DESARROLLO DE UNA PRUEBA DE HABILIDADES PRÁCTICAS CCNA APLICANDO EL SOFTWARE CISCO PACKET TRACER

OSCAR JOSE GARCIA MONROY

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
BARRANQUILLLA
2020

DESARROLLO DE UNA PRUEBA DE HABILIDADES PRÁCTICAS CCNA APLICANDO EL SOFTWARE CISCO PACKET TRACER

OSCAR JOSE GARCIA MONROY

INFORME FINAL PARA OPTAR POR EL TÍTULO DE INGENIERO DE SISTEMAS

DIRECTOR/TUTOR:

JUAN CARLOS VESGA FERREIRA

HECTOR JULIAN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
BARRANQUILLLA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

BARRANQUILLA (22, 05, 2020)

DEDICATORIA

Quiero dedicar a mi Dios celestial, a mi esposa Yolanda, hijos, mi linda nieta Isabella y toda mi hermosa familia

AGRADECIMIENTOS

Quiero agradecer a la UNAD por esa linda gran oportunidad que me brindo, primero en homologar, para poder seguir creciendo en mi vida Profesional, a esos directores, tutores que me apoyaron en mis créditos y en este diplomado al tutor Héctor Julián Parra que siempre estaba presente cuando tenía alguna duda, a mis buenos compañeros que conocí en las diferentes regiones del país y agradecer de manera virtual a todas las plataformas que existen como herramientas de apoyo para estas Formaciones ,como la biblioteca de la UNAD-Sena

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

RESUMEN

La UNAD, bajo su modalidad virtual y su proceso de aprendizaje del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), se presenta como estrategia el uso del software para simular con Cisco Packet Tracer, donde podemos comprobar, virtualmente, cómo trabajan estas redes y podemos ver las diferentes clases de topología para llevar a la realidad al campo laboral cuando se nos presente en la necesidad en el entorno prodductivo.

En el desarrollo de los módulos CCNA1 (CCNA R&S: Introduction to Networks) y CCNA2 (CCNA R&S: Routing and Switching Essentials), se obtiene las bases teóricas y prácticas de laboratorio para el aprendizaje de la tecnología. Con los conocimientos obtenidos y puestos en práctica se busca lograr el desarrollo dela actividad final como prueba de habilidades, donde mediante los escenarios propuestos, se pone en práctica los conocimientos previamente aprendidos, realizando configuraciones como: IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2 y 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, encapsulamiento PPP y su autenticación.

Durante la realización de las configuraciones, se probará y registrará la red mediante el uso de comandos en la Interfaz de línea de comandos (CLI) y algunos ajustes usando la interfaz gráfica de los dispositivos.

Palabras claves: Packet Tracer, Interfaz, Conectividad, tecnología CISCO

INTRODUCCIÓN

Esta actividad evaluativa Escenario 1 y Escenario 2, del Diplomado de Profundización CCNA, busca identificar el grado de desempeño adquirido en estas competencias y demostrar las habilidades y/o destrezas que se adquirieron durante del desarrollo del Diplomado Cisco en cada una de sus etapas.

Esta prueba de habilidades prácticas se desarrolla en el Software de Simulación de Redes Packet Tracer, que es la herramienta que utilice para todas las actividades propuestas y desarrolladas en el Diplomado de Profundización Cisco.

Descripción de los escenarios 1 y 2 propuesto para la prueba de habilidades

Se debe configurar una red pequeña y una red de dos ciudades para que admita conectividad IPv4 e IPv6 para colocarle las ip y restricciones y que tenga conectividad y una confiabilidad.

El cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Aplicar la tecnología CISCO para solucionar dos estudios de caso, a través de la herramienta Packet Tracer

2.2 OBJETIVOS ESPECÍFICOS

1. Analizar e identificar las necesidades de conectividad, accesos y restricciones en cada uno de los dos escenarios.
2. Organizar la topología de acuerdo con las necesidades de conectividad identificadas en los dos escenarios.
3. Instalar las interfases de acuerdo con la tipología establecida para cada caso, a través de las tablas de direccionamiento especificadas.
4. Configurar los comandos para la administración de red, con los accesos y restricciones especificadas en cada escenario

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Actualmente las redes de datos de las entidades o ciudades entre sí, tienen una mayor carga de tráfico debido al uso de sistemas integrados como ERP, base de datos, voz y video, es así que la red del Proyecto, en sus escenarios, presenta varios problemas como latencia, fallas de conexión, ausencia de mecanismos de control del uso del ancho de banda, pérdida de información, y otros.

3.2 JUSTIFICACIÓN

El presente trabajo se justifica por la importancia de contar con una red que garantice el intercambio de información sin retraso alguno y de forma segura, de tal manera que coadyuve al logro de objetivos en ambos escenarios.

En el desarrollo de proyectos de redes, se utilizan tecnologías de información y comunicación para realizar sus labores diarias, es de vital importancia que los sistemas de información y específicamente la red que los conecta y comunica con internet funcionen correctamente, sin fallas, sin retrasos y garantizando la seguridad de la información que por ella fluye. Más aun, para lograr la eficiencia en la gestión pública, es necesario que los equipos, medios, y software de comunicaciones estén correctamente configurados respecto a la necesidad de la entidad, para que los funcionarios puedan laborar de la mejor manera, siendo respaldados por una red de datos confiable y rápida.

Por tanto, se requiere una solución que cumpla los requerimientos de los usuarios, y permita el normal desarrollo de sus funciones, de seguir así, continuarán los retrasos y hasta incumplimiento de los objetivos que exige cada escenario.

4. MARCO TEÓRICO

De acuerdo a la aplicación de forma general, con interfaz de usuaio en Packet Tracer, se identifica un tutorial donde puede establecerse un comparativo respecto a los ejercicios de los casos planteados, teniendo en cuenta la construcción de la interfaz.

A continuación, de forma literal, se relaciona uno de los tutoriales de Packet Tracer, que se utilizan para el desarrollo de soluciones, con relación a la conectividad, accesos, seguridad, entre otros.

4.1 “INTERFAZ DE USUARIO EN PACKET TRACER

De acuerdo a la aplicación de forma general, con interfaz de usuaio en Packet Tracer,

Packet tracer presenta una interfaz de usuario con tres menús principales que permiten acceder a todas las funcionalidades de forma rápida y sencilla (Figura 1), este menú te permiten:

1. Gestionar la red creada.
2. Añadir dispositivos y conectarlos a través de cables o inalámbricamente.
3. Seleccionar, eliminar, inspeccionar, etiquetar y agrupar los componentes dentro de su red

Figura 1. Menús principales en Packet Tracer

1.1. Menú de gestión de Red

El menú de gestión de red le permite:

- Abrir una red existente o demostrativa.
- Guardar la red actual.
- Modificar el perfil de usuario o las preferencias.

El menú Archivo es similar al de un procesador de texto como Word, este menú se encuentra en la barra de menú superior. Los comandos Abrir, Guardar, Guardar como y Salir funcionan como lo harían con cualquier programa, sin embargo, hay dos comandos que son especiales para Packet Tracer:

- El comando “Open Samples” mostrará un directorio de ejemplos pre-diseñados de funciones y configuraciones de varios dispositivos de red e Internet de las cosas incluidas en Packet Tracer (Figura 2).

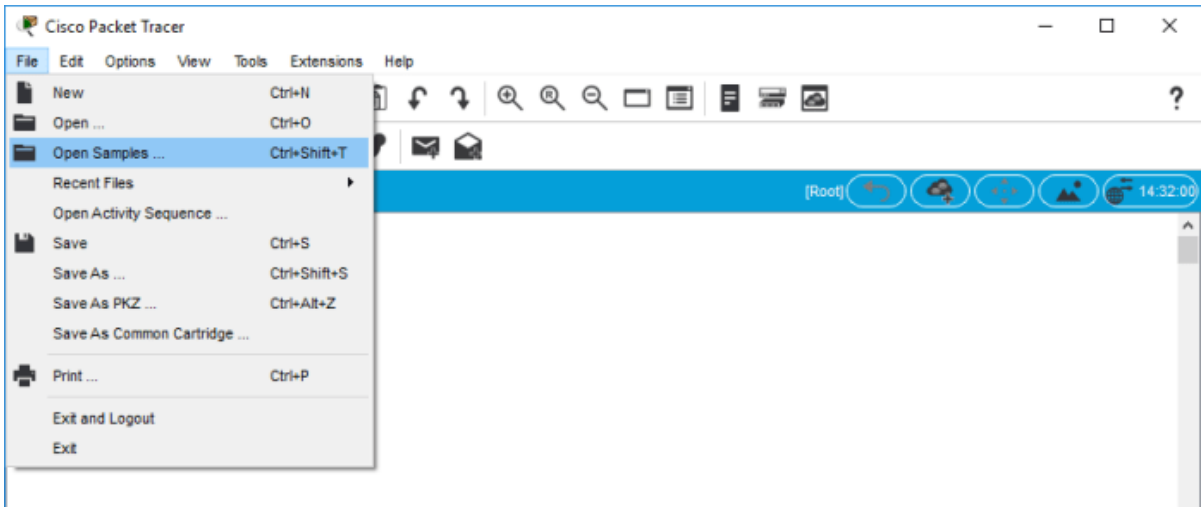


Figura 2. Comando “Open Samples” para abrir ejemplos en Packet Tracer

- El comando “Exit and Logout” eliminará la información de registro para la sesión establecida de Packet Tracer y requerirá que el siguiente usuario de Packet Tracer vuelva a realizar el procedimiento de inicio de sesión (Figura 3).

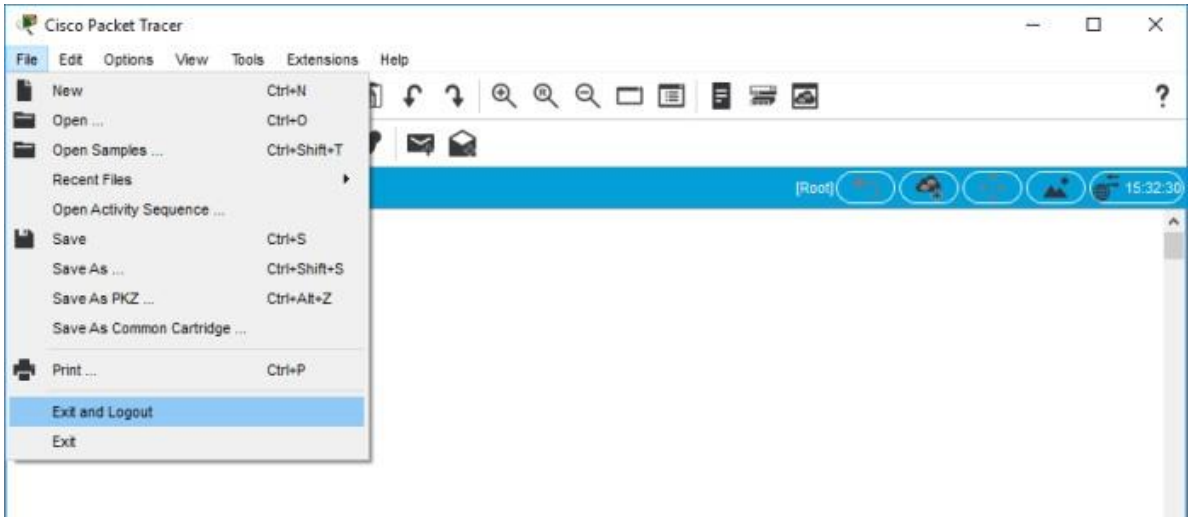


Figura 3. Comando Exit and Logout

1.2. Selección de dispositivos de red

Dado que Packet Tracer simula redes y tráfico de red, los aspectos físicos de estas redes también deben simularse. Esto incluye encontrar y desplegar dispositivos

físicos, personalizarlos y cablearlos. Una vez realizada la instalación física y el cableado, se debe configurar las interfaces utilizadas para conectar los dispositivos.

