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

EIDER LUIS JULIO SALAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
MONTERIA
2021

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

EIDER LUIS JULIO SALAS

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

TUTOR:
RAÚL BAREÑO GUTIÉRREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
MONTERIA
2021

Nota de Aceptación

Presidente del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Montería, 20 de noviembre de 2021

AGRADECIMIENTOS

El desarrollo del presente trabajo fue realizado bajo la supervisión de la tutora NANCY AMPARO GUACA y el tutor RAUL BAREÑO GUTIÉRREZ, a quienes de forma grata les hago un profundo agradecimiento, por su dedicación, compromiso y entrega que tuvieron en toda la realización del Diplomado, generando espacios de interacción sincrónicos y asincrónicos que permitieron alcanzar los objetivos trazados.

CONTENIDO

Pág.
1. INTRODUCCIÓN 16
2. DESARROLLO 17
2.1. ESCENARIO 1 17
2.1.1. Topología 17
2.1.2. Objetivos 17
2.1.3. Aspectos básicos/situación 17
2.1.4. Parte 1: Construya La Red 18
2.1.5. Parte 2: Desarrolle el esquema de direccionamiento IP 18
2.1.5.1. Subneting para LAN 1 cálculo de 100 host requeridos. 19
2.1.5.2. Subneting para LAN 2 cálculo de 50 host requeridos. 19
2.1.6. Parte 3: Configure aspectos básicos 21
2.1.6.1. Paso 1: configurar los ajustes básicos de R1 21
2.1.6.1.1. Desactivar la búsqueda DNS 22
2.1.6.1.2. Nombre del Router 22
2.1.6.1.3. Nombre de dominio 22
2.1.6.1.4. Contraseña cifrada para el modo EXEC privilegiado 22
2.1.6.1.5. Contraseña de acceso a la consola 23
2.1.6.1.6. Establecer la longitud mínima para las contraseñas 23
2.1.6.1.7. Crear un usuario administrativo en la base de datos local 23
2.1.6.1.8. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local 23
2.1.6.1.9. Configurar VTY solo aceptando SSH 24
2.1.6.1.10. Cifrar las contraseñas de texto no cifrado 24
2.1.6.1.11. Configure un MOTD Banner 24
2.1.6.1.12. Configurar interfaz G0/0/0 24
2.1.6.1.13. Configurar interfaz G0/0/1 24
2.1.6.1.14. Generar una clave de cifrado RSA 25
2.1.6.2. Paso 1: configurar los ajustes básicos de S1 25

2.1.6.2.1. Desactivar la búsqueda DNS. 26
2.1.6.2.2. Nombre del Switch 26
2.1.6.2.3. Nombre de dominio 26
2.1.6.2.4. Contraseña cifrada para el modo EXEC privilegiado 26
2.1.6.2.5. Contraseña de acceso a la consola 26
2.1.6.2.6. Crear un usuario administrativo en la base de datos local 27
2.1.6.2.7. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local 27
2.1.6.2.8. Configurar las líneas VTY para que acepten únicamente las conexiones SSH 27
2.1.6.2.9. Cifrar las contraseñas de texto no cifrado 28
2.1.6.2.10. Configurar un MOTD Banner 28
2.1.6.2.11. Generar una clave de cifrado RSA 28
2.1.6.2.12. Configurar la interfaz de administración (SVI) 28
2.1.6.2.13. Configuración del gateway predeterminado 28
2.1.6.3. Paso 2. Configurar los equipos 29
2.2. ESCENARIO 2 34
2.2.1. Topología 34
2.2.2. Inicializar y volver a cargar los routers y los switches 34
2.2.2.1. Eliminar el archivo startup-config de todos los Routers y Volver a cargar todos los Routers. 35
2.2.2.2. Eliminar el archivo startup-config de todos los Switches, eliminar la base de datos de VLAN anterior y volver a cargar ambos Switches. 35
2.2.2.3. Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches. 36
2.2.3. Configurar la computadora de Internet 36
2.2.4. Configurar R1 37
2.2.4.1. Desactivar la búsqueda DNS 38
2.2.4.2. Nombre del Router 38
2.2.4.3. Contraseña de exec privilegiado cifrada 38
2.2.4.4. Contraseña de acceso a la consola 38

2.2.4.5. Contraseña de acceso Telnet 38
2.2.4.6. Cifrar las contraseñas de texto no cifrado 39
2.2.4.7. Mensaje MOTD 39
2.2.4.8. Interfaz S0/0/0 39
2.2.4.9. Rutas predeterminadas 40
2.2.5. Configurar R2 40
2.2.5.1. Desactivar la búsqueda DNS 41
2.2.5.2. Nombre del Router 42
2.2.5.3. Contraseña de exec privilegiado cifrada 42
2.2.5.4. Contraseña de acceso a la consola 42
2.2.5.5. Contraseña de acceso Telnet 42
2.2.5.6. Cifrar las contraseñas de texto no cifrado 43
2.2.5.7. Mensaje MOTD 43
2.2.5.8. Habilitar el servidor HTTP 43
2.2.5.9. Interfaz S0/0/0 43
2.2.5.10. Interfaz S0/0/1 44
2.2.5.11. Interfaz G0/0 (simulación de Internet) 44
2.2.5.12. Interfaz loopback 0 (servidor web simulado) 44
2.2.5.13. Rutas predeterminadas 45
2.2.6. Configurar R3 45
2.2.6.1. Desactivar la búsqueda DNS 46
2.2.6.2. Nombre del Router 46
2.2.6.3. Contraseña de exec privilegiado cifrada 46
2.2.6.4. Contraseña de acceso a la consola 47
2.2.6.5. Contraseña de acceso Telnet 47
2.2.6.6. Cifrar las contraseñas de texto no cifrado 47
2.2.6.7. Mensaje MOTD 48
2.2.6.8. Interfaz S0/0/1 48
2.2.6.9. Interfaz loopback 4 48
2.2.6.10. Interfaz loopback 5 48

2.2.6.11. Interfaz loopback 6 48
2.2.6.12. Interfaz loopback 7 49
2.2.6.13. Rutas predeterminadas 49
2.2.7. Configurar S1 49
2.2.7.1. Desactivar la búsqueda DNS 50
2.2.7.2. Nombre del Router 50
2.2.7.3. Contraseña de exec privilegiado cifrada 50
2.2.7.4. Contraseña de acceso a la consola 50
2.2.7.5. Contraseña de acceso Telnet 51
2.2.7.6. Cifrar las contraseñas de texto no cifrado 51
2.2.7.7. Mensaje MOTD 51
2.2.8. Configurar S3 51
2.2.8.1. Desactivar la búsqueda DNS 52
2.2.8.2. Nombre del Router 52
2.2.8.3. Contraseña de exec privilegiado cifrada 52
2.2.8.4. Contraseña de acceso a la consola 53
2.2.8.5. Contraseña de acceso Telnet 53
2.2.8.6. Cifrar las contraseñas de texto no cifrado 53
2.2.8.7. Mensaje MOTD 53
2.2.9. Verificar la conectividad de la red 54
2.2.10. Configurar la seguridad del switch, las VLAN y el routing entre VLAN 55
2.2.10.1. Configurar S1 55
2.2.10.1.1. Crear la base de datos de VLAN 56
2.2.10.1.2. Asignar la dirección IP de administración 56
2.2.10.1.3. Asignar el gateway predeterminado 56
2.2.10.1.4. Forzar el enlace troncal en la interfaz F0/3 57
2.2.10.1.5. Forzar el enlace troncal en la interfaz F0/5 57
2.2.10.1.6. Configurar el resto de los puertos como puertos de acceso 57
2.2.10.1.7. Asignar F0/6 a la VLAN 21 57

2.2.10.1.8. Apagar todos los puertos sin usar 57
2.2.10.2. Configurar S3 58
2.2.10.2.1. Crear la base de datos de VLAN 58
2.2.10.2.2. Asignar la dirección IP de administración 59
2.2.10.2.3. Asignar el gateway predeterminado 59
2.2.10.2.4. Forzar el enlace troncal en la interfaz F0/3 59
2.2.10.2.5. Configurar el resto de los puertos como puertos de acceso 59
2.2.10.2.6. Asignar F0/18 a la VLAN 23 60
2.2.10.2.7. Apagar todos los puertos sin usar 60
2.2.10.3. Configurar R1 60
2.2.10.3.1. Configurar la subinterfaz 802.1Q .21 en G0/1 61
2.2.10.3.2. Configurar la subinterfaz 802.1Q .23 en G0/1 61
2.2.10.3.3. Configurar la subinterfaz 802.1Q .99 en G0/1 61
2.2.10.3.4. Activar la interfaz G0/1 61
2.2.10.4. Verificar la conectividad de la red 62
2.2.11. Configurar el protocolo de routing dinámico OSPF 63
2.2.11.1. Configurar OSPF área 0, establecer todas las interfaces LAN como pasivas 63
2.2.11.2. Establecer todas las interfaces LAN como pasivas y desactive la sumarización automática. 65
2.2.12. Configurar OSPFv3 en el R2 66
2.2.12.1. Configurar OSPF área 0, Anunciar redes IPv6 conectadas directamente, Establecer todas las interfaces de LAN IPv6 (Loopback) como pasivas y Desactive la sumarización automática. 66
2.2.13. Verificar la información de OSPF 67
2.2.14. Implementar DHCP y NAT para IPv4 69
2.2.14.1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 69
2.2.14.1.1. Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas 70
2.2.14.1.2. Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas 70

2.2.14.1.3. Crear un pool de DHCP para la VLAN 21. 70
2.2.14.1.4. Crear un pool de DHCP para la VLAN 23 70
2.2.14.2. Configurar la NAT estática y dinámica en el R2 71
2.2.14.2.1. Crear una base de datos local con una cuenta de usuario..... 72
2.2.14.2.2. Habilitar el servicio del servidor HTTP 72
2.2.14.2.3. Configurar el servidor HTTP para utilizar la base de datos local para la autenticación 72
2.2.14.2.4. Crear una NAT estática al servidor web. 72
2.2.14.2.5. Asignar la interfaz interna y externa para la NAT estática..... 72
2.2.14.2.6. Configurar la NAT dinámica dentro de una ACL privada 73
2.2.14.2.7. Defina el pool de direcciones IP públicas utilizables. 73
2.2.14.2.8. Definir la traducción de NAT dinámica 73
2.2.15. Verificar el protocolo DHCP y la NAT estática 74
2.2.15.1. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP……. 75
2.2.15.2. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP……. 75
2.2.15.3. Verificar que la PC-A pueda hacer ping a la PC-C 76
2.2.15.4. Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345 76
2.2.16. Configurar NTP 77
2.2.16.1. Ajuste la fecha y hora en R2. 77
2.2.16.2. Configure R2 como un maestro NTP 78
2.2.16.3. Configurar R1 como un cliente NTP. 78
2.2.16.4. Configure R1 para actualizaciones de calendario periódicas con hora NTP……. 78
2.2.16.5. Verifique la configuración de NTP en R1. 78
2.2.17. Configurar y verificar las listas de control de acceso (ACL) 79
2.2.17.1. Restringir el acceso a las líneas VTY en el R2 79

2.2.17.1.1. Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2. 79
2.2.17.1.2. Aplicar la ACL con nombre a las líneas VTY 79
2.2.17.1.3. Permitir acceso por Telnet a las líneas de VTY 79
2.2.17.1.4. Verificar que la ACL funcione como se espera 80
2.2.17.2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente…. 80
CONCLUSIÓN 83
BIBLIOGRAFÍA 84

LISTA DE TABLAS

Tabla 1: Tabla de referencia conversión a números binarios ---------- 19
Tabla 2: Tabla de direccionamiento ---------- 20
Tabla 3: Tareas de configuración para R1 ---------- 21
Tabla 4: Tareas de configuración S1 ---------- 25
Tabla 5: Configuración ipv4 PC-A ---------- 29
Tabla 6: Configuración IPV4 PC-B ---------- 30
Tabla 7: Iniciar Routers y Switches ---------- 34
Tabla 8: Datos de configuración ---------- 36
Tabla 9: Tareas de configuración ---------- 37
Tabla 10: Tareas de configuración ---------- 40
Tabla 11: Tareas de configuración ---------- 45
Tabla 12: Tareas de configuración ---------- 49
Tabla 13: Tareas de configuración ---------- 51
Tabla 14: Datos de conectividad ---------- 54
Tabla 15: Tareas de configuración ---------- 55
Tabla 16: Tareas de configuración ---------- 58
Tabla 17: Tareas de configuración ---------- 60
Tabla 18: Conectividad ---------- 62
Tabla 19: Tareas de configuración ---------- 63
Tabla 20: Tareas de configuración ---------- 66
Tabla 21: Verificación OSPF ---------- 67
Tabla 22: Tareas de configuración ---------- 69
Tabla 23: Tareas de configuración ---------- 71
Tabla 24: verificación de conectividad ---------- 74
Tabla 25: Tareas de configuración ---------- 77
Tabla 26: Tareas de configuración ---------- 79
Tabla 27: Verificación de configuración ---------- 80

