SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

JEAN JAIME IBAGÓN VARON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

INGENIERIA ELECTRONICA

NEIVA

2018

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

JEAN JAIME IBAGÓN VARON

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN) PARA OPTAR POR EL TITULO DE INGENIERO ELECTRONICO

DIRECTOR DE CURSO:

JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

INGENIERIA ELECTRONICA

NEIVA

2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Este informe presenta el desarrollo de la prueba de habilidades prácticas CCNA, en la cual se pone en práctica y se evidencian todas las habilidades y competencias que fueron desarrolladas a lo largo del diplomado en temas como: exploración y configuración de redes, protocolos y comunicaciones de red, Ethernet, direccionamiento IPV6, OSPF, enrutamiento VLAN, VTP y RSTP; entre otras temáticas.

La dinámica y esquema de trabajo para esta prueba final, está basado en el desarrollo de 2 escenarios, en donde es necesario dar respuesta a diferentes aspectos como lo son la seguridad informática, aseguramiento de componentes de Networking, y el correcto funcionamiento de herramientas para determinar enlaces de un punto a otro, bien sea a nivel local o internacional. Teniendo en cuenta lo anterior, en el desarrollo de este informe se explicara paso a paso el desarrollo de cada escenario, dando a entender la forma en que se desarrolló las diferentes configuraciones, y evidenciándolas por capturas de pantalla en donde se muestran las simulaciones de configuración de red simuladas en Packet Tracert.

Uno de los puntos importante a resaltar para el desarrollo de este trabajo es que por medio del simulador Packet Tracer es posible realizar la simulación de las redes, las cuales se pueden encontrar en cualquier parte o lugar del mundo.

En la actualidad, el acceso a la Internet es una necesidad ya que en casi todos los lugares y con los cuales tenemos constante contacto, se utilizan medios para consultas, enviar y recibir información, comunicación a través de diferentes redes sociales, verificación y acceso a la información a través de las nuevas tecnologías.

Los contenidos de este curso son muy completos y son vitales para el desarrollo de esta prueba, cada vez que se avanzó en el desarrollo del diplomado, las temáticas se fueron presentando de forma más compleja, pero con este medio de estudio se pudo avanzar y aprender satisfactoriamente.

Cisco Packet Tracert permite la configuración de muchos dispositivos de red y hacer pruebas en un ambiente virtual que se comporta como el ambiente real.

Adicional, para complementar el presente informe, se anexan los aplicativos PKT de los laboratorios resueltos en Packet Tracert.

1. DESARROLLO DE LOS ESCENARIOS

1.1 ESCENARIO 1

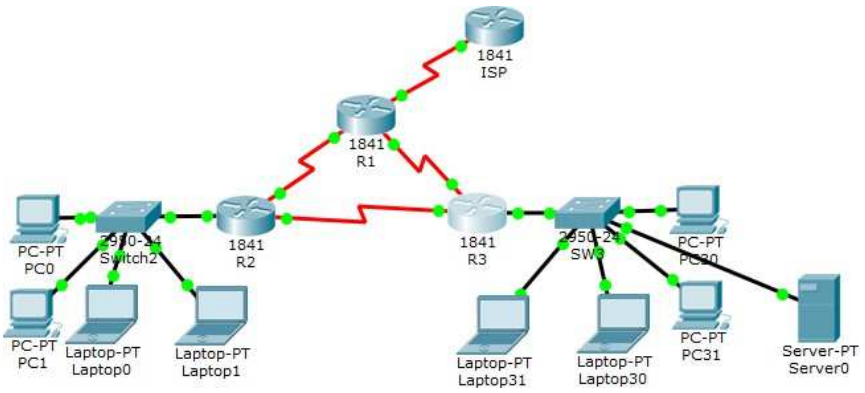


Figura 1: Topología propuesta escenario 1

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	Se0/1/0	10.0.0.1	255.255.255.252	N/D
	Se0/1/1	10.0.0.5	255.255.255.252	N/D
R2	Fa0/0,100	192.168.20.1	255.255.255.0	N/D
	Fa0/0,200	192.168.21.1	255.255.255.0	N/D
	Se0/0/0	10.0.0.2	255.255.255.252	N/D
	Se0/0/1	10.0.0.9	255.255.255.252	N/D
R3	Fa0/0	192.168.30.1	255.255.255.0	N/D
		2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP
PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Tabla 1: Direccionamientos

Dispositivo	VLAN	Nombre	Interfaz
SW2	100	LAPTOPS	Fa0/2-3
SW2	200	DESTOPS	Fa0/4-5
SW3	1	-	Todas las interfaces

Tabla 2: Asignación de VLAN y de puertos

Dispositivo local	Interfaz local	Dispositivo remoto
SW2	Fa0/2-3	100

Tabla 3: Enlaces troncales

Desarrollo

Para el desarrollo del escenario 1 de la prueba de habilidades, en primera instancia se realiza el armado de la red en el Software Packet Tracer, según el diseño de topología que se propone en dicho escenario. Para ello se inicializa el Software Packet Tracer, se seleccionan los elementos a utilizar, y se realiza el cableado de red tal como se muestra en la topología propuesta.

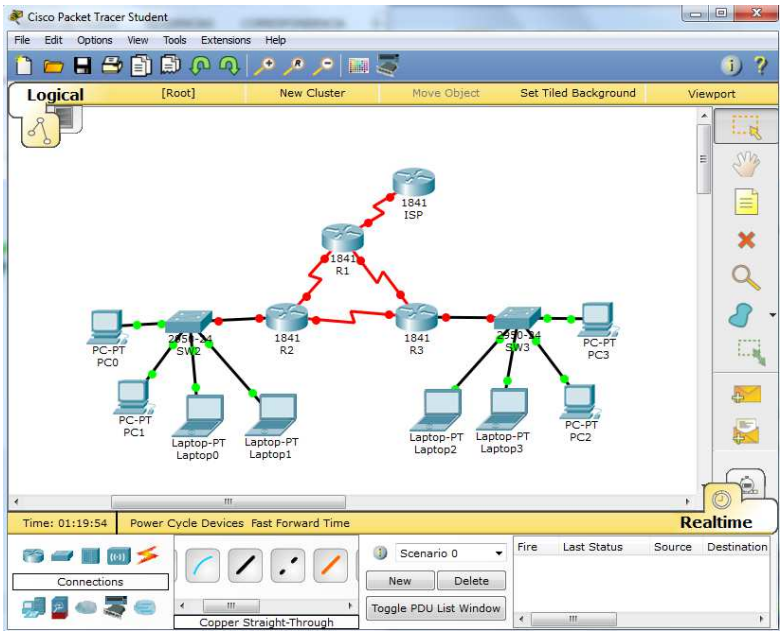


Figura 2: Armado de la red escenario 1

Como se puede apreciar en la Figura 2, se realiza el armado de la red según la topología planteada para el desarrollo del escenario 1.

Paso 1: SW2 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.