Encontrar un dispositivo para implementar requiere buscar en el Cuadro de selección de tipo de dispositivo. El Cuadro de selección de tipo de dispositivo funciona según el concepto de categorías y subcategorías, como se muestra en la Figura 4.

Figura 4. Agrupación de elementos en categorías y sub categorías

La fila superior de iconos representa la lista de categorías que consta de: [Dispositivos de red], [Dispositivos Finales], [Componentes], [Conexiones], [Varios] y [Multiusuario] (Figura 5). Cada categoría contiene al menos un grupo de subcategoría.

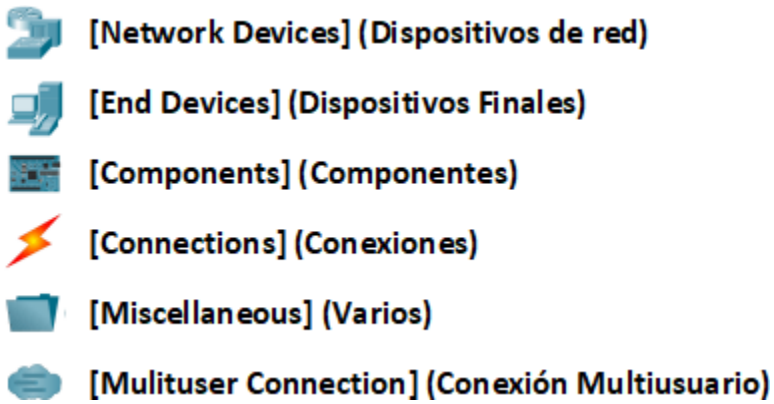


Figura 5. Categorías de elementos

Cada uno de estos elementos puede ser arrastrado al área central de Packet Tracer, por ejemplo, si queremos crear una topología en donde un Router Wireless se conecte mediante cable Ethernet a una PC y mediante WiFi a un Smartphone, deberemos seleccionar la categoría [Network Devices] para poder elegir un router wirless, y luego la categoría [End Devices] para elegir la PC y el Smartphone (Figura 6)

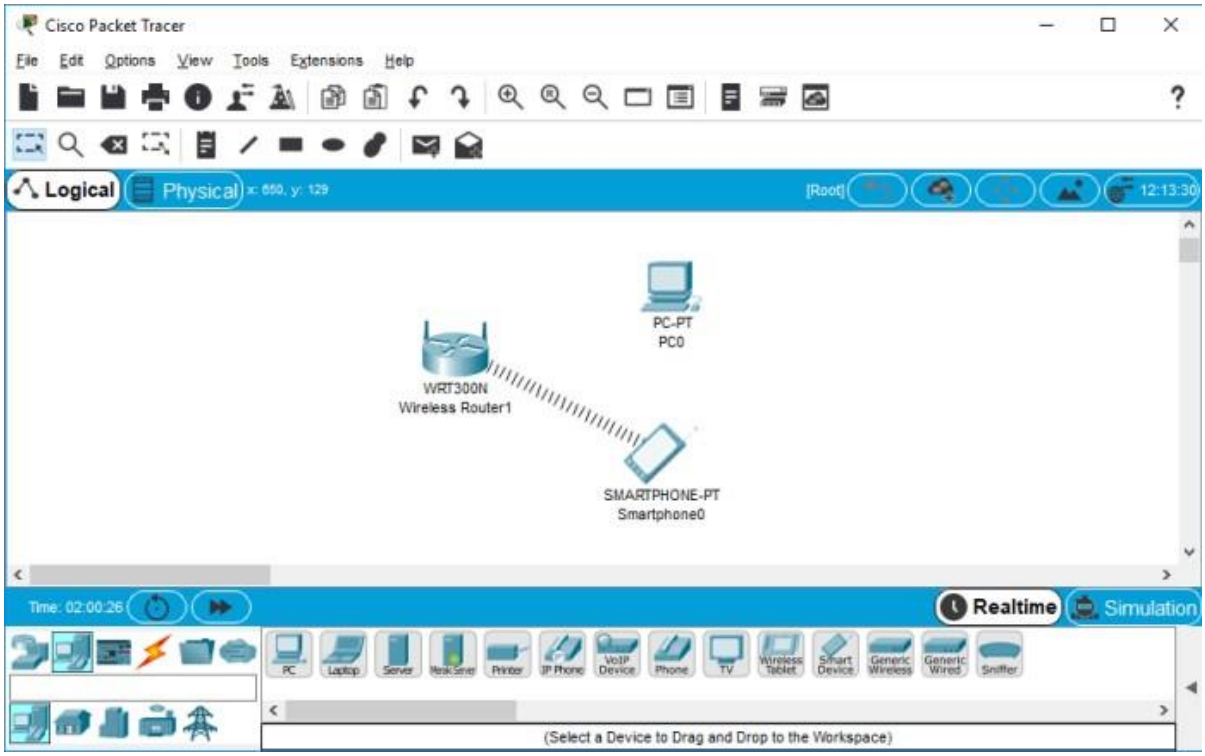


Figura 6. Añadir dispositivos en el área de trabajo"[1]

Como se puede observar en el caso anterio, puede presentarse como un tutorial introductorio del Packet Tracer, a partir el cual y de acuerdo con las topologías diseñadas, se formula la configuración de los comandos específicos para cada caso, de acuerdo con las necesidades.

[1] . Telectrónika, (2019). Packet Tracer: Introducción a la Interfaz de usuario. Recuperado de:https://telectronika.com/tutoriales/packet-tracer-interfaz-usuario/

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Las herramientas tecnológicas aplicadas fueron el programa de Cisco Packet Tracer como el simulador para dar soluciones a los dos escenarios en ellos encuentro las diferentes herramientas como Router, Pc, Switch cables de conexiones y donde lse aplican unas codificaciones y direccionamientos para que cada equipo cumplan con los requisitos solicitados, unos como administradores y otros con ciertas restricciones para controlar ciertas dependencias

5.2 METODOLOGÍA

La metodología de simulación aplicada para el desarrollo de la solución planteada para cada escenario, parte de una formulación del modelo conceptual a aplicar, previo análisis de las necesidades identificadas en cada escenario. A partir de ficho análisis se establece el diseño (topologías), que permitirá la construcción del diseño (interfaces y comandos), aplicando la verificación y validación respectiva, basados en la herramienta Packet Tracer.

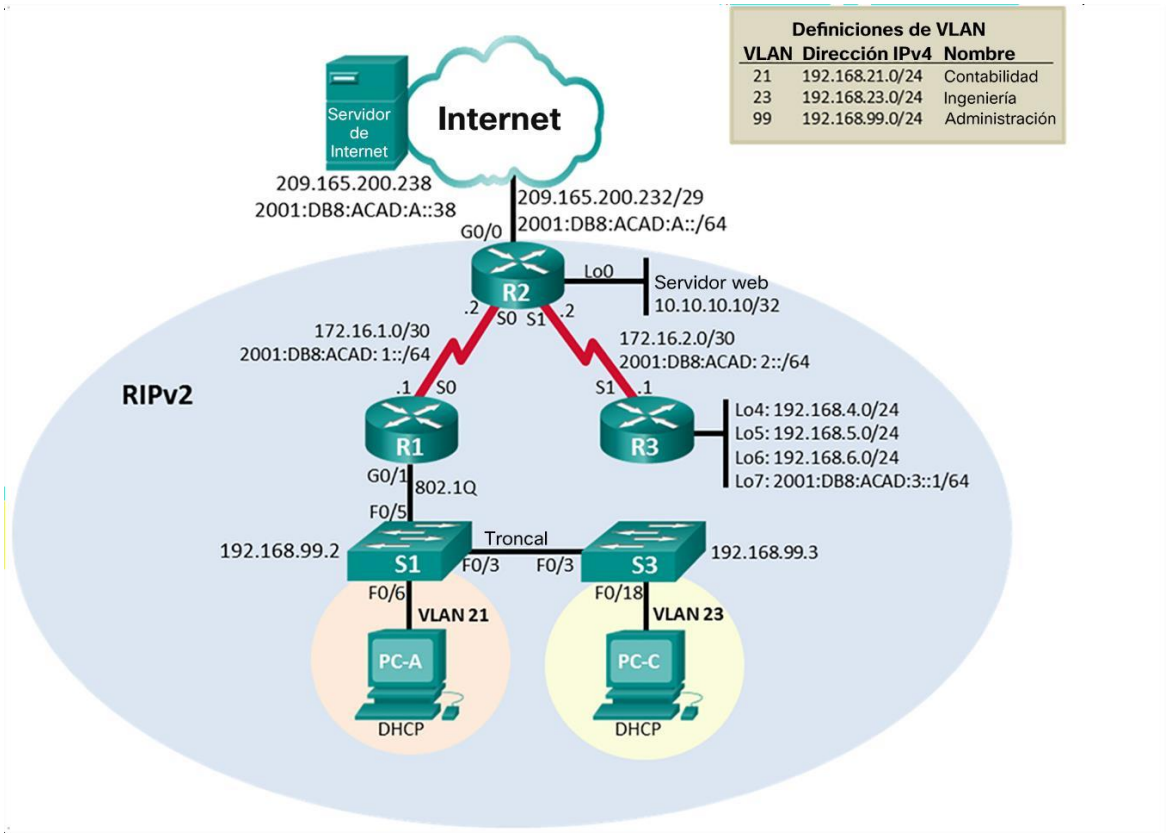
5. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

6.1 ESCENARIO 1

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 7 Topología de red

TOPOLOGIA DE RED



Parte 1: Inicializar dispositivos

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

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

COMPROMISO

Eliminar el archivo startup-config de todos los routers

R1

Router>enable
Router#erase startup-config

R2

Router>enable
Router#erase startup-config

R3

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[

Volver a cargar todos los routers

R1

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

R2

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)

R3

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

S1

Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]

Switch#

S3

Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]

Switch#

S1

Switch#reload
Proceed with reload? [confirm]

.

S3

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

S1

Switch>enable
Switch#show flash
Directory of flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)
Switch#

S3

Switch>enable
Switch#show flash
Directory of flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)
Switch#

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):f.autor

Table 1 Configurar la PC internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200. 238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200. 233

Dirección IPv6/subred	2001:db8:acad:a::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1 No puede ser modificad

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

Tabla 2 ip address

IP Address: 209.165.200.232	209.165.200.232
Network Address: 209.165.200.232	209.165.200.232
Usable host ip range	**209.165.200.233** **209.165.200.238**
Broadcast Address: 209.165.200.239	209.165.200.239
Total Number of Hosts:	8
Number of Usable Hosts:	6
Subnet Mask:	255.255.255.248

Tabla 3 Wildcard Mask:

Wildcard Mask:	0.0.0.7
Binary Subnet Mask	11111111.11111111.11111111.11111000
IP Type:	PUBLIC IP – CLASS C

Tabla 4 Total IP Addresses

IP Address;	2001:db8:acad:a::38/64
Total IP Addresses:	2001:0db8:acad:000a:0000:0000:0000:0038
Total IP Addresses	18,446,744,073,709,551,616
Network:	2001:0db8:acad:000a:: /64 2001:0db8:acad:000a:0000:0000:0000:0000 / 64

Ip Range	2001:db8:acad:a::1 2001:0db8:acad:000a:0000:0000:0000:0001 2001:db8:acad:a:ffff:ffff:ffff:ffff 2001:0db8:acad:000a:ffff:ffff:ffff:ffff
IP Type	GLOBAL UNICAST

