SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

PRESENTADA POR:
JHON JARLIN PALACIOS PALACIOS

PRESENTADO A
DIEGO EDINSON RAMIREZ CLAROS

DIPLOMADO DE PROFUNDIZACION EN REDES CISCO
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS DE TECNOLOGIAS E INGENIERIAS
CEAD QUIBDO

MAYO DE 2020

NOTA DE ACEPTACION:

_____

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

ATRATO – YUTO, 10 DE MAYO DE 2020

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

Enrutamiento: es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad

Protocolos: son una lista de Control de Acceso, las ACLs permiten asignar permisos a usuarios o a grupos. Una ACL puede permitir o denegar el acceso de usuarios concretos a objetos protegidos

Encapsulamiento: son los datos que atraviesan la red y van siendo gestionados por diferentes elementos desde el origan al destino

NAT: Es el proceso de hacer que redes de ordenadores utilicen un rango de direcciones especiales y se conecten a Internet usando una única dirección IP... También se utiliza para conectar redes domésticas a Internet

ACL: es un concepto de seguridad informática usado para fomentar la separación de privilegios, esto permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches

LAN: red de área local en ingles Local Area Network es una red de computadores que funciona espacios limitadamente pequeños, como por ejemplo una casa, edificio.

WAN: es una red de área amplia que se encarga de unir redes de computadoras locales.

RESUMEN

La Universidad Nacional Abierta y a Distancia en convenio con CISCO Networking Academia, han puesto a disposición el diplomado: “CISCO diseño e implementación de redes LAN-WAN”, esto ha hecho que los estudiantes adquieran mayor conocimiento en lo que es la elaboración de prototipos de redes que permitan dar repuestas a las necesidades que día a día surge en las empresas.

Gracias a ello se ha podido establecer que el estudio del material dispuesto en cada una de las unidades que conforman el curso, proporciona grandes competencias en el manejo adecuado de cada uno de los temas que en este se abordan. Como resultado del aprovechamiento de este diplomado hemos entendido que en la actualidad la Tecnologías de la Información y Comunicación han permitido llevar la globalidad al mundo de la comunicación, facilitando la interconexión entre las personas e instituciones a nivel mundial, y eliminando barreras espaciales y temporales.

Palabras claves: redes, tecnología comunicación

ABSTRACT

The National Open and Distance University in agreement with CISCO Networking Academy, have made available the diploma: "CISCO design and implementation of LAN-WAN networks", this has made students acquire greater knowledge in what is the development of prototypes of networks that allow responding to the needs that arise day by day in companies.

Thanks to this, it has been established that the study of the material arranged in each of the units that make up the course provides great competencies in the proper handling of each of the topics covered in it. As a result of taking advantage of this diploma, we have understood that currently Information and Communication Technologies have allowed us to bring globality to the world of communication, facilitating the interconnection between people and institutions worldwide, and eliminating spatial and temporal barriers.

Keywords: networks, technology, communication

INTRODUCCION

Cisco Packet Tracer es un potente programa de simulación de red que permite a los estudiantes experimentar con el comportamiento de la red y se preguntan "¿qué pasaría si" las preguntas. Como parte integral de la experiencia de aprendizaje integral Networking Academy, Packet Tracer ofrece simulación, visualización, creación, evaluación y capacidades de colaboración y facilita la enseñanza y el aprendizaje de los conceptos tecnológicos complejos.

Packet Tracer complementa equipo físico en el aula, al permitir a los estudiantes a crear una red con un número casi ilimitado de dispositivos, fomentar la práctica, el descubrimiento y solución de problemas. El ambiente de aprendizaje basado en la simulación ayuda a los estudiantes a desarrollar habilidades del siglo 21, tales como la toma de decisiones, el pensamiento creativo y crítico y resolución de problemas. Packet Tracer complementa los planes de estudios de Networking Academy, permite a los instructores para enseñar y demostrar fácilmente complejos conceptos técnicos y diseño de sistemas de redes.

En la actualidad los sistemas educativos de todo el mundo se enfrentan al desafío de utilizar las tecnologías de la información y la comunicación para proveer a sus alumnos con las herramientas y conocimientos necesarios que se requieren en el siglo XXI.

Los profesionales de TIC combinan correctamente los conocimientos, prácticas y experiencias para atender tanto la infraestructura de tecnología de información de una organización y las personas que lo utilizan. Asumen la responsabilidad de la selección de productos de hardware y software adecuados para una organización. Se integran los productos con las necesidades y la infraestructura organizativa, la instalación, la adaptación y el mantenimiento de los sistemas de información, proporcionando así un entorno seguro y eficaz que apoya las actividades de los usuarios del sistema de una organización.

OBJETIVOS

OBJETIVO GENERAL

- Solucionar los casos de estudios planteados en la prueba de habilidades que hace parte del diplomado de profundización en redes cisco, mediante la utilización de la herramienta Packet Tracer

OBJETIVOS ESPESIFICOS

- Poner en practica los conocimientos adquiridos en el materiar de estudio que conforman cada una de las unidades de este curso
- Desarrollar hablididades que nos permitan solucionar problemas en nuestra vida diaria como futuros ingenieros de sistemas.
- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Realizar configuración básica a dispositivos de comunicación Como Routers, Switch, Servidores.
- Determinar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing.
- Implementar de DHCP y NAT en dispositivos de comunicación

DESARROLLO

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.

