaz
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0	ruta IPv4 predeterminada de S0/0/0
R1(config)#ipv6 route ::/0 s0/0/0	ruta IPv6 predeterminada de S0/0/0

Paso 3: Configuración R2

se realiza la configuración básica del R2 que incluyen los siguientes códigos

Router(config)#no ip domain-lookup	Desactivar la búsqueda DNS
Router(config)#hostname R2	Nombre del router
R2(config)#enable secret class	Contraseña de exec privilegiado cifrada
R2(config)#line console 0	Acceso a la consola local
R2(config-line)#password cisco	Contraseña de acceso
R2(config-line)#login	Se active la contraseña local
Contraseña de acceso Telnet	
R2config-line)#line vty 0 15	Modo de configuración de vty
R2(config-line)#password cisco	Contraseña para acceder
R2(config-line)#login	Se activa el acceso
R2(config-line)#service password-encryption	Cifrar las contraseñas
R2(config)#banner motd #se prohibe el acceso no autorizado#	Mensaje MOTD

R2(config-line)#ip http server “comando para habilitar http no soportado
R2(config)#ipv6 unicast-routing Habilitar IPv6
R2(config)#int s0/0/0 Acceder a la Interfaz S0/0/0
R2(config-if)#description RED s0/0/0 R2 a R1 s0/0/0 Establezca la descripción
R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establecer la dirección IPv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Establecer la dirección IPv6
R2(config-if)#no shutdown Activar la interfaz
R2(config)#int s0/0/1 Acceder a la Interfaz S0/0/1
R2(config-if)#description RED DCE S0/0/1 R2 A R3 S0/0/1 Establezca la descripción
R2(config-if)#ip address 172.16.2.2 255.255.255.252 la dirección IPv4
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 la dirección IPv6
R2(config-if)#clock rate 128000 Frecuencia de reloj en 128000
R2(config-if)#NO SHUtdown Activar la interfaz
R2(config)#int g0/0 Acceder Interfaz G0/0
R2(config-if)#description Interfaz g0/0 conexion al Servidor internet. Descripción
R2(config-if)#ip address 209.165.200.233 255.255.255.248 Dirección IPv4.
2(config-if)# ipv6 add 2001:DB8:ACAD:A::1/64 Dirección IPv6.
R2(config-if)#no shutdown Activar la interfaz
R2(config)#int lo0 Crear Interfaz loopback 0
R2(config-if)#IP ADDress 10.10.10.10 255.255.255.255 Asignar dirección
R2(config-if)#description servidor web Establecer la descripción

R2(config-if)# ip route 0.0.0.0 0.0.0.0 g0/0 Ruta IPv4 predeterminada de G0/0
R2(config)#ipv6 route ::/0 g0/0 Ruta IPv6 predeterminada de G0/0

Paso 4 Configurar R3

se realiza la configuración básica del R3 que incluyen los siguientes códigos

Router(config)#no ip domain-lookup Desactivar la búsqueda DNS
Router(config)#hostname R3 Nombre del router
R3(config)#enable secret class Contraseña de exec privilegiado cifrada
R3(config)#line console 0 Acceso a la consola local
R3(config-line)#password cisco Contraseña de acceso
R3(config-line)#login Se active la contraseña local
Contraseña de acceso Telnet
R3(config-line)#line vty 0 15 Acceso a modo de configuración de vty
R3(config-line)#password cisco Asignar contraseña
R3(config-line)#login Se activa el acceso
R3(config-line)#service password-encryption Cifrar las contraseñas
R3(config)#banner motd #se prohibe el acceso no autorizado# Mensaje motd

R3(config)#ipv6 unicast-routing	Habilitar Ipv6
R3(config)#int s0/0/1	Acceder a la interfaz S0/0/1
R3(config-if)#description red s0/0/1 R3	Establezca la descripción
R3(config-if)#ip address 172.16.2.1 255.255.255.252	Establecer la dirección IPv4
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64	Establecer la dirección IPv6
R3(config-if)#no shutdown	Activar la interfaz
R3(config-if)#int loopback 4	Crear Interfaz loopback 4
R3(config-if)#ip add 192.168.4.1 255.255.255.0	Establezca la dirección IPv4
R3(config-if)#int loopback 5	Crear Interfaz loopback 5
R3(config-if)#ip add 192.168.5.1 255.255.255.0	Establezca la dirección IPv4
R3(config-if)#int loopback 6	Crear Interfaz loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0	Establezca la dirección IPv4
R3(config-if)#interface loopback 7	Crear Interfaz loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64	Establezca la dirección IPv6
R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/1/	Ruta predeterminada s0/0/1 ipv4
R3(config)#ipv6 route ::/0 S0/0/1	Ruta predeterminada s0/0/1 ipv6