Paso 1: Configurar la computadora de Internet

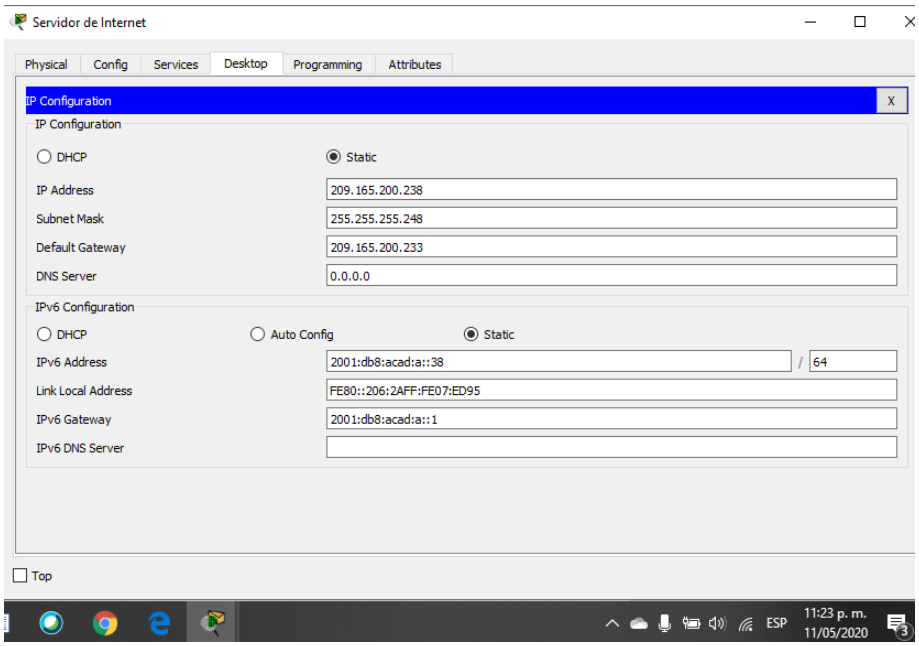


Figura 8 Paso 1: Configurar la computadora de Internet

Paso 2 : Configurar R1

Table 5 Elemento o tarea de configuración

Elemento o tarea de configuración
Desactivar la búsqueda DNS
Nombre del router
Contraseña de exec privilegiado cifrada
Contraseña de acceso a la consola
Contraseña de acceso Telnet
Cifrar las contraseñas de texto no cifrado
Mensaje MOTD
Interfaz S0/0/0
Rutas predeterminadas

Table 6

Especificación
R1
class
cisco
cisco
Se prohíbe el acceso no autorizado.
Establezca la descriptions 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
Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

```
R1#
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#clock rate 128000
^
% Invalid input detected at '^' marker.
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
::/


R1#
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#clock rate 128000
^
% Invalid input detected at '^' marker.
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
::/
^
```

Paso 3 : Configurar R2

La configuración del R2 incluye las siguientes tareas

Tabla 7 La configuración del R2 incluye las siguientes tareas

Elemento o tarea de configuración
Desactivar la búsqueda DNS
Nombre del router R2
Contraseña de exec privilegiado cifrada
Contraseña de acceso a la consola
Contraseña de acceso Telnet
Cifrar las contraseñas de texto no cifrado
Habilitar el servidor HTTP
Mensaje MOTD
Interfaz S0/0/0
Interfaz S0/0/1
Interfaz G0/0 (simulación de Internet)
Interfaz loopback 0 (servidor web simulado)
Ruta predeterminada

Parte 2:
Parte 3: Router>enable
Parte 4: Router#configure terminal
Parte 5: Enter configuration commands, one per line. End with CNTL/Z.
Parte 6: Router(config)#no ip domain-lookup
Parte 7: Router(config)#hostname R2
Parte 8: R2(config)#enable secret class
Parte 9: R2(config)#line console 0
Parte 10: R2(config-line)#password cisco
Parte 11: R2(config-line)#login
Parte 12: R2(config-line)#line vty 0 15
Parte 13: R2(config-line)#password cisco
Parte 14: R2(config-line)#login

Parte 15: R2(config-line)#service password-encryption
Parte 16: R2(config)#ip http server
Parte 17: ^
Parte 18: % Invalid input detected at '^' marker.
Parte 19: R2(config)#banner motd %no se autoriza el acceso prohibido.!%
Parte 20: R2(config)#int s0/0/0
Parte 21: R2(config-if)#description Connection to R1
Parte 22: R2(config-if)#ip address 172.16.1.2 255.255.255.252
Parte 23: R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown

R2>enable
Password:
R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#description Connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

R2(config-if)#
R2(config-if)#int g0/0
R2(config-if)#description Connection to Internet
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown

```
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description Simulated Web Server
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 g0/0
R2(config)#
```

Paso 4 Configurar R3

La configuración del R3 incluye las siguientes tareas

Tabla 8 Configurar R3

Elemento o tarea de configuración
Desactivar la búsqueda DNS
Nombre del router R3
Contraseña de exec privilegiado cifrada
Contraseña de acceso a la consola
Contraseña de acceso Telnet
Cifrar las contraseñas de texto no cifrado
Habilitar el servidor HTTP
Mensaje MOTD
Interfaz S0/0/0
Interfaz S0/0/1
Interfaz G0/0 (simulación de Internet)
Interfaz loopback 0 (servidor web simulado)
Ruta predeterminada

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd %no se autoriza el acceso prohibido.!%
R3(config)#int s0/0/1
R3(config-if)#description Connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown
```

Paso 1: Paso 5 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Configurar S1

Elemento o tarea de configuración
Desactivar la búsqueda DNS
Nombre del switch 1
Contraseña de exec privilegiado cifrada
Contraseña de acceso a la consola
Contraseña de acceso Telnet
Cifrar las contraseñas de texto no cifrado
Mensaje MOTD

witch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %no se autoriza el acceso prohibido.!%

Paso 6: Configurar S3.

La configuración del S3 incluye las siguientes tareas:

Tabla 10 Configurar S3.

Elemento o tarea de configuración
Desactivar la búsqueda DNS
Nombre del switch 2
Contraseña de exec privilegiado cifrada
Contraseña de acceso a la consola
Contraseña de acceso Telnet
Cifrar las contraseñas de texto no cifrado
Mensaje MOTD
Especificación
S3
class
cisco
cisco
Se prohíbe el acceso no autorizado.

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login

S3(config-line)#service password-encryption
S3(config)#banner motd %no se autoriza el acceso prohibido.!%
S3(config)#

Paso 7 : Verificar la conectividad de la red

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

Tabla 11 Verificar la conectividad de la red

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

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 = 1/3/11 ms

Prueba de ping desde R2 a R3

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 = 1/2/7 ms

Prueba de ping desde Servidor de Internet a Gateway predeterminado

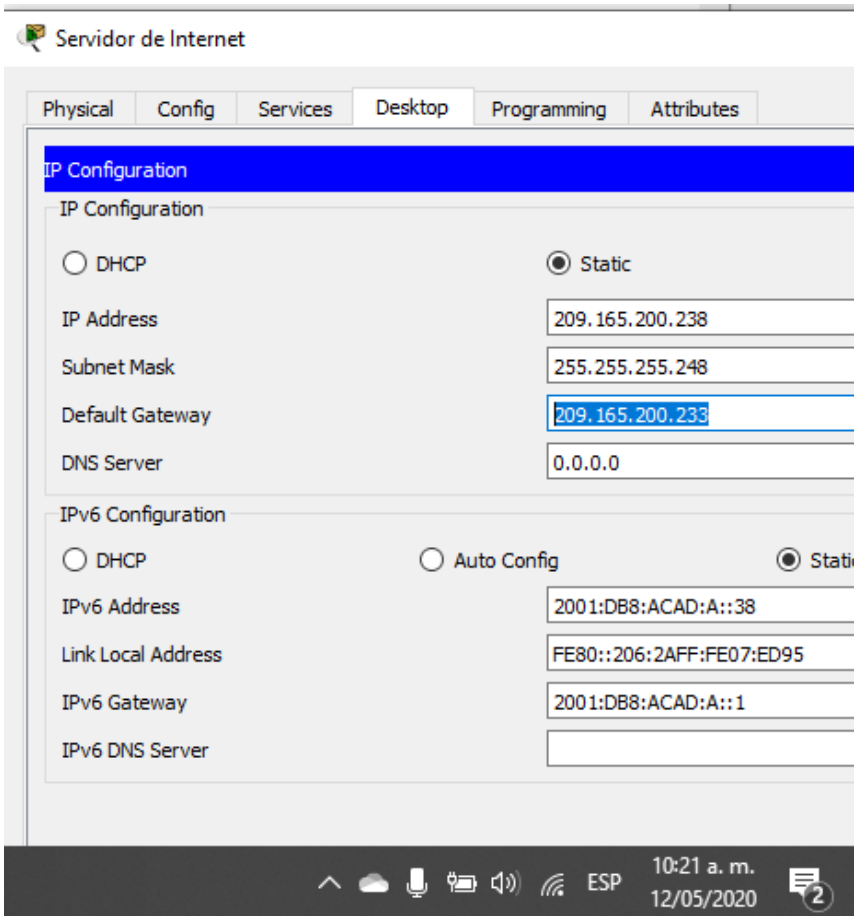


Figura 9 puerta de enlace

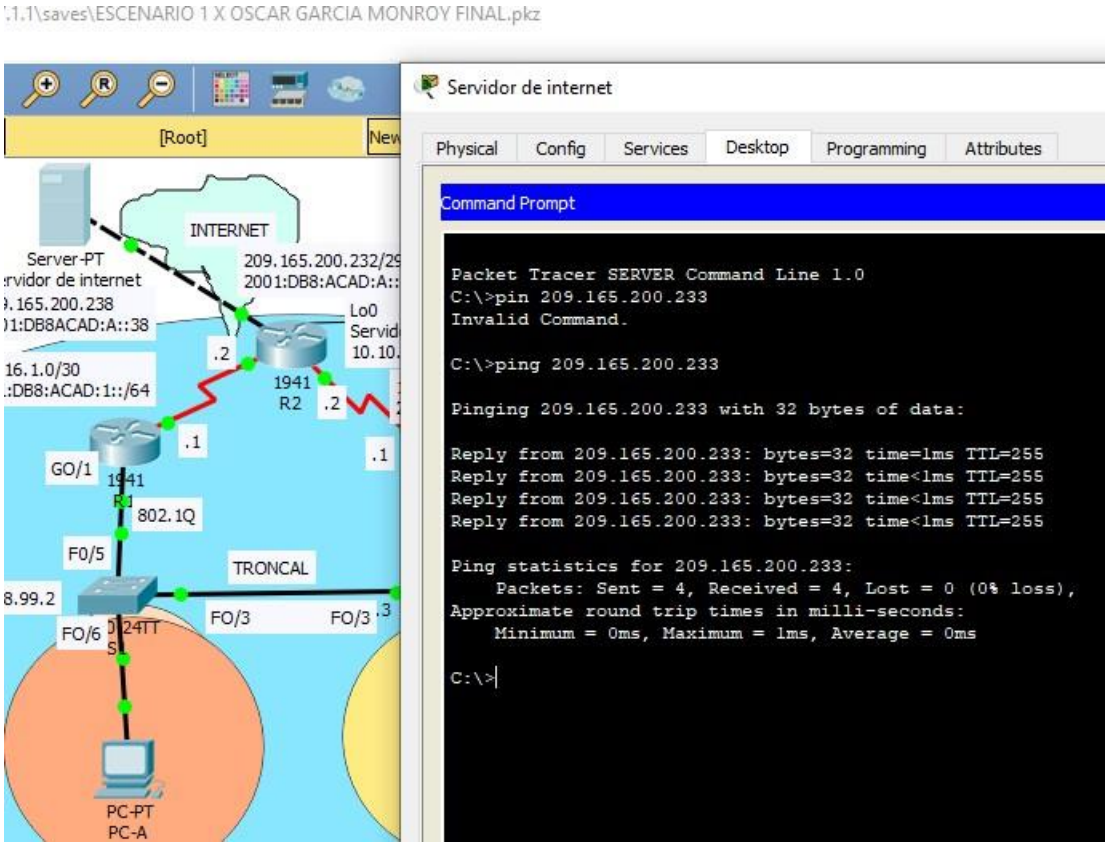


Figura 10 Servidor de internet

Tabla 12 descripción

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

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
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
Establecer la descripción. Establezca la dirección IPv4.
Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Paso 3; Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 13 Configurar R1

Elemento o tarea de configuración
Configurar la subinterfaz 802.1Q .21 en G0/1
Configurar la subinterfaz 802.1Q .23 en G0/1
Configurar la subinterfaz 802.1Q .99 en G0/1
Activar la interfaz G0/1
Especificación

Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Descripción: LAN de Administration Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz

S1
S1>enable
Password:
S1#enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#

S1(config-vlan)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#