Topología

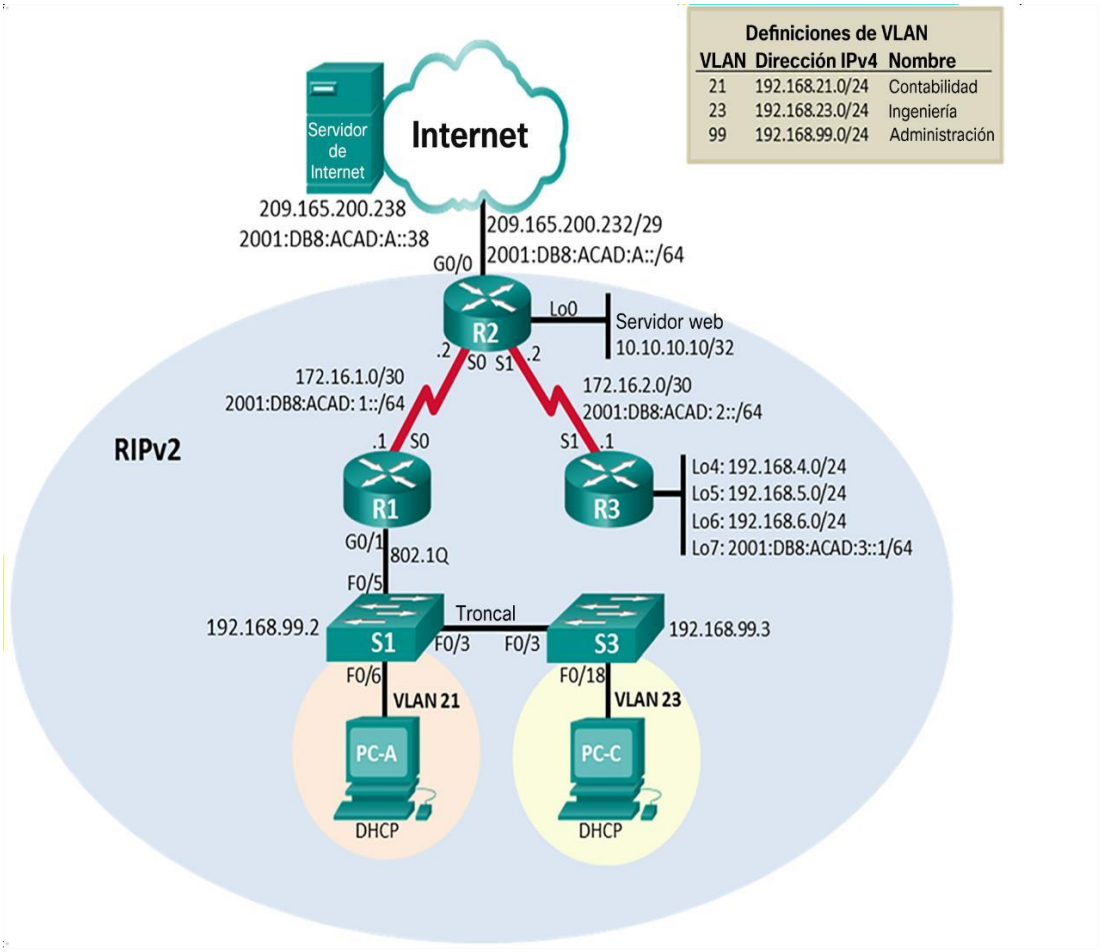


Fig. 1

Tipologia de la Red

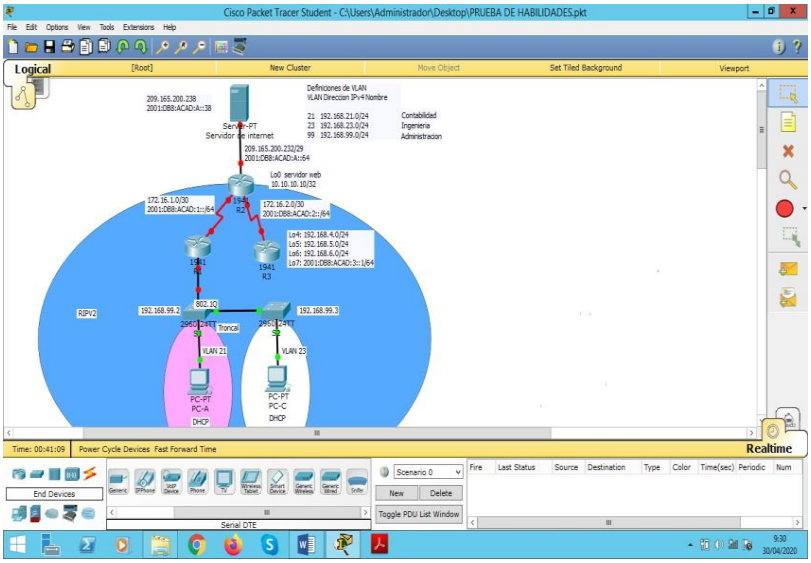


Fig. 2

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.

Tabla 1

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Lo hacemos mediante el condigo: Switch>enable Switch#show vlan brief

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 2

Elemento o tarea de configuración	Especificación
Dirección IPv4	Ingresamos al server en confuraciones, una ves alli configuramos la IPV4, la IPV6 y la subnet mask. Configuramos direcion IPV4: 209.165.200.238
Máscara de subred para IPv4	Ingresamos al server y configuramos la mascara de subred IPV4: 255.255.255.248
Gateway predeterminado	Ingresamos al server y configuramos la puerta de enlace IPV4: 209.165.200.233
Dirección IPv6/subred	Ingresamos al server y configuramos la dirección IPV6: 2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	Finamente ingresamos al server y configuramos la puerta de enlace de IPV6: 2001:DB8:ACAD:A::1

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login

Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd "Unauthorized Access is Prohibite"
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description conection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	Packet tracer no soporta este comando
Mensaje MOTD	R2(config)#banner motd "Unauthorized Acces is Prohibite"

Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description conection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description conection 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 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description conection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int lo0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated Web Server
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Table 5

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login

Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd "Unauthorized Access Is Prohibite"
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description conection 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
Interfaz loopback 4	R3(config-if)#int lo4 R3(config-if)#ip addres 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int lo5 R3(config-if)#ip addres 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int lo6 R3(config-if)#ip addres 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int lo7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login

Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd "Unauthorized Access is Prohibite"

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd "Unauthorized Access is Prohibite"

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 8

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	full

R2	R3, S0/0/1	172.16.2.2	full
PC de Internet	Gateway predeterminado	209.165.200.233	full

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config-if)#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
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk 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
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(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

Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switch mode trunk S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config-if-range)#switchport mode access S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int 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 11

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	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
Configurar la subinterfaz 802.1Q .99 en G0/1	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
Activar la interfaz G0/1	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 12

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

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13

Elemento o tarea de configuración	Especificación
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
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	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 C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	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

Anunciar redes IPv4 conectadas directamente	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
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

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 16

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?	Show ip protocols
¿Qué comando muestra solo las rutas RIP?	Show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	Show run, luego dirijirse a la sesion de rip

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 17

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado 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)#domain-name ccna-sa.com
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 R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

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

La configuración del R2 incluye las siguientes tareas:

Table 18

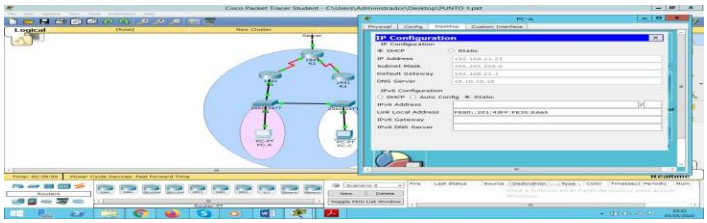
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet tracer no soporta los commandos de habilitacion del servidor HTTP

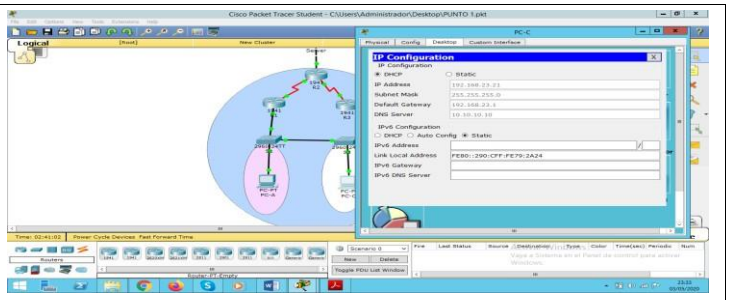
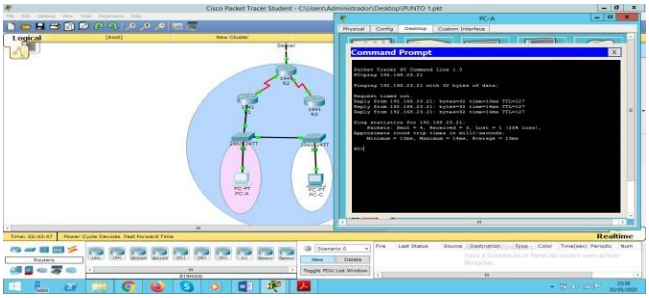
Configurar el servidor HTTP para utilizar la base de datos local para la autenticacion	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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 19

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 Fig. 3

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Fig. 4
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 Fig. 5
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**	Esta prueba no se puede habilitar debido a que como lo dijimos antes no fue possible habilitar el servidor de HTTP.