Paso 5 Configurar S1

Configuración básica del S1

Switch(config)#no ip domain-lookup	Desactivar la búsqueda DNS
Switch(config)#enable secret class	Contraseña de exec
Switch(config)#line console 0	Acceso a la consola local
Switch(config-line)#password cisco	Contraseña de acceso a la consola
Switch(config-line)#login	Se active la contraseña local
Switch(config-line)#line vty 0 15	Acceso a modo vty
Switch(config-line)#password cisco	Contraseña para acceder
Switch(config-line)#login	Se activa el acceso
Switch(config)#banner motd #Se prohibe el acceso no autorizado#Mensaje MOTD	
Switch(config)#hostname S1	Nombre del switch
S1(config)#service password-encryption	Encriptar contraseñas

Paso 6 Configurar S3

Configuración básica del S3

Switch(config)#no ip domain-lookup	Desactivar la búsqueda DNS
Switch(config)#hostname S3	Nombre del switch
S3(config)#enable secret class	Contraseña de exec
S3(config)#line console 0	Acceso a la consola local
S3(config-line)#password cisco	Contraseña de acceso a la consola

S3(config-line)#login Se active la contraseña local
S3(config-line)#line vty 0 4 Modo de configuración de vty
S3(config-line)#password cisco Contraseña para acceder
S3(config-line)#login Se activa el acceso
S3(config)#service password-encryption Encriptar contraseñas
S3(config)#banner motd #Se prohibe el acceso no autorizado# Mensaje MOTD

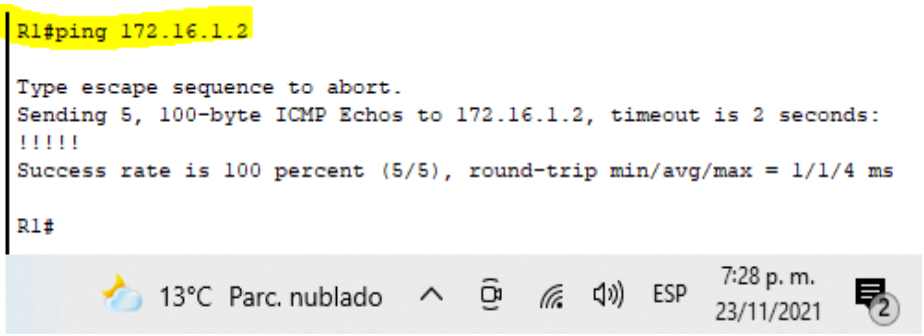
Paso 7: Verificar la conectividad de la red

Tabla 7 verificación de conectividad de la red

desde	a	Dirección ip	Resultados ping
R1	R2, S0/0/0	172.16.1.2	100 percent (5/5)
R2	R3, S0/0/1	172.16.2.2	100 percent (5/5)
PC de Internet	Gateway predeterminado	209.165.200.233	efectivo