```
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
```

Paso 2 configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14 configurar S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
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.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

```
S3>enable
Password:
S3#enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Accounting
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Management
S3(config-vlan)#exit
S3(config)#
S3#enable
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 99
S3(config-vlan)#
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#


S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switxhport mode trunk
               ^

S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#in range f0/1-2,f0/4-24,g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#


S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#in range f0/1-2,f0/4-24,g0/1-2
S3(config-if-range)#switchport mode access
```

```
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#in range f0/1-2,f0/4-17,f0/19-24,g0/1-2
S3(config-if-range)#shutdown
```

Paso 3; Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:
Tabla 14 Configurar R1

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

VLAN 21

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1,21
              ^
% Invalid input detected at '^' marker.

R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapaulation dotiq 21
                  ^
.

R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#
```

VLAN 23

```
R1(config-subif)#int g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#
```

VLAN 99

```
R1(config-subif)#int g0/1.99
R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
```

Paso: 4 Verificar la conectividad de la red

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

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

Tabla 15 Verificar la conectividad de la red

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

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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S3
S3#ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

S1

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 = 0/0/3 ms

S2

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

S3#

Parte 4 : Configurar el protocolo de routing dinámico RIPv2

Paso 2: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 Configurar el protocolo de routing dinámico RIPv2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Configurar RIP versión 2

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
 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(config-router)#network 172.16.1.0
R1(config-router)#network 172.168.21.0
R1(config-router)#network 172.168.23.0
R1(config-router)#network 172.168.99.0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
 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


R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
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

R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
```

```
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
R2(config-router)#
```

R3

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
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(config-router)#network 172.16.2.0
R3(config-router)#network 172.16.4.0
R3(config-router)#network 172.16.5.0
R3(config-router)#network 172.16.6.0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
R3(config-router)#end
R3#
```

Protocolo

```
R3#show ip protocols
Routing Protocol is "rip"
```

Paso 4 : Verificar la información de RIP

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

Tabla 17 Verificar la información de RIP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	
¿Qué comando muestra solo las rutas RIP?	
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	

R3#show ip route rip
10.0.0.0/32 is subnetted, 1 subnets
R 10.10.10.10 [120/1] via 172.16.2.2, 00:00:11, Serial0/0/1
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R 172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:11, Serial0/0/1
192.168.6.0 /24 is variably subnetted, 2 subnets, 2 masks

R3#show run
Building configuration...

Current configuration : 1504 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!

```
ipv6 address 2001:DB8:ACAD:3::1/64
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed  auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed  auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
description Connection to R2
ip address 172.16.2.1 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::1/64
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface Loopback4
passive-interface Loopback5
passive-interface Loopback6
network 172.16.0.0
no auto-summary
!
```

Parte 5 ; Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 Como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 Implementar DHCP y NAT para IPv4

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

Router 1

```
R1 (config)# ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#ip domain-name ccna-sa.com
R1(config)#ip dhcp pool Ingenieria
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#ip domain-name ccna-sa.com
R1(config)#
```

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

La configuración del R2 incluye las siguientes tareas:

Tabla 19 Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la authentication	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** **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	

Router 2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
          ^
% Invalid input detected at '^' marker.

R2(config)#ip http authentication local
          ^
% Invalid input detected at '^' marker.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 20 Verificar el protocolo DHCP y la NAT estática

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**	

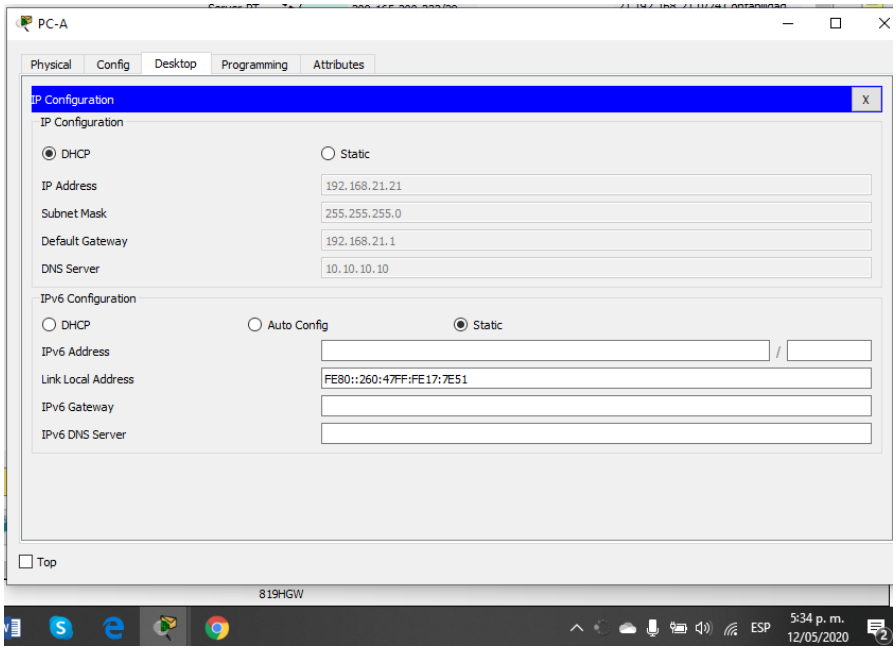


Fig 11
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

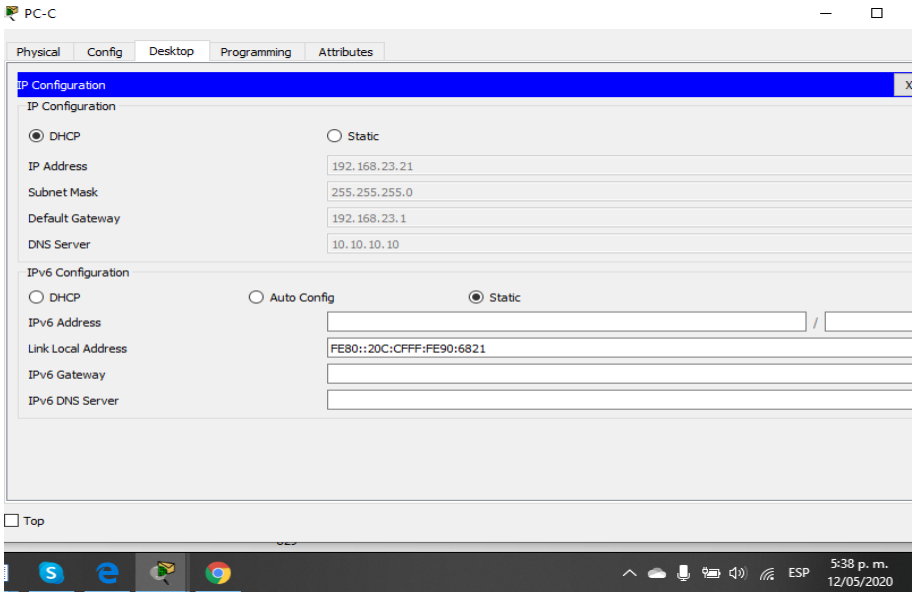


Fig 12
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

Pueda hacer ping a la PC-C

Nota: Quizá sea necesario deshabilitar el firewall de la PC.

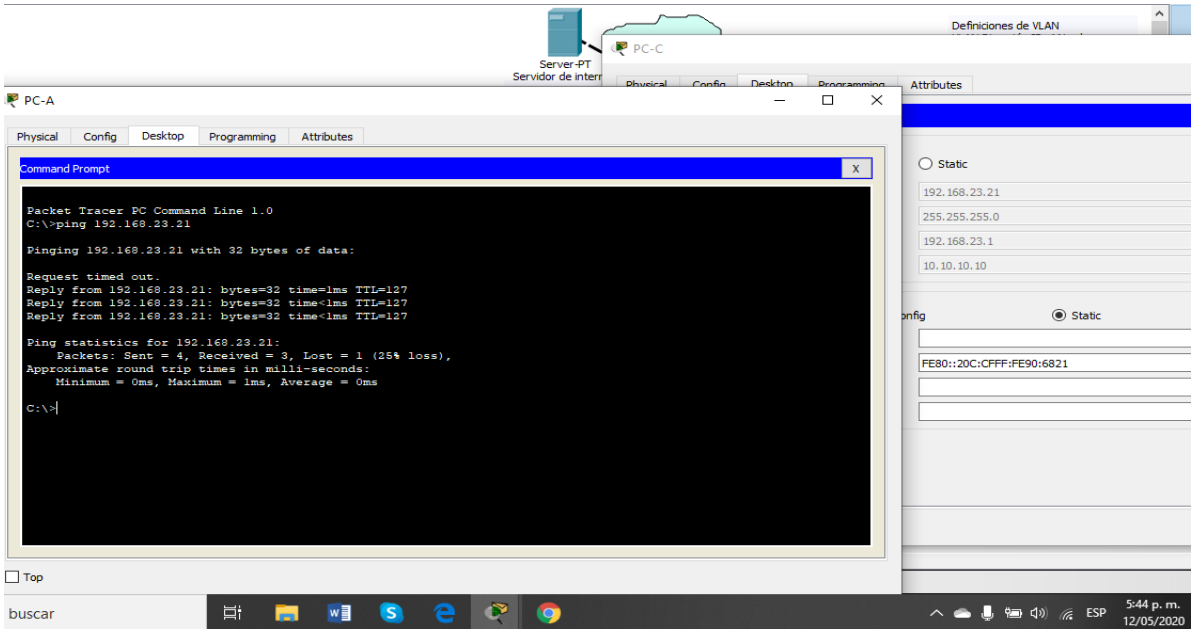


Fig 13

Verificar que la PC-A

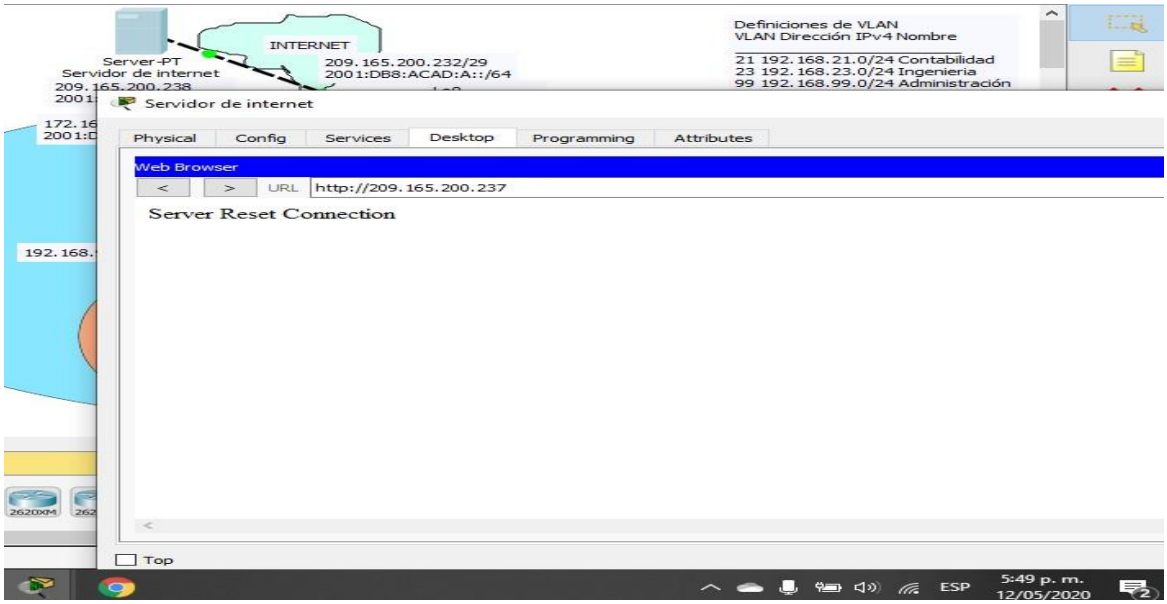


Figura 14 Navegador Web

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.**237**)

Parte 6 : Configurar NTP

Tabla 21 Configurar NTP

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.	