Parte 6: Configurar NTP

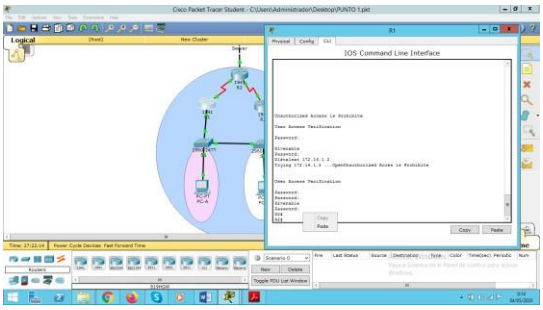
Tabla 20

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 23:52:00 03 may 2020**.**
Configure R2 como un maestro NTP.	Packet tracer no soporta este comando
Configurar R1 como un cliente NTP.	Servidor: **R2 Packet tracer no soporta este comando**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

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

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

Tabla 21

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** 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	(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Packet tracer no soporta el commando “imput”
Verificar que la ACL funcione como se espera	La pruebas es satisfactoria  Fig. 6

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

Tabla 22

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show ip access-list
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?	Show ip interface

¿Con qué comando se muestran las traducciones NAT?	**Show ip nat translations**
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translations

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.

Topología de red

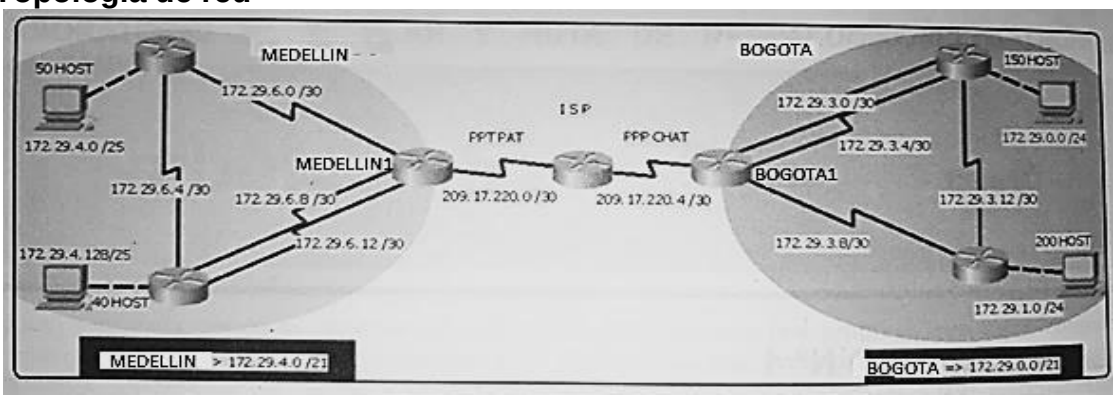


Fig. 7

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

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

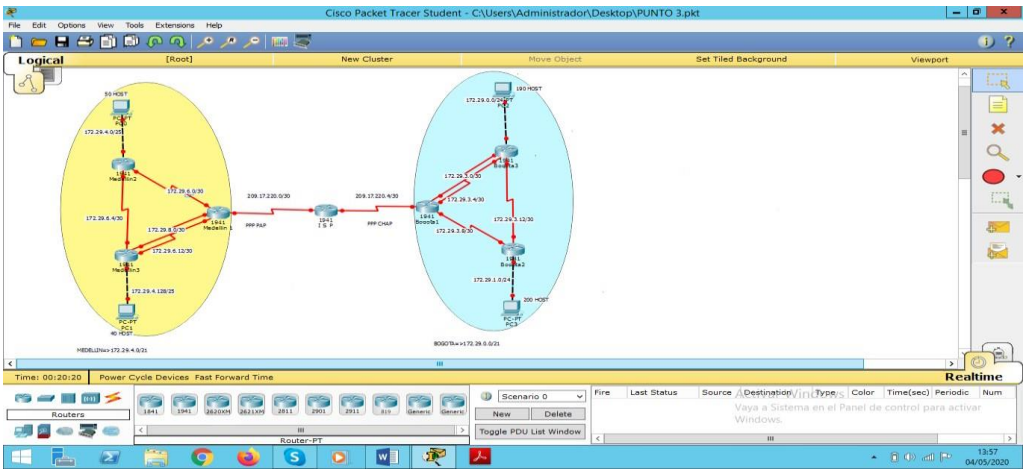


Fig. 8

Parte 1: Configuración del enrutamiento

Incialmente configuraremos el direccionamiento

CONFIGURACION DEL ISP

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int s0/0/0
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown
ISP(config-if)#int s0/0/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 4000000
ISP(config-if)#no shutdown

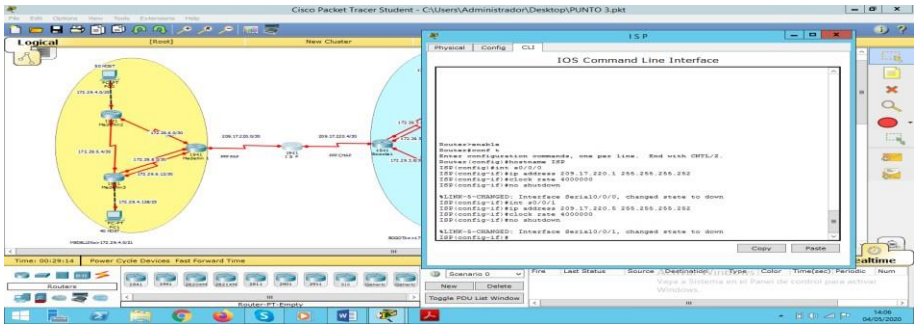


Fig. 9

CONFIGURACION DE MEDELLIN1

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN1

```
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 4000000
MEDELLIN1(config-if)#no shutdown
```

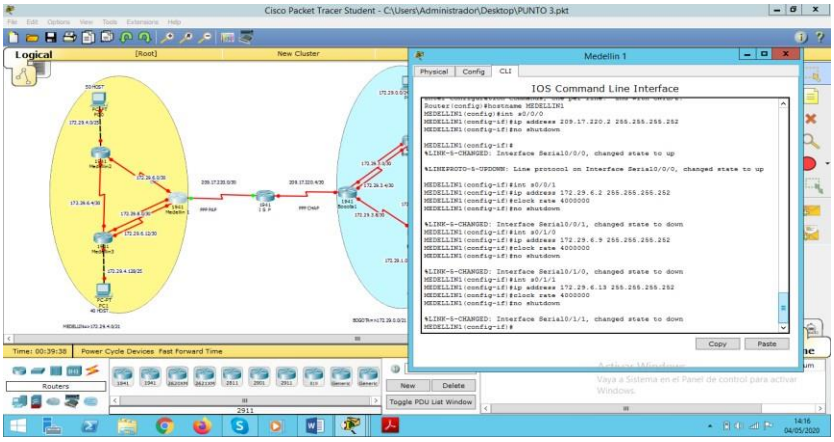


Fig. 10

CONFIGURACION DE MEDELLIN2

```
Router>enable
Router#conf t
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#int s0/0/1
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 4000000
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#int g0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown
```

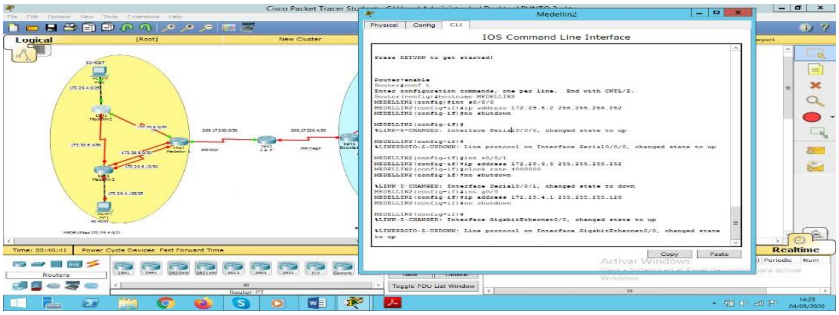


Fig. 11

CONFIGURACION DE MEDELLIN3

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#int s0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#int s0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#int g0/0
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#int s0/1/0
MEDELLIN3(config-if)#ip address 172.29.3.14 255.255.255.252
MEDELLIN3(config-if)#no shutdown