Seguido al armado de la red, se procede a asignar los puertos de VLAN para SW2 Y SW3 los cuales deben cumplir los parámetros de la tabla 1. Para ello, se selecciona el SW2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

SW2>enable

SW2#configure terminal

SW2(config)#vlan 100

SW2(config-vlan)#name LAPTOPS

SW2(config-vlan)#exit

SW2(config)#vlan 200

SW2(config-vlan)#name DESTOPS

SW2(config-vlan)#exit

SW2(config)#end

SW2#wr

SW2#show vlan

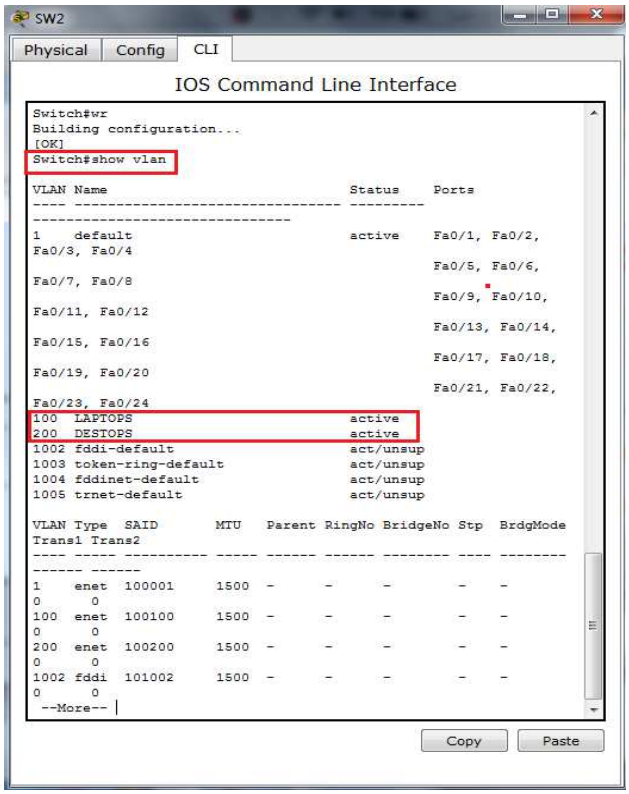


Figura 3: Creación de vlan 100 y vlan 200 en SW2

Como podemos observar en la Figura 3, se verifica con el comando “show vlan” que ya está creada vlan 100 y vlan 200.

Lo siguiente es asignar VLAN 100 y VLAN 200 a las interfaces Fa0/2-3 y F0/4-5 de acuerdo a como se indica en la tabla 2. Para ello, se selecciona nuevamente el

SW2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

SW2#configure terminal

SW2(config)#int range f0/2-3

SW2(config-if-range)#switchport mode access

SW2(config-if-range)#switchport access vlan 100

SW2(config-if-range)#int range f0/4-5

SW2(config-if-range)#switchport mode access

SW2(config-if-range)#switchport access vlan 200

SW2(config-if-range)#exit

SW2(config)#end

SW2#wr

SW2#show vlan

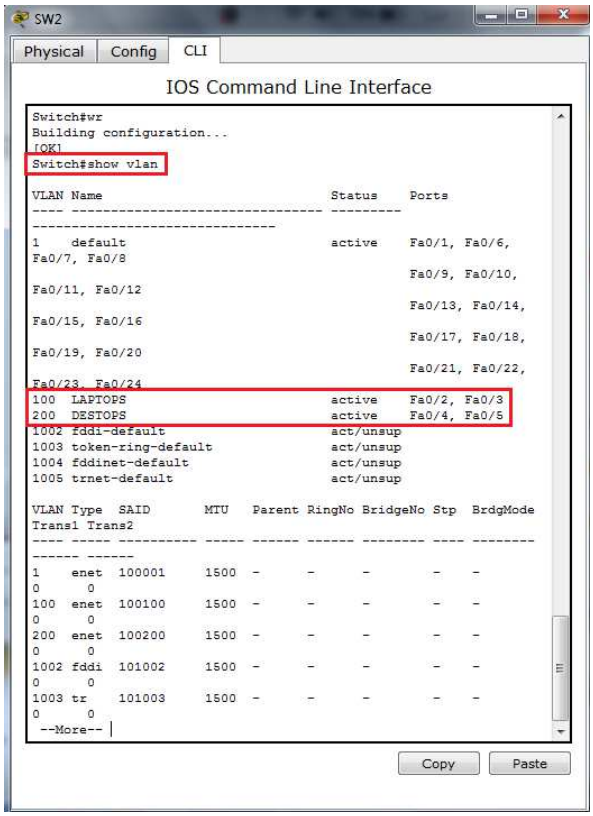


Figura 4: Asignación de interfaces Fa0/2-3 y F0/4-5

Como podemos observar en la Figura 4, se verifica con el comando “show vlan” que ya está asignado para vlan 100 y vlan 200, las interfaces Fa0/2-3 y F0/4-5, respectivamente.

Lo siguiente es asignar el puerto de VLAN para SW3, según los parámetros de la tabla 1. Para ello, se selecciona el SW3, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

SW3>enable

SW3#configure terminal

SW3(config)#vlan 1

SW3(config)#int range f0/1-24

SW3(config-if-range)#switchport mode access

SW3(config-if-range)#switchport access vlan 1

SW3(config-if-range)#exit

SW3(config)#end

SW3#wr

SW3#show vlan

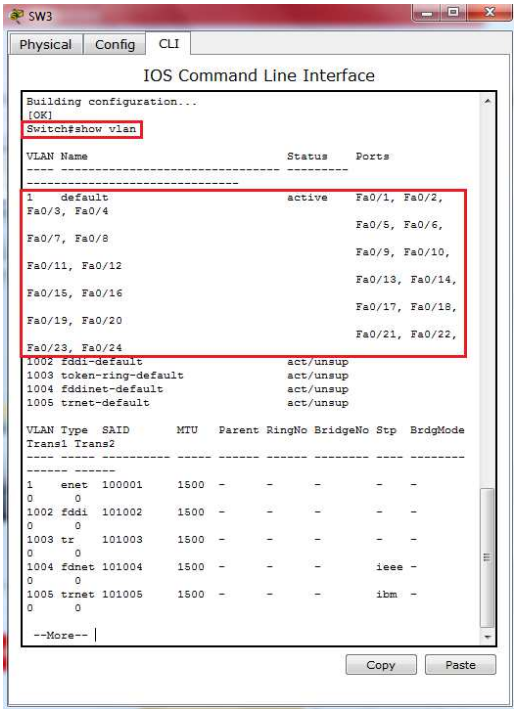


Figura 5: Creación de vlan 1 en SW3

Como podemos observar en la Figura 5, se creó VLAN 1 y por defecto esta contiene todas las interfaces activas.

Paso 2: Los puertos de red que no se utilizan se deben deshabilitar.