LISTA DE FIGURAS

Figure 1: Topología de escenario 1---------- 17
Figure 2: Construcción de la red de acuerdo a la topología ---------- 18
Figure 3: Configuración IPV4---------- 29
Figure 4: Ejecución del comando ipconfig /all---------- 30
Figure 5: Ejecución del comando ping desde el PC-A al PC-B---------- 31
Figure 6: Ping desde la consola del router a la PC-A y PC-B---------- 32
Figure 7: ejecución del comando tracert a PC-B ---------- 33
Figure 8: ejecución del comando arp---------- 33
Figure 9: Topología escenario 2 ---------- 34
Figure 10: Estableciendo conectividad desde R1 a R2, S0/0/0 ---------- 54
Figure 11: Estableciendo conectividad desde R2 a R3, S0/0/1 ---------- 54
Figure 12: Estableciendo conectividad PC – Internet a Gateway predeterminado 55
Figure 13: Estableciendo conectividad desde S1 a R1, dirección VLAN 99 -------- 62
Figure 14: Estableciendo conectividad desde S3 a R1, dirección VLAN 99 -------- 62
Figure 15: Estableciendo conectividad desde S1 a R1, dirección VLAN 21 -------- 63
Figure 16: Estableciendo conectividad desde S3 a R1, dirección VLAN 23 -------- 63
Figure 17: Ejecución del comando show ip protocols ---------- 68
Figure 18: Ejecución del comando show ip route OSPF ---------- 68
Figure 19: Ejecución del comando show run---------- 69
Figure 20: Información del servidor DHCP en la PC-A ---------- 75
Figure 21: Información del servidor DHCP en la PC-A ---------- 75
Figure 22: Ping desde PC – A hasta PC – C---------- 76
Figure 23: Acceso al servidor web desde el PC-C---------- 76
Figure 24: Acceso al servidor web desde el PC-A---------- 77
Figure 21: configuración NTP en R1 ---------- 78
Figure 26: Acceso a R2 desde R1 ---------- 80
Figure 27: Ping PC-A al servidor de Internet ---------- 81
Figure 28: Ping PC-C al servidor de Internet---------- 82
Figure 29: verificación de la configuración NAT ---------- 82

GLOSARIO

RED TRONCAL (o network backbone): Es la parte de la infraestructura de red informática que interconecta diferentes redes, lo que les permite comunicarse entre sí, y proporciona una ruta para el intercambio de datos entre estas diferentes redes.

HTTP (Hypertext Transfer Protocol): Proporciona un estándar de protocolo de red que los navegadores web y los servidores usan para comunicarse.

ROUTER: conecta todos los equipos entre sí.

NAT (Network Address Translation): Es un intérprete o traductor de peticiones.

SUBNETTING: Es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

DNS (Sistema de Nombres de Dominio): Traduce los nombres de dominios aptos para lectura humana.

INTERFAZ DE RED: Es el software específico de red que se comunica con el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes.

SWITCH: Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus.

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

TELNET: Es un protocolo de red TCP/IP que es utilizado desde 1960 para establecer conexiones remotas con otros ordenadores, servidores, y dispositivos con un sistema compatible.

RESUMEN

Para el desarrollo del trabajo final del diplomado de profundización cisco Diseño e Implementación de Soluciones Integradas LAN / WAN se realizan dos escenarios utilizando el software de simulación Cisco Packet Tracer. En el primer escenario se configuran los dispositivos de una red pequeña Routers, Switches y PC; diseñando un esquema de direccionamiento IPV4 para las redes LAN y verificando la conectividad entre los componentes de la red.

En el desarrollo de segundo escenario se 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. Además, se describen los comandos del sistema operativo CISCO IOS presentes en los diferentes dispositivos que componen de red.

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

ABSTRACT

For the development of the final work of the cisco deepening diploma Design and Implementation of Integrated LAN / WAN Solutions two scenarios are carried out using the Cisco Packet Tracer simulation software. In the first scenario, the devices of a small network are configured: Routers, Switches and PCs; designing an IPV4 addressing scheme for LAN networks and verifying connectivity between network components.

In the second scenario development, you will configure a small network to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), dynamic and static network (NAT), access control lists (ACL), and network time protocol (NTP) server / client. In addition, the CISCO IOS operating system commands present in the different devices that make up the network are described.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics.

1. INTRODUCCIÓN

En el desarrollo del presente Escenario 1, concerniente a la construcción de una red y la configuración de sus componentes. Se plantea la construcción de una topología de red en el software de simulación Packet Tracer, donde se identificarán sus componentes físicos y sus medios de conexión. Para determinar el funcionamiento de la red se construyeron dos redes LAN 1 y LAN 2, las cuales se configurarán mediante direccionamiento IPV4 a través de una IP física asignada por el tutor. Para hallar los parámetros o datos de la red se utiliza el procedimiento de subneteo de redes donde se calcularán de forma manual las subredes presentes en cada una de las LAN.

Los datos de la red que estudiaremos serán: la IP de los diferentes hosts, la puerta de enlace o Gateway y la máscara de red, esta última importante para asegurar el envío de los paquetes entre las subredes.

Se propone en la red dada la configuración de sus componentes mediante la conexión de consola de los equipos Router, Switch y PCS; donde a través de la ejecución de comandos se realizará la configuración apropiada para el respectivo funcionamiento entre los equipos que forman las subredes, esto se verifica haciendo PING entre los hosts y verificando la recepción y envío de paquetes de datos.

En el desarrollo del presente Escenario 2, se utiliza el software de simulación CISCO PACKET TRACER donde se plantea una topología de red a la cual se le realizan diferentes configuraciones para lograr la conectividad y seguridad en la comunicación entre sus componentes. La topología propuesta está conformada por los dispositivos Routers, Switches, servidor de internet y PCS, a los cuales se les configura direccionamiento IPV4 e IPV6 en las interfaces aplicando protocolos como OSPF que mantienen la información topológica en un área y la conecta con el resto de las áreas, permitiendo encaminar paquetes a cualquier punto de la red, el traductor de direcciones NAT que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna, el protocolo de configuración dinámica de host DHCP que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP, entre otros. Además, se realiza la verificación de las conexiones realizando ping entre los diferentes dispositivos.

2. DESARROLLO

2.1. ESCENARIO 1

2.1.1. Topología

Figure 1: Topología de escenario 1

Fuente: propia

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

2.1.2. Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

2.1.3. Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección

suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

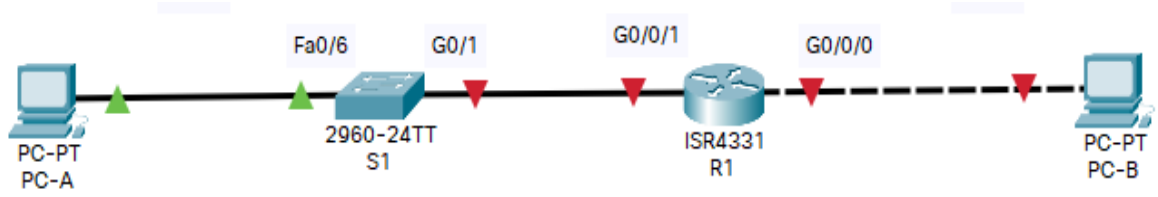
2.1.4. Parte 1: Construya La Red

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

- Dispositivos presentes en la red:
  PC-A
  PC-B
  Router (R1)
  Switch (S1)

- Medio de red
  Cable de conexión directa.
  Cable cruzado entre R1 y PC-B

Figure 2: Construcción de la red de acuerdo a la topología



Fuente: propia

2.1.5. Parte 2: Desarrolle el esquema de direccionamiento IP

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

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

Para este caso en particular los últimos dos números de mi cedula es el 58, lo que permite indicar que la dirección IPV4 dada es 192.168.58.0

2.1.5.1. Subneting para LAN 1 cálculo de 100 host requeridos.

Tenemos una dirección de clase C = 192.168.58.0, cuya mascara de red por defecto es 255.255.255.0/24 que expresada en notación binaria seria 11111111.11111111.11111111.00000000.

Tabla 1: Tabla de referencia conversión a números binarios

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Fuente: propia

Para calcular la cantidad de hosts aplicamos la siguiente formula:

$2^n - 2 = h$

$2^7 - 2 =$ **126**

n = cantidad de bits en cero o apagados

h = cantidad de host obtenidos

Para obtener la nueva mascara de red tenemos que:

255.255.255.128 /25 = 11111111.11111111.11111111.10000000.

Tenemos que las 100 direcciones de host de la red 192.168.58.0 se encuentran en el rango de:

192.168.58.1 - 192.168.58.127

Y la última utilizable es la 192.168.58.126

2.1.5.2. Subneting para LAN 2 cálculo de 50 host requeridos.

Aplicamos los mismos pasos del cálculo anterior, pero esta vez para la LAN 2. Tenemos una dirección de clase C = 192.168.58.0

$2^n - 2 = h$

$2^6 - 2 =$ **62**

Para obtener la nueva mascara de red tenemos que:

255.255.255.192 /26 = 11111111.11111111.11111111.11000000.

Tenemos que las 50 direcciones de host de la red 192.168.58.0 se encuentran en el rango de:
192.168.58.128 - 192.168.58.191

Y la última utilizable es la 192.168.58.190

Tabla 2: Tabla de direccionamiento

Item	**Requerimiento**
Dirección de Red	192.168.58.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1 = **192.168.58.1 - 255.255.255.128 /25**
R1 G0/0/0	Primera dirección de host de la subred LAN2 = **192.168.58.129 - 255.255.255.192 /26**
S1 SVI	Segunda dirección de host de la subred LAN1 = **192.168.58.2**
PC-A	Última dirección de host de la subred LAN1 = **192.168.58.126**
PC-B	Última dirección de host de la subred LAN2 = **192.168.58.190**

Fuente: propia

2.1.6. Parte 3: Configure aspectos básicos

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

2.1.6.1. Paso 1: configurar los ajustes básicos de R1

Tabla 3: Tareas de configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Ok
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: propia

2.1.6.1.1. Desactivar la búsqueda DNS

Para desactivar la búsqueda de DNS en el Router utilizamos los siguientes comandos por consola:

Router>enable	*Entrar al modo EXEC Privilegiado*
Router#configure terminal	*Entrar al modo configuración Global*
Router(config)#no ip domain-lookup	*Desactivar la búsqueda DNS*
Router(config)#exit	*Sale del modo de configuración*

2.1.6.1.2. Nombre del Router

Cambiamos el nombre del Router a R1 utilizando los siguientes comandos:

Router>enable	*Entrar al modo EXEC Privilegiado*
Router#configure terminal	*Entrar al modo configuración Global*
Router(config)#hostname R1	*Cambia el nombre del Router*
R1(config)#	*Sale del modo de configuración*

2.1.6.1.3. Nombre de dominio

Router>enable	*Entrar al modo EXEC Privilegiado*
Router#configure terminal	*Entrar al modo configuración Global*
R1(config)#ip domain-name ccna-lab.com	*Se define el nombre del dominio*
R1(config)#exit	*Sale del modo de configuración*

2.1.6.1.4. Contraseña cifrada para el modo EXEC privilegiado

El usuario debe ingresar la contraseña ciscoenpass

R1#configure terminal	*Entrar al modo configuración Global*
R1(config)#enable password ciscoenpass	*Configura la contraseña de acceso*
R1(config)#	

2.1.6.1.5. Contraseña de acceso a la consola

El usuario debe ingresar la contraseña ciscoenpass para acceder a la consola

R1(config)#line console 0 *Ingresa al modo de configuración*
R1(config-line)#password ciscoenpass *Configura la contraseña consola*
R1(config-line)#login *Nos pide autenticación al momento de iniciar*
R1(config-line)#exit *Sale del modo de configuración*

2.1.6.1.6. Establecer la longitud mínima para las contraseñas

Se establece como la longitud mínima de 10 caracteres para las contraseñas.