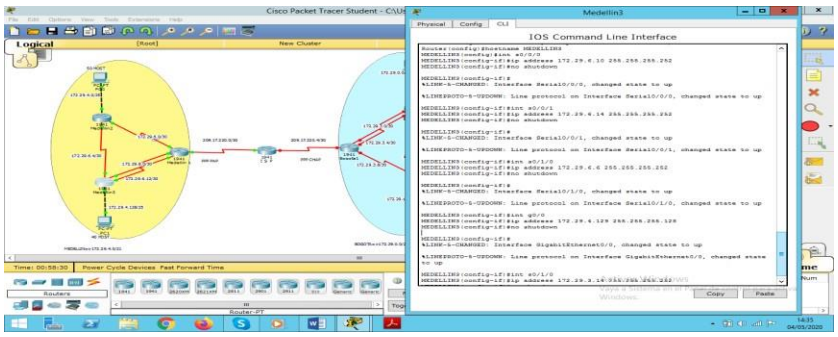


Fig. 12

Como se observa hemos configurado exitosamente el direccionamiento en los router correspondientes al area de Medellin, Ahora procedemos a configurar el otro lado de la red correspondientes a el area de Bogota

CONFIGURAMOS DE BOGOTA1

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA1
BOGOTA1(config)#int s0/0/0

BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown

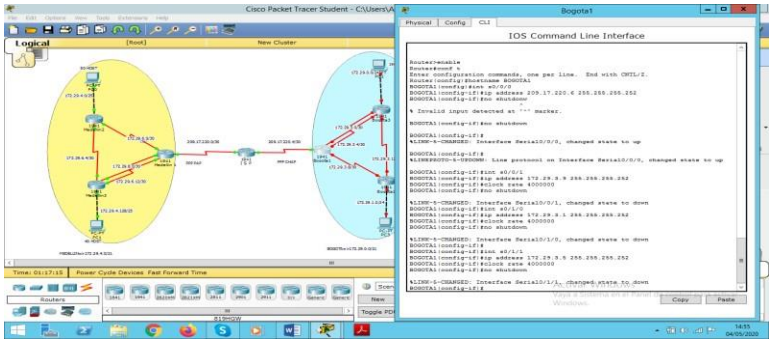


Fig. 13

CONFIGURACION DE BOGOTA2

Router>enable
Router#conf t
Router(config)#hostname BOGOTA2
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#int s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 4000000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#int g0/0
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no shutdown