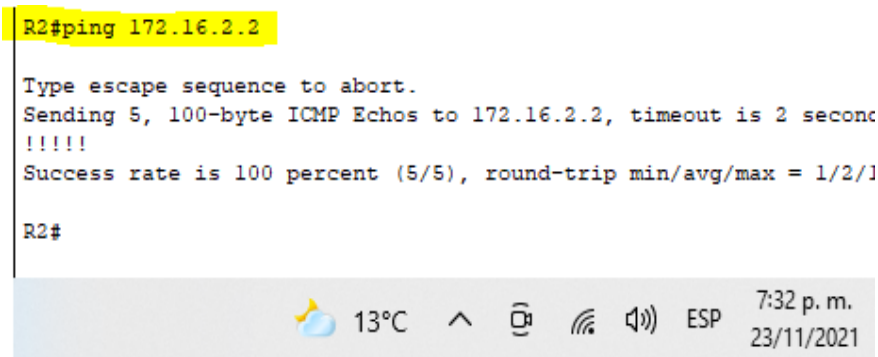
Fuente: Propia

Figura 5 Pantallazo ping de R1 A R2 S0/0/0



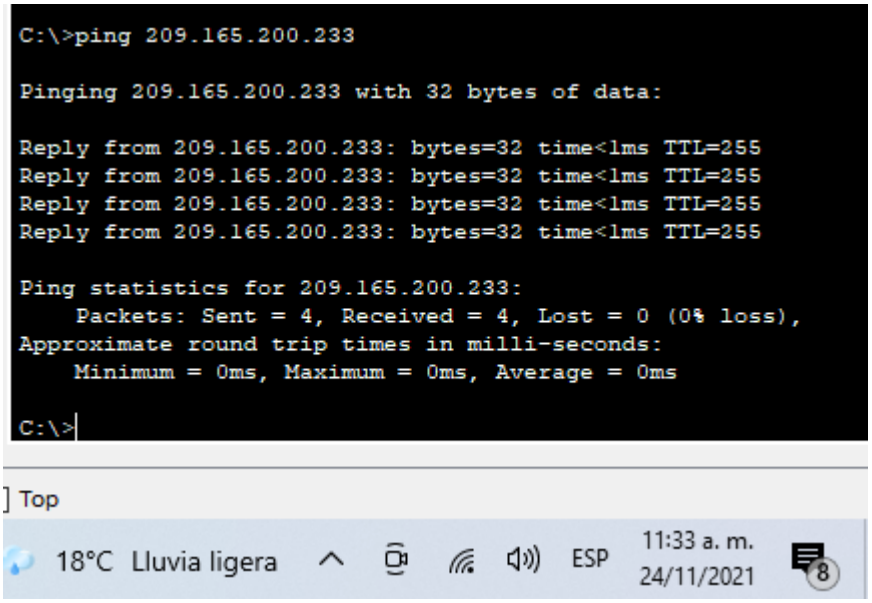
Fuente: Propia

Figura 6 Pantallazo ping R2 a R3 S0/0/1



Fuente: Propia

Figura 7 Ping Servidor web a Gateway



Fuente: Propia

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN
Paso 1: Configurar S1

Crear la base de datos de VLAN

S1(config)#vlan 21	Creación Vlan 21
S1(config-vlan)#name contabilidad	Asignando Nombre a la Vlan
S1(config-vlan)#vlan 23	Creación Vlan 23
S1(config-vlan)#name ingenieria	Asignando Nombre a la Vlan
S1(config-vlan)#vlan 99	Creación Vlan 99
S1(config-vlan)#name administración	Asignando Nombre a la Vlan

Asignar la dirección IP de administración.

S1(config-vlan)#int vlan 99	Entrar a la interfaz de vlan 99
S1(config-if)#ip add 192.168.99.2 255.255.255.0	Asignando Dirección ip
S1(config-if)#no shutdown	Activando la vlan

S1(config)#ip default-gateway 192.168.99.1 Asignar el gateway predeterminado

Forzar el enlace troncal en la interfaz F0/3, utilizando la red vlan 1 como nativa

S1(config)#int f0/3	Acceder a la interfaz
S1(config-if)#switchport mode trunk	Enlace truncal a la interfaz
S1(config-if)#switchport trunk native vlan 1	Asignando vlan 1 como nativa

Forzar el enlace troncal en la interfaz F0/5, utilizando a la red VLAN 1 como VLAN nativa

S1(config)#int f0/5	Acceder a la interfaz
S1(config-if)#switchport mode trunk	Enlace truncal a la interfaz
S1(config-if)#switchport trunk native vlan 1	Asignando vlan 1 como nativa

Configurar el resto de los puertos como puertos de acceso

S1(config-if)#int range f0/1-2	Se escoge el Puerto f0/1 y el f0/2
S1(config-if-range)#switchport mode access	Se asigna como puertos de acceso
S1(config-if-range)#int range f0/7-24	Se escoge el rango de puertos de f0/7 hasta f0/24
S1(config-if-range)#switchport mode access	Se asigna como puertos de acceso

Asignar F0/6 a la VLAN 21

S1(config)#int f0/6	Acceder a la interfaz
S1(config-if)#switchport mode access	Modo de acceso de la interfaz
S1(config-if)#switchport access vlan 21	Se le asigna la vlan 21 al f0/6

Apagar todos los puertos sin usar

S1(config)#int range f0/7-24	Rango de puertos de f0/7 hasta f0/24
S1(config-if-range)#shutdown	Apagar puertos

Paso 2: Configurar el S3

Crear la base de datos de VLAN

S3(config)#vlan 21	Creación Vlan 21
S3(config-vlan)#name contabilidad	Asignando Nombre a la Vlan
S3(config-vlan)#vlan 23	Creación Vlan 23
S3(config-vlan)#name ingenieria	Asignando Nombre a la Vlan
S3(config-vlan)#vlan 99	Creación Vlan 99
S3(config-vlan)#name administración	Asignando nombre a la Vlan

Asignar la dirección IP de administración

Asignar la dirección IP de administración.

S3(config-vlan)#int vlan 99	Entrar a la interfaz de vlan 99
S3(config-if)#ip add 192.168.99.3 255.255.255.0	Asignando dirección ip
S3(config-if)#no shutdown	Activando la vlan

S3(config)#ip default-gateway 192.168.99.1	Asignar el gateway predeterminado

Forzar el enlace troncal en la interfaz F0/3, utilizando la red vlan 1 como nativa

S3(config)#int f0/3	Acceder a la interfaz

S3(config-if)#switchport mode trunk Enlace truncal a la interfaz
S3(config-if)#switchport trunk native vlan 1 Asignando vlan 1 como nativa

Configurar el resto de los puertos como puertos de acceso
S3(config-if)#int range f0/1-2 Se escoge el Puerto f0/1 y el f0/2
S3(config-if-range)#switchport mode access Se asigna como puertos de acceso
S3(config-if-range)#int range f0/4-17 Se escoge el rango de puertos de f0/4 hasta f0/17
S3(config-if-range)#switchport mode access Se asigna como puertos de acceso
S3(config-if-range)#int range f0/19-24 Se escoge el rango de puertos de f0/19 Hasta f0/24
S3(config-if-range)#switchport mode access Se asigna como puertos de acceso