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
R1(config)#security password min-length 10 *Configura el tamaño mínimo*

2.1.6.1.7. Crear un usuario administrativo en la base de datos local

Nombre de usuario: **admin**
Password: **admin1pass**

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
R1(config)#username admin password admin1pass *Crea usuarios en la BD*

2.1.6.1.8. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
R1(config)#line vty 0 4 *Modo de configuración de la línea vty*
R1(config-line)#password ciscoenpass *Asignamos la contraseña*
R1(config-line)#login local *Para que pida el inicio de sesión al ingresar*

R1(config-line)#exit *Sale del modo de configuración*

2.1.6.1.9. Configurar VTY solo aceptando SSH

R1#configure terminal *Entrar al modo configuración Global*
R1(config)#enable password ciscoenpass *Asigna la contraseña*
R1(config)#ip domain-name ccna-lab.com *Se define el nombre del dominio*
R1(config)#crypto key generate rsa general-Keys modulus 1024
R1(config)#line VTY 0 15 *Modo configuración de la linea vty*
R1(config-line)#password ciscoenpass *Contraseña para ingresar a SSH*
R1(config-line)#login *Configura el inicio de sesión en la linea vty*
R1(config-line)#transport input ssh *Activa la linea SSH en VTY*
R1(config-line)#exit *Sale del modo de configuración*

2.1.6.1.10. Cifrar las contraseñas de texto no cifrado

R1(config-line)#service password-encryption *Cifrar las contraseñas*

2.1.6.1.11. Configure un MOTD Banner

Crear un mensaje para los usuarios de la red
Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
R1(config)#banner motd #Practica Escenario 1 # *Crear un mensaje*

2.1.6.1.12. Configurar interfaz G0/0/0

R1(config)#interface Gig0/0/0 *Configurar la interface*
R1(config-if)#ip address 192.168.58.129 255.255.255.192 *Asigna la ip*
R1(config-if)#no shutdown *Activa la interface*

2.1.6.1.13. Configurar interfaz G0/0/1

R1(config)#interface Gig0/0/1 *Configurar interface*

R1(config-if)#ip address 192.168.58.1 255.255.255.128 *Asigna ip*

R1(config-if)#no shutdown *Activa la interface*

2.1.6.1.14. Generar una clave de cifrado RSA

Router>enable *Entrar al modo EXEC Privilegiado*

Router#configure terminal *Entrar al modo configuración Global*

R1(config)#crypto key generate rsa general-keys modulus 1024 *Genera clave de cifrado*

2.1.6.2. Paso 1: configurar los ajustes básicos de S1

Tabla 4: Tareas de configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	**S1**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	
Configurar las líneas VTY para que acepten únicamentelas conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento

Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla dedireccionamiento.

Fuente: propia

2.1.6.2.1. Desactivar la búsqueda DNS.

Switch>enable *Entrar al modo EXEC Privilegiado*

Switch#configure terminal *Entrar al modo configuración Global*

Switch(config)#no ip domain-lookup *Desactiva busqueda DNS*

2.1.6.2.2. Nombre del Switch

Switch>enable *Entrar al modo EXEC Privilegiado*

Switch#configure terminal *Entrar al modo configuración Global*

Switch(config)#hostname S1 *Cambia el nombre del Router*

2.1.6.2.3. Nombre de dominio

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#ip domain name ccna-lab.com *Asignar dominio*

2.1.6.2.4. Contraseña cifrada para el modo EXEC privilegiado

Switch>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#enable secret ciscoenpass *Contraseña cifrada*

2.1.6.2.5. Contraseña de acceso a la consola

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#line console 0 *Modo de configuración linea de consola*

S1(config-line)#password ciscoconpass *Contraseña linea de consola*

S1(config-line)#login *Configura el inicio de sesión*

2.1.6.2.6. Crear un usuario administrativo en la base de datos local

Nombre de usuario: **admin**
Password: **admin1pass**

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#username admin password admin1pass *Crear usuario*

2.1.6.2.7. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#line vty 0 4 *Modo de configuración de la linea vty*
S1(config-line)#password ciscoenpass *Asigna una contraseña*
S1(config-line)#login local *Configura el inicio de sesión*
S1(config-line)#exit *Sale del modo de configuración*

2.1.6.2.8. Configurar las líneas VTY para que acepten únicamente las conexiones SSH

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1 (config)#enable password ciscoenpass *Asignación de una contraseña*
S1 (config)#line VTY 0 15 *Modo de configuración de la linea vty*
S1(config-line)#password ciscoenpass *Contraseña para ingresar a SSH*
S1 (config-line)#login *Configura el inicio de sesión*
S1(config-line)#transport input ssh *Activa la linea SSH en VTY*
S1 (config-line)# exit *Sale del modo de configuración*

2.1.6.2.9. Cifrar las contraseñas de texto no cifrado

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#service password-encryption *Cifra las contraseñas*

2.1.6.2.10. Configurar un MOTD Banner

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#banner motd #Practica Escenario 1 # *Crear un mensaje*

2.1.6.2.11. Generar una clave de cifrado RSA

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#crypto key generate rsa general-keys modulus 1024 *Genera la clave de cifrado RSA*

2.1.6.2.12. Configurar la interfaz de administración (SVI)

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#interface Vlan1 *Modo de configuración de la interface*

S1(config-if)#ip address 192.168.58.2 255.255.255.128 *Asigna la ip*

S1(config-if)#no shutdown *Activa la interface*

2.1.6.2.13. Configuración del gateway predeterminado

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#ip default-gateway 192.168.58.1 *Configuramos el Gateway*

2.1.6.3. Paso 2. Configurar los equipos

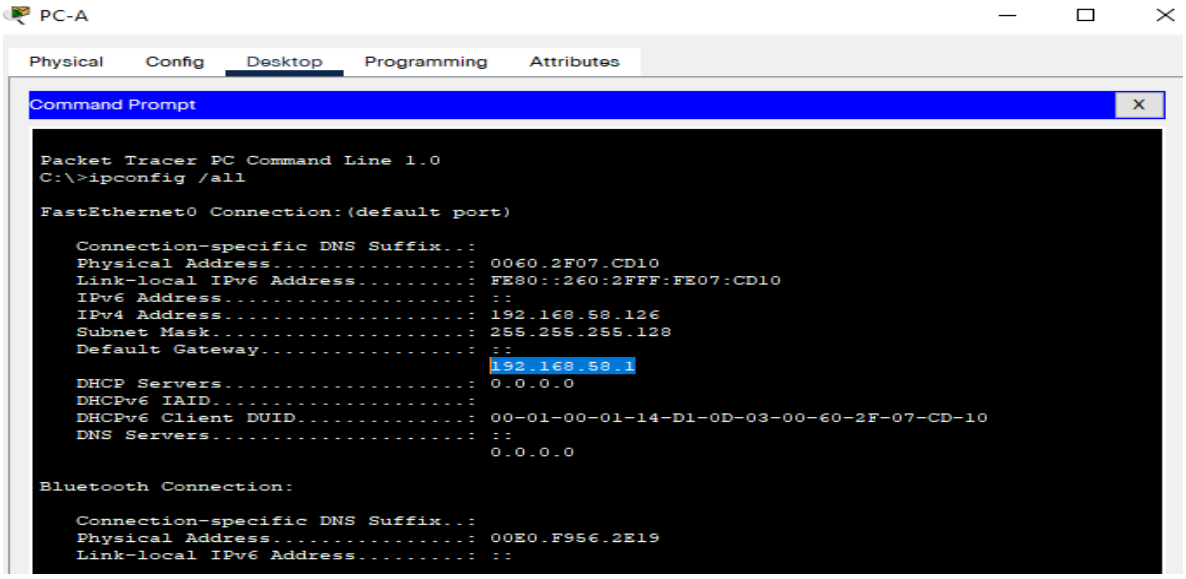
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all.**

Tabla 5: Configuración ipv4 PC-A

PC-A Network Configuration	
Descripción	Topología Direccionamiento IPV4
Dirección física	0060.2F07.CD10
Dirección IP	192.168.58.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.58.1

Fuente: propia

Figure 3: Configuración IPV4



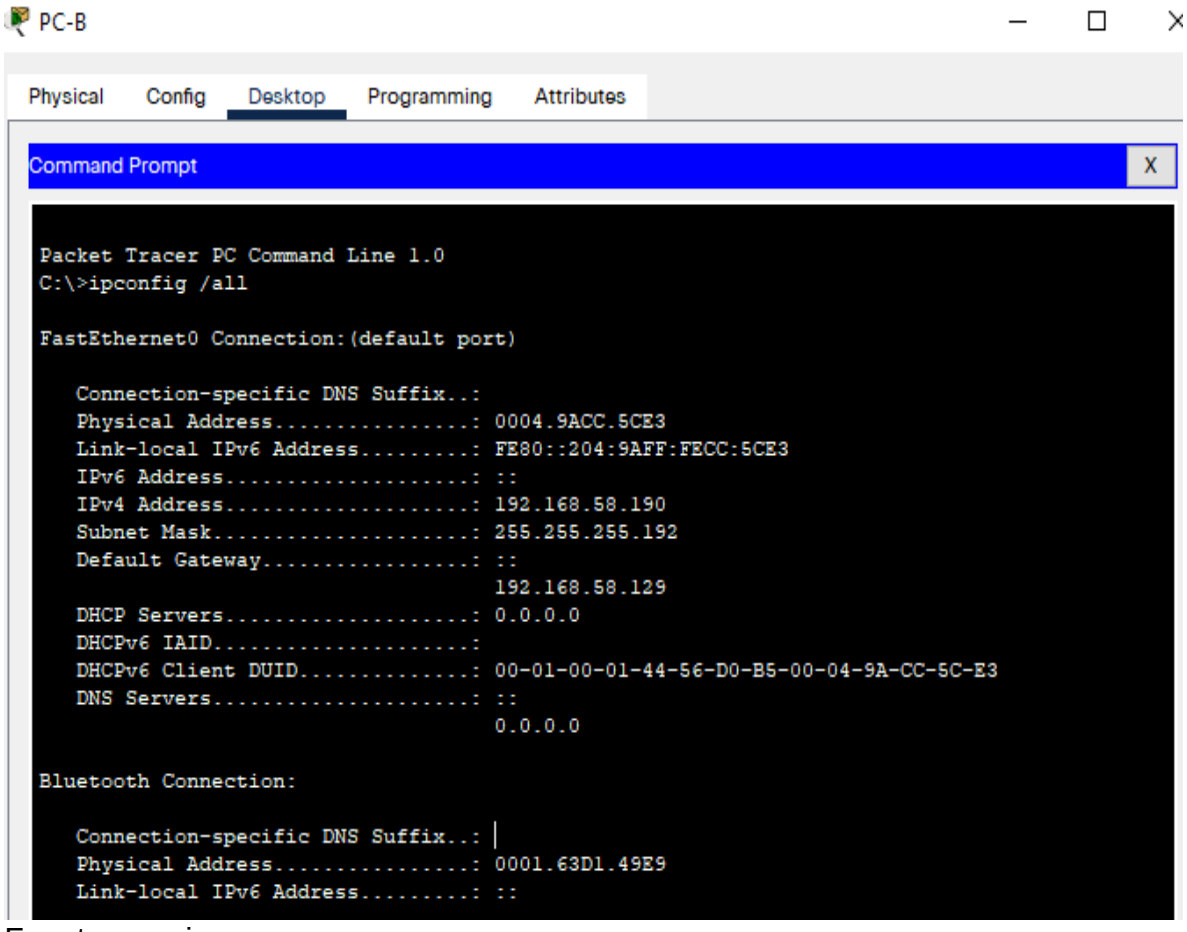
Fuente: propia

Tabla 6: Configuración IPV4 PC-B

PC-B Network Configuration	
Descripción	Topología Direccionamiento IPV4
Dirección física	0004.9ACC.5CE3
Dirección IP	192.168.58.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.58.129