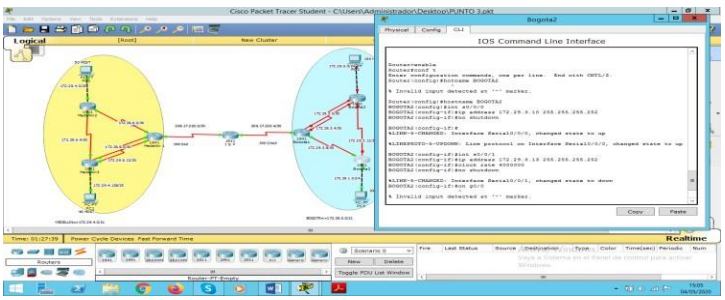


Fig. 14

CONFIGURACION DE BOGOTA3

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA3
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#int s0/0/1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#int g0/0
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#int s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#no shut
```

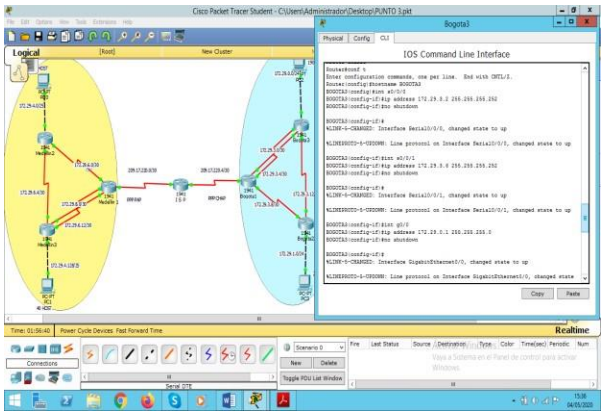


Fig. 15

Parte 2: Tabla de Enrutamiento.

Empezamos configurando ospf en el ISP, el cual se denominara como área 0, ya que es el punto de conexión entre los router que conforman la red de Medellín y la de Bogotá

Como primera medida observamos las redes que se encuentran conectadas a este router

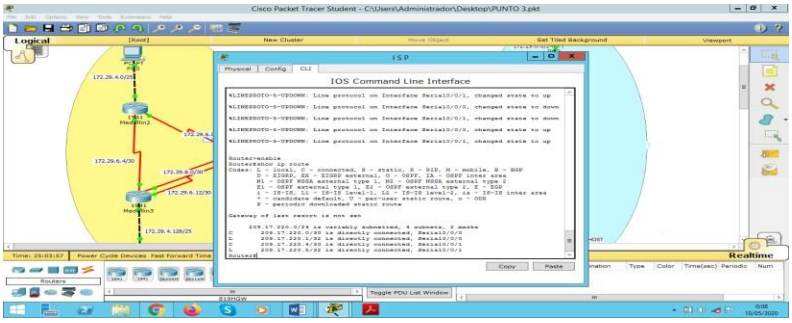


Fig. 16

Ahora procedemos a notificar las redes

ISP(config)#router ospf 1

ISP(config-router)#router-id 1.1.1.1

ISP(config-router)#network 209.17.220.0 0.0.0.255 area 0

ISP(config-router)#network 209.17.220.4 0.0.0.3 area 0

ISP(config-router)#

Ahora configuramos ospf en el router medellin1, primero miramos las redes conectadas al router

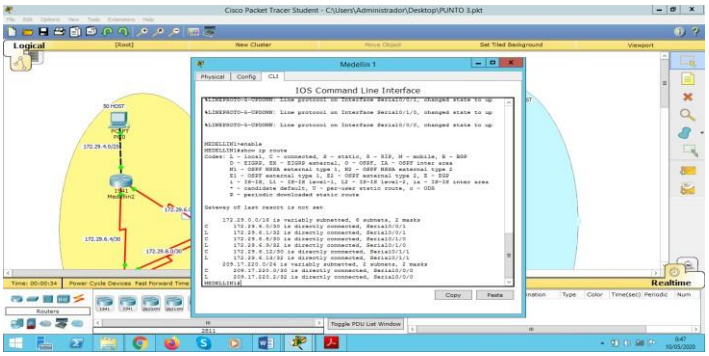


Fig. 17

Ahora las anunciaremos

MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.255 area 1
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 1
MEDELLIN1(config-router)#network 172.29.6.12 0.0.0.3 area 1
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0
MEDELLIN1(config-router)#

Ahora configuraremos ospf en el router Medellin2

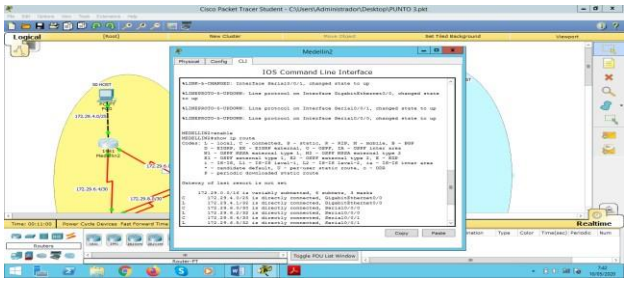


Fig. 18

MEDELLIN2(config)#route ospf 1

MEDELLIN2(config-router)#router-id 3.3.3.3

MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.255 area 1

MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 1

MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 1

MEDELLIN2(config-router)#

Finamente configuramos ospf en el router Medellin3

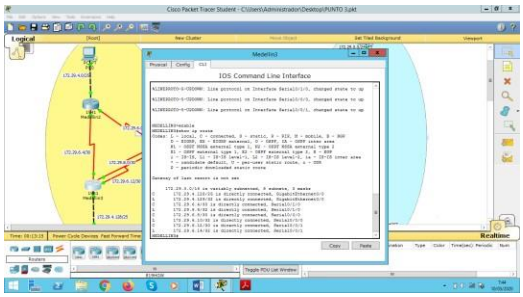


Fig. 19

Ahora anunciamos las redes conectadas

MEDELLIN3(config)#router ospf 1

MEDELLIN3(config-router)#router-id 4.4.4.4

MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.255 area 1

MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1

MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 1

MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 1

MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 1

MEDELLIN3 (config-router)#

Terminado todo el proceso de configuración de protocolos ospf en los router que conforman la red Medellín, ahora configuraremos protocolos ospf en los router que conforman la red Bogotá.

Empezamos con Bogota1, como primero miramos las redes conectadas al router

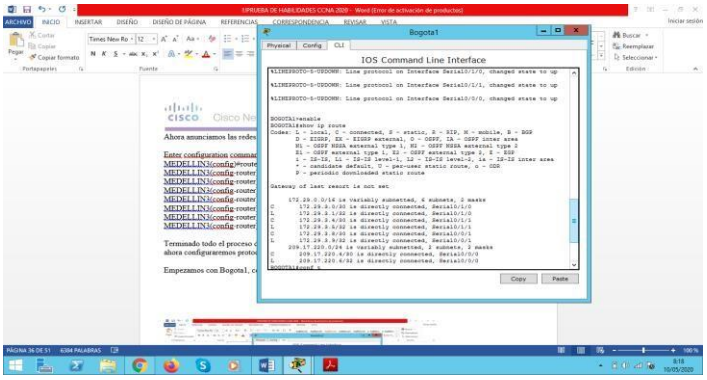


Fig. 20

Ahora procedemos a anunciar las redes conectadas

BOGOTA1(config)#router ospf 1

BOGOTA1(config-router)#router-id 5.5.5.5

BOGOTA1(config-router)#network 172.29.3.0 0.0.0.255 area 2

BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 2

BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 2

BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0

BOGOTA1(config-router)#

Continuamos con el router Bogota2. Actualmente tiene conectada las siguientes redes

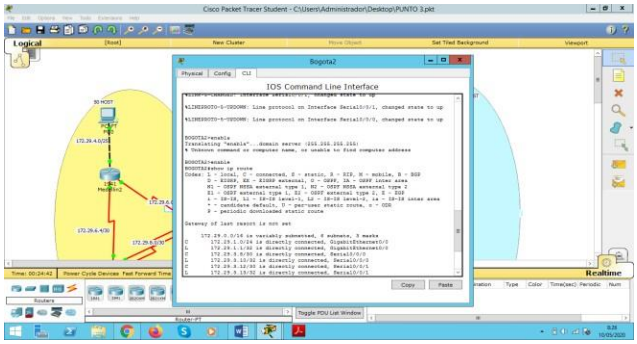


Fig. 21

Ahora notificamos las redes

BOGOTA2(config)#router ospf 1

BOGOTA2(config-router)#router-id 6.6.6.6

BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 2

BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 2

BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 2

BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 2

BOGOTA2(config-router)#

Finalmente configuramos ospf en el router Bogota3, verificamos las redes conectadas

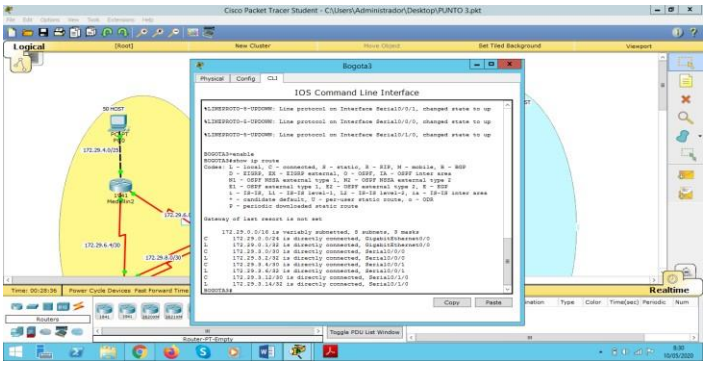


Fig. 22

Ahora notificamos las redes conectadas

BOGOTA3(config)#router ospf 1

BOGOTA3(config-router)#router-id 7.7.7.7

BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 2

BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 2

BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 2

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 2

BOGOTA3(config-router)#

Ahora verificamos la configuración ospf en cada uno de los router de las diferentes áreas

Comenzamos verificando en el router ISP.

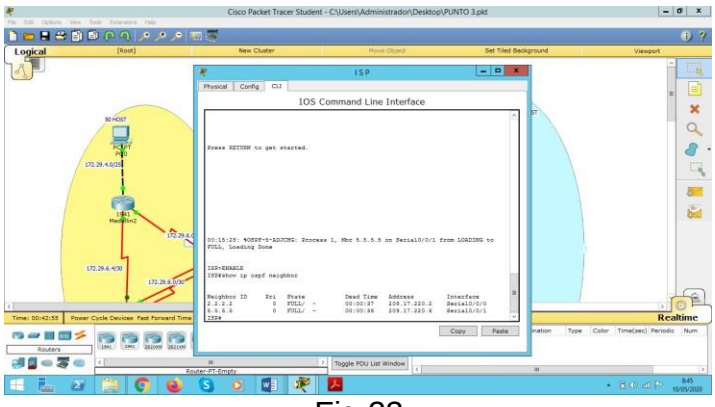


Fig.23

Verificamos en los router de la red Medellín

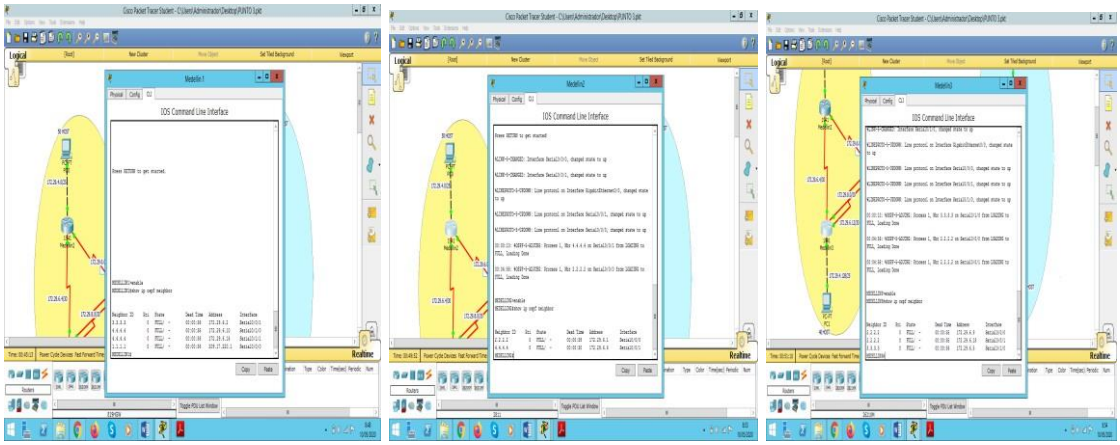


Fig. 24

Ahora verificamos en los router que conforman el área Bogotá

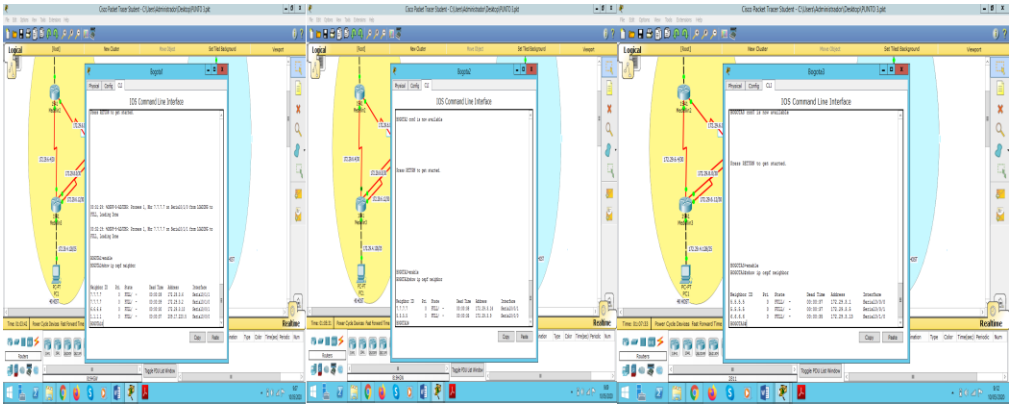


Fig. 25

Como se puede ver la configuración ospf se ha ejecutado de manera satisfactoria en cada uno de los router.

Los router Bogota1 y medellin1 deberan añadir a su configuracion de enrutamiento una ruta por defecto hacia el ISP y a su vez, redistribuirla dentro de las publicaciones de protocolos

Comenzamos a configurar la ruta por defecto en el router Medellin1

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#
```