Una vez hechas las configuraciones, lo siguiente será deshabilitar todos los puertos que no se utilicen. Para ello, se selecciona nuevamente el SW3, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

SW3#configure terminal

SW3(config)#int range f0/6-23

SW3(config-if-range)#shutdown

SW3(config-if-range)#exit

SW3(config)#end

SW3#wr

Se realiza el mismo procedimiento para SW2. Para ello, se selecciona nuevamente el SW2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

SW2#configure terminal

SW2(config)#int range f0/6-24

SW2(config-if-range)#shutdown

SW2(config-if-range)#exit

SW2(config)#end

SW2#wr

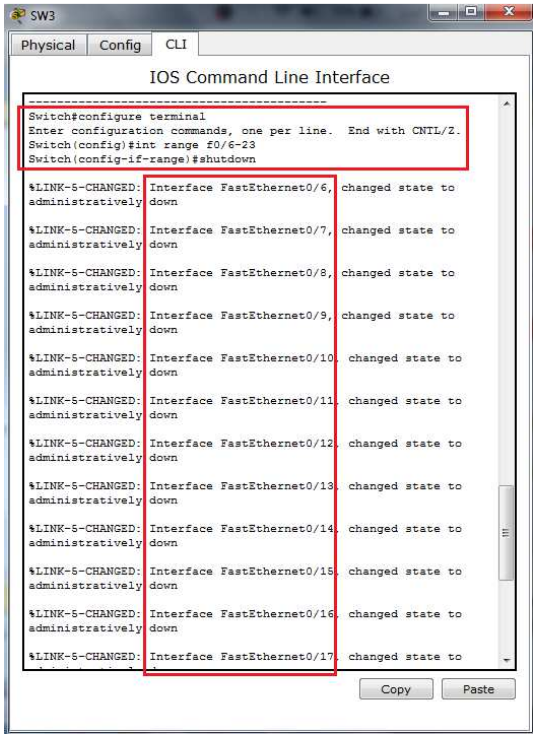


Figura 6: Deshabilitación de puertos no utilizados

Con esta configuración y como se aprecia en la figura 6, los puertos que no se utilizan en SW2 y SW3 están deshabilitados (Down). Siguiendo los parámetros de la tabla 2, los puertos Fa0/2-3 y Fa0/4-5 están activos en SW2.

Por último, se configura el puerto troncal de SW2 con la siguiente configuración:

SW2#configure terminal

SW2(config)#int f0/1

SW2(config-if)#switchport mode trunk

SW2(config-if)#exit

SW2(config)#end

SW2#wr

Se realiza la misma configuración del puerto troncal en SW3:

SW3#configure terminal

SW3(config)#int f0/1

SW3(config-if)#switchport mode trunk

SW3(config-if)#exit

SW2(config)#end

SW2#wr

Paso 3: La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

Para configurar los respectivos direccionamientos IP de R1, se selecciona el R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1>enable

R1#configure terminal

R1(config)#int s0/0/0

R1(config-if)#ip address 200.123.211.2 255.255.255.0

R1(config-if)#exit

R1(config)#int s0/1/0

R1(config-if)#ip address 10.0.0.1 255.255.255.252

R1(config-if)#exit

R1(config)#int s0/1/1

R1(config-if)#ip address 10.0.0.5 255.255.255.252

R1(config-if)#exit

R1(config)#end

R1#wr

Para configurar los respectivos direccionamientos IP de R2, se selecciona el R2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R2>enable

R2#configure terminal

R2(config)#int f0/0.100

R2(config-subif)#encapsulation dot1Q 100

R2(config-subif)#ip address 192.168.20.1 255.255.255.0

R2(config-subif)#exit

R2(config)#int f0/0.200

R2(config-subif)#encapsulation dot1Q 200

R2(config-subif)#ip address 192.168.21.1 255.255.255.0

R2(config-subif)#exit

R2(config)#int s0/0/0

R2(config-if)#ip address 10.0.0.2 255.255.255.252

R2(config-subif)#exit

R2(config)#int s0/0/1

R2(config-if)#ip address 10.0.0.9 255.255.255.252

R2(config-if)#exit

R2(config)#end

R2#wr

Para configurar los respectivos direccionamientos IP de R3, se selecciona el R3, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R3>enable

R3#configure terminal

R3(config)#int f0/0

R3(config-if)#ip address 192.168.30.1 255.255.255.0

R3(config-if)#exit

R3(config)#ipv6 unicast-routing

R3(config-if)#int s0/0/0

R3(config-if)#ip address 192.168.30.1 255.255.255.0

R3(config-if)#exit

R3(config)#int s0/1/1

R3(config-if)#ip address 10.0.0.6 255.255.255.252

R3(config-if)#exit

R3(config)#int s0/0/1

R3(config-if)#ip address 10.0.0.10 255.255.255.252

R3(config-if)#exit

R3(config)#end

R3#wr

Si observamos la tabla 1, es posible comparar y verificar que todas las direcciones IP de R1, R2 y R3 concuerdan con las direcciones que se colocaron en las configuraciones.

Paso 4: Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.

Para que todos los equipos estén en comunicación DHCP, es necesario verificar que todos tengan seleccionada la casilla de configuración IP DHCP, y no una IP estática. Para esto, en cada equipo (Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31) se da click en “IP Configuration”, y se selecciona la casilla DHCP.

Paso 5: R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

Para desarrollar este paso, se selecciona R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1>enable

R1#configure terminal

R1(config)#int s0/1/1

R1(config-if)#ip nat inside

R1(config-if)#exit

R1(config)#int s0/1/0

R1(config-if)#ip nat inside

R1(config-if)#exit

R1(config)#int s0/0/0

R1(config-if)#ip nat outside

R1(config-if)#exit

R1(config)#ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128 netmask 255.255.255.0

R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255

R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255

R1(config)#ip nat inside source list 1 interface s0/0/0 overload

R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 10.0.0.0

R1(config-router)#exit

R1(config)#end

R1#wr

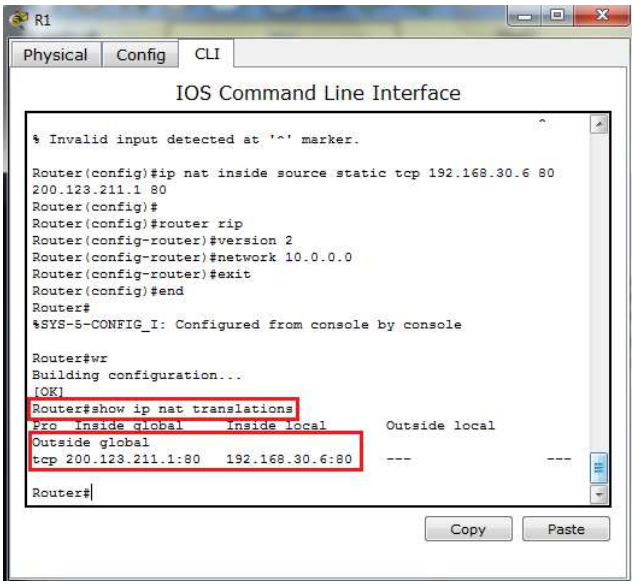


Figura 7: Traslación de direccionamiento

Como se puede apreciar en la figura 7, con el comando “show ip nat translations” se verifica que se hizo una traslación de direccionamiento, al igual que con el comando “show ip nat statistics” se verifica que existe una ruta estática configurada junto con las interfaces de salida y de entrada.

Paso 6: R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.

Previamente ya se ha configurado RIPv2 en R1 (en el paso 4), también se ha configurado la ruta estática en el Nat (en el paso 5).