Asignar F0/18 a la VLAN 21
S3(config)#int f0/18 Acceder a la interfaz
S3(config-if)#switchport mode access Modo de acceso de la interfaz
S3(config-if)#switchport access vlan 21 Se le asigna la vlan 21 al f0/18

Apagar todos los puertos sin usar
S3(config-if)#int range f0/1-2 Rango de puertos de f0/1 hasta f0/2
S3(config-if-range)#shutdown Apagar puertos
S3(config-if-range)#int range f0/4-17
S3(config-if-range)#shutdown Apagar puertos
S3(config-if-range)#int range f0/19-24
S3(config-if-range)#shutdown Apagar puertos

Paso 3: Configurar R1

R1(config)#int g0/1.21 Crear subinterfaz 802.1Q .21 en G0/1
description LAN contabilidad Descripción: LAN de Contabilidad
R1(config-subif)#encapsulation dot1Q 21 Asignar la VLAN 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Asignar dirección

R1(config)#int g0/1.23 Crear subinterfaz 802.1Q .23 en G0/1
R1(config-subif)#description Lan ingenieria Descripción: LAN de Ingeniería
R1(config-subif)#encapsulation dot1Q 23 Asignar la VLAN 23
R1(config-subif)#ip add 192.168.23.1 255.255.255.0 Asignar dirección

R1(config-subif)#int g0/1.99 Crear la subinterfaz 802.1Q .99 en G0/1
R1(config-subif)#description Lan administracion Descripción: LAN
R1(config-subif)#encapsulation dot1Q 99 Asignar la VLAN 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Asignar dirección
R1(config)#int g0/1 Acceder a la interfaz g0/1

R1(config-if)#no shutdown Activar la interfaz G0/1

Al darle al comando no shutdown a la interfaz GigabitEthernet0/1, no solamente se subió esa interfaz sino también las subinterfaces GigabitEthernet0/1.21, GigabitEthernet0/1.23 y GigabitEthernet0/1.99, ahora se encuentran activas, creando las subinterfaces se intentaba activar, no permitiendo, pero cuando se activó la interfaz global se activaron las otras interfaces.

Paso 4: Verificar la conectividad de la red

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

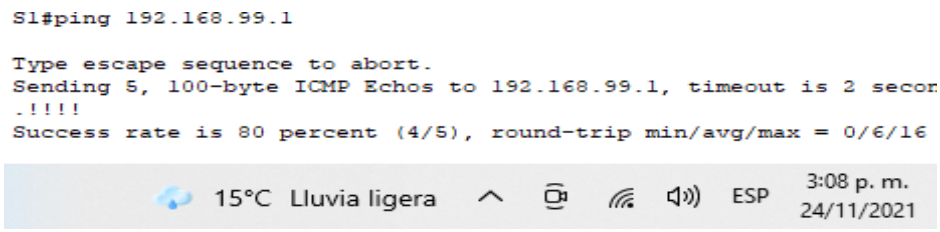
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8 Verificación de conectividad de los switchs