Ahora verificamos en el router Medellin2 para ver si se guardo la configuración

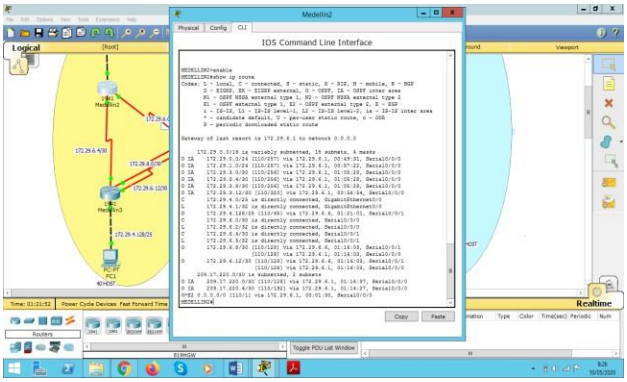


Fig. 26

Verificada la información en los routers del area Medellin, procedemos a configurar la misma informacion en los router que conforman el area Bogota

Configuramos Bogota1

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)#

Una vez realizada esta configuracion en el Bogota1, procederemos a verificar en el router Bogota3

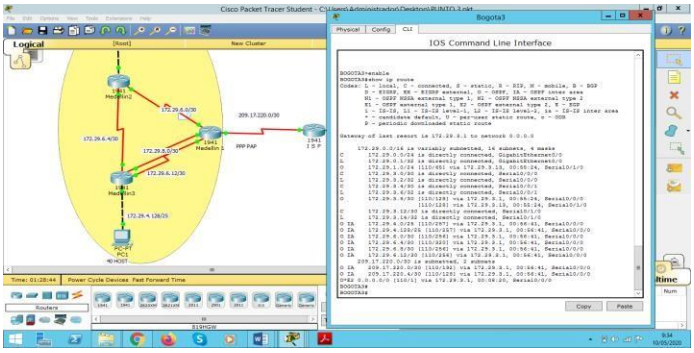


Fig. 27

El router ISP debera tener una ruta estatica dirigida hacia cada red interna del area Bogota y Medellin, para el caso se sumarizan sobre las subredes de cada uno a/22

Para esta confguracon comenzamos mrando que redes estan conectadas al ISP, esto lo hacemos utlzando el comando “show p router”

ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 209.17.220.2 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 12 subnets, 3 masks
O IA 172.29.0.0/24 [110/129] via 209.17.220.6, 01:00:24, Serial0/0/1
O IA 172.29.1.0/24 [110/129] via 209.17.220.6, 01:08:14, Serial0/0/1
O IA 172.29.3.0/30 [110/128] via 209.17.220.6, 01:16:30, Serial0/0/1
O IA 172.29.3.4/30 [110/128] via 209.17.220.6, 01:16:30, Serial0/0/1
O IA 172.29.3.8/30 [110/128] via 209.17.220.6, 01:16:30, Serial0/0/1
O IA 172.29.3.12/30 [110/192] via 209.17.220.6, 01:07:46, Serial0/0/1
O IA 172.29.4.0/25 [110/129] via 209.17.220.2, 01:25:21, Serial0/0/0
O IA 172.29.4.128/25 [110/129] via 209.17.220.2, 01:25:21, Serial0/0/0
O IA 172.29.6.0/30 [110/128] via 209.17.220.2, 01:25:21, Serial0/0/0
O IA 172.29.6.4/30 [110/192] via 209.17.220.2, 01:25:21, Serial0/0/0
O IA 172.29.6.8/30 [110/128] via 209.17.220.2, 01:25:21, Serial0/0/0
O IA 172.29.6.12/30 [110/128] via 209.17.220.2, 01:25:21, Serial0/0/0
209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/0/0
L 209.17.220.1/32 is directly connected, Serial0/0/0
C 209.17.220.4/30 is directly connected, Serial0/0/1
L 209.17.220.5/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 209.17.220.2, 00:12:17, Serial0/0/0
[110/1] via 209.17.220.6, 00:06:37, Serial0/0/1
ISP#

Ahora procederemos a crear rutas estaticas que conyeven a ISP llegar a las redes de Bogota y Medellin o configurar NAT en cada una de estas sucursales. Inicialmente hacemos la sumarizacion y nos queda
Medellin 172.29.4.0/22
Bogota 172.29.0.0/22

Ahora procedemos a configurar esta información en el ISP

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#

Para confirmar que esta configuración ha sido correcta procederemos a verificar mediante un ping en el router bogota3