Fuente: propia

Figure 4: Ejecución del comando ipconfig /all



Fuente: propia

Figure 5: Ejecución del comando ping desde el PC-A al PC-B

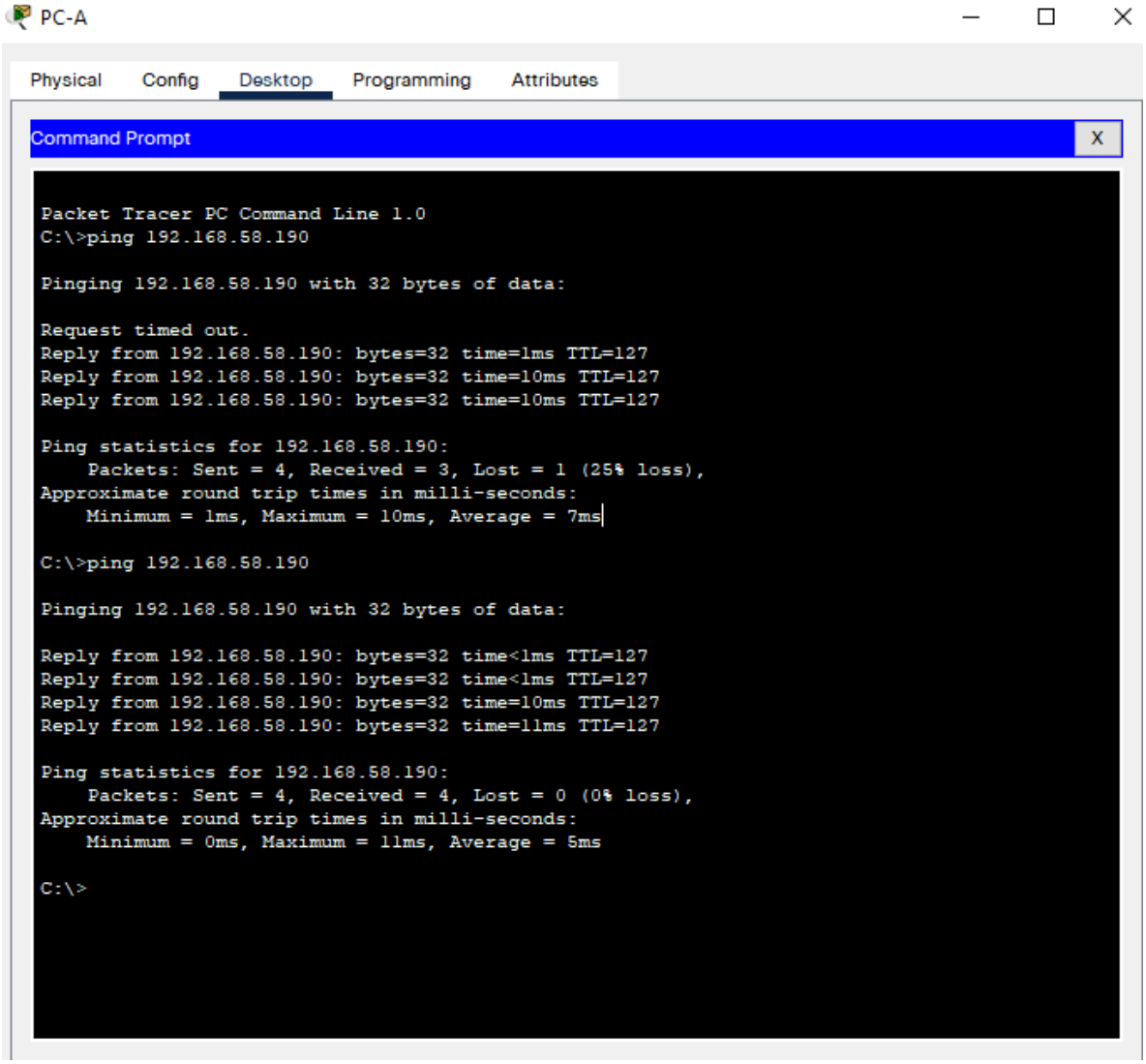
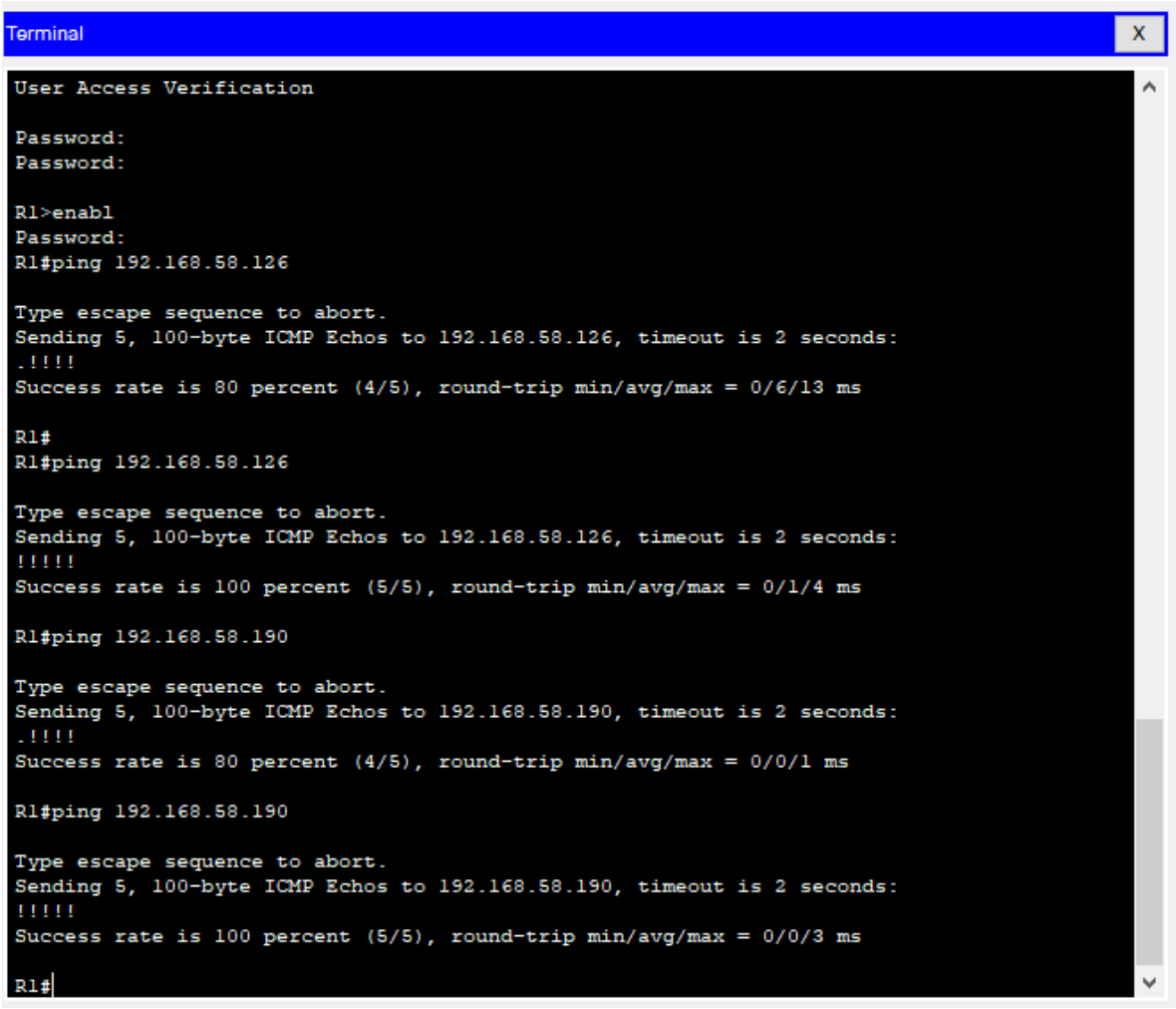
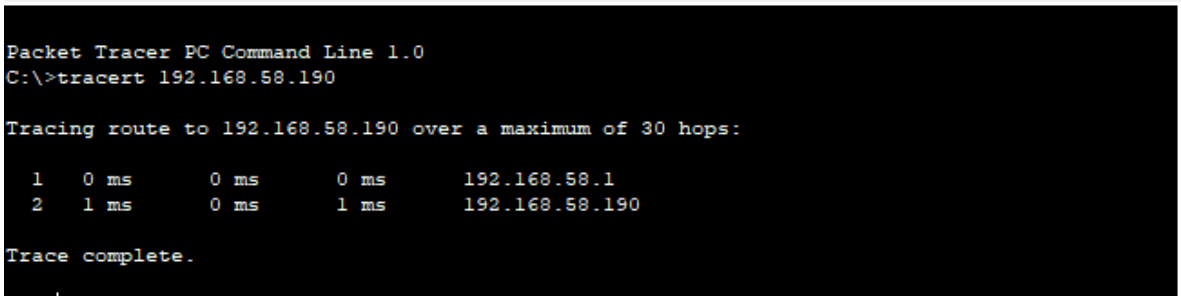


Figure 6: Ping desde la consola del router a la PC-A y PC-B



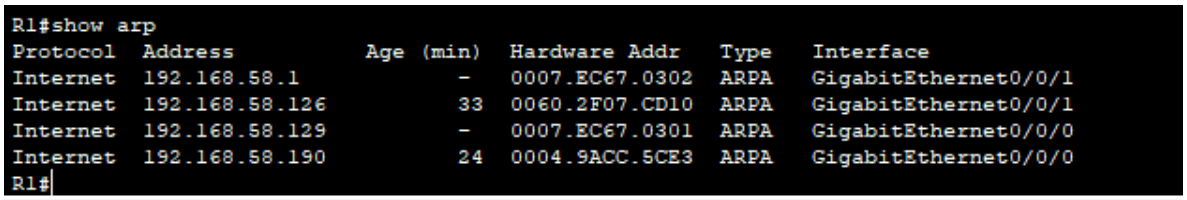
Fuente: propia

Figure 7: ejecución del comando tracert a PC-B



Fuente: propia

Figure 8: ejecución del comando arp

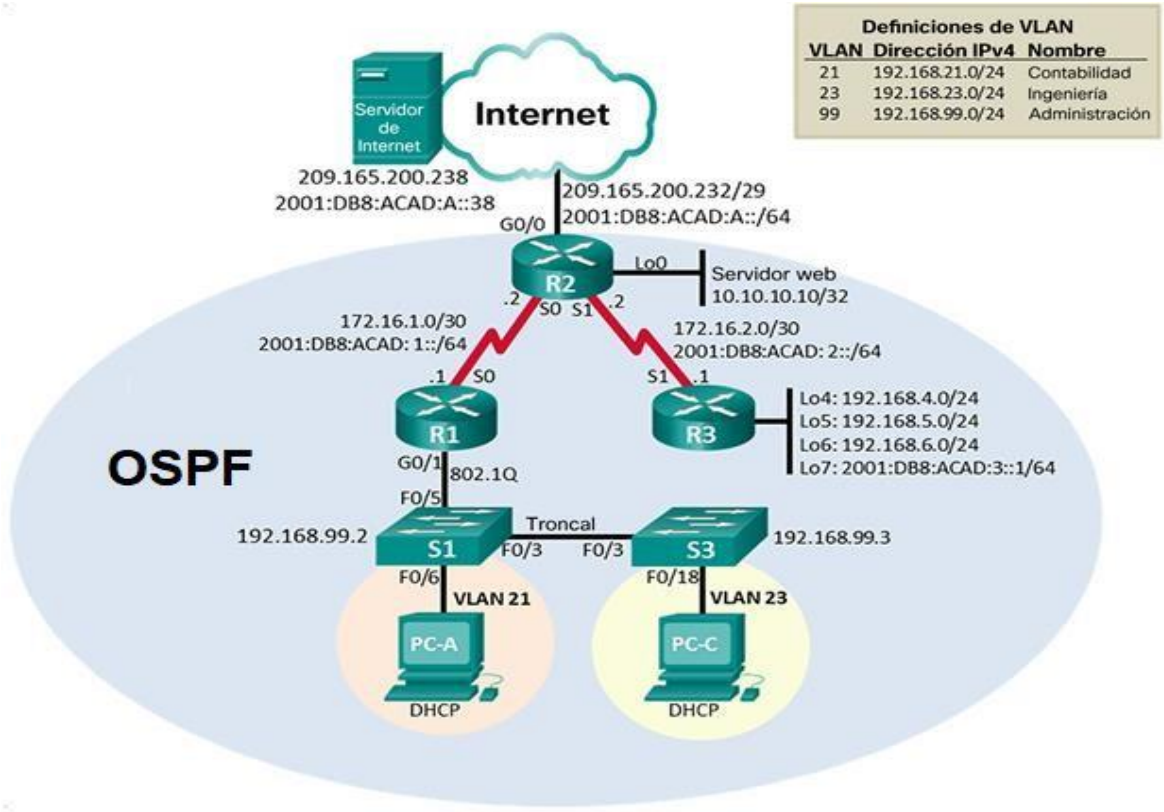


Fuente: propia

2.2. ESCENARIO 2

2.2.1. Topología

Figure 9: Topología escenario 2



Fuente: propia

2.2.2. Inicializar y volver a cargar los routers y los switches

Tabla 7: Iniciar Routers y Switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los Routers.	
Volver a cargar todos los Routers.	

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior.	
Volver a cargar ambos Switches.	
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches.	

Fuente: propia

2.2.2.1. Eliminar el archivo startup-config de todos los Routers y Volver a cargar todos los Routers.

R1:

R1>enable	*Entrar al modo EXEC Privilegiado*
R1#erase startup-config	*Elimina el archivo de configuración nvram*
R1#reload	*Volvemos a cargar el Router*

R2:

R2>enable	*Entrar al modo EXEC Privilegiado*
R2#erase startup-config	*Elimina el archivo de configuración nvram*
R2#reload	*Volvemos a cargar el Router*

R3:

R3>enable	*Entrar al modo EXEC Privilegiado*
R3#erase startup-config	*Elimina el archivo de configuración nvram*
R3#reload	*Volvemos a cargar el Router*

2.2.2.2. Eliminar el archivo startup-config de todos los Switches, eliminar la base de datos de VLAN anterior y volver a cargar ambos Switches.

S1:

S1>enable	*Entrar al modo EXEC Privilegiado*
S1#erase startup-config	*Elimina el archivo de configuración nvram*

S1#delete vlan.dat *Elimina la Base de datos vlan*

S1#reload *Volvemos a cargar el Switch*

S3:

S3>enable *Entrar al modo EXEC Privilegiado*

S3#erase startup-config *Elimina el archivo de configuración nvram*

S3#delete vlan.dat *Elimina la Base de datos vlan*

S3#reload *Volvemos a cargar el Switch*

2.2.2.3. Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches.