Paso 7: R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

Para desarrollar este paso, se selecciona R2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R2>

R2>enable

R2#configure terminal

R2(config)#ip dhcp excluded-address 10.0.0.2 10.0.0.9

R2(config)#ip dhcp pool INSIDE-DEVS

R2(dhcp-config)#NETwork 192.168.20.1 255.255.255.0

R2(dhcp-config)#NETwork 192.168.21.1 255.255.255.0

R2(dhcp-config)#default-router 192.168.1.1

R2(dhcp-config)#dns-server 0.0.0.0

R2(dhcp-config)#exit

Paso 8: R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

Para desarrollar este paso, se ingresa la siguiente configuración (seguidamente del paso anterior y en la misma ventana de R2):

R2(config)#int vlan 100

R2(config-if)#ip address 192.168.20.1 255.255.255.0

R2(config-if)#exit

R2(config)#int vlan 200

R2(config-if)#ip address 192.168.21.1 255.255.255.0

R2(config-if)#end

R2#wr

Paso 9: El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

Para programar el servidor 0 en modo DHCP versión IPv6, se da click en “IP Configuration”, y se selecciona la casilla DHCP. Por defecto está configurado en estático, razón por la cual es necesario seleccionar, bien sea la casilla DHCP, o la casilla Auto config, en las dos configuraciones funciona correctamente. Seguido a esto, para comprobar la correcta configuración, se hace Ping desde cualquier equipo que este dentro de la misma red del Servidor 0.

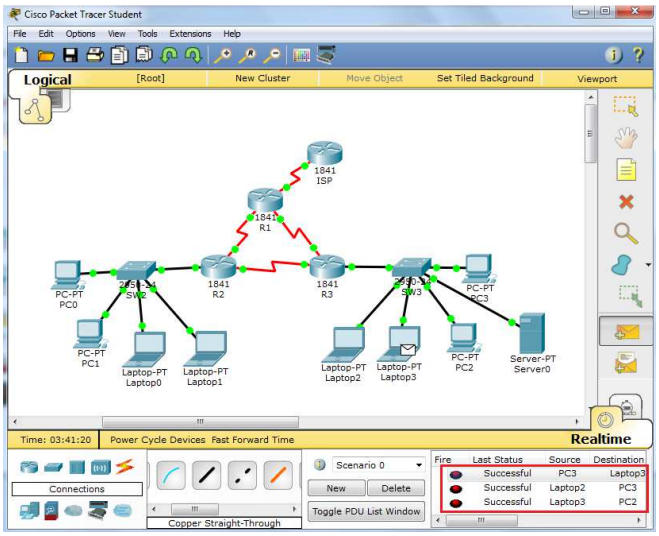


Figura 8: Realización de Ping

Como se puede apreciar en la figura 8, se realiza Ping desde Laptop30 hasta PC2, con el fin de verificar que este servidor es accesible para cualquier dispositivo que este en la misma red (conectado a R3).

Paso 10: La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.

Para comprobar que todos los dispositivos mencionados estén configurados con direcciones IPv4 e IPv6, en cada equipo (Laptop30, Laptop31, PC30, y PC31) se da click en “IP Configuration”, y se selecciona, bien sea la casilla DHCP, o la casilla Auto config, en las dos configuraciones funciona correctamente (es el mismo procedimiento que se hizo en el paso 4).

Paso 11: La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

Para desarrollar este paso, se selecciona R3, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R3>enable

R3#configure terminal

R3(config)#ipv6 unicast-routing

R3(config)#int f0/0

R3(config-if)#ipv6 enable

R3(config-if)#ip address 192.168.30.1 255.255.255.0

R3(config-if)#ipv6 address 2001:db8::9c0:80F:301/64

R3(config-if)#no shutdown

Paso 12: R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

Se configura RIP versión 2 para cada uno de los routers. Para R1, se selecciona R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1#configure terminal

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#do show ip route connected

R1(config-router)#network 10.0.0.0

R1(config-router)#network 10.0.0.4

R1(config-router)#end

R1#wr

Para R2, se selecciona R2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R2#configure terminal

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 10.0.0.0

R2(config-router)#network 10.0.0.8

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

R2(config-router)#end

R2#wr

Para R3, se selecciona R3, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R2#configure terminal

R3(config)#router rip

R3(config-router)#version 2

R3(config-router)#network 10.0.0.0

R3(config-router)#network 10.0.0.8

R3(config-router)#do show ip route connected

R3(config-router)#end

R3#wr

Paso 13: R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

Esta configuración de ruta predeterminada ya se hizo previamente en pasos anteriores, por lo tanto cada Router conoce sus rutas gracias al protocolo de RIP versión 2 (cada Router ya tiene su protocolo activo). Para estar seguros de la ruta estática predeterminada al ISP, se selecciona R1, se da click en la pestaña “Config”, se selecciona RIP, y se agrega la ISP.

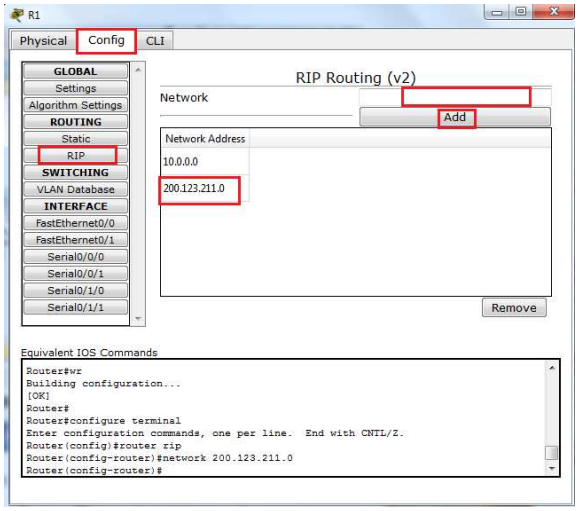


Figura 9: Ruta estática predeterminada al ISP

Como se aprecia en la figura 9, se agrega el RIP desde el Router 1. Se realiza el mismo procedimiento para el R2 y R3.

Paso 14: Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

Para finalizar este escenario, se realizan las últimas pruebas de conectividad. Para ello se hace Ping desde cualquier equipo hacia otro dentro de la misma red, en este caso dentro R3. El resultado es satisfactorio, como se puede evidenciar en la figura 10.