Ajuste la fecha y hora en R2.

R2#clock set 00:40:00 12 Mayo 2020
R2#configure termina
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5 (no lo permite)

Configurar R1 como un cliente NTP.

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

R1(config)#ntp update-calendar
R1(config)#

Verifique la configuración de NTP en R1.

R1#show ntp associations
% This command is not supported by Packet Tracer.

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

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

Tabla 22 Configurar y verificar las listas de control de acceso (ACL)

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	

Nombre de la ACL: **ADMIN-MGT**

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1

Aplicar la ACL con nombre a las líneas VTY

R2(config-std-nacl)#exit
R2(config)#line vty 0 15

R1#
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Openno se autoriza el acceso prohibido.!
User Access Verification
Password:
R2>exit
[Connection to 172.16.1.2 closed by foreign host]
R1#

```
R3#enable
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#
```

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

Tabla 23 comando de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	
Restablecer los contadores de una lista de acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	

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

R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

Restablecer los contadores de una lista de acceso

R2#clear ip access-list counters
^

R2#clear ip ?
bgp Clear BGP connections
dhcp Delete items from the DHCP database
nat Clear NAT
ospf OSPF clear commands
route Delete route table entries

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?
R2#show ip interface

IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected)
Internet address is 172.16.2.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled

IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Loopback0 is up, line protocol is up (connected)
Internet address is 10.10.10.10/32
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1514bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled

- ICMP redirects are always sent

¿Con qué comando se muestran las traducciones NAT?

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---

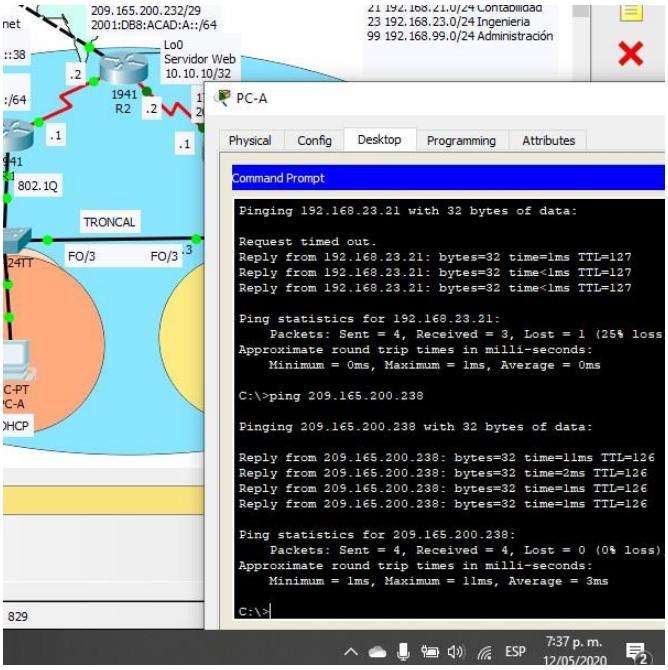


Fig 15
Prueba de ping al Servidor de Internet desde la PC-A

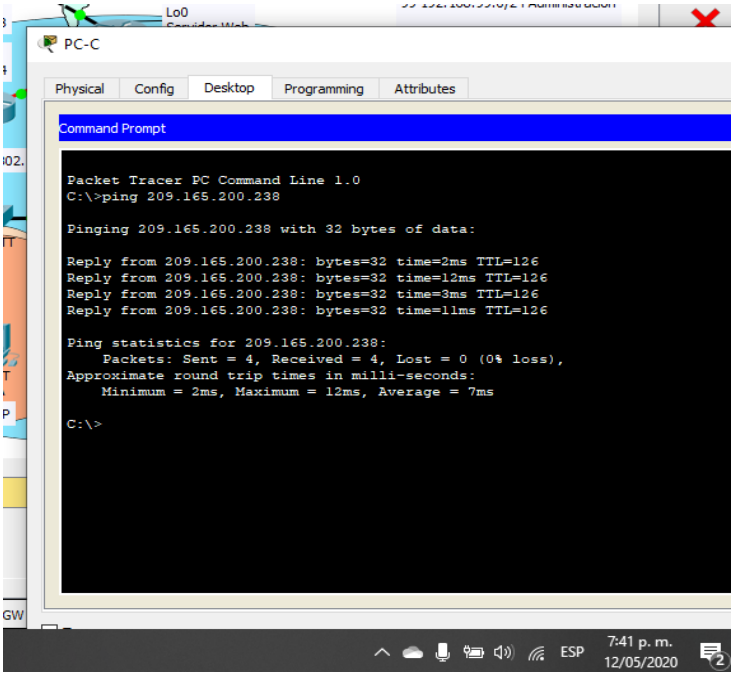


Fig 16
Prueba de ping al Servidor de Internet desde la PC-C

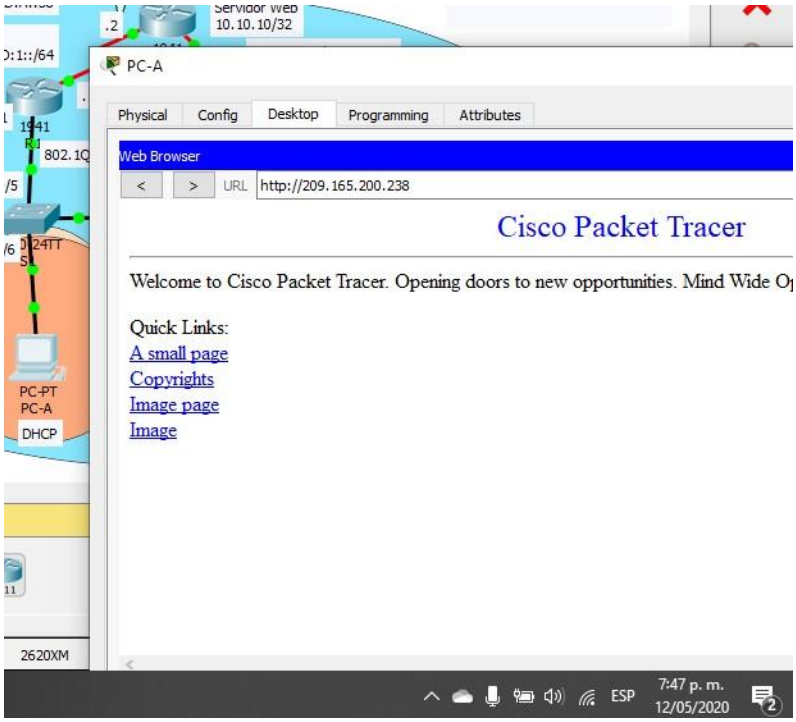


Fig 17
Prueba de acceso al Servidor de Web desde PC-A

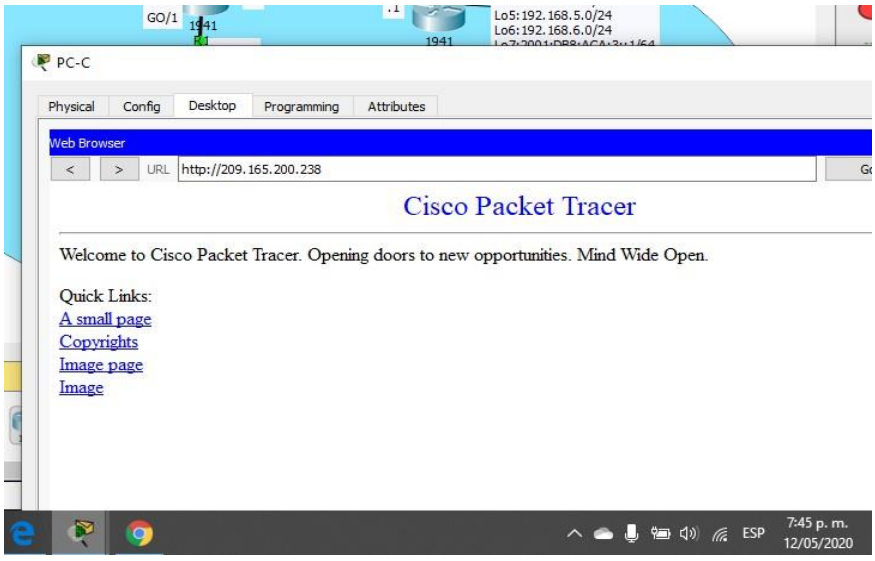


Fig 18
Prueba de acceso al Servidor de Web desde PC-C

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

Pro Inside global Inside local Outside local Outside global --- 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 209.165.200.234:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80 tcp 209.165 200.237:80 10.10.10.10:80 209.165.200.238:1033209.165.200.238:1033

R2#clear ip nat translation * R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.237 10.10.10.10 --- ---

Eliminar las traducciones de NAT dinámicas

Router#clear ip nat translation *
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---