S1:

S1>enable *Entrar al modo EXEC Privilegiado*

S1#show flash *Verifica la existencia de la base de datos vlan*

S3:

S3>enable *Entrar al modo EXEC Privilegiado*

S3#show flash *Verifica la existencia de la base de datos vlan*

2.2.3. Configurar la computadora de Internet

Tabla 8: Datos de configuración

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

2.2.4. Configurar R1

Tabla 9: Tareas de configuración

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción. Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones. Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente: propia

2.2.4.1. Desactivar la búsqueda DNS

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
Router(config)#no ip domain-lookup *Desactivar la búsqueda DNS*
Router(config)#exit *Sale del modo de configuración*

2.2.4.2. Nombre del Router

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
Router(config)#hostname R1 *Cambia el nombre del Router*
R1(config)#

2.2.4.3. Contraseña de exec privilegiado cifrada

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#enable password class *Configura la contraseña de acceso*
R1(config)#

2.2.4.4. Contraseña de acceso a la consola

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#line console 0 *Ingresa al modo de configuración de la línea de consola*
R1(config-line)#password cisco *Configura la contraseña consola*
R1(config-line)#login *Nos pide autenticación al momento de iniciar*
R1(config-line)#exit *Sale del modo de configuración*

2.2.4.5. Contraseña de acceso Telnet

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*
R1(config)#line VTY 0 15 *Modo configuración de la linea vty*
R1(config-line)#password cisco *Contraseña acceso telnet*
R1(config-line)#login *Configura el inicio de sesión en la linea vty*

2.2.4.6. Cifrar las contraseñas de texto no cifrado

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#line VTY 0 15 *Modo configuración de la linea vty*
R1(config-line)#password cisco *Contraseña acceso telnet*
R1(config-line)#login *Configura el inicio de sesión en la linea vty*
R1(config-line)#service password-encryption *Cifra las contraseñas de texto no cifrado*

2.2.4.7. Mensaje MOTD

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#banner motd #Se prohíbe el acceso no autorizado# *Crear un mensaje*

2.2.4.8. Interfaz S0/0/0

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#interface s0/0/0 *Modo de configuración interface*
R1(config-if)#description connection to R2 *Establece la descripción*
R1(config-if)#ip address 172.16.1.1 255.255.255.252 *Asignación ipv4*
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 *Asignación ipv6*
R1(config-if)#clock rate 128000 *Establecer frecuencia de reloj*
R1(config-if)#no shutdown *Activar la interface*

2.2.4.9. Rutas predeterminadas

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*

R1(config)# ip route 172.16.1.0 255.255.255.252 s0/0/0 *Ruta Gateway ipv4*

R1(config)#ipv6 route ::/0 s0/0/0 *Ruta Gateway ipv6*

2.2.5. Configurar R2

Tabla 10: Tareas de configuración

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la

	información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Fuente: propia

2.2.5.1. Desactivar la búsqueda DNS

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
Router(config)#no ip domain-lookup *Desactivar la búsqueda DNS*
Router(config)#exit *Sale del modo de configuración*

2.2.5.2. Nombre del Router

Router>enable *Entrar al modo EXEC Privilegiado*
Router#configure terminal *Entrar al modo configuración Global*
Router(config)#hostname R2 *Cambia el nombre del Router*
R2(config)#

2.2.5.3. Contraseña de exec privilegiado cifrada

R2>enable *Entrar al modo EXEC Privilegiado*
R2#configure terminal *Entrar al modo configuración Global*
R2(config)#enable password class *Configura la contraseña de acceso*
R2(config)#

2.2.5.4. Contraseña de acceso a la consola

R2>enable *Entrar al modo EXEC Privilegiado*
R2#configure terminal *Entrar al modo configuración Global*
R2(config)#line console 0 *Ingresa al modo de configuración de la línea de consola*
R2(config-line)#password cisco *Configura la contraseña consola*
R2(config-line)#login *Nos pide autenticación al momento de iniciar*
R2(config-line)#exit *Sale del modo de configuración*

2.2.5.5. Contraseña de acceso Telnet

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*
R2(config)#line VTY 0 15 *Modo configuración de la linea vty*
R2(config-line)#password cisco *Contraseña acceso telnet*
R2(config-line)#login *Configura el inicio de sesión en la linea vty*

2.2.5.6. Cifrar las contraseñas de texto no cifrado

R2>enable *Entrar al modo EXEC Privilegiado*
R2#configure terminal *Entrar al modo configuración Global*
R2(config)#line VTY 0 15 *Modo configuración de la linea vty*
R2(config-line)#password cisco *Contraseña acceso telnet*
R2(config-line)#login *Configura el inicio de sesión en la linea vty*
R2(config-line)#service password-encryption *Cifra las contraseñas de texto no cifrado*

2.2.5.7. Mensaje MOTD

R2>enable *Entrar al modo EXEC Privilegiado*
R2#configure terminal *Entrar al modo configuración Global*
R2(config)#banner motd #Se prohíbe el acceso no autorizado# *Crear un mensaje*

2.2.5.8. Habilitar el servidor HTTP

R2>enable *Entrar al modo EXEC Privilegiado*
R2#configure terminal *Entrar al modo configuración Global*
R2(config)#ip http server *Habilita el servidor http*

2.2.5.9. Interfaz S0/0/0

R2>enable *Entrar al modo EXEC Privilegiado*
R2#configure terminal *Entrar al modo configuración Global*
R2(config)#interface s0/0/0 *Modo de configuración interface*

R2(config-if)#description connection to R1 Establece la descripción
R2(config-if)#ip address 172.16.1.2 255.255.255.252 Asignación ipv4
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 Asignación ipv6
R2(config-if)#no shutdown Activar la interface

2.2.5.10. Interfaz S0/0/1

R2>enable Entrar al modo EXEC Privilegiado
R2#configure terminal Entrar al modo configuración Global
R2(config)#interface s0/0/1 Modo de configuración interface
R2(config-if)#description connection to R3 Establece la descripción
R2(config-if)#ip address 172.16.2.2 255.255.255.252 Asignación ipv4
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 Asignación ipv6
R2(config-if)#clock rate 128000 Establecer frecuencia de reloj
R2(config-if)#no shutdown Activar la interface

2.2.5.11. Interfaz G0/0 (simulación de Internet)

R2>enable Entrar al modo EXEC Privilegiado
R2#configure terminal Entrar al modo configuración Global
R2(config)#interface g0/0 Modo de configuración interface
R2(config-if)# description connection to Internet Establece la descripción
R2(config-if)#ip address 209.165.200.233 255.255.255.248 Asignación ipv4
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 Asignación ipv6
R2(config-if)#no shutdown Activar la interface

2.2.5.12. Interfaz loopback 0 (servidor web simulado)

R2>enable Entrar al modo EXEC Privilegiado
R2#configure terminal Entrar al modo configuración Global
R2(config)#interface loopback 0 Modo de configuración interface
R2(config-if)# description simulacin de Internet Establece la descripción

R2(config-if)#ip address 10.10.10.10 255.255.255.255 Asignación ipv4

R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 Asignación ipv6

R2(config-if)#no shutdown

2.2.5.13. Rutas predeterminadas

R2>enable Entrar al modo EXEC Privilegiado

R2#configure terminal Entrar al modo configuración Global

R2(config)# ip route 172.16.1.0 255.255.255.252 g0/0 Ruta Gateway ipv4

R2(config)#ipv6 route ::/0 g0/0 Ruta Gateway ipv6

2.2.6. Configurar R3

Tabla 11: Tareas de configuración

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

Fuente: propia

2.2.6.1. Desactivar la búsqueda DNS

Router>enable *Entrar al modo EXEC Privilegiado*

Router#configure terminal *Entrar al modo configuración Global*

Router(config)#no ip domain-lookup *Desactivar la búsqueda DNS*

Router(config)#exit *Sale del modo de configuración*

2.2.6.2. Nombre del Router

Router>enable *Entrar al modo EXEC Privilegiado*

Router#configure terminal *Entrar al modo configuración Global*

Router(config)#hostname R3 *Cambia el nombre del Router*

R3(config)#

2.2.6.3. Contraseña de exec privilegiado cifrada

R3>enable *Entrar al modo EXEC Privilegiado*

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#enable password class *Configura la contraseña de acceso*

R3(config)#

2.2.6.4. Contraseña de acceso a la consola

R3>enable *Entrar al modo EXEC Privilegiado*

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#line console 0 *Ingresa al modo de configuración de la línea de consola*

R3(config-line)#password cisco *Configura la contraseña consola*

R3(config-line)#login *Nos pide autenticación al momento de iniciar*

R3(config-line)#exit *Sale del modo de configuración*

2.2.6.5. Contraseña de acceso Telnet

R3>enable *Entrar al modo EXEC Privilegiado*

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#line VTY 0 15 *Modo configuración de la linea vty*

R3(config-line)#password cisco *Contraseña acceso telnet*

R3(config-line)#login *Configura el inicio de sesión en la linea vty*

2.2.6.6. Cifrar las contraseñas de texto no cifrado

R3>enable *Entrar al modo EXEC Privilegiado*

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#line VTY 0 15 *Modo configuración de la linea vty*

R3(config-line)#password cisco *Contraseña acceso telnet*

R3(config-line)#login *Configura el inicio de sesión en la linea vty*

R3(config-line)#service password-encryption *Cifra las contraseñas de texto no cifrado*

2.2.6.7. Mensaje MOTD

R3>enable Entrar al modo EXEC Privilegiado
R3#configure terminal Entrar al modo configuración Global
R3(config)#banner motd #Se prohíbe el acceso no autorizado# Crear un mensaje

2.2.6.8. Interfaz S0/0/1

R3>enable Entrar al modo EXEC Privilegiado
R3#configure terminal Entrar al modo configuración Global
R3(config)#interface s0/0/1 Modo de configuración interface
R3(config-if)#description connection to R3 Establece la descripción
R3(config-if)#ip address 172.16.2.2 255.255.255.252 Asignación ipv4
R3(config-if)#ipv6 address 2001:db8:acad:2::2/64 Asignación ipv6
R3(config-if)#no shutdown Activar la interface

2.2.6.9. Interfaz loopback 4

R3>enable Entrar al modo EXEC Privilegiado
R3#configure terminal Entrar al modo configuración Global
R3(config)#interface loopback4 Modo de configuración interface
R3(config-if)#ip address 192.168.4.1 255.255.255.0 Asignación ipv4

2.2.6.10. Interfaz loopback 5

R3>enable Entrar al modo EXEC Privilegiado
R3#configure terminal Entrar al modo configuración Global
R3(config)#interface loopback5 Modo de configuración interface
R3(config-if)#ip address 192.168.5.1 255.255.255.0 Asignación ipv4

2.2.6.11. Interfaz loopback 6

R3>enable Entrar al modo EXEC Privilegiado

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#interface loopback6 *Modo de configuración interface*

R3(config-if)#ip address 192.168.6.1 255.255.255.0 Asignación ipv4

2.2.6.12. Interfaz loopback 7

R3>enable *Entrar al modo EXEC Privilegiado*

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#interface loopback7 *Modo de configuración interface*

R3(config-if)#ipv6 address 2001:db8:acab:3::1/64 Asignación ipv6

2.2.6.13. Rutas predeterminadas

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)# ip route 172.16.1.0 255.255.255.252 s0/0/1 Ruta Gateway ipv4

R2(config)#ipv6 route ::/0 s0/0/1 *Ruta Gateway ipv6*

2.2.7. Configurar S1

Tabla 12: Tareas de configuración

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del Switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: propia

2.2.7.1. Desactivar la búsqueda DNS

Switch>enable *Entrar al modo EXEC Privilegiado*
Switch#configure terminal *Entrar al modo configuración Global*
Switch(config)#no ip domain-lookup *Desactivar la búsqueda DNS*
Switch(config)#exit *Sale del modo de configuración*

2.2.7.2. Nombre del Router

Switch>enable *Entrar al modo EXEC Privilegiado*
Switchr#configure terminal *Entrar al modo configuración Global*
Switch(config)#hostname S1 *Cambia el nombre del Switch*
S1(config)#

2.2.7.3. Contraseña de exec privilegiado cifrada

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#enable password class *Configura la contraseña de acceso*
S1(config)#

2.2.7.4. Contraseña de acceso a la consola

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#line console 0 *Ingresa al modo de configuración de la línea de consola*
S1(config-line)#password cisco *Configura la contraseña consola*

S1(config-line)#login *Nos pide autenticación al momento de iniciar*

S1(config-line)#exit *Sale del modo de configuración*

2.2.7.5. Contraseña de acceso Telnet

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#line VTY 0 15 *Modo configuración de la linea vty*

S1(config-line)#password cisco *Contraseña acceso telnet*

S1(config-line)#login *Configura el inicio de sesión en la linea vty*

2.2.7.6. Cifrar las contraseñas de texto no cifrado

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#line VTY 0 15 *Modo configuración de la linea vty*

S1(config-line)#password cisco *Contraseña acceso telnet*

S1(config-line)#login *Configura el inicio de sesión en la linea vty*

S1(config-line)#service password-encryption *Cifra las contraseñas de texto no cifrado*