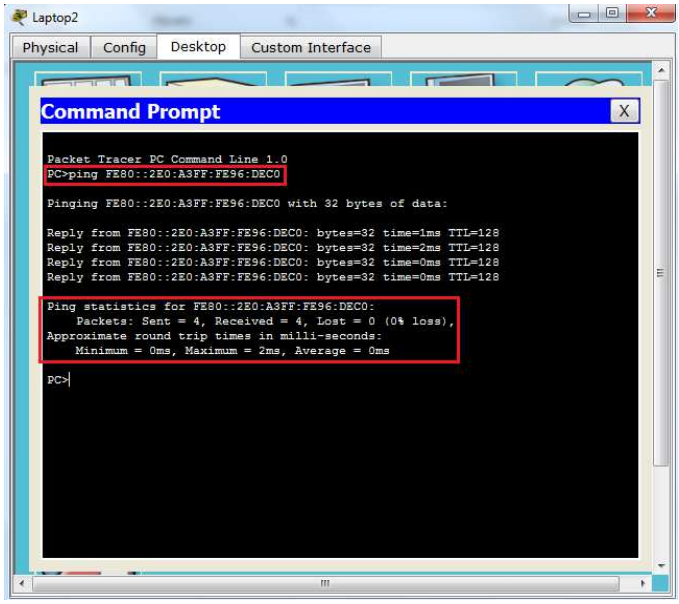
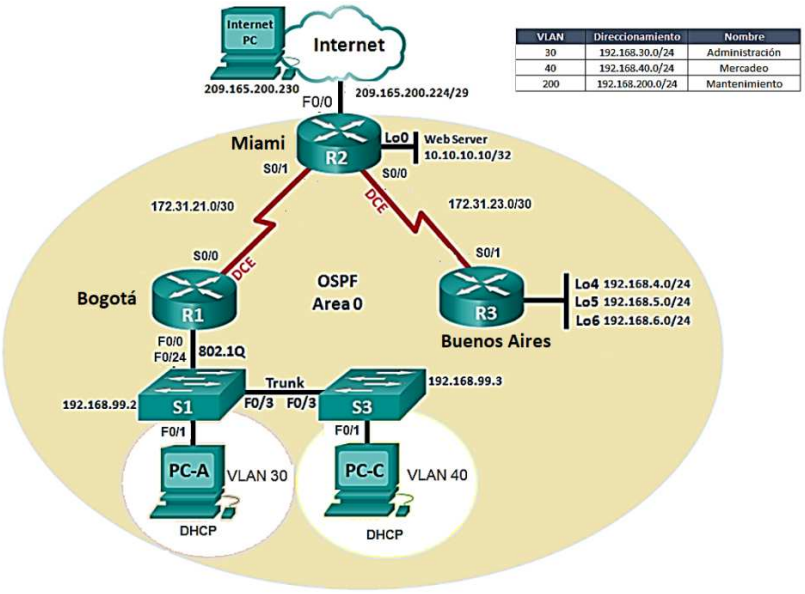


Figura 10: Ping de verificación entre equipos

1.2 ESCENARIO 2



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Figura 11: Topología propuesta escenario 2

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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.

Desarrollo

Para el desarrollo del escenario 2 de la prueba de habilidades, en primera instancia se realiza el armado de la red en el Software Packet Tracer, según el diseño de topología que se propone en dicho escenario. Para ello se inicializa el Software Packet Tracer, se seleccionan los elementos a utilizar, y se realiza el cableado de red tal como se muestra en la topología propuesta.

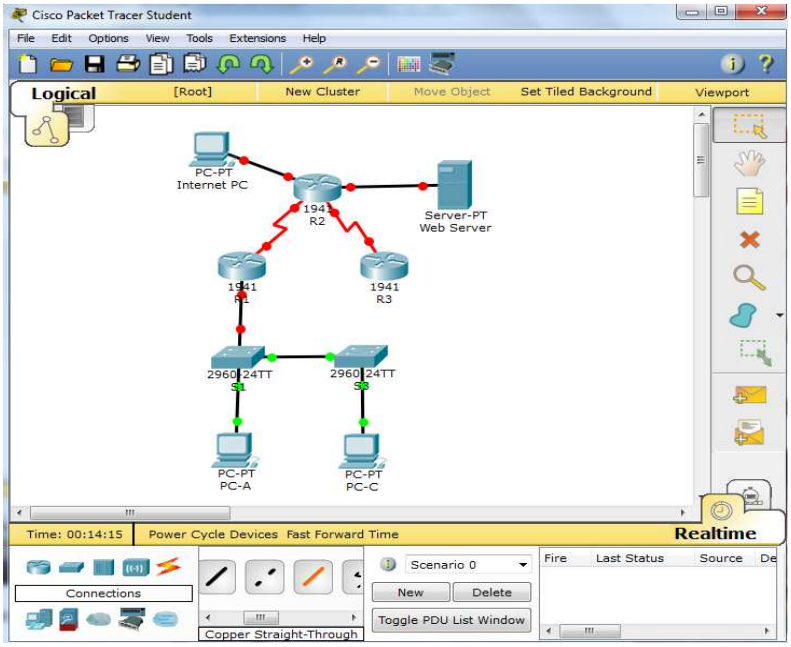


Figura 12: Armado de la red escenario 2

Como se puede apreciar en la Figura 12, se realiza el armado de la red según la topología planteada para el desarrollo del escenario 2.

Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

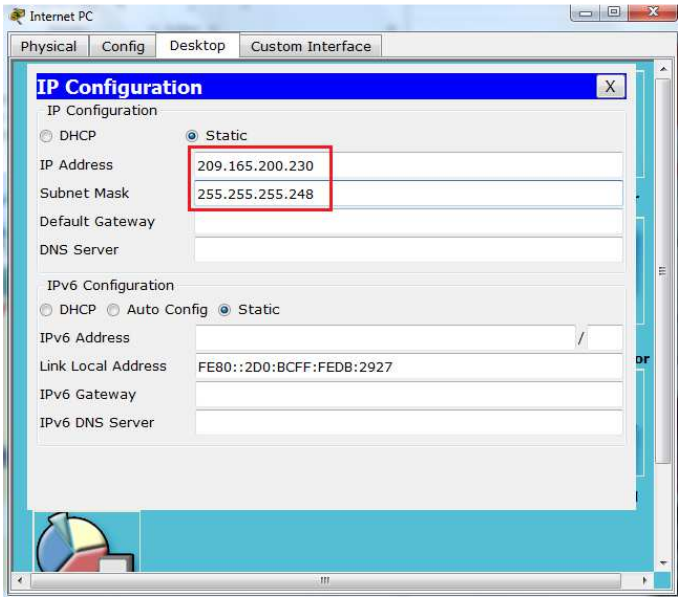


Figura 13: Direccionamiento IP para Internet PC

Como se puede apreciar en la figura 13, se realiza la configuración de dirección IP para el equipo Internet PC, teniendo en cuenta el direccionamiento que requiere este escenario y como lo ilustra la topología propuesta.

Para configurar los respectivos direccionamientos IP de R1, se selecciona el R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

Router>enable

Router>conf t

Router(config)#no ip domain-lookup

Router(config)#hostname R1

R1(config)#enable secret class

R1(config)#line con 0

R1(config-line)#pass cisco

R1(config-line)#login

R1(config-line)#line vty 0 4

R1(config-line)#pass cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#service password-encryption