Router# Cleanup

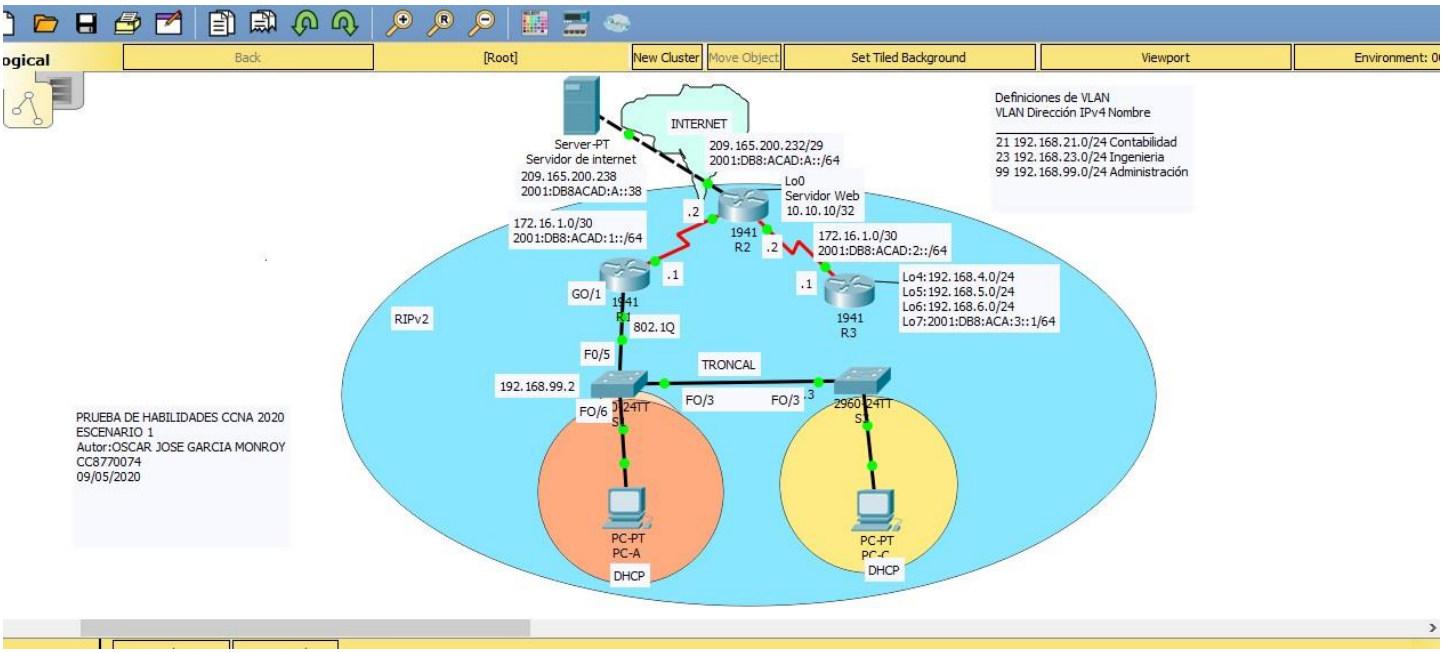
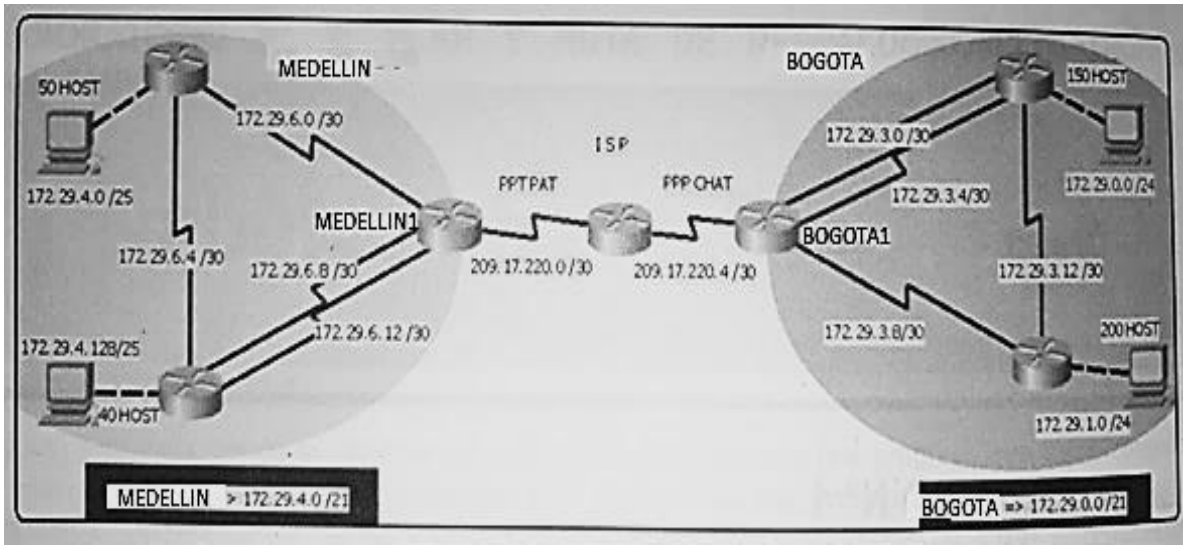


Fig 19
Evidencia de la topología del escenario 1

6.2 ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Figura 20 escenario 2



Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

Desarrollo

Como trabajo inicial se debe realizar lo siguiente:

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

- Realizar la conexión fisica de los equipos con base en la topología de red

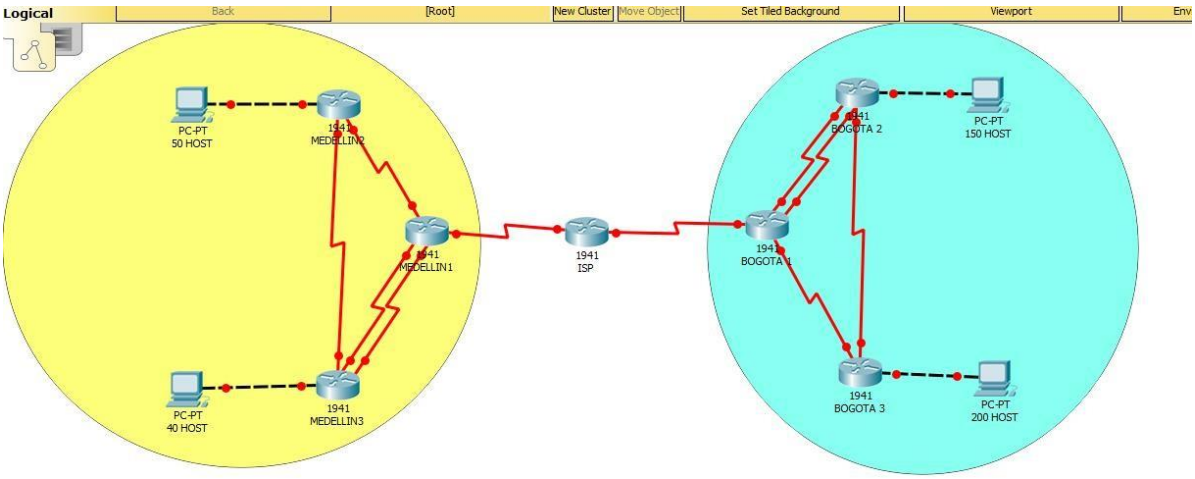


Figura 21 topologia del escenario 2

Identificación de Router Medellin2

```
R1>enable
password:
R1#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R1(config)#hostname Medellin2
Medellin2(config)#enable secret class
Medellin2(config)#service password-encryption
Medellin2(config)#banner motd "solo acceso autorizado"
Medellin2(config)#line console 0
Medellin2(config-line)#password cisco
Medellin2(config-line)#login
Medellin2(config-line)#exit
Medellin2(config)#line vty 0 15
Medellin2(config-line)#end
Medellin2(config-line)#login
Medellin2(config-line)#end
Medellin2#
```

Identificación de Router Medellin3

```
R2>enable
password:
R2#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R2(config)#hostname Medellin3
Medellin3(config)#enable secret class
Medellin3(config)#service password-encryption
Medellin3(config)#banner motd "solo acceso autorizado"
Medellin3(config)#line console 0
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#exit
```

Medellin3(config)#line vty 0 15
Medellin3(config-line)#password cisco
Medellin3(config-line)#login
Medellin3(config-line)#end
Medellin3#

Identificación de Router Medellin1

R3>enable
password:
R3#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R3(config)#hostname Medellin1
Medellin1(config)#enable secret class
Medellin1(config)#service password-encryption
Medellin1(config)#banner motd "solo acceso autorizado"
Medellin1(config)#line console 0
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#exit
Medellin1(config)#line vty 0 15
Medellin1(config-line)#password cisco
Medellin1(config-line)#login
Medellin1(config-line)#end
Medellin1#

Identificación de Router ISP

R4>enable
password:
R4#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R4(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#service password-encryption
ISP(config)#banner motd "solo acceso autorizado"
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login

ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#end

Identificación de Router Bogota1

R5>enable
password:
R5#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R5(config)#hostname Bogota1
Bogota1(config)#enable secret class
Bogota1 (config)#service password-encryption
Bogota1 (config)#banner motd "solo acceso autorizado"
Bogota1 (config)#line console 0
Bogota1 (config-line)#password cisco
Bogota1 (config-line)#login
Bogota1 (config-line)#exit
Bogota1 (config)#line vty 0 15
Bogota1 (config-line)#password cisco
Bogota1 (config-line)#login
Bogota1 (config-line)#end
Bogota1#

Identificación de Router Bogota2

R6>enable
password:
R6#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R6(config)#hostname Bogota2
Bogota2(config)#enable secret class
Bogota2 (config)#service password-encryption
Bogota2 (config)#banner motd "solo acceso autorizado"
Bogota2 (config)#line console 0
Bogota2 (config-line)#password cisco
Bogota2 (config-line)#login
Bogota2 (config-line)#exit

Bogota2 (config)#line vty 0 15
Bogota2 (config-line)#password cisco
Bogota2 (config-line)#login
Bogota2 (config-line)#end
Bogota2#

Identificación de Router Bogota3

R7>enable
password:
R7#configure terminal
Enter configuration commands, one per lien. End with CNTL/Z.
R7(config)#hostname Bogota3
Bogota3(config)#enable secret class
Bogota3 (config)#service password-encryption
Bogota3 (config)#banner motd "solo acceso autorizado"
Bogota3 (config)#line console 0
Bogota3 (config-line)#password cisco
Bogota3 (config-line)#login
Bogota3 (config-line)#exit
Bogota3 (config)#line vty 0 15
Bogota3 (config-line)#password cisco
Bogota3 (config-line)#login
Bogota3 (config-line)#end
Bogota3#

Especificaciones de la topologia de red
Tabla 23

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Máscara wildcard	Gateway predeterminado
Medellin1	S0/0/0	172.29.6.9	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.1	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.6.13	255.255.255.252	0.0.0.3	NA
	S0/1/1	209.17.220.1	255.255.255.252	0.0.0.3	NA
Medellin2	S0/0/0	172.29.6.5	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.2	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.4.1	255.255.255.128	0.0.0.127	NA
Medellin3	S0/0/0	172.29.6.6	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.6.10	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.6.14	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.4.129	255.255.255.128	0.0.0.127	NA
ISP	S0/0/0	209.17.220.2	255.255.255.252	0.0.0.3	NA
	S0/0/1	209.17.220.5	255.255.255.252	0.0.0.3	NA
Bogota1	S0/0/0	209.17.220.6	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.1	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.3.9	255.255.255.252	0.0.0.3	NA
	S0/1/1	172.29.3.5	255.255.255.252	0.0.0.3	NA
Bogota2	S0/0/0	172.29.3.2	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.13	255.255.255.252	0.0.0.3	NA
	S0/1/0	172.29.3.6	255.255.255.252	0.0.0.3	NA

	G0/0	172.29.0.1	255.255.255.0	0.0.0.255	NA
Bogota3	S0/0/0	172.29.3.10	255.255.255.252	0.0.0.3	NA
	S0/0/1	172.29.3.14	255.255.255.252	0.0.0.3	NA
	G0/0	172.29.1.1	255.255.255.0	0.0.0.255	NA
PC1_Med	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.1
PC2_Med	NIC	DHCP	255.255.255.128	0.0.0.127	172.29.4.129
PC1_Bog	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.0.1
PC2_Bog	NIC	DHCP	255.255.255.0	0.0.0.255	172.29.1.1

Configuración IP de los Router del Sistema de Red

Configuración IP de los Router Medellin 1

```
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#description Connection to Medellin3
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#description Connection to Medellin2
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#description Connection to Medellin3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
```

```
MEDELLIN1(config-if)#no shutdown

MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#description Connection to ISP
MEDELLIN1(config-if)#ip address 209.17.220.1 255.255.255.252
MEDELLIN1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#
```

Configuración IP Router Medellin2

```
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#security passwords min-length 10
MEDELLIN2(config)#interface s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN2(config-if)#exit
MEDELLIN2(config)#interface g0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.0
MEDELLIN2(config-if)#no shutdown

MEDELLIN2(config)#in g0/0
MEDELLIN2(config-if)#description Connection to PC1_Med
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#
```

Configuración IP Router Medellin3

```
MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)#description Connection to Medellin2
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

MEDELLIN3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up

MEDELLIN3(config-if)#exit
MEDELLIN3(config)#int s0/0/1
MEDELLIN3(config-if)#description Connection to Medellin1
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

MEDELLIN3(config-if)#e
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#int s0/1/0
MEDELLIN3(config-if)#description Connection to Medellin1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
MEDELLIN3(config-if)#
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#description Connection to PC2_Med
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

MEDELLIN3(config-if)#exi

Configuración IP Router ISP

ISP(config)#int s0/0/0
ISP(config-if)#description Connection to Medellin1
ISP(config-if)#ip address 209.17.220.2 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

ISP(config)#int s0/0/1
ISP(config-if)#description Connection to Bogota1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown

Configuración IP Router Bogota 1

BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#description Connection to ISP
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BOGOTA1(config-if)#
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#description Connection to Bogota2
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA1(config-if)#exit

int s0/1/0
BOGOTA1(config-if)#description Connection to Bogota3
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252

BOGOTA1(config-if)#description Connection to Bogota3
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BOGOTA1(config-if)#
BOGOTA1(config-if)#exit
BOGOTA1(config)#

BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#description Connection to Bogota2
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit

Configuración IP Router Bog

BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#description Connection to Bogota1
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#no shutdown

BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

BOGOTA2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BOGOTA2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down

BOGOTA2(config)#int s0/0/1
BOGOTA2(config-if)#description Connection to Bogota3
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 128000

BOGOTA2(config-if)#int s0/1/0
BOGOTA2(config-if)#description Connection to Bogota1
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.
^
% Invalid input detected at '^' marker.
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#no shutdown

BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

BOGOTA2(config)#int g0/0
BOGOTA2(config-if)#description Connection to PC1_Bog
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#no shutdown

BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Configuracion ip router Bogota 3

BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#description Connection to Bogota1
BOGOTA3(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA3(config-if)#no shutdown

BOGOTA3(config-if)#

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

BOGOTA3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

BOGOTA3(config-if)#exit
BOGOTA3(config)#int s0/0/1
BOGOTA3(config-if)#description Connection to Bogota2
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA3(config-if)#
BOGOTA3(config-if)#exit
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#description Connection to PC2_Bog
BOGOTA3(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA3(config-if)#no shutdown

BOGOTA3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

BOGOTA3(config-if)#exit
BOGOTA3(config)#

Parte 1: Configuración del enrutamiento

a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

Punto a:
Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 1.1.1.1
MEDELLIN1(config-router)#do show ip route

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C 172.29.6.0/30 is directly connected, Serial0/0/1
L 172.29.6.1/32 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/0/0
L 172.29.6.9/32 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/1/0
L 172.29.6.13/32 is directly connected, Serial0/1/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/1/1
L 209.17.220.1/32 is directly connected, Serial0/1/1

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.127 area 0
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3(config-router)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0

MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.127 area 0
```

```
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN3(config-router)#exit
```

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 4.4.4.4
BOGOTA1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/1/0
C 209.17.220.4/30 is directly connected, Serial0/0/0

BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#exit
BOGOTA1(config)#
```

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 5.5.5.5
BOGOTA2(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/0/1

BOGOTA2(config-router)#network 172.29.0.0 0.0.0.255 area 0
BOGOTA2(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA2(config-router)#
```

```
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 6.6.6.6
BOGOTA3(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1

BOGOTA3(config-router)#network 172.29.1.0 0.0.0.255 area 0
BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 0
```

```
ISP(config)#router ospf 1
ISP(config-router)#router-id 7.7.7.7
ISP(config-router)#do show ip route connected
C 209.17.220.0/30 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1

ISP(config-router)#network 209.17.220.0 0.0.0.3 area
% Incomplete command.
ISP(config-router)#network 209.17.220.0 0.0.0.3 area 0
```

Punto b

Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#exit
MEDELLIN1(config)#

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#exit
BOGOTA1(config)#
```

Punto C

El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

```
ISP#enable
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#
```

Parte 2: Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

b. Verificar el balanceo de carga que presentan los routers.

c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Punto a:
Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

MEDELLIN1#show ip route

MEDELLIN2#show ip route

MEDELLIN3#show ip route

BOGOTA1#show ip route

BOGOTA2#show ip route

BOGOTA3#show ip route

ISP#show ip route

Parte 3: Deshabilitar la propagación del protocolo OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 24 protocolo OSPF

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

```
MEDELLIN1#enable
MEDELLIN1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#


MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#exit


BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface s0/1/1
BOGOTA1(config-router)#
06:59:27: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1/1 from FULL to
DOWN, Neighbor Down: Interface down or detached

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface s0/1/0
BOGOTA2(config-router)#passive-interface g0/0

BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface g0/0
BOGOTA3(config-router)#exit
```

Parte 4: Verificación del protocolo OSPF.

a) Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

b) Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

a). Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

MEDELLIN1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
Passive Interface(s):
Serial0/1/0
Routing Information Sources:
Gateway Distance Last Update
Distance: (default is 110)

MEDELLIN2#show ip protocols

Routing Protocol is "ospf 1"
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:
172.29.4.0 0.0.0.127 area 0
172.29.6.0 0.0.0.3 area 0
172.29.6.4 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
2.2.2.2 110 00:03:42

MEDELLIN3#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.4.128 0.0.0.127 area 0
172.29.6.4 0.0.0.3 area 0
172.29.6.8 0.0.0.3 area 0
172.29.6.12 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
3.3.3.3 110 00:06:17
Distance: (default is 110)

BOGOTA1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 4.4.4.4
It is an autonomous system boundary router
Redistributing External Routes from,
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.3.0 0.0.0.3 area 0
172.29.3.4 0.0.0.3 area 0
172.29.3.8 0.0.0.3 area 0
209.17.220.4 0.0.0.3 area 0
Passive Interface(s):
Serial0/1/1
Routing Information Sources:
Gateway Distance Last Update
4.4.4.4 110 00:27:04
5.5.5.5 110 00:40:13
Distance: (default is 110)

BOGOTA2#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 5.5.5.5
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.0.0 0.0.0.255 area 0
172.29.3.0 0.0.0.3 area 0
172.29.3.4 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/1/0
Routing Information Sources:
Gateway Distance Last Update
4.4.4.4 110 00:41:56
5.5.5.5 110 00:28:14

BOGOTA3#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 6.6.6.6
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.1.0 0.0.0.255 area 0
172.29.3.8 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
6.6.6.6 110 00:13:41
Distance: (default is 110)

ISP#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 7.7.7.7
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
209.17.220.0 0.0.0.3 area 0
Routing Information Sources:
Gateway Distance Last Update
7.7.7.7 110

b .Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.
Resuelto el punto anterior con **show ip route**.

Parte 5: Configurar encapsulamiento y autenticación PPP.

a).Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

b).El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT.

a).Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

MEDELLIN1(config-if)#interface Serial 0/1/1
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#username ISP secret cisco
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN password cisco
MEDELLIN1(config-if)#exit

MEDELLIN1(config)#

```
BOGOTA1(config)#interface Serial 0/0/0
BOGOTA1(config-if)#encapsulation  ppp
BOGOTA1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to down

BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#exit
BOGOTA1(config)#username ISP secret cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#exit
    BOGOTA1(config)#


ISP(config)#interface Serial0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface Serial0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#username MEDELLIN secret cisco
ISP(config)#int s0/0/0
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#ex
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up

ISP(config)#username BOGOTA secret cisco
ISP(config)#int s0/0/1
ISP(config-if)#ppp authentication chap
ISP(config-if)#exit
    ISP(config)#
```

Parte 6: Configuración de PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

```
MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.127
MEDELLIN1(config-std-nacl)#ip nat inside source list HOST interface s0/1/1
overload
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#

MEDELLIN1#show ip nat translation
```

```
BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
BOGOTA1(config)#ip nat inside source list HOST interface s0/0/0 overload
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#exit
BOGOTA1#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA1#show ip nat translation
BOGOTA1#
```

```
MEDELLIN1#ping 172.29.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN1#enable
MEDELLIN1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#int s0/0/1
MEDELLIN1(config-if)#description Connection to Medellin2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/0/0
MEDELLIN1(config-if)#description Connection to Medellin3
```

MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up

MEDELLIN1(config-if)#int s0/0/0
MEDELLIN1(config-if)#description Connection to Medellin3
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN1(config-if)#

MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN1#ping 172.29.6.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.2, timeout is 2 seconds:

BOGOTA1#ping 172.29.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

BOGOTA1#ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

BOGOTA1#ping 172.29.3.10

BOGOTA1#

Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
d.Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2

MEDELLIN2>enable
Password:
MEDELLIN2#enable
MEDELLIN2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.29
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#

Como el router Medellin3 tiene una red LAN conectada pero no realizará las veces de servidor DHCP, es necesario configurar “ip helper” el cual permitirá ser un router de tránsito para llegar al router con el rol de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de Medellin2, se debe utilizar la dirección IP de la interfaz de salida Medellin2 (s0/0/0 - 172.29.6.5):

MEDELLIN3#enable
MEDELLIN3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address **172.29.6.5**
MEDELLIN3(config-if)#exit
MEDELLIN3(config)#

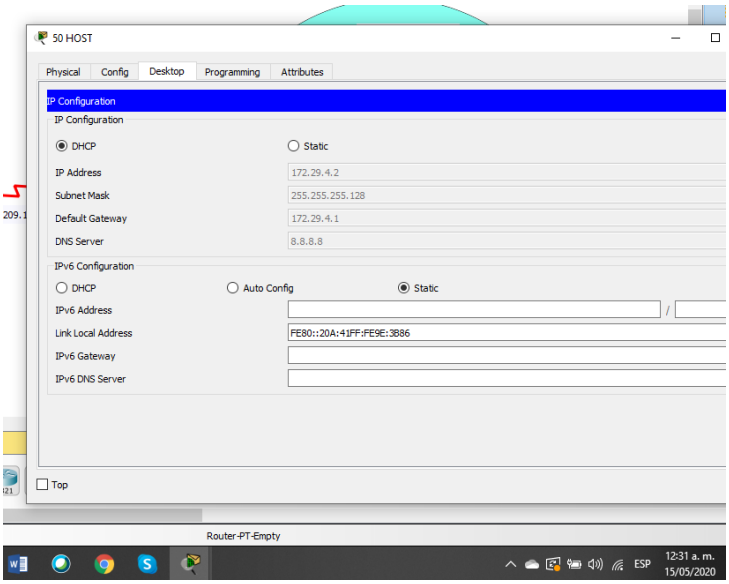


Fig 22 del DHCP de la PC A

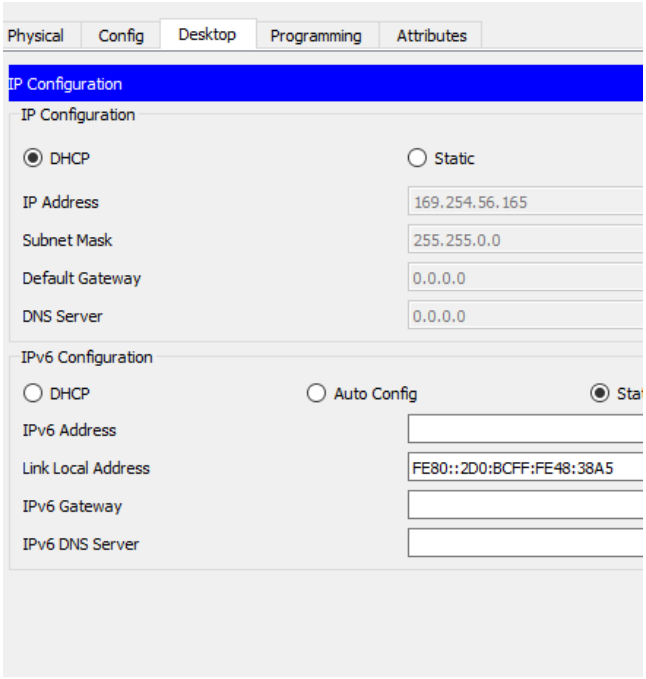


Figura 23 DHCP PC b

c.Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

d.Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1
BOGOTA2(config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#
```

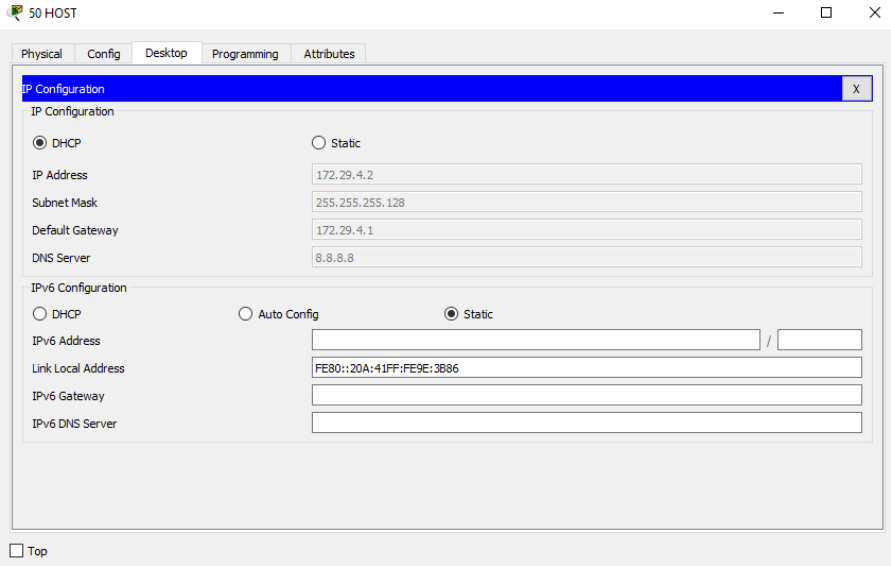


Figura 24 del DHCP pc c

Se puede decir que el router Bogota3 tiene una red LAN conectada pero no realizará las veces de servidor DHCP, es necesario configurar “ip helper” el cual permitirá ser un router de tránsito para llegar al router con el rol de DHCP. Por lo anterior utilizamos el comando ip helper-addres para atrapar los broadcasts y redireccionarlos hacia la IP del router de Bogota2, se debe utilizar la dirección IP de la interfaz de salida Bogota2 (s0/0/1 - 172.29.3.13):

```
BOGOTA3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
BOGOTA3(config-if)#exit
BOGOTA3(config)#
```

Configuarcion del Pc 1

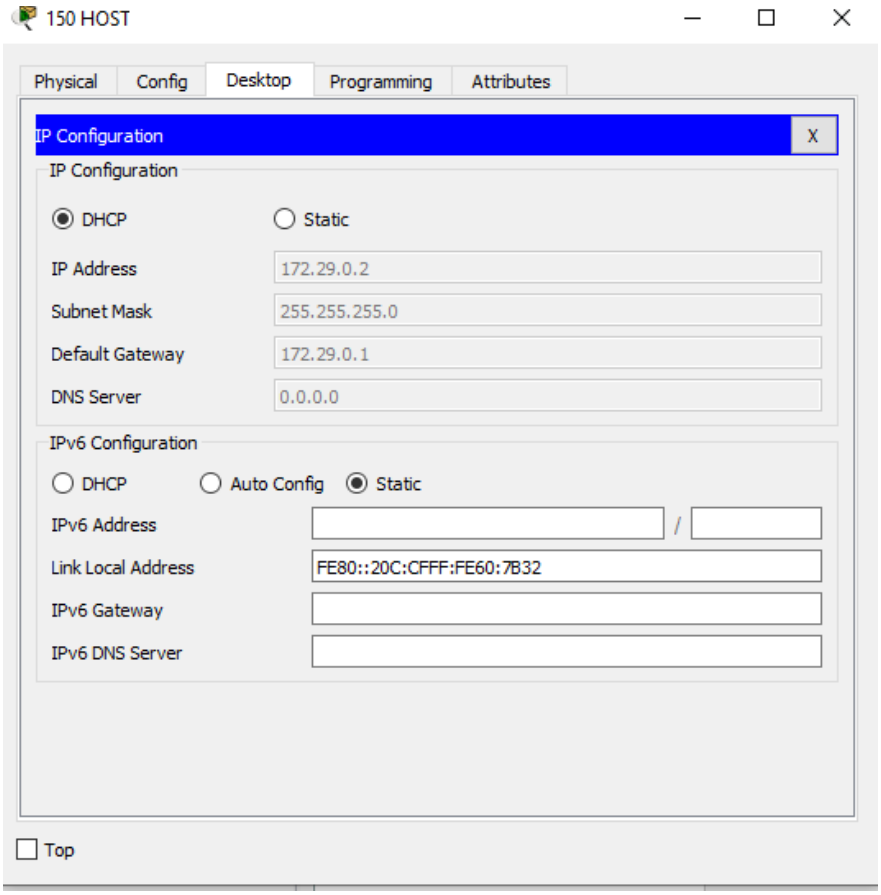


Figura 25 Configuarcion del Pc 1

Configuarcion del Pc 2

Guardar los cambios realizados en la configuración activa (RAM) a un archivo de configuración de respaldo (NVRAM) que es el que será utilizado en caso de que por cualquier motivo el dispositivo sea reiniciado.

ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#

MEDELLIN1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

MEDELLIN2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

MEDELLIN3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

BOGOTA1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

BOGOTA2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration..BOGOTA3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

Topologia de red escenario 2 - Cisco Packet Tracer

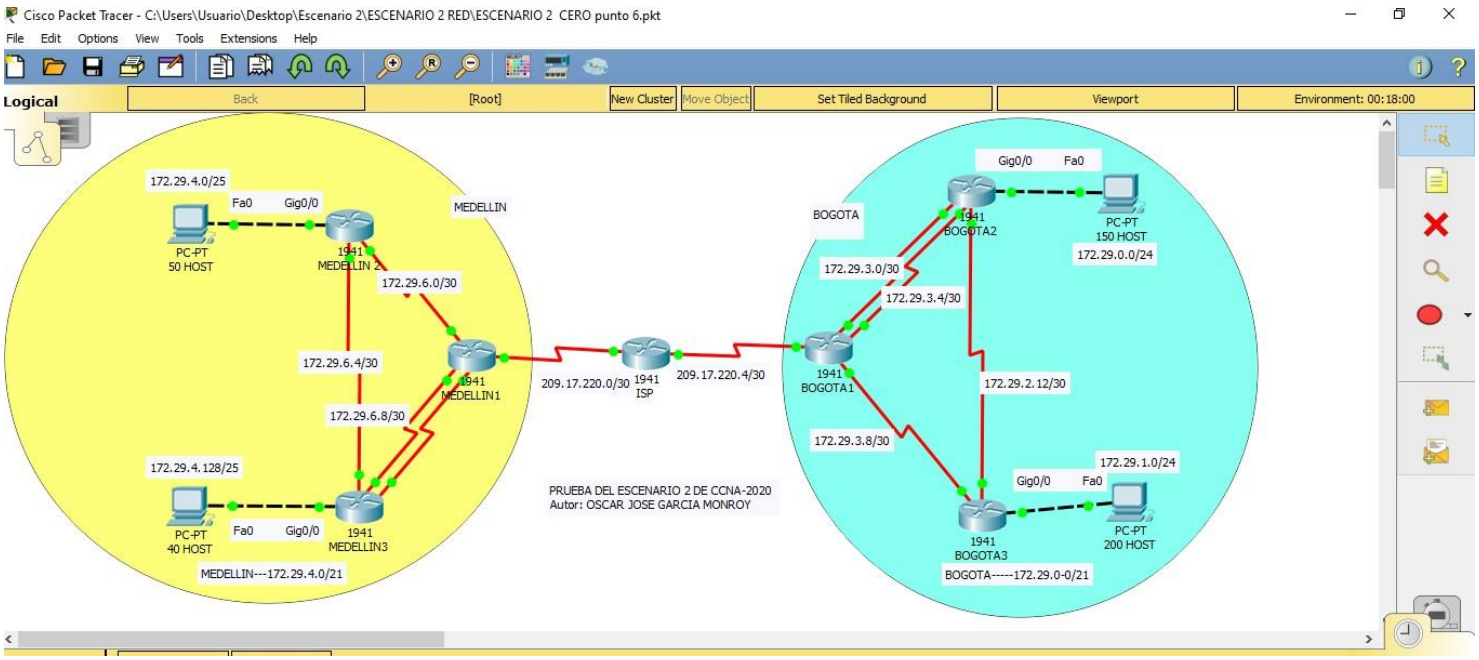


Figura 26 topologia de red del escenario 2

6.3 ANÁLISIS DEL DESARROLLO DEL PROYECTO

- Se dio solución práctica del escenario propuesto teniendo como base fundamental cada uno de los conocimientos adquiridos durante el desarrollo del Diplomado de Profundización CCNA en cuanto a la implementación y diseño de la topología física y lógica de una red.

- Se identificó cada uno de los dispositivos que intervienen en el proceso de configuración del sistema de redes y su implementación de acuerdo a los requisitos establecido en la guía de actividades prácticas.

- Se reconocieron los dispositivos PC, Router, Swiches, y los diferentes cables y tarjetas de configuración de cada componente utilizado en el Sistema.

- Aplicación de los protocolos de conexión de acuerdo al requisito indicado en la Guia de Actividades, aplicando todo el conocimiento adquirido durante el desarrollo del Diplomado. Implementados en la Herramienta de Simulación Packet Tracer.

- Se demostró el conocimiento, habilidades y destrezas en la configuración y enrutamiento de cada uno de los dispositivos que conforman el sistema de redes de acuerdo al requisito establecido en esta actividad

- Se aplicó los conceptos fundamentales aprendidos en la unidad CCNA2, como lo es el protocolo de Routing dinámico, OSPFv2 para el caso de ipv4 respectivamente

- Se aplicaron los conocimientos adquiridos a lo largo del curso de Profundización Cisco CCNA I y II, y sobre todo relacionados con el protocolo de enrutamiento denominado OSPF, aplicando la configuración para cada dispositivo de red de acuerdo a la tipología de red establecida.

- Se Impulsa el uso de nuevas tecnologías en base a lo aprendido en el diplomado como es el uso del Software o herramienta de simulación Cisco Packet Tracert, en la cual permite simular en forma real la configuración de cada red de acuerdo a su topología.

CONCLUSIONES

El análisis, a nivel personal, es la satisfacción de sacar adelante este proyecto con las dos pruebas de escenario, y obtener un resultado positivo cumpliendo con las expectativas con el Diplomado.

Lo más significativo del desarrollo, primero lograr la topología que cumplieran con las interfaces y después el desarrollo de cada pregunta que era siempre una expectativa que dieran el resultado esperado.

Aplicar los protocolos de conexión de acuerdo al requisito indicado en la Guía de Actividades, aplicando todo el conocimiento adquirido durante el desarrollo del Diplomado. Implementados en la Herramienta de Simulación Packet Tracer.

Demostrar el conocimiento, habilidades y destrezas en la configuración y enrutamiento de cada uno de los dispositivos que conforman el sistema de redes de acuerdo al requisito establecido en esta actividad

Aplicar los conceptos fundamentales aprendidos en la unidad CCNA2, como lo es el protocolo de Routing dinámico, OSPFv2 para el caso de ipv4 respectivamente

Aplicar los conocimientos adquiridos a lo largo del curso de Profundización Cisco CCNA I y II, y sobre todo relacionados con el protocolo de enrutamiento denominado OSPF, aplicando la configuración para cada dispositivos de red de acuerdo a la tipología de red establecida.

Impulsar el uso de nuevas tecnologías en base a lo aprendido en el diplomado como es el uso del Software o herramienta de simulación Cisco Packet Tracert, en la cual permite simular en forma real la configuración de cada red de acuerdo a su topología.

Quiero concluir de manera personal de acuerdo a mi perfil profesional, son los nuevos conocimientos adquiridos para colocarlos en práctica en mi vida profesional y como un diplomado puede hacerte competente en Redes.

BIBLIOGRAFÍA

Arumadigital (Dirección). (2013). Redes 110 Switching Enrutamiento Inter Vlan Tradicional Practica.

Capa de Aplicación CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1. (s.f.).

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

Felipe, J. (2012). *Juan Felipe*. https://youtu.be/OSACL0bLJrY (Compositor). (2013). configuracion de red con dos routers packet tracer.-Networking, C. (23 de 05 de 2018).

Telectrónika, (2019). Packet Tracer: Introducción a la Interfaz de usuario. Recuperado de:https://telectronika.com/tutoriales/packet-tracer-interfaz-usuario/