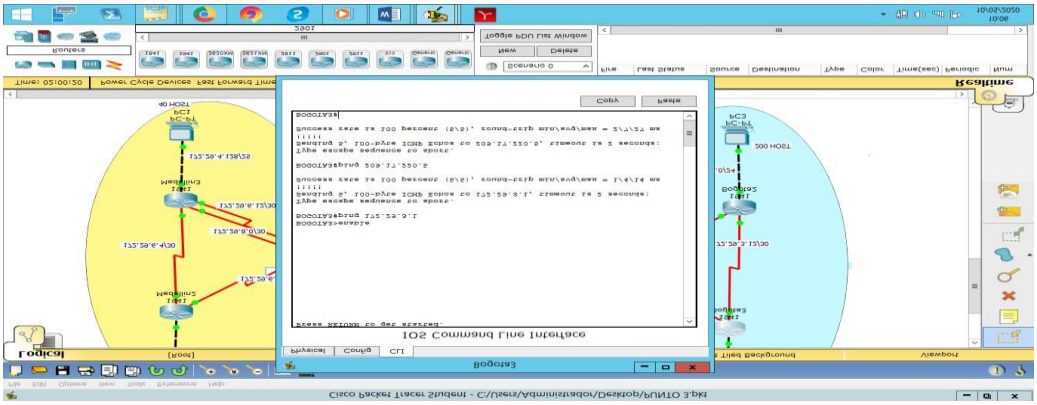


Fig. 28

Como podemos ver las pruebas se ejecutan satisfactoriamente

Verificar el balanceo de carga que presentan los router Bogota1 y Medellin1

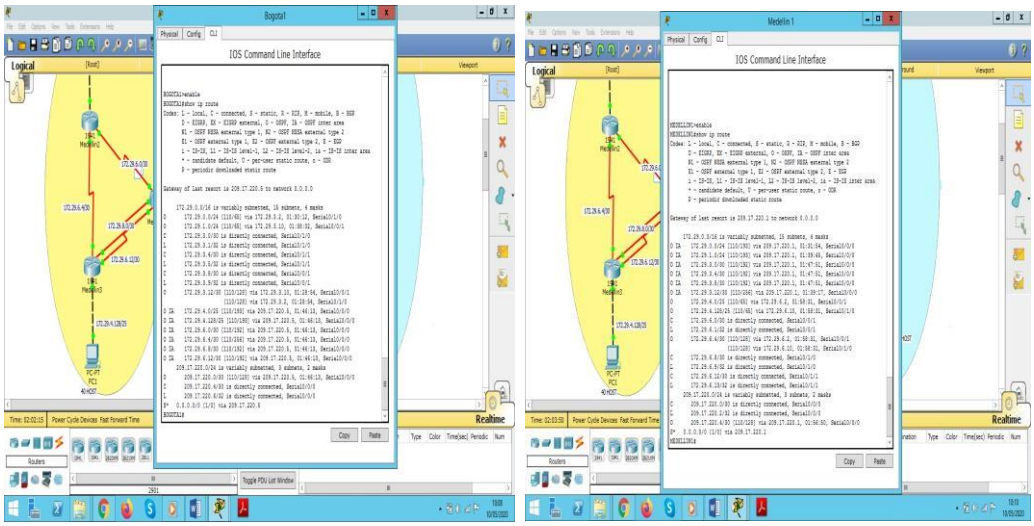


Fig. 29

Según la tipologia se requiere que el enlace medellin1 con el ISP sea configurado con autenticacion PAP.

Comenzamos con la configuracion desde el ISP, crearemos un usuario que permita acceso a Medellin

El enlace Bogota1 con el ISP se debe configurar con autenticacion CHAP

```
ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
ISP(config-if)#
```

De igual modo creamos Usuario en el router Medellin

```
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco
MEDELLIN1(config-if)#
```

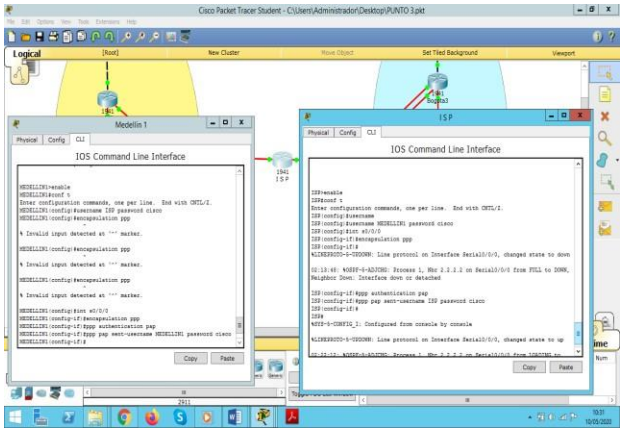


Fig. 30

Una vez realizado la autenticacion procedemos a verificarla mediante ping
MEDELLIN1#ping 209.17.220.1

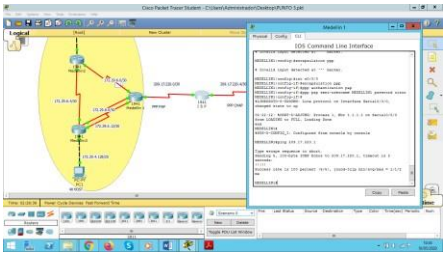


Fig. 31

Como podemos ver el ping funciona satisfactoriamente

Ahora repetimos la configuración en el area de BOGOTA

ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#

BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#

Ahora verificamos mediante ping

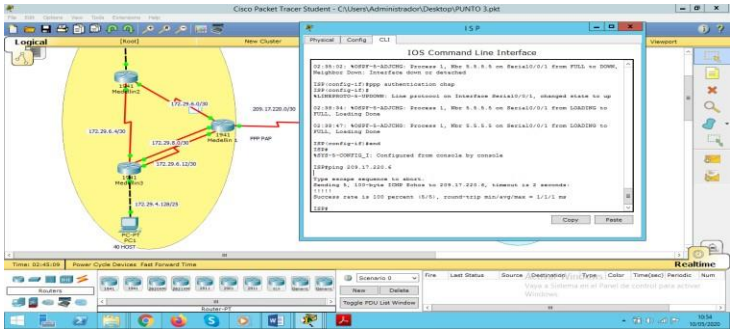


Fig. 32

Como podemos ver el ping se ejecuta de forma correcta

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.

```
MEDELLIN2>enable
MEDELLIN2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.133
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 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)#
```

Verificamos en PC0 para corroborar que halla adquirido la información

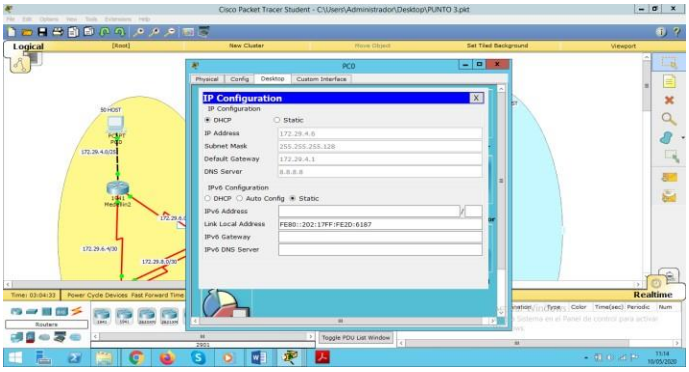


Fig. 33

De igual menera configuramos el router Medellin3 para que el PC-1 pueda conectarse con el servidor dhcp.

```
MEDELLIN3(config)#int g0/0
```

```
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#
```

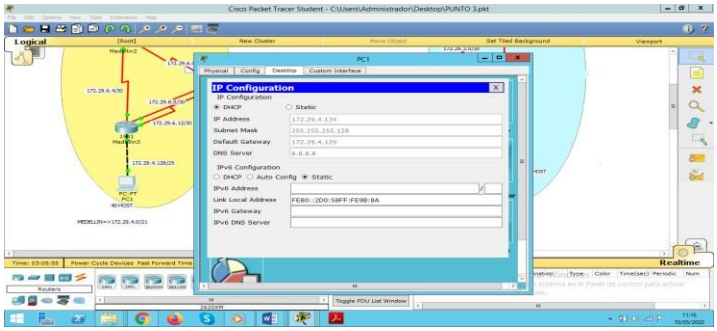


Fig. 34

El router MEDELLIN3 debera halilitar el paso de los mensajes broadcast hacia la IP del router MEDELLIN2