R1(config)#banner motd $Acceso prohibido$

R1(config)#int s0/0/0

R1(config-if)#description Connection to R2

R1(config-if)#ip add 172.31.21.1 255.255.255.252

R1(config-if)#clock rate 128000

R1(config-if)#no shutdown

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

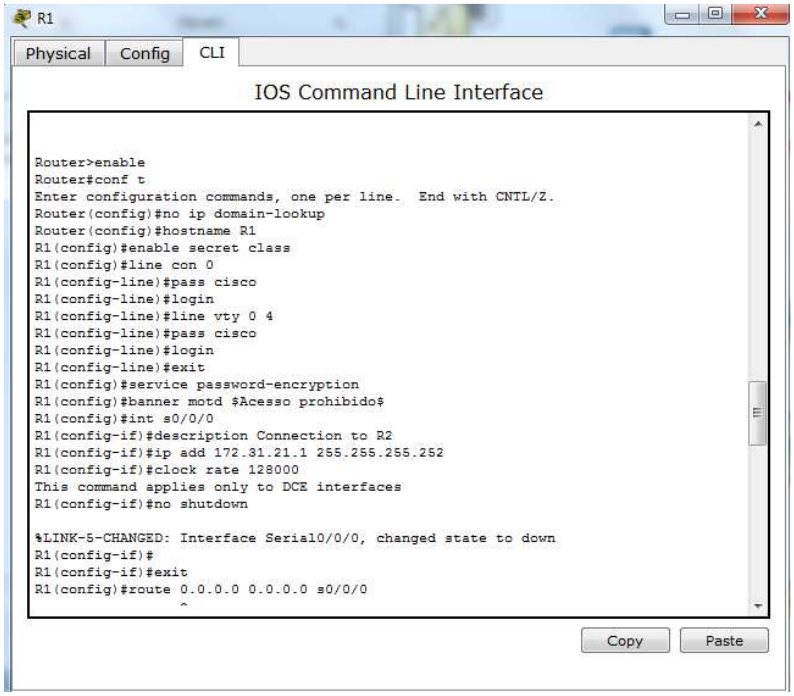


Figura 14: Direccionamiento IP para R1

Para configurar los respectivos direccionamientos IP de R2, se selecciona el R2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

Router>enable

Router>conf t

Router(config)#no ip domain-lookup

Router(config)#host R2

R2(config)#enable secret class

R2(config)#line con 0

R2(config-line)#pass cisco

R2(config-line)#login

R2(config-line)#line vty 0 4

R2(config-line)#pass cisco

R2(config-line)#login

R2(config-line)#exit

R2(config)#service password-encryption

R2(config)#banner motd $acceso prohibido$

R2(config)#int s0/0/0

R2(config-if)#descrip Connection to R1

R2(config-if)#ip add 172.16.12.2 255.255.255.252

R2(config-if)#no shut

R2(config-if)#int s0/0/1

R2(config-if)#descrip Connection to R3

R2(config-if)#ip add 172.16.23.1 255.255.255.252

R2(config-if)#clock rate 128000

R2(config-if)#no shut

R2(config-if)#int g0/1

R2(config-if)#ip add 10.10.10.1 255.255.255.0

R2(config-if)#no shut

R2(config-if)#description Connection to Web Server

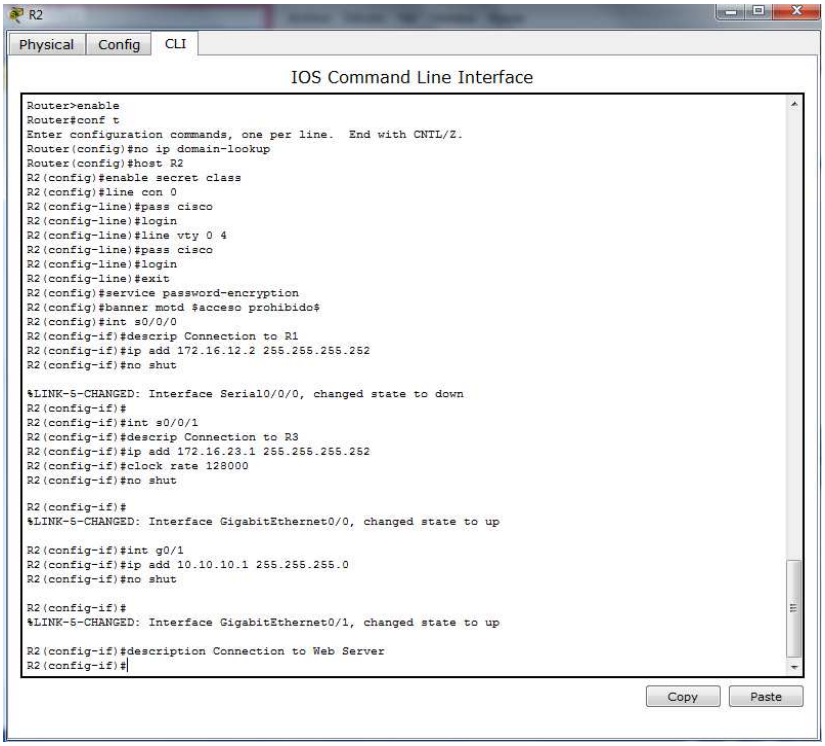


Figura 15: Direccionamiento IP para R2

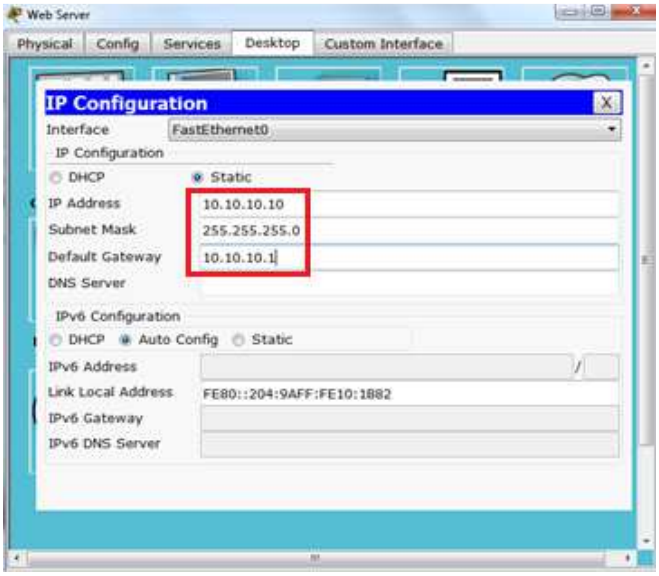


Figura 16: Direccionamiento IP para Web Server

Como se puede apreciar en la figura 16, se realiza la configuración de dirección IP para el equipo Web Server, teniendo en cuenta el direccionamiento que requiere este escenario y como lo ilustra la topología propuesta.

Para configurar los respectivos direccionamientos IP de R3, se selecciona el R3, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

Router>enable

Router>conf t

Router(config)#no ip domain-lookup

Router(config)#host R3

R3(config)#enable secret class

R3(config)#line con 0

R3(config-line)#pass cisco

R3(config-line)#login

R3(config-line)#line vty 0 4

R3(config-line)#pass cisco

R3(config-line)#login

R3(config-line)#exit

R3(config)#service password-encryption

R3(config)#banner motd $Acceso denegado$

R3(config)#int s0/0/1

R3(config-if)#description Connection to R2

R3(config-if)#ip add 172.16.23.2 255.255.255.252

R3(config-if)#no shut

R3(config-if)#int lo4

R3(config-if)#ip add 192.168.4.1 255.255.255.0

R3(config-if)#no shut

R3(config-if)#int lo5

R3(config-if)#ip add 192.168.5.1 255.255.255.0

R3(config-if)#no shut

R3(config-if)#int lo6

R3(config-if)#ip add 192.168.6.1 255.255.255.0

R3(config-if)#exit

R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

Para configurar los respectivos direccionamientos IP de S1, se selecciona el S1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