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

Fuente: Propia

Figura 8 ping S1 a R1



Fuente: Propia

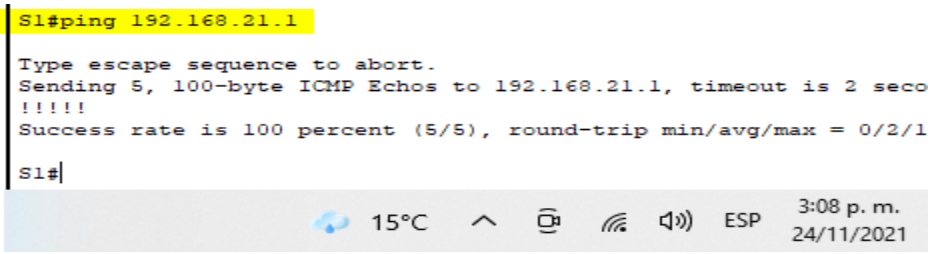
Figura 9 ping S3 a R1 VLAN 99

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

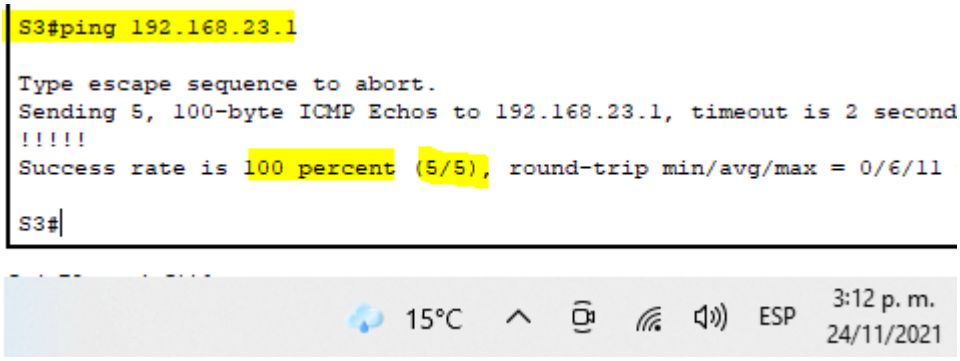
Fuente: Propia

Figura 10 Ping S1 a R1 VLAN 21



Fuente: Propia

Figura 11 S3 A R1 VLAN 23



Fuente: Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

R1(config)#router ospf 10 Configurar OSPF área 0

Anunciar las redes conectadas directamente
Asigne todas 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

Desactive la sumarización automática
R1(config-router)#no auto-summary "Comando no soportado"

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

R2(config)#router ospf 10 Configurar OSPF área 0

Anunciar las redes conectadas directamente
R2(config-router) #network 172.16.1.0 0.0.0.3 area 0
R2(config-router) #network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.232 0.0.0.7 area 0

Establecer la interfaz loopback 0 como pasivas
R2(config-router)#passive-interface lo0 La interfaz LAN (loopback) como pasiva

Desactive la sumarización automática
R2(config-router)#no auto-summary "comando no soportado

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Configurar OSPF área 0 R3
R3(config-if)#router ospf 10

Anunciar redes IPv4 conectadas directamente
R3(config-router) #network 172.16.2.0 0.0.0.3 area 0
R3(config-router) #network 192.168.4.0 0.0.0.255 area 0
R3(config-router) #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 de LAN IPv4 (Loopback) como pasivas
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6

Desactive la sumarización automática
R3(config-router)#no auto-summary Desactive la sumarización automática

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:

- ¿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 .
  Figura 12 Show ip protocols R1

```
R1#Show Ip Protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10          110      00:22:59
    192.168.6.1          110      00:22:36
    192.168.99.1         110      00:24:52
  Distance: (default is 110)
```

Fuente: Propia

- ¿Qué comando muestra solo las rutas OSPF?
  Show ip route ospf

Figura 13 Show ip route ospf

```
R1#Show ip route ospf
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.2.0 [110/128] via 172.16.1.2, 12:32:18, Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/129] via 172.16.1.2, 12:30:25, Serial0/0/0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/129] via 172.16.1.2, 12:30:14, Serial0/0/0
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/129] via 172.16.1.2, 12:30:03, Serial0/0/0
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.232 [110/65] via 172.16.1.2, 12:32:00, Serial0/0/0
```

Fuente: Propia

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

  show running-config. Y Show ip ospf database

Figura 14 Show ip ospf database R1

```
R1#Show ip ospf database
            OSPF Router with ID (192.168.99.1) (Process ID 10)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.99.1    192.168.99.1    176         0x8000000d 0x00a2db 5
10.10.10.10     10.10.10.10     64          0x8000000d 0x000f54 5
192.168.6.1     192.168.6.1     39          0x8000000d 0x00b5fe 5
R1#
```

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:

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.
R1(config)#ip dhcp pool ACCT Nombre: ACCT
R1(dhcp-config) #network 192.168.21.0 255.255.255.0
R1(dhcp-config) #dns-server 10.10.10.10 Servidor DNS: 10.10.10.10
R1(dhcp-config) #ip domain-name ccna-sa.com Dominio: ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1 Gateway predeterminado

Crear un pool de DHCP para la VLAN 23
R1(config)#ip dhcp pool ENGNR Nombre: ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10 Servidor DNS: 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com Nombre de dominio: ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1 Gateway predeterminado

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

La configuración del R2 incluye las siguientes tareas:
Crear una base de datos local con una cuenta de usuario
R2(config)#username webuser privilege 15 password cisco12345 Cuenta Usuario

Habilitar el servicio del servidor HTTP
Comando no soportado

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación
Comando no soportado

Crear una NAT estática al servidor web.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238

Asignar la interfaz interna y externa para la NAT estática
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#int lo0
R2(config-if)#ip nat inside

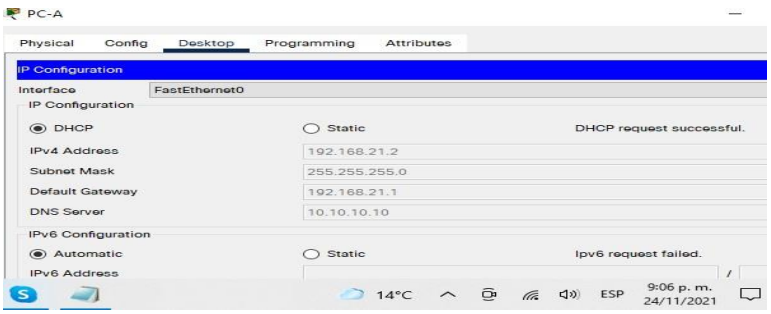
Configurar la NAT dinámica dentro de una ACL privada
Lista de acceso: 1
Permitir redes de Contabilidad
R2(config)#access-list 1 permit 192.68.21.0 0.0.0.255
permitir redes de Ingeniería
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

Defina el pool de direcciones IP públicas utilizables.
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

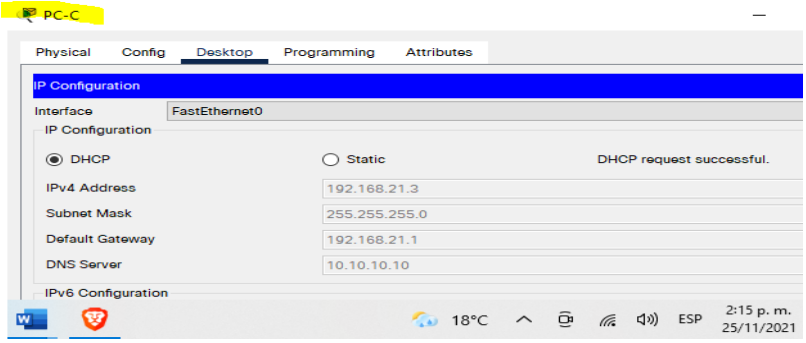
Paso 3: Verificar el protocolo DHCP y la NAT estática
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Figura 15 Pantallazo ip PC-A por DHCP



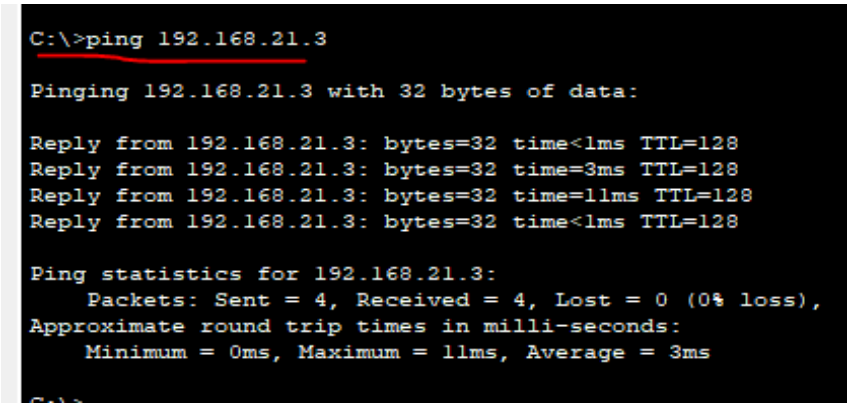
Fuente: Propia

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP
Figura 16 Pantallazo ip PC-C por DHCP