2.2.7.7. Mensaje MOTD

S1>enable *Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#banner motd #Se prohíbe el acceso no autorizado# *Crear un mensaje*

2.2.8. Configurar S3

Tabla 13: Tareas de configuración

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	

Nombre del Switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: propia

2.2.8.1. Desactivar la búsqueda DNS

Switch>enable *Entrar al modo EXEC Privilegiado*
Switch#configure terminal *Entrar al modo configuración Global*
Switch(config)#no ip domain-lookup *Desactivar la búsqueda DNS*
Switch(config)#exit *Sale del modo de configuración*

2.2.8.2. Nombre del Router

Switch>enable *Entrar al modo EXEC Privilegiado*
Switchr#configure terminal *Entrar al modo configuración Global*
Switch(config)#hostname S3 *Cambia el nombre del Switch*
S3(config)#

2.2.8.3. Contraseña de exec privilegiado cifrada

S3>enable *Entrar al modo EXEC Privilegiado*
S3#configure terminal *Entrar al modo configuración Global*
S3(config)#enable password class *Configura la contraseña de acceso*
S3(config)#

2.2.8.4. Contraseña de acceso a la consola

S3>enable Entrar al modo EXEC Privilegiado

S3#configure terminal Entrar al modo configuración Global

S3(config)#line console 0 Ingresa al modo de configuración de la línea de consola

S3(config-line)#password cisco Configura la contraseña consola

S3(config-line)#login Nos pide autenticación al momento de iniciar

S3(config-line)#exit Sale del modo de configuración

2.2.8.5. Contraseña de acceso Telnet

S3>enable Entrar al modo EXEC Privilegiado

S3#configure terminal Entrar al modo configuración Global

S3(config)#line VTY 0 15 Modo configuración de la linea vty

S3(config-line)#password cisco Contraseña acceso telnet

S3(config-line)#login Configura el inicio de sesión en la linea vty

2.2.8.6. Cifrar las contraseñas de texto no cifrado

S3>enable Entrar al modo EXEC Privilegiado

S3#configure terminal Entrar al modo configuración Global

S3(config)#line VTY 0 15 Modo configuración de la linea vty

S3(config-line)#password cisco Contraseña acceso telnet

S3(config-line)#login Configura el inicio de sesión en la linea vty

S3(config-line)#service password-encryption Cifra las contraseñas de texto no cifrado

2.2.8.7. Mensaje MOTD

S3>enable Entrar al modo EXEC Privilegiado

S3#configure terminal Entrar al modo configuración Global

S3(config)#banner motd #Se prohíbe el acceso no autorizado# Crear un mensaje

2.2.9. Verificar la conectividad de la red

Tabla 14: Datos de conectividad

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

Fuente: propia

Figure 10: Estableciendo conectividad desde R1 a R2, S0/0/0

```
R1>enab
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/16/76 ms
```

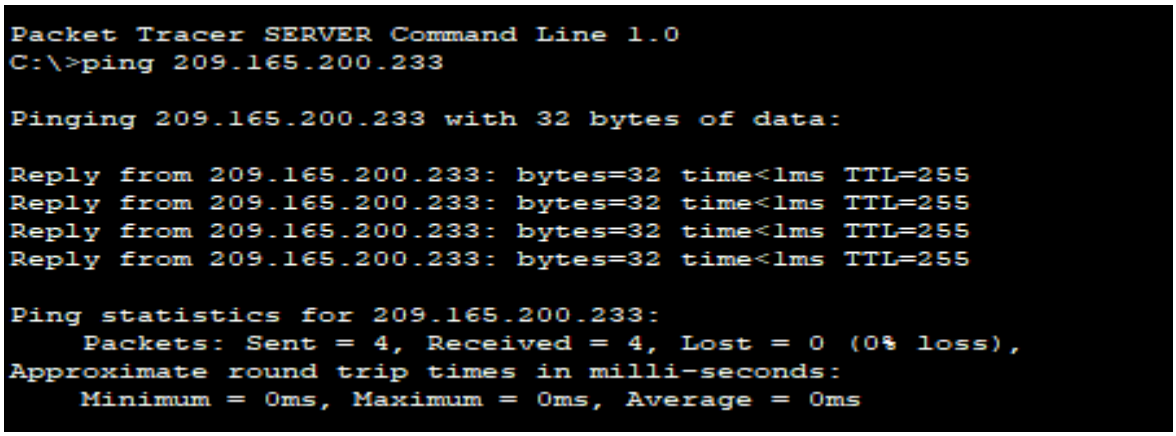
Fuente: propia

Figure 11: Estableciendo conectividad desde R2 a R3, S0/0/1

```
R2>ena
Password:
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Fuente: propia

Figure 12: Estableciendo conectividad PC – Internet a Gateway predeterminado



Fuente: propia

2.2.10. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

2.2.10.1. Configurar S1

Tabla 15: Tareas de configuración

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	

	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente: propia

2.2.10.1.1. Crear la base de datos de VLAN

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#vlan 21 *Entrar al modo configuración vlan*
S1(config-vlan)#name contabilidad *Nombra la vlan*
S1(config-vlan)#vlan 23 *Entrar al modo configuración vlan*
S1(config-vlan)#name ingeniería *Nombra la vlan*
S1(config-vlan)#vlan 99 *Entrar al modo configuración vlan*
S1(config-vlan)#name administración *Nombra la vlan*

2.2.10.1.2. Asignar la dirección IP de administración

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#interface vlan 99 *Configuración de la interface*
S1(config-if)#ip address 192.168.99.2 255.255.255.0 *Asigna dirección ipv4*
S1(config-if)#no shutdown *Activa la interface*

2.2.10.1.3. Asignar el gateway predeterminado

S1>enable *Entrar al modo EXEC Privilegiado*
S1#configure terminal *Entrar al modo configuración Global*
S1(config)#ip default-gateway 192.168.99.1 *Asigna Gateway predeterminado*

2.2.10.1.4. Forzar el enlace troncal en la interfaz F0/3

S1>enable	*Entrar al modo EXEC Privilegiado*
S1#configure terminal	*Entrar al modo configuración Global*
S1(config)#interface f0/3	*Configuración de la interface*
S1(config-if)#switchport mode trunk	*Modo enlace troncal*
S1(config-if)#switchport trunk native vlan 1	*Asigna vlan nativa*

2.2.10.1.5. Forzar el enlace troncal en la interfaz F0/5

S1>enable	*Entrar al modo EXEC Privilegiado*
S1#configure terminal	*Entrar al modo configuración Global*
S1(config)#interface f0/5	*Configuración de la interface*
S1(config-if)#switchport mode trunk	*Modo enlace troncal*
S1(config-if)#switchport trunk native vlan 1	*Asigna vlan nativa*

2.2.10.1.6. Configurar el resto de los puertos como puertos de acceso

S1>enable	*Entrar al modo EXEC Privilegiado*
S1#configure terminal	*Entrar al modo configuración Global*
S1(config)#interface range f0/1-2, f0/4, f0/6-24, g0/1-2	*Modo configuración puertos de acceso*
S1(config-if-range)#switchport mode access	Config. Puertos de acceso

2.2.10.1.7. Asignar F0/6 a la VLAN 21

S1>enable	*Entrar al modo EXEC Privilegiado*
S1#configure terminal	*Entrar al modo configuración Global*
S1(config)#interface f0/6	*Configuración de la interface*
S1(config-if)#switchport access vlan 21	*Asigna F0/6 a la VLAN 21*

2.2.10.1.8. Apagar todos los puertos sin usar

S1>enable	*Entrar al modo EXEC Privilegiado*

S1#configure terminal *Entrar al modo configuración Global*

S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 *Modo configuración puertos de acceso*

S1(config-if-range)#shutdown *Apaga los puertos*

2.2.10.2. Configurar S3

Tabla 16: Tareas de configuración

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el Gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el Gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	
Apagar todos los puertos sin usar	

Fuente: propia

2.2.10.2.1. Crear la base de datos de VLAN

S3>enable *Entrar al modo EXEC Privilegiado*

S3#configure terminal *Entrar al modo configuración Global*

S3(config)#vlan 21 *Entrar al modo configuración vlan*

S3(config-vlan)#name contabilidad *Nombra la vlan*

S3(config-vlan)#vlan 23	*Entrar al modo configuración vlan*
S3(config-vlan)#name ingeniería	*Nombra la vlan*
S3(config-vlan)#vlan 99	*Entrar al modo configuración vlan*
S3(config-vlan)#name administración	*Nombra la vlan*

2.2.10.2.2. Asignar la dirección IP de administración

S3>enable	*Entrar al modo EXEC Privilegiado*
S3#configure terminal	*Entrar al modo configuración Global*
S3(config)#interface vlan 99	*Configuración de la interface*
S3(config-if)#ip address 192.168.99.3 255.255.255.0	*Asigna dirección ipv4*
S3(config-if)#no shutdown	*Activa la interface*

2.2.10.2.3. Asignar el gateway predeterminado

S3>enable	*Entrar al modo EXEC Privilegiado*
S3#configure terminal	*Entrar al modo configuración Global*
S3(config)#ip default-gateway 192.168.99.1	*Asigna Gateway predeterminado*

2.2.10.2.4. Forzar el enlace troncal en la interfaz F0/3

S3>enable	*Entrar al modo EXEC Privilegiado*
S3#configure terminal	*Entrar al modo configuración Global*
S3(config)#interface f0/3	*Configuración de la interface*
S3(config-if)#switchport mode trunk	*Modo enlace troncal*
S3(config-if)#switchport trunk native vlan 1	*Asigna vlan nativa*

2.2.10.2.5. Configurar el resto de los puertos como puertos de acceso

S3>enable	*Entrar al modo EXEC Privilegiado*
S3#configure terminal	*Entrar al modo configuración Global*
S3(config)#interface range f0/1-2, f0/4-24, g0/1-2	*Modo configuración puertos de acceso*

S3(config-if-range)#switchport mode access Config. Puertos de acceso

2.2.10.2.6. Asignar F0/18 a la VLAN 23

S3>enable *Entrar al modo EXEC Privilegiado*

S3#configure terminal *Entrar al modo configuración Global*

S3(config)#interface f0/18 *Configuración de la interface*

S3(config-if)#switchport access vlan 23 *Asigna F0/6 a la VLAN 21*

2.2.10.2.7. Apagar todos los puertos sin usar

S3>enable *Entrar al modo EXEC Privilegiado*

S3#configure terminal *Entrar al modo configuración Global*

S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 *Modo configuración puertos de acceso*

S3(config-if-range)#shutdown *Apaga los puertos*

2.2.10.3. Configurar R1

Tabla 17: Tareas de configuración

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz

Activar la interfaz G0/1	

Fuente: propia

2.2.10.3.1. Configurar la subinterfaz 802.1Q .21 en G0/1

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#interface g0/1.21 *Modo configuración de la interface*
R1(config-subif)#description VLAN 21 *Descripción vlan*
R1(config-subif)#encapsulation dot1q 21 *Asigna la VLAN 21*
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 *Asigna dirección ipv4*

2.2.10.3.2. Configurar la subinterfaz 802.1Q .23 en G0/1

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#interface g0/1.23 *Modo configuración de la interface*
R1(config-subif)#description VLAN 23 *Descripción vlan*
R1(config-subif)#encapsulation dot1q 23 *Asigna la VLAN 21*
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 *Asigna dirección ipv4*

2.2.10.3.3. Configurar la subinterfaz 802.1Q .99 en G0/1

R1>enable *Entrar al modo EXEC Privilegiado*
R1#configure terminal *Entrar al modo configuración Global*
R1(config)#interface g0/1.99 *Modo configuración de la interface*
R1(config-subif)#description VLAN 99 *Descripción vlan*
R1(config-subif)#encapsulation dot1q 99 *Asigna la VLAN 21*
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 *Asigna dirección ipv4*

2.2.10.3.4. Activar la interfaz G0/1

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal	*Entrar al modo configuración Global*
R1(config)#interface g0/1	*Modo configuración de la interface*
R1(config-if)#no shutdown	*Activa la interface*

2.2.10.4. Verificar la conectividad de la red

Tabla 18: Conectividad

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

Fuente: propia

Figure 13: Estableciendo conectividad desde S1 a R1, dirección VLAN 99

```
S1#ping 192.168.99.1

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

Fuente: propia

Figure 14: Estableciendo conectividad desde S3 a R1, dirección 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 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: propia

Figure 15: Estableciendo conectividad desde S1 a R1, dirección VLAN 21

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: propia

Figure 16: Estableciendo conectividad desde S3 a R1, dirección VLAN 23

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: propia

2.2.11. Configurar el protocolo de routing dinámico OSPF

Tabla 19: Tareas de configuración

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

Fuente: propia

2.2.11.1. Configurar OSPF área 0, establecer todas las interfaces LAN como pasivas

R1:

R1>enable *Entrar al modo EXEC Privilegiado*

R1#show ip route connected *Mostrar las redes conectadas*

C 172.16.1.0/30 is directly connected, Serial0/0/0

C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21

C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23

C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

R1#configure terminal *Entrar al modo configuración Global*

R1(config)#router ospf 10 *Asigna un numero de proceso*

R1(config-router)#router-id 1.1.1.1 *Asigna un id*

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 *Asigna las redes a un área*

R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 *Asigna las redes área*

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 *Asigna las redes área*

R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 *Asigna las redes a un área*

R2:

R2>enable *Entrar al modo EXEC Privilegiado*

R2#show ip route connected *Mostrar las redes conectadas*

C 10.10.10.10/32 is directly connected, Loopback0

C 172.16.1.0/30 is directly connected, Serial0/0/0

C 172.16.2.0/30 is directly connected, Serial0/0/1

C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#router ospf 10 *Asigna un numero de proceso*

R2(config-router)#router-id 2.2.2.2 *Asigna un id*

R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 *Asigna las redes a un área*

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 *Asigna las redes a un área*

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 *Asigna las redes a un área*

R2(config-router)#network 209.165.200.232 0.0.0.7 area 0 *Asigna las redes a un área*

R3:

R3>enable *Entrar al modo EXEC Privilegiado*

R3#show ip route connected *Mostrar las redes conectadas*

C 172.16.2.0/30 is directly connected, Serial0/0/1

C 192.168.4.0/24 is directly connected, Loopback4

C 192.168.5.0/24 is directly connected, Loopback5

C 192.168.6.0/24 is directly connected, Loopback6

R3#configure terminal *Entrar al modo configuración Global*

R3(config)#router ospf 10 *Asigna un numero de proceso*

R3(config-router)#router-id 3.3.3.3 *Asigna un id*

R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 *Asigna las redes a un área*

R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 Asigna las redes área

R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 Asigna las redes área

R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 Asigna las redes área

2.2.11.2. Establecer todas las interfaces LAN como pasivas y desactive la sumarización automática.

R1:

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*

R1(config)#router ospf 10 *Modo de configuración OSPF*

R1(config-router)#passive-interface g0/1.21 *Establece interface pasiva*

R1(config-router)#passive-interface g0/1.23 *Establece interface pasiva*

R1(config-router)#passive-interface g0/1.99 *Establece interface pasiva*

R1(config-router)#no auto-summary *Desactiva la sumarización automática*

R2:

R2>enable	*Entrar al modo EXEC Privilegiado*
R2#configure terminal	*Entrar al modo configuración Global*
R2(config)#router ospf 10	*Modo de configuración OSPF*
R2(config-router)#passive-interface g0/0	*Establece interface pasiva*
R2(config-router)#no auto-summary	*Desactiva la sumarización automática*

R3:

No aplica la configuración de la interface pasiva porque este Router no conecta una LAN.

2.2.12. Configurar OSPFv3 en el R2

Tabla 20: Tareas de configuración

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	
Anunciar redes IPv6 conectadas directamente	
Establecer todas las interfaces de LAN IPv6 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente: propia

2.2.12.1. Configurar OSPF área 0, Anunciar redes IPv6 conectadas directamente, Establecer todas las interfaces de LAN IPv6 (Loopback) como pasivas y Desactive la sumarización automática.

R2>enable	*Entrar al modo EXEC Privilegiado*
R2#show ipv6 route	*Mostrar todas las redes*

S ::/0 [1/0] via GigabitEthernet0/0, directly connected

C 2001:DB8:ACAD:1::/64 [0/0] via Serial0/0/0, directly connected

L 2001:DB8:ACAD:1::2/128 [0/0] via Serial0/0/0, receive

C 2001:DB8:ACAD:2::/64 [0/0] via Serial0/0/1, directly connected

L 2001:DB8:ACAD:2::2/128 [0/0] via Serial0/0/1, receive

C 2001:DB8:ACAD:A::/64 [0/0] via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:A::1/128 [0/0] via GigabitEthernet0/0, receive

L FF00::/8 [0/0] via Null0, receive

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ipv6 router ospf 10 *Modo de configuración OSPFv3*

R2(config-rtr)#interface s0/0/0 *Modo de configuración interface*

R2(config-if)#ipv6 ospf 10 area 0 *Asigna la interface al proceso OSPF*

R2(config-if)#interface s0/0/1 *Modo de configuración interface*

R2(config-if)#ipv6 ospf 10 area 0 *Asigna la interface al proceso OSPF*

R2(config-if)#interface g0/0 *Modo de configuración interface*

R2(config-if)#ipv6 ospf 10 area 0 *Asigna la interface al proceso OSPF*

2.2.13. 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 21: Verificación OSPF

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route OSPF
	Show run | section router OSPF: no soporta el packet tracer.

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show run: en la sección OSPF en la sección OSPF

Fuente: propia

Figure 17: Ejecución del comando show ip protocols

```
R2>enab
Password:
R2#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 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    209.165.200.232 0.0.0.7 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:08:47
    2.2.2.2              110      00:08:47
    3.3.3.3              110      00:08:47
  Distance: (default is 110)
```

Fuente: propia

Figure 18: Ejecución del comando show ip route OSPF

```
R2#Show ip route OSPF
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/65] via 172.16.2.1, 00:11:28, Serial0/0/1
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/65] via 172.16.2.1, 00:11:28, Serial0/0/1
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/65] via 172.16.2.1, 00:11:28, Serial0/0/1
O    192.168.21.0 [110/65] via 172.16.1.1, 00:11:28, Serial0/0/0
O    192.168.23.0 [110/65] via 172.16.1.1, 00:11:28, Serial0/0/0
O    192.168.99.0 [110/65] via 172.16.1.1, 00:11:28, Serial0/0/0
```

Fuente: propia

Figure 19: Ejecución del comando show run

```
R2#show run
Building configuration...

Current configuration : 2368 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2

router ospf 10
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 passive-interface Loopback0
 network 10.10.10.10 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 209.165.200.232 0.0.0.7 area 0
!
```

Fuente: propia

2.2.14. Implementar DHCP y NAT para IPv4

2.2.14.1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 22: Tareas de configuración

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com

	Establecer el gateway predeterminado

Fuente: propia

2.2.14.1.1. Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Reserva ip vlan

2.2.14.1.2. Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 Reserva ip vlan

2.2.14.1.3. Crear un pool de DHCP para la VLAN 21.

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*

R1(config)#ip dhcp pool ACCT *Asigna nombre al pool*

R1(dhcp-config)#network 192.168.21.0 255.255.255.0 Asigna la red

R1(dhcp-config)#default-router 192.168.21.1 *Asigna Gateway*

R1(dhcp-config)#dns-server 10.10.10.10 Configura servidor dns

R1(dhcp-config)#domain-name ccna-sa.com Configura nombre de dominio

2.2.14.1.4. Crear un pool de DHCP para la VLAN 23

R1>enable *Entrar al modo EXEC Privilegiado*

R1#configure terminal *Entrar al modo configuración Global*

R1(config)#ip dhcp pool ENGNR *Asigna nombre al pool*

R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Asigna la red

R1(dhcp-config)#default-router 192.168.23.1 *Asigna Gateway*

R1(dhcp-config)#dns-server 10.10.10.10 Configura servidor dns

R1(dhcp-config)#domain-name ccna-sa.com Configura nombre de dominio

2.2.14.2. Configurar la NAT estática y dinámica en el R2

Tabla 23: Tareas de configuración

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237**
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	

Fuente: propia

2.2.14.2.1. Crear una base de datos local con una cuenta de usuario

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#username webuser privilege 15 secret cisco12345 Crea base de datos

2.2.14.2.2. Habilitar el servicio del servidor HTTP

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ip http server - No soporta packet Tracer Habilita servidor http

2.2.14.2.3. Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ip http authentication - No soporta Packet Tracer Configura servidor http

2.2.14.2.4. Crear una NAT estática al servidor web.

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 Crea la NAT estática

2.2.14.2.5. Asignar la interfaz interna y externa para la NAT estática

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#int g0/0 *Modo de configuración de la interface*

R2(config-if)#ip nat outside *Configuración NAT externa*

R2(config-if)#interface s0/0/0 *Modo de configuración de la interface*

R2(config-if)#ip nat inside *Configuración NAT interna*

R2(config-if)#interface s0/0/0 *Modo de configuración de la interface*

R2(config-if)#ip nat inside *Configuración NAT interna*

2.2.14.2.6. Configurar la NAT dinámica dentro de una ACL privada

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 Configura ACL privada

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Configura ACL privada

R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 Configura ACL privada

2.2.14.2.7. Defina el pool de direcciones IP públicas utilizables.

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 *Pool de direcciones utilizables*

2.2.14.2.8. Definir la traducción de NAT dinámica

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ip nat inside source list 1 pool INTERNET Define traducción NAT dinámica

2.2.15. Verificar el protocolo DHCP y la NAT estática

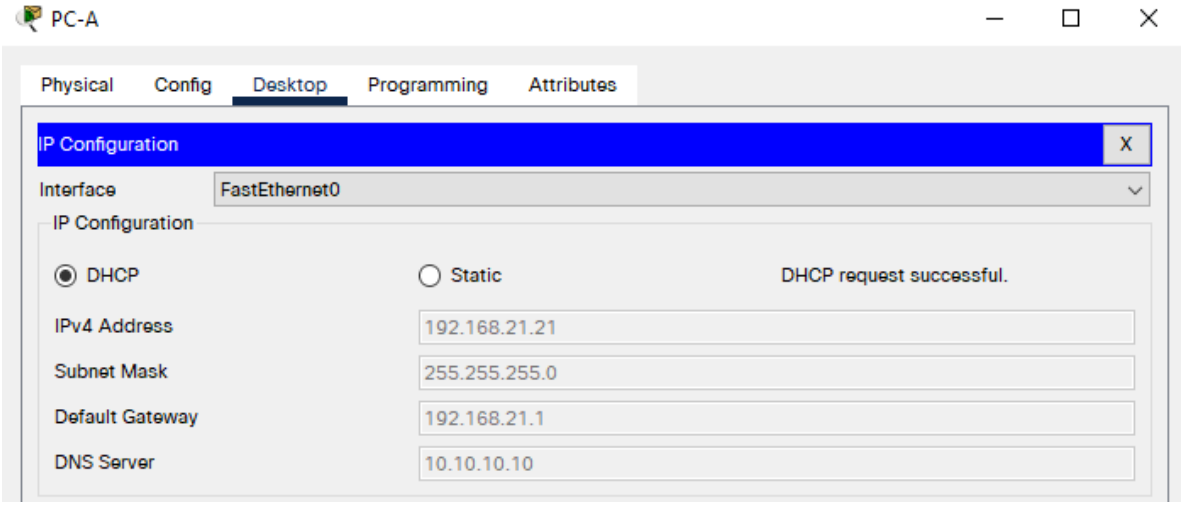
Tabla 24: verificación de conectividad

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 **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

2.2.15.1. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

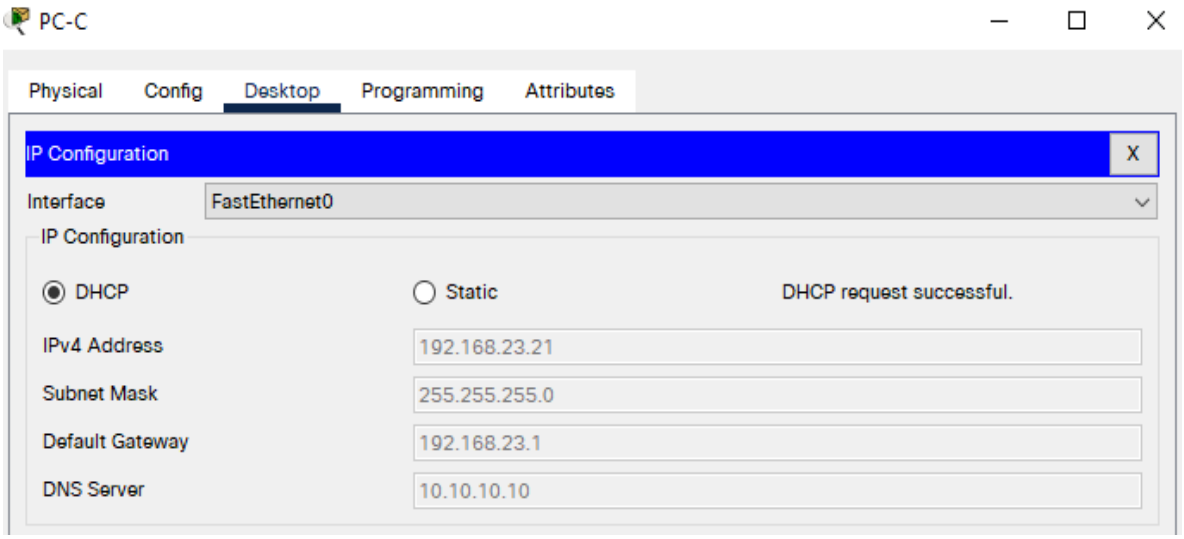
Figure 20: Información del servidor DHCP en la PC-A



Fuente: propia

2.2.15.2. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

Figure 21: Información del servidor DHCP en la PC-A



Fuente: propia

2.2.15.3. Verificar que la PC-A pueda hacer ping a la PC-C

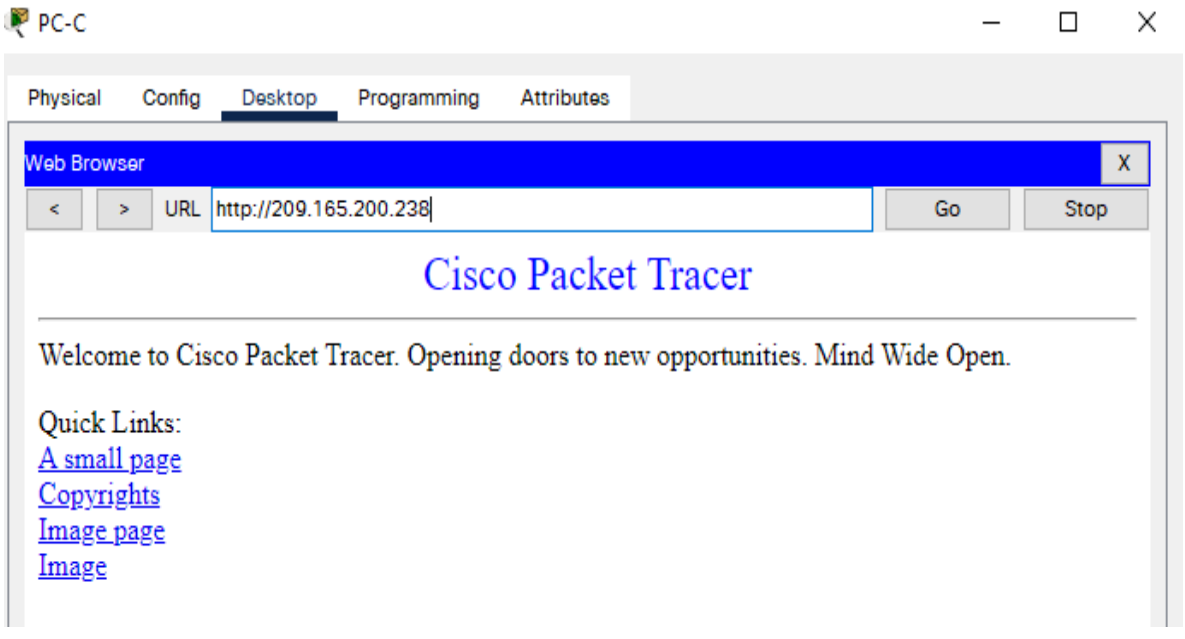
Figure 22: Ping desde PC – A hasta PC – C

```
C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time=12ms TTL=127
Reply from 192.168.23.21: bytes=32 time=14ms TTL=127
Reply from 192.168.23.21: bytes=32 time=14ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 10ms
```

Fuente: propia

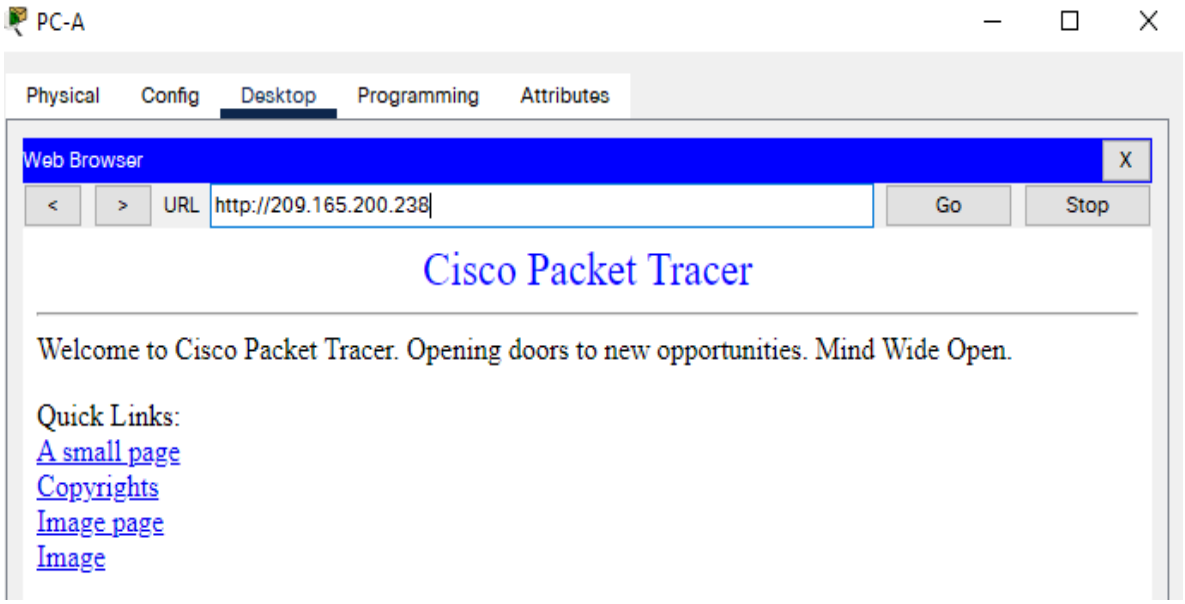
2.2.15.4. Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Figure 23: Acceso al servidor web desde el PC-C



Fuente: propia

Figure 24: Acceso al servidor web desde el PC-A



Fuente: propia

2.2.16. Configurar NTP

Tabla 25: Tareas de configuración

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

Fuente: propia

2.2.16.1. Ajuste la fecha y hora en R2.

R2>enable *Entrar al modo EXEC Privilegiado*

R2#clock set 09:00:00 06 march 2016 *Ajuste de fecha y hora*

2.2.16.2. Configure R2 como un maestro NTP

R2>enable	*Entrar al modo EXEC Privilegiado*
R2#configure terminal	*Entrar al modo configuración Global*
R2(config)#ntp master 5	*Configuración ntp master*

2.2.16.3. Configurar R1 como un cliente NTP.

R1>enable	*Entrar al modo EXEC Privilegiado*
R1#configure terminal	*Entrar al modo configuración Global*
R1(config)#ntp server 172.16.1.2	*Configura cliente NTP*

2.2.16.4. Configure R1 para actualizaciones de calendario periódicas con hora NTP.

R1>enable	*Entrar al modo EXEC Privilegiado*
R1#configure terminal	*Entrar al modo configuración Global*
R1(config)#ntp update-calendar	*Configura actualizaciones de calendario*

2.2.16.5. Verifique la configuración de NTP en R1.

R1>enable	*Entrar al modo EXEC Privilegiado*
R1#show ntp associations	*Muestra la configuración NTP*

Figure 25: configuración NTP en R1

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
*~172.16.1.2    127.127.1.1     5    4        16      377    3.00           0.00
0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Fuente: propia

2.2.17. Configurar y verificar las listas de control de acceso (ACL)

2.2.17.1. Restringir el acceso a las líneas VTY en el R2

Tabla 26: Tareas de configuración

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN- MGT**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Fuente: propia

2.2.17.1.1. Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2.

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#ip access-list standard ADMIN-MGT Configurar lista de acceso

R2(config-std-nacl)#permit host 172.16.1.1 *Permite acceso al host*

2.2.17.1.2. Aplicar la ACL con nombre a las líneas VTY

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#line vty 0 15 *Modo configuración de la línea*

R2(config-line)#access-class ADMIN-MGT in *Aplica ACL con nombres VTY*

2.2.17.1.3. Permitir acceso por Telnet a las líneas de VTY

R2>enable *Entrar al modo EXEC Privilegiado*

R2#configure terminal *Entrar al modo configuración Global*

R2(config)#line vty 0 15 *Modo configuración de la línea*

R2(config-line)#transport input telnet *Acceso a telnet*

2.2.17.1.4. Verificar que la ACL funcione como se espera

R1>enable *Entrar al modo EXEC Privilegiado*

R1#telnet 172.16.1.2 *Acceso telnet*

Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado

User Access Verification

Password:

R2>enable *Acceso a R2*

Password: cisco

R2#

Figure 26: Acceso a R2 desde R1

```
R1>ena
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado


User Access Verification

Password:
R2>ena
Password:
R2#
R2#
```

Fuente: propia

2.2.17.2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

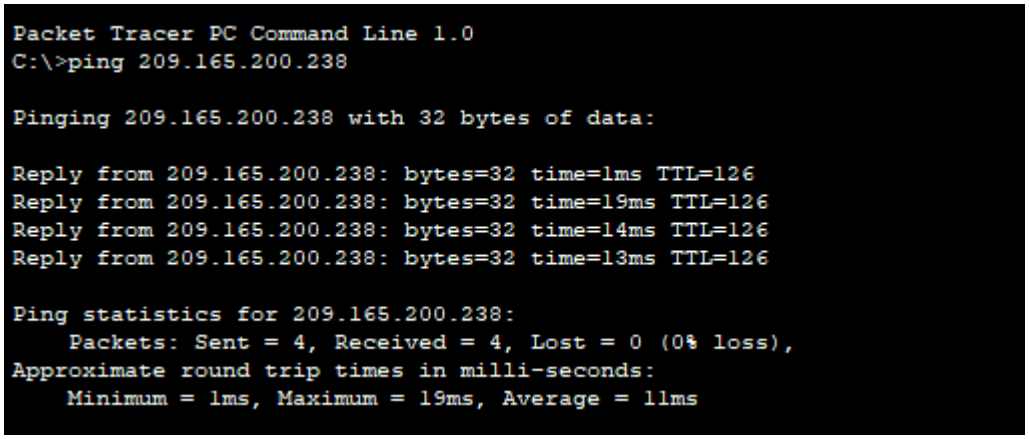
Tabla 27: Verificación de configuración

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show ip Access-list

Restablecer los contadores de una lista de acceso	Clear ip Access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations **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

Figure 27: Ping PC-A al servidor de Internet



Fuente: propia

Figure 28: Ping PC-C al servidor de Internet

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=8ms TTL=126
Reply from 209.165.200.238: bytes=32 time=16ms TTL=126
Reply from 209.165.200.238: bytes=32 time=16ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 10ms
```

Fuente: propia

Figure 29: verificación de la configuración NAT

```
R2>show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.233:1 192.168.23.21:1    209.165.200.238:1  209.165.200.238:1
icmp 209.165.200.233:2 192.168.23.21:2    209.165.200.238:2  209.165.200.238:2
icmp 209.165.200.233:3 192.168.23.21:3    209.165.200.238:3  209.165.200.238:3
icmp 209.165.200.233:4 192.168.23.21:4    209.165.200.238:4  209.165.200.238:4
---  209.165.200.237   10.10.10.10        ---                ---
tcp 209.165.200.233:1025192.168.23.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1026192.168.23.21:1026 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1026192.168.21.21:1026 209.165.200.238:80 209.165.200.238:80
```

Fuente: propia

CONCLUSIÓN

Del presente Escenario 1 podemos concluir que mediante el simulador Packet Tracer podemos diseñar una red utilizando cualquier topología, debido a que presenta componentes que representan los elementos que hacen parte de la red. Esto permite practicar las distintas configuraciones que se utilizan al momento de configurar y administrar una red. Dentro de los dispositivos de red utilizados están los Router, Switch y PC, los cuales mediante la conexión por consola podemos ingresar los datos de configuración mediante el sistema operativo CISCO IOS que se encuentra instalados en todos los dispositivos.

Para administrar la red debemos tener organizada una tabla de direccionamiento con todos los datos de configuración de los hosts. En la ventana CLI de los equipos, ingresamos al modo de usuario privilegiado con el comando Enable y al modo de configuración global con el comando Configure Terminal para ingresar a la configuración de los equipos. Las medidas de seguridad que se implementan en estas configuraciones son de muncha importancia, toda vez que los controles de seguridad se establecen en los equipos mediante comandos que encriptan contraseñas y verifican la autenticidad del administrador.

Para garantizar el envío de paquetes en toda la red y la conexión entre estos, se utiliza el comando PING más la dirección IP del host donde queremos probar la conectividad. De esta forma verificamos que la red quedo bien configurada y con las medidas de seguridad instaladas.

Del desarrollo del escenario 2, se concluye que en la configuración de cualquier topología de red se deben tener presentes las distintas configuraciones que se realizan a los dispositivos que la conforman; cada uno de estos dispositivos Routers, Switches, PC y servidores contienen interfaces de red que son importantes para la recepción y envío de paquetes en toda la red. Esta comunicación se establece configurando direcciones IPV4 o IPV6 para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN. Además, proporciona conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.

BIBLIOGRAFÍA

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.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In International Conference on Knowledge Management in Organizations (pp. 331-344). Springer, Cham.

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

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

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

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

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

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

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

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

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

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

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