Finalizado este proceso en los router del area de Medellin, lo realizamos de la misma manera en los router del area de BOGOTA

```
BOGOTA1>enable
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA1(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA1(config)#ip dhcp pool BOGOTA2
BOGOTA1(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA1(dhcp-config)#default-router 172.29.1.1
BOGOTA1(dhcp-config)#dns-server 8.8.8.8
BOGOTA1(dhcp-config)#ip dhcp pool BOGOTA3
BOGOTA1(dhcp-config)#exit
BOGOTA1(config)#ip dhcp pool BOGOTA3
BOGOTA1(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA1(dhcp-config)#default-router 172.29.0.1
BOGOTA1(dhcp-config)#dns-server 8.8.8.8
BOGOTA1(dhcp-config)#
```

Configuramos en BOGOTA3

```
BOGOTA3#conf t
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)#
```

Ahora verificamos que PC-2 y PC-3 reciban la información

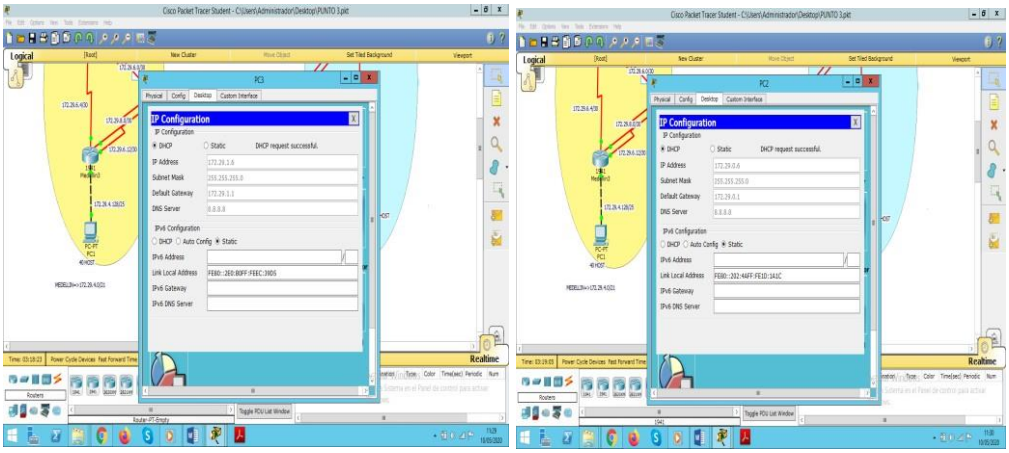


Fig. 35

Una vez realizada la configuración procedemos a observar que las equipos se encuentran configurado de manera correcta. Ahora procedemos a verificar mediante ping de pc a pc para ver su funcionamiento.

Ping de PC-2 a PC-3, Ping de PC-2 a PC-0, Ping de PC-2 a PC-1

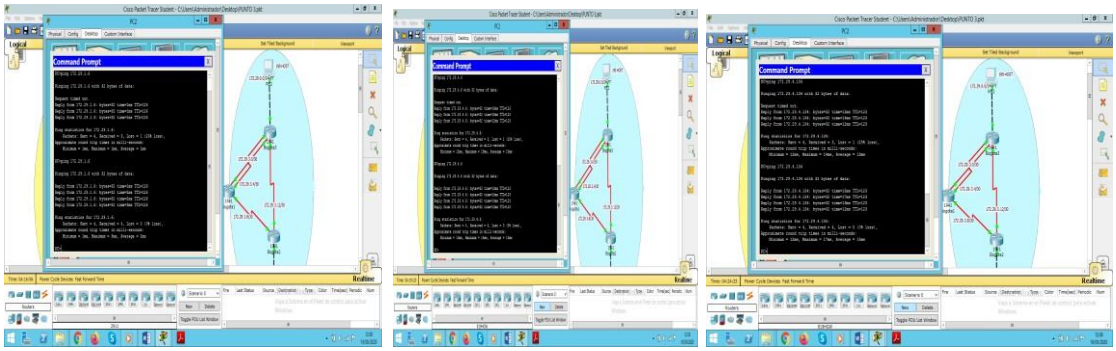


Fig. 36

Una vez realizado todos los pin podemos comprobar que hay conexión de extremo a extremo lo que significa que hemos configurado perfectamente nuestro prototipo.

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.

MEDELLIN1

```
MEDELLIN>en
MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#ip nat outside
```

```
MEDELLIN(config-if)#int s0/0/1
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)#int s0/1/0
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)#int s0/1/1
MEDELLIN(config-if)#ip nat inside
MEDELLIN(config-if)#
```

BOGOTA1

```
BOGOTA>EN
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#ip nat outside
BOGOTA(config-if)#int s0/0/1
BOGOTA(config-if)#ip nat inside
BOGOTA(config-if)#int s0/1/0
BOGOTA(config-if)#ip nat inside
BOGOTA(config-if)#int s0/1/1
BOGOTA(config-if)#ip nat inside
BOGOTA(config-if)#
BOGOTA#
```

Una vez realizada esta configura la probaremos haciendo pin desde el PC-2 a ISP, ping PC-0 al ISP

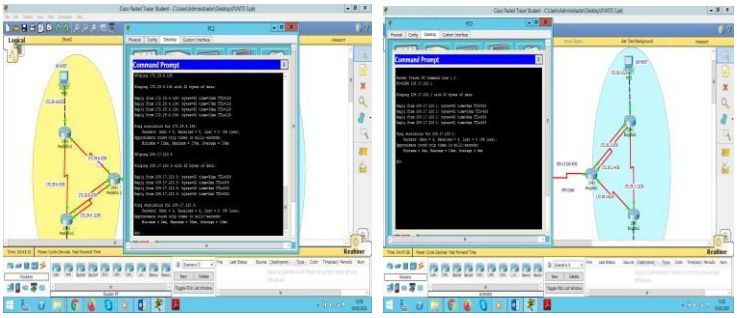


Fig. 37

Despues de verificado los ping se puede evidencias que la configuración se ha realizado de forma satisfactoria, lo que significa que hemos hecho un buen aprovechamiento de cada uno de los materiales de estudio que contempla este diplomado.

CONCLUSION

Este trabajo lo realicé con el objetivo de poner en práctica los conocimientos adquiridos en el material de estudio de cada una de las unidades que conforma este diplomado de profundización en redes cisco, gracias a este material pude afianzar mis conocimientos en cada uno de los temas relacionados. Como muestra de ello pude plantear soluciones positivas a los dos casos de estudios que conforman la prueba de habilidades, apoyado en la herramienta packet tracer.

Al finalizar cada uno de los escenarios pude evidenciar un positivo aprovechamiento de los recursos adaptados, como son los equipos utilizados y lo más importante que fue la configuración de estos utilizando adecuadamente cada uno de los protocolos necesarios, como lo fue el OSPF, DHCP, NAT, RIPV2, VLAN, ACL, NTP.

También fue importante poner en práctica el enrutamiento IPV4, el cual hace referencia a la cuarta versión del Protocolo de Internet IP y es un protocolo sin conexión el cual es implementado en redes que hacen uso de conmutación de paquetes. Al usar IPv4 estamos ante un protocolo que cada día va siendo más limitado ya que IPv4 requiere varios complementos adicionales para funcionar como ICMP y ARP.

Finalmente también fue importante configurar el enrutamiento IPV6, el cual es el protocolo más actual de IP y se posiciona como la actualización de IPv4 en términos de capacidad, cubrimiento y seguridad.

REFERENCIAS BILIOGRAFICAS

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). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

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

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

UNAD (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1CISCO.

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). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

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

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-