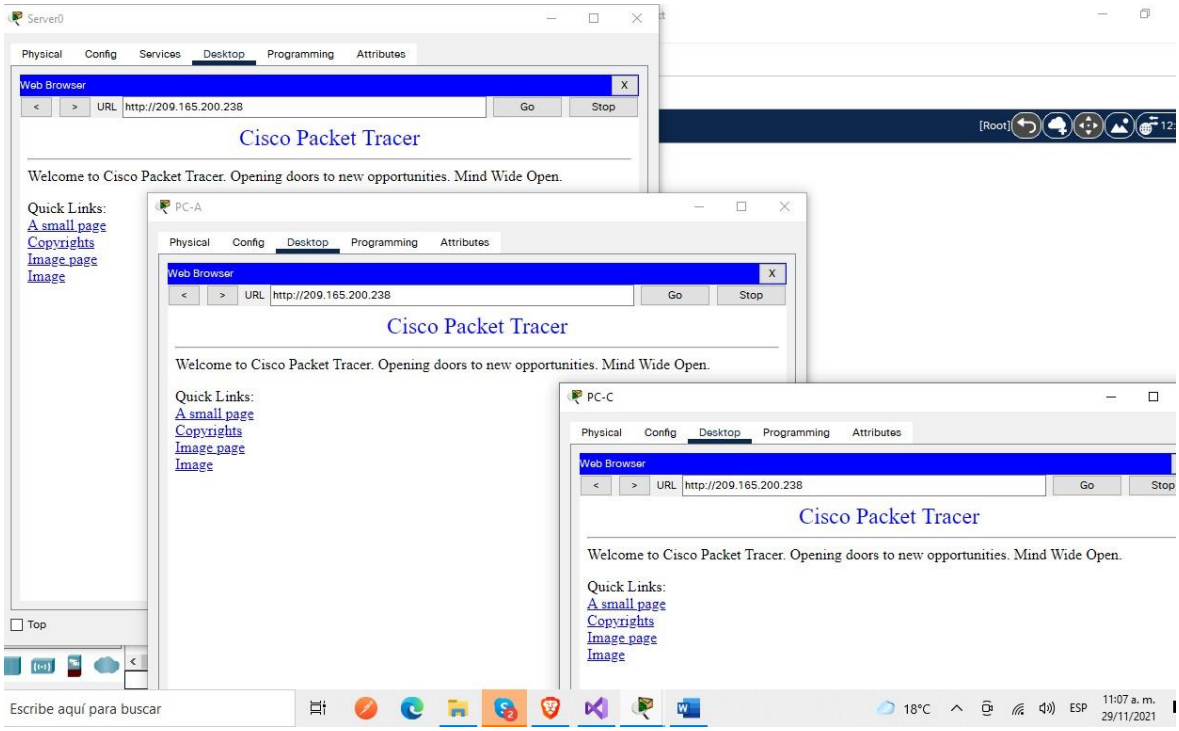
Fuente: Propia

Figura 17 Ping la PC-A pueda hacer ping a la PC-C



Fuente: Propia

Figura 18 acceder al servidor web (209.165.200.238)



Fuente: Propia

Parte 6: Configurar NTP

Ajuste la fecha y hora en R2.

R2#clock set 09:00:00 05 march 2016 5 de marzo de 2016, 9 a. m.

Configure R2 como un maestro NTP.

R2(config)#ntp master 5 Nivel de estrato: 5

R1(config)#ntp server 172.16.1.2 Configurar R1 como un cliente NTP.

Servidor:

R1(config)#ntp update-calendar actualizaciones de calendario periódicas con hora NTP.

Verifique la configuración de NTP en R1

Figura 19 show ntp associations

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
*~172.16.1.2    127.127.1.1     5    10       16      377    5.00           4.00
 ~127.127.1.1   .LOCL.          4    10       64      377    0.00           0.00
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

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

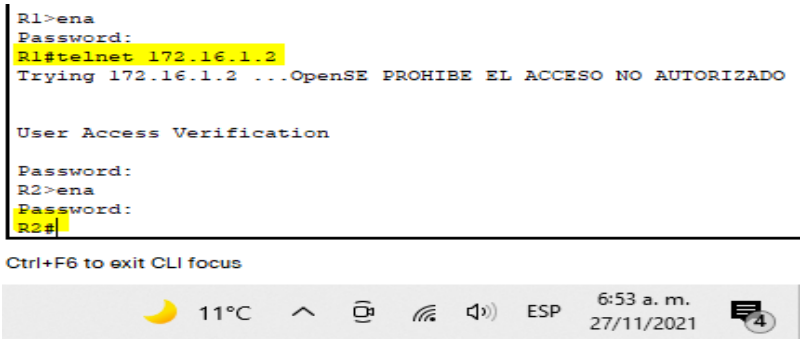
Paso 1: Restringir el acceso a las líneas VTY en el R2

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2
Nombre de la ACL: ADMINMGT

R2(config)#ip access-list standard ADMIN-MGT

Aplicar la ACL con nombre a las líneas VTY
R2(config-std-nacl)#permit host 172.16.1.1

Aplicar la ACL con nombre a las líneas VTY
Permitir acceso por Telnet a las líneas de VTY
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
Figura 20 Verificación ACL telnet



Fuente: Propia

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

- Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

  Show access list

Figura 21 show acces list R2

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255 (12 match(es))
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1

R2#
```

Fuente: Propia

- 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

- ¿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.

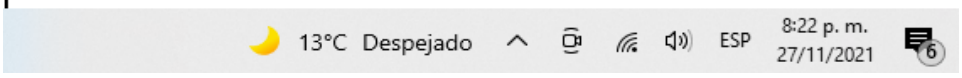
  Show ip nat translations

- ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

  Clear ip nat translation

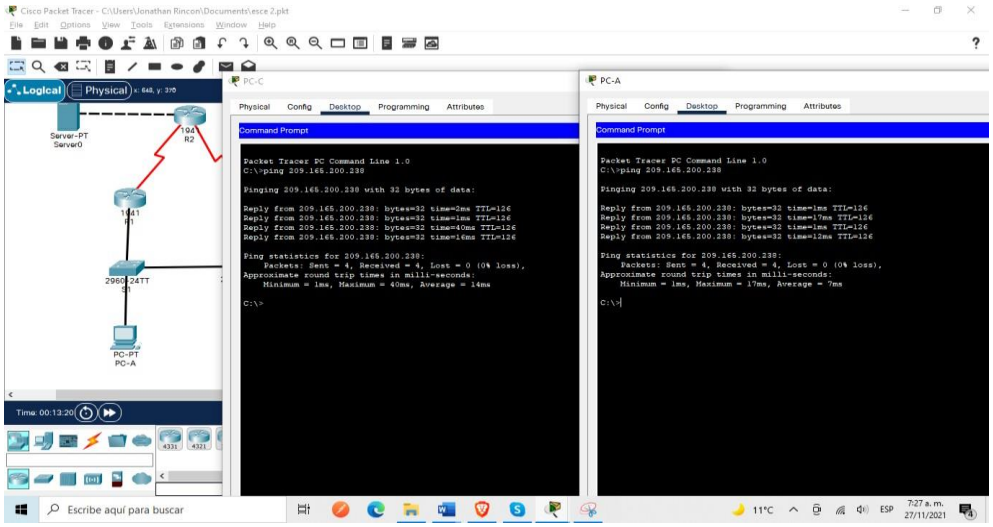
Figura 22 show ip nat translations

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.233:4 192.168.21.22:4    209.165.200.238:4  209.165.200.238:4
icmp 209.165.200.233:8 192.168.21.22:8    209.165.200.238:8  209.165.200.238:8
icmp 209.165.200.233:9 192.168.21.22:9    209.165.200.238:9  209.165.200.238:9
icmp 209.165.200.234:12192.168.21.21:12   209.165.200.238:12 209.165.200.238:12
icmp 209.165.200.234:13192.168.21.21:13   209.165.200.238:13 209.165.200.238:13
icmp 209.165.200.234:5 192.168.21.21:5    209.165.200.238:5  209.165.200.238:5
---  209.165.200.238   10.10.10.10        ---                ---
```



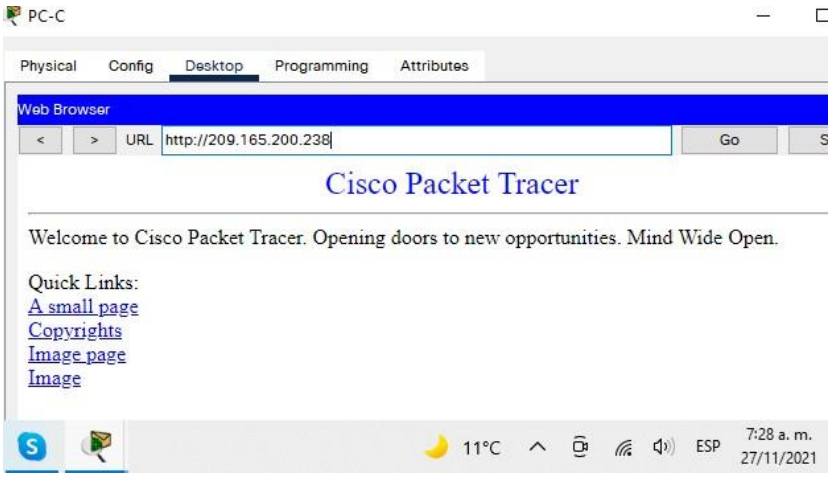
Fuente: Propia

Figura 23 Ping de pc -a y pc -c así el servidor



Fuente: Propia

Figura 24 Se accede al servidor web desde el pc-c



Fuente: Propia

CONCLUSIONES

Realizando este informe de grado aporto unas excelentes bases de configuración de dispositivos de red, identificando el proceso y los comandos necesarios para administrar y configurar, una red pequeña como también una red de gran tamaño, minimizando la transmisión y tráfico de datos por medios de conexión, creando igualmente vlan en los switches, en los router se creó interfaces con la norma IEEE 802.1Q para las vlan e interfaces.

Se realiza la configuración de las redes y su implementación cumpliendo con los requerimientos establecidos según la aplicación de prueba de habilidades CCNA, aplicando todo el conocimiento adquirido durante el diplomado, aplicando los comandos show para verificar su exactitud y veracidad de la configuración de los dispositivos de red utilizando el simulador de packet tracer

Se demuestra el conocimiento adquirido durante 4 meses estudiando el CCNA I y el CCNA II, del diplomado de profundización, con todos los aspectos como los protocolos de enrutamiento, routing entre vlan, el protocolo de routing dinámico OSPF y OSPFv3, 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.

REFERENCIAS BIBLIOGRÁFICAS

[1] VESGA, J. Diseño y configuración de redes con Packet Tracer [OVA]. (2014).

[2] CISCO. “Protocolos y comunicaciones de red. Fundamentos de Networking”. (2019).

[3] CISCO. “Capa de red. Fundamentos de Networking”. (2019).

[4] CISCO. “División de redesIP en subredes. Fundamentos de Networking. (2019).

[5] UNAD. “Configuración de Switches y Routers [OVA] (2017).

[6] CISCO. “Redes Conmutadas. Principios de Enrutamiento y Conmutación. (2019).

[7] UNAD. Principios de Enrutamiento [OVA]. (2017).

[8] CISCO. “VLAN Principios de Enrutamiento y Conmutación”. (2019).

[9] CISCO. “Listas de Control de Acceso. Principios de Enrutamiento y Conmutación”. (2019).

[10] CISCO. “DHCP Principios de Enrutamiento y Conmutación”. 2019).

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] CISCO. “NAT para IPv4. Principios de Enrutamiento y Conmutación”. (2019).