S*witch>enable*

Switch#conf t

Switch(config)#no ip domain-lookup

Switch(config)#host S1

S1(config)#enable secret class

S1(config)#line con 0

S1(config-line)#pass cisco

S1(config-line)#login

S1(config-line)#line vty 0 4

S1(config-line)#pass cisco

S1(config-line)#login

S1(config-line)#service pass

S1(config)#service password-encryption

S1(config)#banner motd $Acceso Denegado$

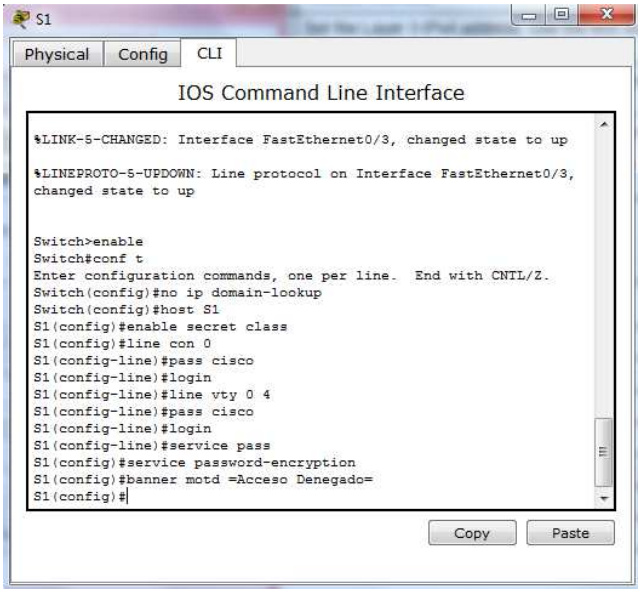


Figura 17: Direccionamiento IP para S1

Para configurar los respectivos direccionamientos IP de S2, se selecciona el S2, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

Switch>enable

Switch#conf t

Switch(config)#no ip domain-lookup

Switch(config)#host S2

S2(config)#enable secret class

S2(config)#line con 0

S2(config-line)#pass cisco

S2(config-line)#login

S2(config-line)#line vty 0 4

S2(config-line)#pass cisco

S2(config-line)#login

S2(config-line)#service pass

S2(config)#service password-encryption

S2(config)#banner motd $Acceso Denegado$

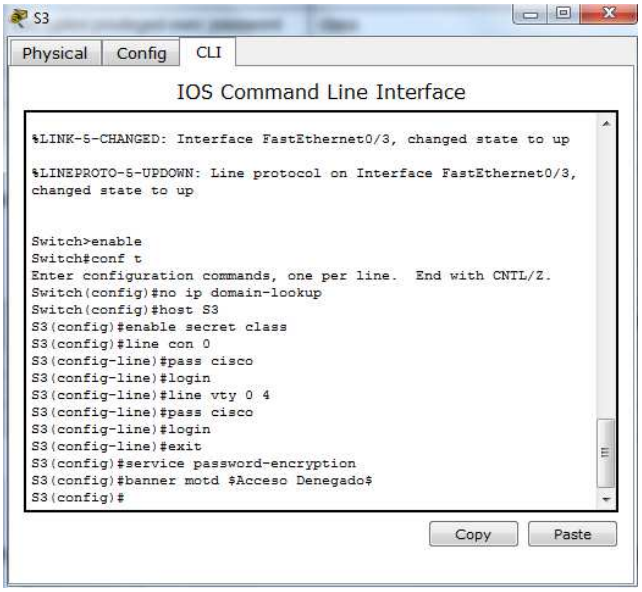


Figura 18: Direccionamiento IP para S2

Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Tabla 4: Criterios para enrutamiento

Para Configurar el protocolo de enrutamiento OSPFv2 en R1, se selecciona R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1>enable

R1#conf t

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1

R1(config-router)#network 172.31.21.0 0.0.0.3 area 0

R1(config-router)#network 192.168.30.0 0.0.0.255 area 0

R1(config-router)#network 192.168.40.0 0.0.0.255 area 0

R1(config-router)#network 192.168.200.0 0.0.0.255 area 0

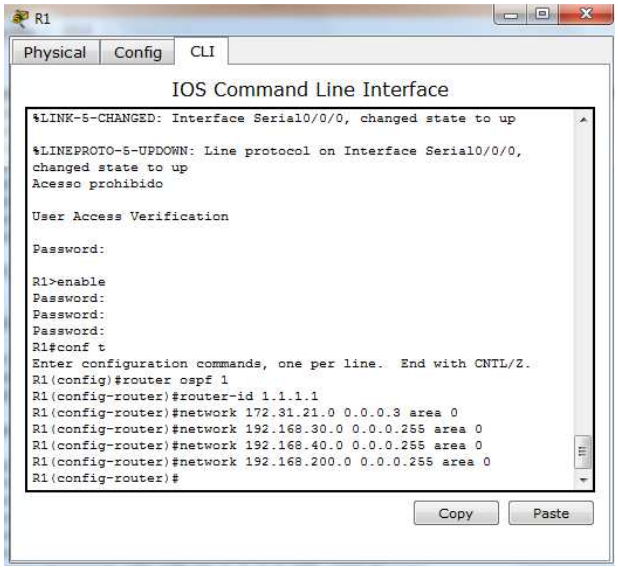


Figura 19: Enrutamiento OSPFv2 en R1

Como se puede apreciar en la figura 19, se realiza el enrutamiento OSPFv2 en R1, siguiendo con los parámetros requeridos en la tabla 4. Allí se especifica que el ID para el R1 debe ser 1.1.1.1.

Para configurar todas las interfaces LAN como pasivas, se selecciona R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1(config-router)#passive-interface g0/1.30

R1(config-router)# passive-interface g0/1.40

R1(config-router)# passive-interface g0/1.200

Se configuran todas las interfaces LAN como pasivas desde R1, siguiendo con los parámetros requeridos en la tabla 4.

Para establecer el ancho de banda para enlaces seriales en 256kb/s, y ajustar el costo en la métrica de s0/0 a 9500, se selecciona R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1(config)#int s0/0/0

R1(config-if)#bandwidth 256

R1(config-if)#ip ospf cost 7500

De este modo, ya quedan configurado el ancho de banda y el costo en la métrica según los parámetros requeridos.

Para visualizar las tablas de enrutamiento y routers conectados por OSPFv2, se ejecuta el comando “show ip ospf neighbor” en R2.

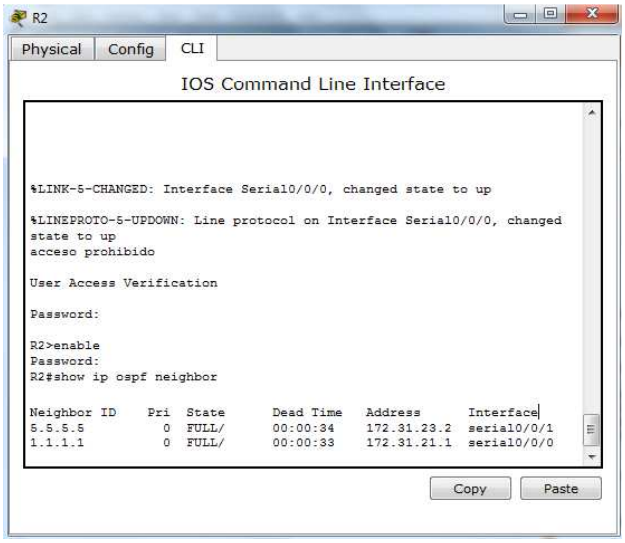


Figura 20: Routers conectados por OSPFv2

Como se visualiza en la figura 20, con el comando “show ip ospf neighbor” comprobamos los routers enrutados por OSPFv2, y allí están Router ID para R1 y R2 (1.1.1.1 y 5.5.5.5).

Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

S1>enable

Password:

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#vlan 30

S1(config-vlan)#name administracion

S1(config-vlan)#banner motd $acceso restringido$

S1(config)#vlan 40

S1(config-vlan)#name mercadeo

S1(config-vlan)#vlan 200

S1(config-vlan)#name mantenimiento

S1(config-vlan)#exit

S1(config)#

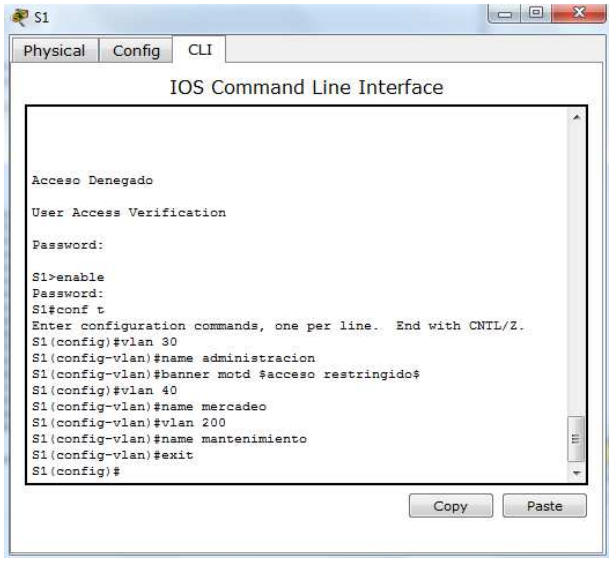


Figura 21: VLAN administración, mercadeo y mantenimiento

Implement DHCP and NAT for IPv4

Para implementar DHCP y NAT for IPv4, se selecciona R1, se da click en la pestaña “CLI”, y se procede a ingresar la siguiente configuración:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30

R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30

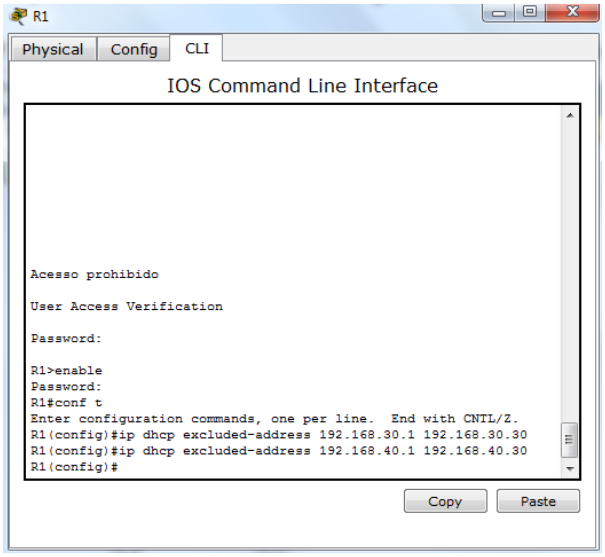


Figura 22: Implementación DHCP y NAT

Por ultimo para comprobar del correcto funcionamiento del escenario 2, se realizan las respectivas pruebas de ping. Para ello, se hace Ping entre pc-A y pc- C. A continuación se presenta dicha prueba.

Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

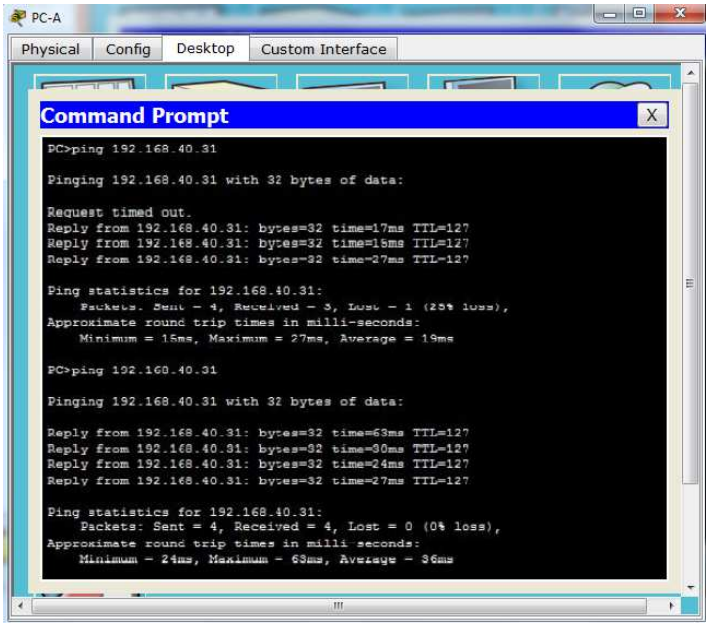


Figura 23: Pruebas de Ping de comprobación

Como se puede apreciar en la figura 23, el ping realizado entre pc-A y pc-C es exitoso, ya que al enviarse 4 paquetes, se recibieron la misma cantidad desde otro

equipo. Por tanto, se logra configurar e interconectar entre sí cada uno de los dispositivos que forman parte de la red, cumpliéndose los criterios que se proponen para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

CONCLUSIONES

Se dio respuesta completa y suficiente a las dos situaciones propuestas en esta prueba de habilidades, evidenciando el grado de conocimiento a modo personal en temas de Networking, componentes relacionados con el aseguramiento de la calidad y de estructuras de funcionamiento que hace posible el flujo de datos entre redes.

En la solución de estos escenarios se logró implementar virtualmente las redes propuestas y configurar los parámetros básicos de los dispositivos utilizados, en los que se encuentran routers, switches, pcs, y servidores; luego se logra configurar igualmente los switches con vlan y enlaces troncales. Para finalizar la prueba se configura el routing entre vlan y lo basamos en enlaces troncales.

Con esta prueba de habilidades he logrado perfeccionar mi conocimiento en cuanto a configurar redes con sus dispositivos y hacer uso de simuladores que hacen que nuestro ámbito profesional tenga un mejor perfil y, además, aumentar mi conocimiento para ampliar el campo de acción en la vida laboral.

En los ejercicios que desarrollo pude visualizar que problemas se pueden presentar en nuestro ambiente profesional y tener unas bases sólidas para dar respuestas a estas situaciones.

Se pudo conocer los diferentes medios de conexión que existen para comunicar dispositivos de networking.

Se aprendió a conectar los equipos entre si verificando esas conexiones con el programa de simulación Packet Tracer.

También se aprendió a determinar los permisos de acceso mediante las listas de control de acceso, encontrando que su principal objetivo es filtrar el tráfico para la separación de privilegios.

ANEXOS

Para complementar el presente informe, se anexan los aplicativos PKT de los laboratorios resueltos en Packet Tracert, los cuales pueden ser descargados en el siguiente Link: https://drive.google.com/file/d/1ZvJye1QDF105oQBRXdmk9f-11_F_lf9N/view?usp=sharing

BIBLIOGRAFIA

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

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

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado dehttps://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado dehttp://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado

de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU

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

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

Macfarlane, J. (2014). etwork Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf